
UE 215 → MANAGEMENT DES SYSTÈMES D'INFORMATION

Année 2013-2014

Ce fascicule comprend :
La série 4
Le devoir 6 à envoyer à la correction

ARCHITECTURES, SÉCURITÉ, NORMES ET AUDIT

En collaboration avec
le Centre National
d'Enseignement à Distance
Institut de Lyon

CNED

Fabien CLEUET
Nathalie DAGORN
Philippe EYNAUD
Philippe GERMAK
Jean-Pierre MARCA

W2151-F4/4

Les auteurs :

Fabien CLEUET : Spécialiste du conseil et de l'audit du SI, administrateur de l'AFAI.

Nathalie DAGORN : Professeur assistant à ICN Business School Nancy-Metz et spécialiste en sécurité des systèmes d'information et sécurité informatique.

Philippe EYNAUD : Maître de conférences en science de gestion.

Philippe GERMAK : Professeur agrégé au Cnam-Intec.

Jean-Pierre MARCA : Consultant en systèmes d'information et enseignant au Cnam-Intec.

⟨••• www.cnamintec.fr •••⟩

L'ensemble des contenus (textes, images, données, dessins, graphiques, etc.) de ce fascicule est la propriété exclusive de l'INTEC-CNAM.

En vertu de l'art. L. 122-4 du Code de la propriété intellectuelle, la reproduction ou représentation intégrale ou partielle de ces contenus, sans autorisation expresse et préalable de l'INTEC-CNAM, est illicite. Le Code de la propriété intellectuelle n'autorise que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » (art. L. 122-5).

«... **O**BJECTIFS ...»

La présente série a pour objet de :

- savoir définir les architectures technologiques de l'information ;
- connaître les grands types d'infrastructure informatique ;
- connaître les politiques de sécurité ;
- maîtriser la sécurité des systèmes d'information.



TABLE DES MATIÈRES

PARTIE 6. LES INFRASTRUCTURES TECHNOLOGIQUES DE L'INFORMATIQUE

9

| | |
|---|-----------|
| I. Architectures informatiques..... | 9 |
| A. Quels critères pour structurer une architecture complexe ? | 9 |
| B. Logiciel et progiciel..... | 13 |
| C. Au sein d'une architecture cohérente..... | 13 |
| II. Technologies de base et des architectures de machines | 14 |
| A. Pour traiter l'information | 14 |
| B. Pour stocker l'information | 21 |
| C. Une course perpétuelle | 23 |
| D. Bilan..... | 24 |
| III. Architectures de systèmes..... | 24 |
| A. Systèmes d'exploitation | 24 |
| B. Les systèmes d'IBM | 25 |
| C. Les systèmes Unix..... | 25 |
| D. La famille Microsoft | 26 |
| IV. Architectures de réseau | 28 |
| A. Assurer la connexion des postes de travail distants | 28 |
| B. Faciliter le développement des applications transactionnelles | 30 |
| C. Proposer un véritable concept de réseau..... | 31 |
| D. Et pendant ce temps-là... les opérateurs de télécoms | 32 |
| E. Retour au sein des organisations : fédérer les postes dans des groupes de travail | 35 |
| F. Mettre en place une structure de réseau hiérarchisée | 35 |
| G. La révolution Internet..... | 36 |
| H. Analyse du processus d'évolution et bilan | 40 |
| I. Des progrès techniques continus..... | 43 |
| V. Évolution des architectures de données..... | 44 |
| A. Les ensembles de données : documents, fichiers, bases de données..... | 44 |
| B. Évolution du degré de structuration | 45 |
| VI. Évolution des architectures de traitement..... | 52 |
| A. Le besoin : clients et serveurs | 52 |
| B. La réponse..... | 53 |

| | |
|---|------------|
| VII. Évolution des architectures globales | 55 |
| A. Évolution des architectures de 1970 à 2010 | 55 |
| B. Architectures pour les services B2E..... | 59 |
| C. Architectures pour les services B2C | 64 |
| D. Architectures B2B..... | 66 |
| E. Évoluer vers le Web 2.0 | 68 |
| F. Répondre aux enjeux de la mobilité | 71 |
| G. Une architecture devenue très complexe..... | 72 |
| VIII. Architecture technique d'aujourd'hui..... | 73 |
| A. Les infrastructures actuelles..... | 73 |
| B. Le <i>cloud computing</i> | 76 |
| PARTIE 7. LA SÉCURITÉ DES SYSTÈMES D'INFORMATION | 79 |
| I. La protection des actifs..... | 80 |
| II. L'évaluation des risques | 81 |
| A. Gérer le paradoxe de l'ouverture et de la protection..... | 81 |
| B. Quantifier les pertes dues aux sinistres..... | 82 |
| C. L'analyse des risques | 83 |
| III. L'identification des menaces | 84 |
| A. Les mécanismes de l'intrusion | 85 |
| B. Les organismes de soutien..... | 85 |
| IV. La mise en place d'une politique SSI (PSSI) | 86 |
| A. L'impératif d'une approche globale, systémique et préventive | 87 |
| B. Définition de la PSSI | 88 |
| C. Les qualités d'un système d'information sécurisé | 90 |
| V. La sécurité opérationnelle..... | 92 |
| A. La sécurité des réseaux..... | 92 |
| B. La sécurité des serveurs..... | 94 |
| C. La sécurité des postes de travail..... | 95 |
| D. La sauvegarde | 95 |
| E. La signature électronique | 99 |
| VI. Informatique et libertés | 104 |
| A. Contenu de la loi..... | 104 |
| B. Les formalités requises..... | 106 |
| C. Six questions essentielles (<i>Source : Cnil</i>) | 107 |
| D. Le droit d'accès et de rectification | 108 |
| E. La Cnil..... | 108 |
| F. La sanction | 108 |

PARTIE 8. LES NORMES ET LES RÉFÉRENTIELS DES AUDITS DES SYSTÈMES D'INFORMATION

111

| | |
|--|------------|
| I. Définitions et vocabulaire..... | 112 |
| A. Contexte | 112 |
| B. Définitions..... | 113 |
| II. Le contexte international et les enjeux | 115 |
| A. Forum de stabilité financière (FSF) | 116 |
| B. Enron et la suite | 117 |
| C. La protection des systèmes d'information | 118 |
| D. Conclusion..... | 120 |
| III. Les sources des normes et référentiels..... | 120 |
| A. COBIT, le référentiel de l'ISACA..... | 122 |
| B. Le référentiel ITIL | 126 |
| C. CMMI : La rationalisation du développement informatique | 129 |
| D. ISO 27000 : 2005 normes pour le management de la sécurité informatique | 130 |
| E. Les normes isa élaborées par l'IFAC | 131 |
| F. L'IIA, concepteur des standards de l'audit interne..... | 132 |
| IV. Le contrôle fiscal des comptabilités informatisées | 133 |
| A. Rappel du dispositif réglementaire | 133 |
| B. Le bulletin officiel des impôts n° 12 du 24 janvier 2006 | 134 |
| C. Impacts..... | 139 |
| D. Recommandations | 140 |
| E. Les aménagements | 141 |

ANNEXES

143

EXERCICE AUTOCORRIGÉ

145

INDEX

149

DEVOIR 6

151

LES INFRASTRUCTURES TECHNOLOGIQUES DE L'INFORMATIQUE

I. ARCHITECTURES INFORMATIQUES

A. QUELS CRITÈRES POUR STRUCTURER UNE ARCHITECTURE COMPLEXE ?

C'est un architecte du XVIII^e siècle, E. L. Boullée, qui nous donne cette définition de l'architecture :

« Il faut concevoir pour effectuer. Nos premiers pères n'ont bâti leurs cabanes qu'après en avoir conçu l'image. »

C'est cette production de l'esprit, c'est cette création qui constitue l'architecture. Le concept d'**architecture** est très présent dans le monde des systèmes et technologies d'information.

Au-delà de la définition liée à l'art de la construction d'un édifice : l'architecture est définie aujourd'hui comme l'« *organisation des divers éléments constitutifs d'un système en vue d'optimiser la conception d'un ensemble pour un usage déterminé* »¹.

L'architecture fonctionnelle (ou logique) d'un système d'information est constituée par une liasse de plans qui regroupe les modèles issus de l'analyse : modèles dépeignant l'enchaînement des tâches au sein des processus et modèles détaillant les entités de l'organisation et les relations qui les unissent.

Ces modèles décrivent les flux d'information dans l'organisation, les nœuds où ces informations sont collectées, traitées et stockées, les canaux par où elles sont transmises. Ils s'intéressent à la structure conceptuelle des ensembles des données, à la description des processus (Quoi ? Qui ? Comment ? Pourquoi ? Où ? Quand ?) et à la cartographie des échanges.

L'architecture technique (ou physique) du système d'information s'intéresse aux divers composants techniques mis en place pour matérialiser l'architecture fonctionnelle : serveurs et systèmes d'exploitation associés, postes de travail, équipements de réseaux, support de bases de données et logiciels.

Ces composants exploitent les technologies de base : les postes de travail exploitent les technologies de collecte et de traitement, les serveurs exploitent les technologies de traitement, les supports des bases de données exploitent les technologies de stockage, les équipements de réseau exploitent les technologies de communication.

1. Ordinateurs et réseau

Il est rare de rencontrer aujourd'hui une organisation ne reposant que sur des Personnes, des Procédures et du Papier². L'instrument d'aide au pilotage des organisations que constitue le **système d'information** est toujours assisté de moyens plus ou moins automatiques qui tendent à faciliter son fonctionnement. Ces assistants sont le téléphone, les machines à dupliquer, la télécopie, les systèmes de classement et d'archivage et les systèmes informatiques. Tous ces moyens contribuent à faciliter la **collecte**, le **stockage**, le **traitement**, la **communication** et la **présentation** de l'information.

1. Dictionnaire Robert.

2. Le système 3P fonctionne aussi en anglais (Personnel, Procedure, Paper). À ne pas confondre avec les 4P (Produit, Promotion, Prix, Packaging).

Parmi tous les assistants techniques du système d'information, ceux qui ont le degré d'automatisation le plus poussé sont les assistants « informatiques ». Ils occupent une place sans cesse croissante et ont rejeté aux oubliettes d'autres assistants comme la machine à écrire ou, sauf pour certains irréductibles, l'agenda papier. Bénéficiant des progrès enregistrés dans le secteur des composants électroniques et intégrant dans son champ d'activités les avancées du secteur des télécommunications, l'**ordinateur** a élargi à l'infini son domaine d'application en devenant le nœud d'un **réseau**. Les réseaux informatiques irriguent les organisations, décentralisent la saisie des données, distribuent la puissance de calcul et permettent à l'ensemble du personnel d'accéder, en temps utile, aux référentiels de données et aux capacités de traitement.

2. Matériel et logiciel

L'importance de l'outil informatique est justifiée par le fait qu'il possède, outre la capacité d'assurer simultanément ces cinq fonctions fondamentales que sont la collecte, le stockage, le traitement, la transmission et la présentation des informations, une propriété bien particulière, l'aptitude à être **programmé**.

Même s'ils ont des performances et des fonctionnalités différentes, tous les ordinateurs, qu'ils soient postes de travail individuels ou machines puissantes hébergeant des services partageables par de nombreux utilisateurs, sont construits selon le même principe architectural. Ce sont des machines programmables capables d'exécuter des tâches très différentes selon la nature de la séquence d'instructions chargée.

Le **matériel** est constitué par des cartes électroniques et de dispositifs de stockage magnétique ou optique de l'information. Il peut enregistrer et dérouler des séquences d'**instructions** élémentaires structurées sous forme de **programmes**.

La capacité d'enregistrer est associée à une fonction de **mémoire**. Celle-ci est temporaire avec les circuits électroniques qui perdent les informations enregistrées dès coupure de l'alimentation en énergie. Elle est permanente avec les dispositifs magnétiques et optiques.

La capacité de dérouler une séquence d'instructions est associée à la fonction de **traitement**. Cette capacité est associée au concept de processeur. Le traitement inclut le décodage des instructions et l'exécution de l'opération ainsi décodée.

Par opposition au matériel, l'ensemble des programmes constitue le **logiciel**.

3. Programme et langage

Les séquences d'instructions des programmes ont une consistance physique : celle de chaînes de 1 et de 0. Ce sont les unités élémentaires d'information, les « bits »³. Ces chaînes n'ont de sens que pour les circuits du matériel qui vont être capables de les décoder, puis d'exécuter les commandes et les opérations qui résultent du décodage. La machine ne sait exécuter les instructions fournies que si elles sont connues de son répertoire d'instructions. C'est pour cette raison qu'un programme codé en binaire sur une machine ne s'exécutera pas sur une machine d'un autre type.

Le programme est enregistré dans la mémoire de l'ordinateur. L'utilisateur peut charger un programme et en lancer l'exécution à tout moment.

3. Abréviation de l'expression anglaise « binary digit », chiffre binaire.

Il suffit de charger un autre programme pour faire de l'ordinateur un outil adapté à un autre besoin. Vous transformez aisément votre PC qui vient de traiter votre comptabilité personnelle en un simulateur de vol ou en un outil de création graphique. Cette étonnante propriété, qui fait de l'ordinateur un outil commun et adaptable à tous les métiers, explique pourquoi il a été choisi comme l'outil de gestion par excellence et pourquoi il a rencontré un succès auquel étaient loin de s'attendre ses promoteurs⁴.

Si les chaînes de bits ont une signification pour le processeur de la machine, elles n'en ont plus guère pour le concepteur du programme. Ce paradoxe s'explique par les transformations qu'a subies son programme entre la phase de conception et la phase d'exécution. Ces transformations sont associées à la notion de **langage** et de **traduction**.

Un langage est un ensemble de signes formant un système, destiné à l'expression et à la communication. Notre langage est assertionnel. C'est ainsi que vous montez dans un taxi et annoncez au conducteur : « Merci de me conduire à la gare de Lyon pour que je puisse avoir le train de 19 h 04. » Vous pourriez aussi formuler votre requête sous la forme d'une suite de consignes : « Démarrez... Accélérez... Tournez à droite... Freinez... Arrêtez-vous tant que le feu est rouge... Redémarrez... Passez la troisième... Si c'est encombré devant, prenez la rue à gauche... » Votre chauffeur vous aura sans doute débarqué avant d'arriver à destination, vous reprochant peut-être de communiquer avec lui sous forme d'un langage procédural et non d'un langage assertionnel.

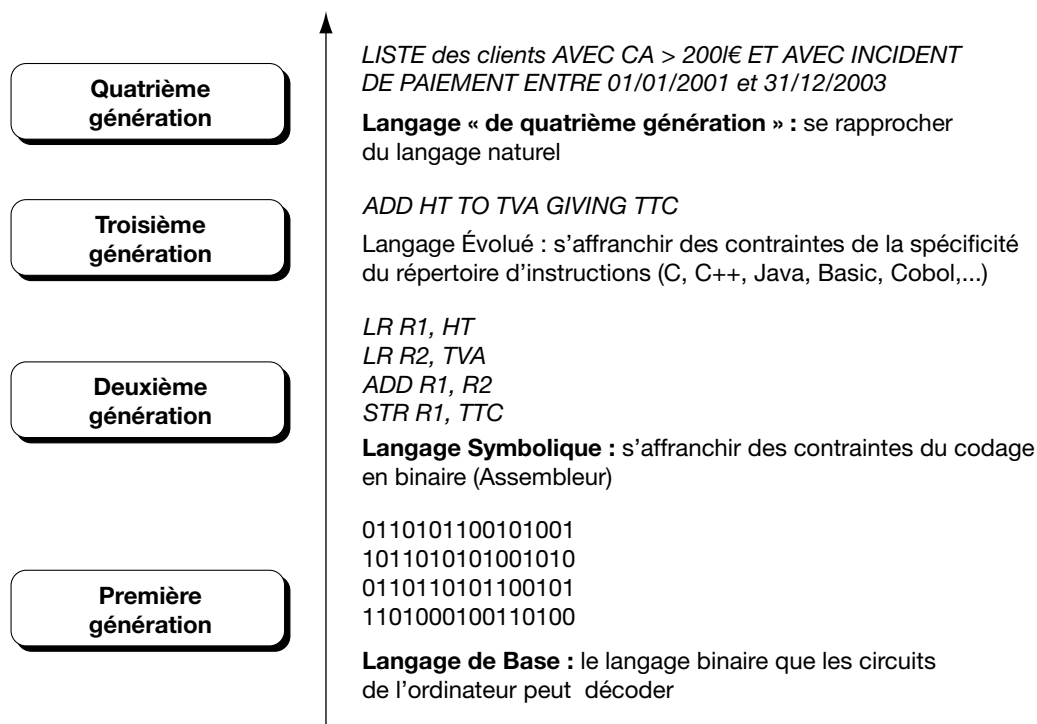
Dans la plupart des cas, un ordinateur ne vous fera jamais le même reproche. Il attend que vous lui communiquiez une liste d'instructions à exécuter sous forme d'un langage procédural. Dans ce langage, on pourra reconnaître les mêmes propositions que celles employées avec notre chauffeur de taxi : « Faire... tant que..., Si... alors... sinon..., Répéter... jusqu'à... » Ce langage procédural est un langage de programmation, c'est-à-dire un ensemble de signes permettant à celui qui veut écrire un programme, d'exprimer et de formaliser son besoin pour le communiquer aux circuits de l'ordinateur de manière compréhensible par ceux-ci.

Il est courant de classer les langages en générations :

- La première génération est celle du langage binaire de base que les circuits de l'ordinateur savent décoder.
- La deuxième génération est celle du langage symbolique qui permet de s'affranchir des contraintes du codage en binaire mais reste asservi à celle du répertoire d'instructions de la machine. **L'assembleur** est l'outil qui permet la traduction du langage symbolique en langage binaire.
- La troisième génération est celle du langage évolué qui permet de s'affranchir de la spécificité du répertoire d'instructions. La même phrase « *ADD HorsTaxe To TVA giving TTC* » pourra être traduite de diverses manières pour être exécutée sur diverses machines. C'est le **compilateur** qui assure cette traduction.
- Le langage « de quatrième génération » (L4G) avait pour objectif de se rapprocher du langage naturel. Il en est encore loin si ce n'est pour formuler quelques requêtes simples d'interrogation.

4. Thomas Watson, fondateur d'IBM, en 1943 : *"I think there is a world market for maybe five computers."* (Je pense que le marché mondial des ordinateurs correspond à 5 machines.) Howard Aiken, créateur du calculateur Mark I : *"Only a very small number of computers would be needed to serve the needs of the whole world, perhaps a dozen."* (Il suffira d'un petit nombre de calculateurs pour satisfaire les besoins mondiaux, peut-être une douzaine.)

Figure 1 : Les générations de langage



Cette typologie des générations est commode. Elle est liée à la chronologie d'apparition de ces langages, mais elle ne signifie pas que seuls les L4G soient utilisés aujourd'hui.

Les circuits des ordinateurs ne connaissent toujours que le langage de base de la première génération, à l'image des premiers programmeurs qui codaient en binaire leurs instructions et leurs données et les introduisaient dans les registres de la mémoire à l'aide de panneaux de petits commutateurs positionnés en haut (1) ou en bas (0).

Certaines applications techniques très pointues exigent une gestion optimale des ressources de la machine qui ne peut être atteinte qu'avec un langage de deuxième génération.

Les programmeurs qui développent les logiciels d'application travaillent avec des langages de troisième génération comme C/C++, Java, Basic, Pascal, Cobol. Ils accèdent aux données en formulant des requêtes formulées selon le langage normalisé SQL : « *SELECT Client_No, Client.RaisonSociale, Client_Ville FROM Clients WHERE Client_CA > 200000 AND Client_FlagIncident = 1 ;* ».

Les langages dits « de Quatrième Génération » (L4G) ont pour vocation de s'affranchir du caractère hermétique des langages informatiques classiques. Cependant, le développement d'applications s'est avéré un domaine trop complexe pour autoriser l'utilisation d'un langage très proche du langage naturel, par nature trop imprécis et trop ambigu.

Certes, les L4G de ce domaine ont apporté des gains de lisibilité et de productivité importants, mais ils ne sont en fait que des supers L3G, généralement adaptés à un environnement donné. Le langage ABAP, associé à l'ERP⁵ de SAP, constitue un bon exemple de ce type de langage.

Par contre, les langages spécialisés dans le domaine de l'interrogation des Bases de Données, domaine plus simple parce que bien délimité, ont tenté avec plus de succès, sur la base définie par SQL, de se rapprocher du langage naturel. Le L4G Français de la société XX, souvent associé aux machines de la société Intertechnique, a même tenté ce pari pour la langue française, au début des années 1980.

5. Nous aborderons en détail le concept ERP dans le chapitre consacré à l'évolution des architectures de traitement.

B. LOGICIEL ET PROGICIEL

Un logiciel est un ensemble cohérent de programmes destiné à supporter une fonction clairement identifiée. Un logiciel de comptabilité offre l'ensemble des services nécessaires à une bonne gestion des journaux et des livres comptables.

Le mot **Progiciel** a été inventé en 1973 par J.E. Forge, fondateur du Centre d'expérimentation des Progiciels (CXP) pour traduire le concept de « *packaged software* », c'est-à-dire de produit logiciel. Le progiciel est un produit réalisé par un **éditeur** qui peut être acheté par le client final sur l'étagère d'un **distributeur**.

C. AU SEIN D'UNE ARCHITECTURE COHÉRENTE

Au sein d'un ordinateur, matériels et logiciels sont disposés selon une architecture cohérente où nous pouvons identifier :

- des composants matériels en charge de la **collecte** (ou saisie) des informations ;
- des composants matériels en charge du **stockage** des informations collectées ;
- des composants matériels en charge du **traitement** des informations collectées et stockées ;
- des composants matériels en charge de la **transmission** des informations (informations collectées ou informations résultant du traitement) ;
- des composants matériels en charge de la **présentation** des informations, accompagnées parfois de dispositifs de **pointage** des informations ;
- des composants logiciels en charge des services de gestion et des services métiers ;
- des composants logiciels en charge du bon fonctionnement des composants matériels et de la gestion (conception, création, déploiement, exploitation) des composants logiciels de la première catégorie.

La liste qui suit met en évidence ces différents composants pour une architecture relativement simple, connue de tous aujourd'hui, celle de l'ordinateur personnel (PC pour *Personal Computer*) :

- des composants matériels en charge de la collecte (ou saisie) des informations :
 - le clavier,
 - le scanner ;
- des composants matériels en charge du stockage des informations collectées :
 - les composantes de mémoire vive (barrettes de mémoire électronique),
 - les mémoires mortes,
 - le disque « dur »,
 - l'unité CD/DVD,
 - l'unité de disquette (en voie de disparition),
 - l'unité de sauvegarde (disque « zip », clef USB, cartouche...) ;
- des composants matériels en charge du traitement des informations collectées et stockées :
 - les circuits de la carte mère autour du microprocesseur (unité centrale) ;
- des unités en charge de la transmission des informations (informations collectées ou informations résultant du traitement) :
 - les circuits, les bus et la connectique permettant à la machine de se relier à des réseaux locaux ou distants regroupant lignes de transmission (réseau téléphonique, réseau numérique à intégration de services (RNIS), Internet, réseaux spécialisés) et équipements actifs spécialisés (modems, routeurs, commutateurs, concentrateurs, multiplexeurs, etc.) ;
- des composants matériels en charge de la présentation des informations, accompagnés parfois de dispositifs de pointage des informations :
 - l'écran,
 - l'imprimante,
 - la souris (pointage) ;
- des composants logiciels en charge des services de gestion et des services métiers :
 - un progiciel de comptabilité,
 - la suite bureautique,
 - le navigateur Internet,
 - un logiciel d'autoformation ;

- des composants logiciels en charge du bon fonctionnement des composants matériels et de la gestion (conception, création, déploiement, exploitation) des composants logiciels de la catégorie précédente :
 - le système d'exploitation,
 - les pilotes de l'imprimante, du modem...,
 - les outils de génie logiciel (éditeurs, compilateurs, bibliothécaires...).

Une architecture cohérente regroupe au sein d'un réseau d'ordinateurs des composants matériels (processeur, mémoires, dispositifs de communication...) et logiciels (système d'exploitation, programme d'application...) pour assurer les fonctions de collecte, de stockage, de traitement, de transmission et de présentation au sein d'un système d'information.

II. TECHNOLOGIES DE BASE ET DES ARCHITECTURES DE MACHINES

A. POUR TRAITER L'INFORMATION

1. Des informations (bien) traitées

En quoi consiste le traitement des informations collectées et stockées ?

Ce traitement est assuré par un programme lui-même stocké dans la mémoire de l'ordinateur. Ce programme doit être capable de lire des données opérantes et de réécrire les données résultantes du calcul. Il doit être capable d'effectuer des opérations de codage et décodage, des opérations de calcul arithmétique, des manipulations sur les chaînes de caractères.

Ces opérations élémentaires doivent pouvoir être combinées pour réaliser des opérations plus complexes (calculs arithmétiques et ensemblistes, comparaisons, tris, sélections, pilotage des organes de dialogue et de mémoire auxiliaire...).

Pour cela il faut pouvoir effectuer en séquence plusieurs opérations élémentaires. Cette séquence doit pouvoir être interrompue lors de la détection d'une condition quelconque, pour permettre un branchement vers une autre séquence d'opérations.

2. Les précurseurs

On remonte traditionnellement au boulier chinois pour trouver la première machine que l'homme ait utilisée pour l'aider à traiter des données numériques. Son modèle le plus élémentaire se présente sous la forme d'un cadre de bois qui supporte des tiges. Sur chaque tige coulisent neuf boules. Les boules de la première tige représentent les unités, celles de la deuxième les dizaines, celles de la troisième les centaines, etc. Pour enregistrer un nombre il suffit de déplacer les boules correspondantes sur chaque tige, la prise en compte des retenues lors d'un calcul s'effectuant en déplaçant une boule sur la tige placée immédiatement à gauche. Ce mécanisme permet de conserver des nombres et d'effectuer des opérations manuelles. C'est un support et non un automate.

Au XVII^e siècle (1642), le philosophe et physicien français Blaise Pascal eut l'idée de rendre automatique non seulement le calcul élémentaire mais aussi la prise en compte de la retenue, grâce à une machine entièrement mécanique⁶ considérée comme l'ancêtre des calculatrices de bureau. Pascal utilisa le concept de la roue dentée. Sa machine était composée de roues de 10 dents correspondant aux positions 0 à 9, placées les unes à côté des autres, représentant successivement les unités, les dizaines, les centaines, etc.

Le report automatique était alors possible. Lorsqu'on dépassait la valeur 9 en additionnant deux chiffres, le passage par la position 0 entraînait l'avancement automatique de la roue dentée placée immédiatement à gauche d'un dixième de tour. D'autre part l'action de calcul, caractérisée par la rotation des roues, devenait, elle aussi, automatique grâce à l'emploi d'une manivelle. La machine de Pascal traitait l'addition et la soustraction.

6. Visible au musée des Arts et Métiers.

Le philosophe et mathématicien allemand Leibniz l'améliore en lui ajoutant la multiplication et la division.

Au XVIII^e siècle, l'Anglais Babbage franchit l'étape suivante dans la mécanisation du calcul. Il eut l'idée de rendre automatique l'enchaînement en séquence des opérations en s'appuyant sur le concept de programme développé par Jacquard pour l'automatisation des métiers à tisser. La « Machine Analytique » de Babbage comprenait un dispositif mémoire (le « magasin ») permettant d'enregistrer mille nombres de cinquante chiffres décimaux, et un dispositif de commande séquentielle enchaînant des opérations décrites sur un support extérieur. Cette machine n'a jamais pu fonctionner mais est l'ancêtre des premières machines électriques à relais construites dans certaines firmes et universités américaines pendant la Seconde Guerre mondiale.

3. Les concepts de Turing et de Von Neumann

À la veille de la seconde guerre mondiale, le mathématicien britannique Alan Turing, dans la continuité des travaux de Gödels, Hilbert et Newman, formalise le principe d'algorithme et élabore le concept de « Machine de Turing » qui constitue le fondement de toutes les théories sur les automates. Le conflit lui donne l'occasion de mettre ses théories en pratique pour décrypter les messages codés de l'ennemi. L'automatisation du processus de décryptage conduit à la réalisation de machines électromécaniques (les « bombes »), puis électroniques. Avec sa mémoire interne (registres), ses branchements conditionnels, sa logique modifiable et son fonctionnement automatique, la machine Colossus préfigure les premiers ordinateurs de l'après-guerre (Eniac, Maniac).

En 1945, Von Neumann introduit deux concepts qui vont permettre une avancée décisive :

- Le concept de programme enregistré : la mémoire de la machine peut être utilisée non seulement pour stocker les données, opérandes et résultats, mais aussi la séquence des opérations élémentaires à exécuter. Ainsi, plutôt que de lire un support extérieur, on procède à l'enregistrement préalable du programme en mémoire. Le déroulement de ce programme est alors rythmé par les accès à une mémoire interne beaucoup plus rapide qu'un dispositif externe.
- Le concept de rupture de séquence : le programme étant chargé dans une mémoire où l'accès direct à l'information est possible, il devient possible d'automatiser les processus de branchement à une séquence de programme particulière chaque fois qu'une condition particulière est satisfaite.

4. Les générations d'ordinateurs

Ces principes étant acquis, les architectures n'ont plus évolué de manière significative. C'est essentiellement au niveau de la technologie que des progrès vont être enregistrés.

Nous retrouvons ici le concept de **génération** déjà entrevu avec les langages, mais pour ce qui concerne les machines, chaque nouvelle génération a effectivement chassé l'autre :

- Dans le courant de la seconde guerre mondiale et dans les années qui suivent, les circuits de calcul des ordinateurs de la première génération sont réalisés à base de tubes électroniques, fragiles, encombrants et dissipateurs d'énergie. Cette génération se clôt avec l'IBM 704, doté d'un coprocesseur mathématique et d'une mémoire magnétique à tores de ferrite de 32 768 mots de 36 bits. Sa fiabilité est jugée exceptionnelle car il ne tombe en panne qu'une fois par semaine. C'est sur cette machine que sera développé le langage Fortran.
- Dans les années 1960, la « seconde génération », celle des ordinateurs IBM 1401 (gestion) et 1130 (scientifique), intègre la technologie des transistors.
- La « troisième génération », celle de l'IBM 360, annoncée le 7 avril 1964. Cette machine, qui se veut universelle, c'est-à-dire capable de résoudre à la fois des problèmes scientifiques et des problèmes de gestion, intègre la technologie des microcircuits, développe l'idée de gamme, et confie la gestion de l'ensemble à un programme particulier : le système d'exploitation. Nous reviendrons sur ce concept.

Cette génération est toujours actuelle même si certains ont tenté d'imposer les concepts de machines de 4^e, voire de 5^e génération. Elle bénéficie chaque jour des améliorations issues d'une miniaturisation et d'une intégration toujours plus poussées, mais les principes de base guidant le traitement des informations restent les mêmes.

La classification selon les générations n'est plus pertinente. Celle qui va s'imposer dès les années 1960 est liée à la taille des machines.

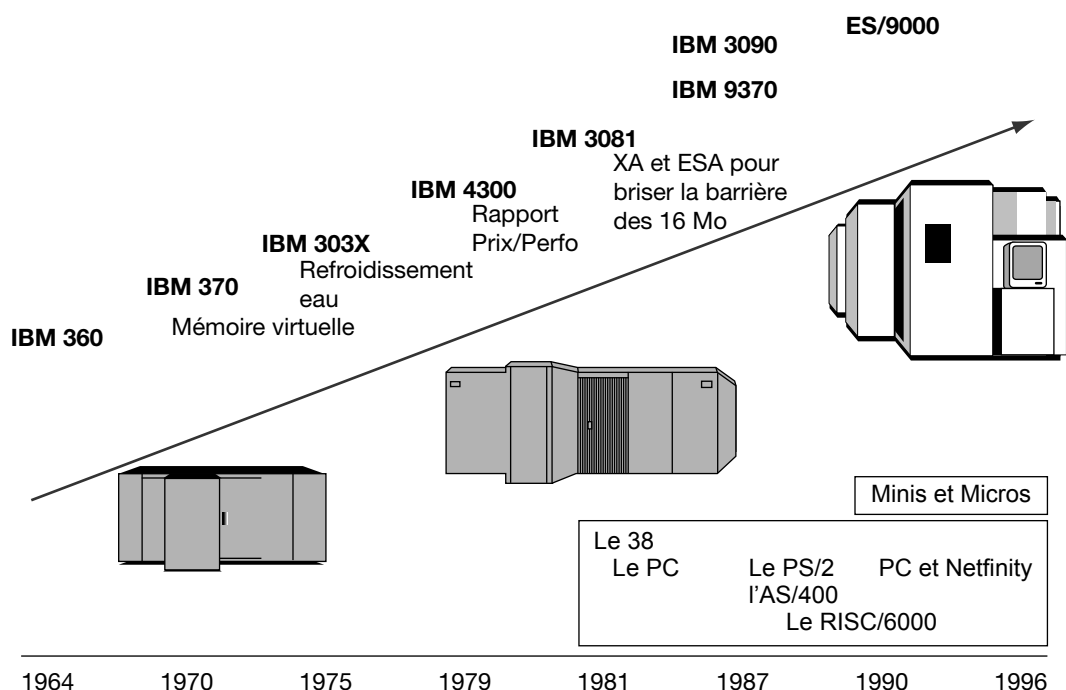
5. Des mainframes aux minis

L'IBM 360 est l'archétype du « mainframe » : le gros ordinateur centralisateur, quelquefois baptisé « Big brother », en référence au roman 1984 de Georges Orwell, à une époque où IBM, elle-même, est surnommée Big Blue. Derrière IBM suivent, loin derrière, les membres du BUNCH (*Burroughs, Univac, NCR, Control Data et Honeywell*), non encore associé au franco-suédois Bull. En Europe, outre Bull, la Compagnie Internationale pour l'Informatique issue du Plan Calcul français, l'anglais ICL et l'allemand Siemens tentent en vain de construire un Airbus informatique : Unidata. Les enjeux politiques nuisent à la logique industrielle. Les Japonais NEC, Hitachi et Fujitsu tentent de se développer au-delà des limites du marché de l'Extrême-Orient.

L'innovation viendra, comme toujours, de nouveaux acteurs. La société Digital Equipment Corp (DEC) et son fondateur, Ken Olsen, prennent un départ foudroyant grâce au concept de mini-ordinateur. Le PDP/1 ouvre la voie mais c'est le PDP/11 qui assurera le succès du concept qui trouvera son point d'orgue avec le mythique couple VAX/VMS. D'autres suivront : Hewlett Packard qui vient de l'instrumentation scientifique, Texas Instrument qui vient du monde des composants, Prime qui vient de nulle part. Puisque le concept a du succès, IBM ouvre une division DSGD (Division des systèmes de grande diffusion) qui concurrence sa grande sœur la DO (Division des ordinateurs) avec ses machines 32, 34 et 38 qui ouvre la voie à l'AS 400.

Ces minis cohabitent avec les « mainframes » qui ont cessé de s'appeler 360/370 pour se nommer 4300, 3081, 3090. La compatibilité ascendante est assurée.

Figure 2 : Évolution des gammes IBM avant la grande crise



Étonnants par la taille et le prix (à l'époque) ces minis ne remettent pas fondamentalement en cause l'architecture de base. Ils introduisent cependant quelques concepts intéressants : le « **bus** » facilite la gestion des organes périphériques, le « **cluster** » permet à un groupe de minis de concurrencer un « mainframe ».

En 1981, IBM était n° 1 avec un CA de 24 Md de \$. DEC était n° 2 avec un CA de 3,5 Md de \$. Le n° 2 représentait 14 % du n° 1.

En 1994, IBM restait n° 1 avec 64 Md de \$. Le n° 2 était Fujitsu avec 21,8 Md de \$. Le n° 2 représentait 34 % du n° 1 mais celui-ci est en pleine crise. Entre le plus haut cours de 1987 et celui de septembre 1993, la perte de capitalisation boursière est de 80 Md de \$. Les pertes d'exploitation cumulées entre 1988 et 1993 représentent plus de 23 Md de \$.

En 1999, IBM est toujours n° 1 de la profession avec un CA de 78,5 Md de \$ mais, à partir de cette date, il n'est plus constructeur informatique. Les matériels représentent moins de 50 % de son chiffre d'affaires. IBM est devenu une société d'ingénierie et de services en informatique.

Son nouveau président, Lou Gerstner, qui ne vient pas du sérail mais du marketing des produits de grande consommation (CPG), a pris conscience d'une nouvelle réalité : le marché mondial des logiciels et services a dépassé en 1990 le marché des équipements.

6. Le phénomène PC et la banalisation des processeurs

La caractéristique la plus significative de l'offre actuelle est sans doute la banalisation des processeurs.

Autrefois chaque ordinateur disposait d'un processeur particulier. Aujourd'hui les constructeurs, réduits au rôle d'intégrateurs, assemblent les composants autour d'un processeur qu'ils peuvent acheter à un « fondeur ».

À l'image des autres disciplines (radio, télévision, automatismes) astreintes à l'état de l'art électronique les premiers ordinateurs ont utilisé la technologie des relais, puis celle des tubes et enfin celle des transistors discrets⁷.

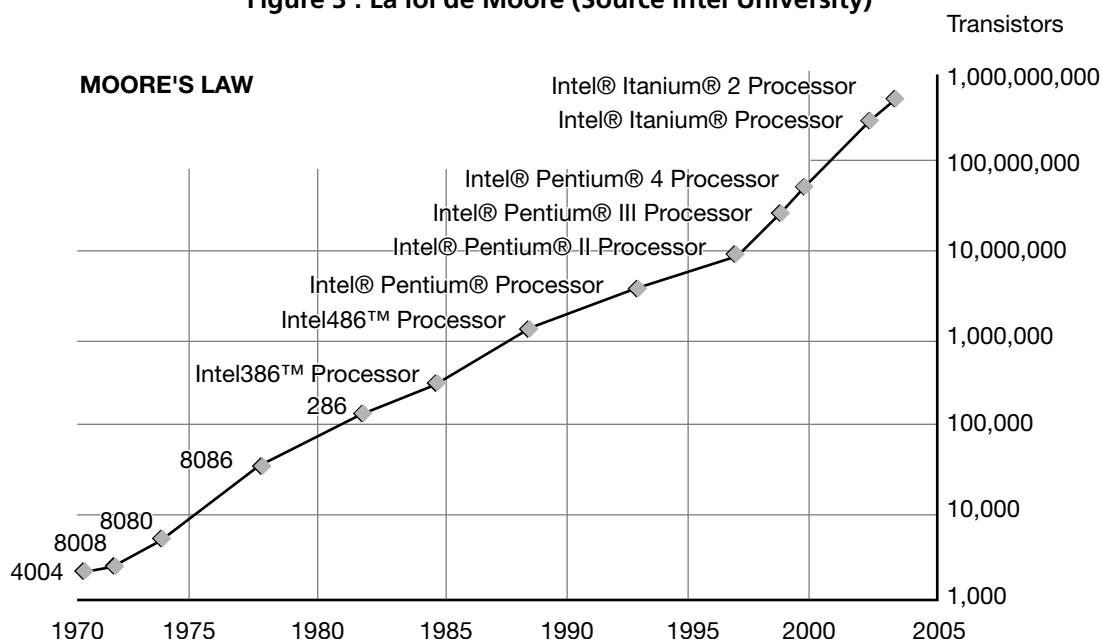
L'ère de la microélectronique commence avec les circuits logiques de Bob Noyce (futur fondateur d'Intel) chez Fairchild et de Jack Kilby chez Texas, qui intègrent des dizaines de transistors dans un circuit unique (puce ou chip). Une étape importante est celle de l'apparition en 1971 de l'Intel 4004, premier microprocesseur, c'est-à-dire première unité de commande et de calcul intégrée dans une puce. Une unité centrale joue à la fois de rôle d'unité de commande (décodage de chaque instruction élémentaire du programme) et d'unité de calcul (exécution de cette instruction qui correspond souvent à une opération de calcul mais peut correspondre aussi à une fonction de lecture ou d'écriture en mémoire centrale (électronique) ou secondaire (disque)). En 1980, IBM sélectionne l'Intel 8088 pour son PC.

L'autre fondateur d'Intel, Gordon Moore, établit une loi : le nombre de transistors intégrés sur un microprocesseur double tous les deux ans. Les produits 80286 (1983), 80386 (1985), 80486 (1989) et Pentium⁸ (1993) d'Intel, mais aussi ceux de ses concurrents, Motorola qui équipe le Macintosh avec le 68000, Mips, Sun, AMD Cyrix, accompagnent l'explosion du phénomène micro-informatique et valident la pertinence de la loi de Moore.

7. L'emballage d'un transistor discret ne comporte qu'un exemplaire du composant, par opposition aux circuits intégrés qui en regroupent plusieurs. Ne comptez pas sur lui pour garder un secret.

8. Avec le Pentium, Intel abandonne l'identification de ses produits par des numéros pour des raisons de protection de marque. Le Pentium II apparaît en 1996. Le Pentium III apparaît en 1998. Le Pentium IV apparaît en 2000.

Figure 3 : La loi de Moore (Source Intel University)



La micro-informatique n'est pas née avec le PC, annoncé le 12 août 1981 par IBM. Elle n'est même pas née avec l'Apple II. Elle est née avec des entreprises aujourd'hui disparues : Altair, Imsai, Tandy, Commodore, Osborne, Sinclair. Digital Research impose son système d'exploitation CP/M. Microsoft naît en 1975.

Ce nouveau marché inspire de nouveaux acteurs : Compaq, Victor, Dell plus tard avec le concept de vente directe. Mais IBM et Bull, comme HP et DEC, comme Toshiba, Sony et Fujitsu, font aussi des PC.

Les pionniers de l'ordinateur personnel sont supportés par les produits d'Intel (8008 et 8080), de Zilog (Z80) et de MOS Technologies (6502 qui équipe le mythique Apple II). En 1979, pour IBM, le PC n'est pas un produit stratégique. Philip Estridge de la Division Data Entry System, ne peut compter sur les « labos » pour des composants « *made in IBM* » et doit utiliser des produits du marché. Ce sera une chance pour Intel (le fournisseur du 8088) et pour Microsoft (le fournisseur du système d'exploitation DOS et de l'interpréteur Basic). DOS est « *le plus petit projet d'IBM, le plus grand projet de Microsoft* ».

Cette course à la puissance s'est traduite par :

- l'accroissement de la finesse de la gravure (un trait inférieur au micron) ;
- la prise en compte de nouvelles technologies de micro-circuit ;
- la taille de l'instruction traitée. Elle passe de 8 à 64 bits, ce qui permet d'enrichir le répertoire des opérations possibles (zone code instruction) et de multiplier le nombre de positions mémoire accessibles (zones adresses) ;
- l'augmentation de la vitesse d'horloge (de 5 MHz à 3 000 MHz) pour traiter plus vite chaque instruction élémentaire ;
- le développement de nouvelles générations de « bus » : IDE, PCI, AGP, USB, etc. ;
- diverses autres améliorations qui ont contribué à augmenter les performances et la facilité d'emploi.

L'augmentation de la taille du répertoire, donc du nombre d'instructions reconnues par le processeur, n'apparaît pas comme un progrès à tous les constructeurs. Pourquoi rendre un circuit plus complexe (donc plus lent, plus gourmand en énergie, moins fiable) pour des instructions qui ne sont employées que très rarement. Autant réaliser un circuit plus simple, plus rapide, qui simule avec un jeu d'instruction réduit toutes les instructions complexes chaque fois que cela s'avère nécessaire. C'est le concept du processeur RISC⁹, mis au point par les chercheurs d'IBM en liaison avec les universités de Stanford et de Berkeley.

9. RISC : Reduced Instruction Set Computer : ordinateur à jeu d'instruction réduit, par opposition au CISC.

Sortir de l'architecture Von Neuman : architectures parallèles

En voyant la file d'attente des travaux qui patientaient à l'entrée de l'unité centrale, les ingénieurs ont vite pris conscience que cette architecture constituait un goulot d'étranglement, un « *bottleneck* ».

L'idée est donc venue de la multiprogrammation, puis du multitraitement.

La « **multiprogrammation** » a résolu le problème des temps morts en chassant le processus en attente d'une ressource ou de l'annonce de la fin de l'opération qu'il a initialisé sur un disque, une unité de bande ou une imprimante. Il attendra au sein d'un empilement de sauvegardes de contextes qu'il puisse reprendre effectivement le fil des traitements. Place est laissée au suivant dans la file d'attente. Les travaux progressent ainsi plus vite mais à un instant donné, un seul programme monopolise les ressources de l'unité centrale de traitement.

Le « **multitraitement** » tire parti de la multiplication des processeurs. Puisqu'un travail passe sans cesse de l'état de veille à l'état actif, il peut à l'instant de son réveil être pris en charge par n'importe quel groupe de processeurs.

Mais ces concepts ne remettaient nullement en cause l'architecture Von Neuman. Le multitraitement multipliait des architectures de ce type mais la mise en commun de n unités centrales n'engendrait pas une machine n fois plus rapide. Le temps d'« *overhead* » nécessaire à la gestion de la pile des travaux devenait rapidement important.

Les supercalculateurs qui apparaissent en 1976 avec l'apparition de la machine à architecture vectorielle, conçue de Seymour Cray. Refroidie au fréon et dotée de 8 Mo de mémoire vive cette machine pesait près de 5 tonnes et coûtait environ 700 000 dollars. Elle équipe rapidement tous les grands centres de recherche du monde, ce qui permet d'annoncer que les chercheurs de la fin du xx^e siècle n'ont besoin que d'un tableau noir et d'un morceau de Cray !

L'architecture vectorielle est un premier pas vers la rupture du modèle Von Neuman car elle est conçue pour traiter simultanément les éléments d'un vecteur. Il faut que les applications soient adaptées à ce mode de calcul et certains langages, comme APL de Keith Iverson, sont conçus pour résoudre tous types de problèmes, y compris ceux de gestion, par des manipulations de vecteurs et de matrices. APL est à la base du concept d'hypercube aujourd'hui très utilisé dans le monde de l'informatique décisionnelle.

Il faut attendre l'arrivée des architectures massivement parallèles pour enregistrer la réelle rupture avec l'architecture classique. Cette architecture implique que l'on puisse décomposer un programme en un ensemble de tâches indépendantes, qui sont exécutées simultanément sur des processeurs différents. Selon la manière dont les processus coopèrent au cours du traitement, on distingue les systèmes « fortement couplés » des systèmes « faiblement couplés ».

Plusieurs architectures types caractérisent ce domaine.

Les architectures MIMD (*Multiple Instructions Multiple Data*) attribuent à chaque processeur une mémoire de données et de programme indépendante. Les échanges entre processeurs s'effectuent par passage de message. Cette architecture impose de segmenter l'application ou les données. Le nombre de processeurs varie généralement entre quelques dizaines à plusieurs centaines.

Les architectures SIMD (*Single Instruction Multiple Data*) proposent une mémoire centrale partagée par tous les processeurs qui exécutent de manière synchrone le même programme sur des données différentes. La Connection Machine CM-1 de la société Thinking Machines, avec ses 65 536 processeurs, est représentative de cette famille. La machine est conçue sur le modèle cerveau humain (réseau neuronal) car chaque processeur, de puissance modeste, effectue un travail très ciblé. L'ordinateur reconfigure les connexions internes entre les processeurs pour résoudre un problème donné. Les performances dépendent du type d'application à traiter.

Tous ces systèmes exigent des techniques de communication entre les différents composants, de contrôle de cohérence des mémoires, de parallélisation et d'allocation des tâches. Celles-ci les cantonnent dans des domaines d'application très précis et la quasi-totalité des ordinateurs dédiés à la gestion des entreprises sont encore du type Von Neuman.

7. Grilles et constellations

Le *Monde Informatique*¹⁰ rappelait récemment une prévision de Len Kleinrock, professeur à l'UCLA en 1969 : « Nous allons certainement assister à l'émergence de services de calcul qui, comme les actuels services téléphoniques ou électriques, vont desservir les domiciles et les entreprises de tout le pays. »

Les connexions Internet à haut débit représentent une composante de cette construction. Le concept de « **Grid** » en représente une autre. Ce concept réside dans la capacité à négocier des accords de partage des ressources informatiques entre un certain nombre de fournisseurs et de consommateurs et à utiliser cette mutualisation pour autoriser l'accès à des logiciels, à des capacités de calcul et d'accès aux données.

Le « grid » se distingue du « cluster » en ce sens que les ressources mises en œuvre ne sont pas soumises à un contrôle centralisé. Le Grid exige cependant la mise en place de systèmes de contrôle, des « ordonnanceurs », pour définir et administrer les règles de partage.

Le mot « **Constellation** » a été utilisé pour la première fois en l'an 2000 à la conférence internationale d'informatique scientifique de Dallas pour désigner un cluster constitué d'un nombre restreint de nœuds hyperpuissants, à grosse mémoire partagée.

L'Idris (Institut du développement et des ressources en informatique scientifique) du CNRS entame le *xxi*^e siècle avec des constellations scalaires (IBM) et vectorielles (NEC), dont les nœuds possèdent une puissance comprise entre 128 et 160 Gigaflops et une taille mémoire variant de 64 à 256 Gigaoctets.

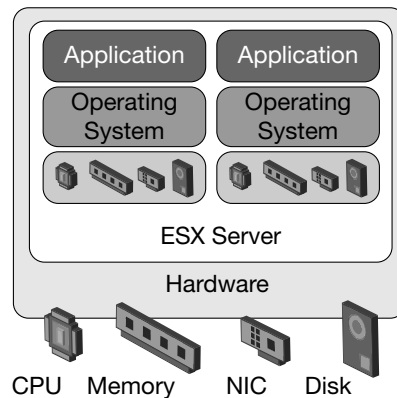
Ces constellations sont intégrées dans un environnement complexe comprenant, d'une part, un nombre important de machines de support et de serveurs de visualisation et de pré et post-traitement performants et, d'autre part, un système d'avant-garde de gestion de données, capable de stocker jusqu'à 800 Téraoctets de données produites par les simulations numériques.

8. Virtualisation

- La virtualisation est l'ensemble des techniques matérielles et/ou logicielles qui permettent de faire fonctionner sur une machine unique plusieurs systèmes d'exploitation et/ou plusieurs applications, séparément les uns des autres, comme s'ils fonctionnaient sur des machines physiques distinctes.
- La virtualisation est la solution la plus efficace pour exploiter à plein les serveurs. C'est particulièrement utile quand on sait qu'un serveur wintel est généralement exploité à 10- 5 % de ses capacités et un serveur Unix à 30 %.
- Elle permet de faire cohabiter plusieurs environnements indépendants et de simuler une machine physique et tous ses composants (les outils de virtualisation qui simulaient sur PC les anciennes consoles de jeu Atari ou Sega ont eu un grand succès). Pour exploiter à plein le processeur, la couche d'abstraction agit comme un hyperviseur dont le travail est d'allouer la ressource processeur aux applications, en fonction de leurs besoins et du niveau de service requis.
- La virtualisation n'est pas un concept récent : elle fut développée dans les années 1970 par IBM qui développa le système expérimental CP/CMS, qui devint ensuite l'hyperviseur VM/CMS (cf. § 3.3.2).
- La société VMware développa et popularisa à la fin des années 1990 un système propriétaire de virtualisation logicielle des architectures de type x86. Suivirent ensuite les solutions Xen, QEMU, Bochs, Linux-VServer, Virtual Box (open source) ainsi que VirtualPC et VirtualServer (propriétaire) ont achevé de populariser la virtualisation dans le monde x86. Les fabricants de processeurs x86 AMD et Intel ont implémenté la virtualisation matérielle dans leurs gammes en 2000. Les grands acteurs restent VMWare, racheté par EMC, avec ESX server, et Microsoft qui propose Virtual Server, racheté à la société Connectix.

10. N° 1095 du 16 décembre 2005.

Figure 4 : La virtualisation avec ESX Server



Divers avantages militent en faveur de la virtualisation des serveurs :

- capacité à déployer très rapidement des infrastructures et plateformes nouvelles pour couvrir les besoins des nouveaux projets ;
- réduction des coûts d'infrastructure : les experts estiment que l'on peut diviser par 2 les coûts de possession associés. En corollaire, la virtualisation offre l'opportunité de réinvestir les ressources dégagées dans d'autres postes ;
- simplification des plans de reprise d'activité (PRA) ;
- augmentation du cycle de vie de certaines solutions (par exemple, allongement de la durée de vie des applications tournant sous Windows NT4).

La contribution de la virtualisation et la pertinence de chacun des points ci-dessus dépendent considérablement du contexte et des objectifs propres à chaque entreprise. Une étude d'opportunité préalable est recommandée pour éclairer les impacts économiques, techniques et organisationnels d'un projet de virtualisation. Par ailleurs, il faut prendre garde à certains points faibles, en particulier ceux touchant l'apparition de nouvelles failles de sécurité.

B. POUR STOCKER L'INFORMATION

1. Le stockage électronique

L'usage du calcul binaire va faciliter à la fois le traitement et le stockage. En ce qui concerne le stockage, la règle est simple. L'élément lu est actif : c'est la valeur 1. L'élément lu est passif : c'est la valeur 0. Il est possible de construire des circuits électroniques (les bascules) capables de prendre un état parmi deux possibles. Au premier état correspond la valeur 0, au second la valeur 1.

En réunissant des millions de circuits de ce type, on peut constituer une mémoire de bonne capacité et très rapide d'accès. L'information collectée peut être stockée dans cette mémoire.

Une fois stockée, l'information peut être lue et modifiée (mémoire RAM) ou simplement lue (mémoire ROM pour *Read Only Memory*). La mémoire RAM est volatile, c'est-à-dire qu'elle exige d'être alimentée en énergie électrique pour conserver l'information. Cette mémoire RAM va constituer la mémoire centrale.

2. Le stockage magnétique

Construire un dispositif capable de prendre et de conserver un état stable parmi deux possibles n'est pas réservé à l'électronique. Une particule magnétique peut être magnétisée (1) ou non (0) par un courant électrique. Nous avons vu, avec l'IBM 705, que les mémoires des premiers ordinateurs, à tores de ferrites, fonctionnaient selon ce principe.

L'ingénieur danois Valdemar Paulsen a présenté le premier enregistrement magnétique à l'exposition universelle de Paris en 1900. Depuis cette date, la corde à piano a été remplacée par des matériaux magnétiques enduits sur des bandes de plastiques ou des disques rigides, mais le principe de l'enregistrement des données est resté le même que dans l'appareil de Paulsen.

La mise en application des découvertes relatives à l'électromagnétisme conjuguée avec l'avènement des nouvelles techniques des matières plastiques a permis de développer de nouveaux supports d'information aujourd'hui familiers : bandes, disques, disquettes, badges, cassettes... ou déjà oubliés : tambours, feuillets, comptes à piste, etc.

Les temps d'accès aux informations contenues dans ces mémoires magnétiques sont beaucoup plus longs que ceux associés aux mémoires électroniques. En contrepartie, la capacité de stockage est beaucoup plus forte, et l'information est conservée sans apport d'énergie externe.

Ces supports constituent une mémoire dite auxiliaire.

La densité des enregistrements magnétiques atteint plusieurs millions d'octets par cm^2 . Comme pour les microcircuits électroniques, la diminution de la taille améliore non seulement la densité et la vitesse de lecture des données. À vitesse de lecture constante, la quantité d'information lue est plus grande. En revanche, la diminution de la taille des zones magnétiques réduit l'intensité du champ magnétique qu'il est possible de lire. Les limites de l'enregistrement magnétique sont atteintes.

3. Le stockage optique

Une autre technologie devait prendre le relais. La réponse à ces besoins est venue des technologies optiques : le DON (Disque Optique Numérique). Le terme générique de disque optique recouvre en fait plusieurs catégories de produits.

Avec la technologie optique, l'énergie nécessaire à la lecture n'est plus stockée dans le support. Un rayon laser extérieur lit les données, ce qui a pour effet de repousser les limites de la taille des informations stockées. Cette technologie a été utilisée pour le compact-disc audio introduit en 1983. Celui-ci a connu le succès que l'on connaît, chassant en quelques années le disque analogique en vinyle.

Ce compact disc a rapidement gagné les faveurs de l'industrie informatique, sous le nom de CD-ROM par analogie avec les ROM (*Read Only Memory*) car il n'était pas réinscriptible, ce qui a prolongé la durée de vie des supports magnétiques réinscriptibles. De même format physique que les compact-discs audio, les CD-ROMs de 12 cm, pressés à partir d'une matrice, ont marqué une première étape à 800 Mo. Les images fixes et, plus encore, la vidéo numérique, nécessitent des capacités beaucoup plus importantes. Les principaux fabricants mondiaux se sont mis d'accord fin 1995 sur un standard de CD-ROM permettant de stocker 6,4 milliards de caractères.

Le WORM (*Write One Read Many*) est un support de stockage non réinscriptible. Cette caractéristique a priori pénalisante est particulièrement intéressante pour l'archivage légal des données et le respect de l'exigence de garantie de la preuve. Il répond à la norme Afnor Z42-013.

À peine le DVD s'est-il généralisé que les fabricants se battent pour imposer son successeur. Comme souvent, deux technologies s'affrontent : le Blu-Ray promu par Sony et Matsushita et le HD-DVD soutenu par NEC et Toshiba. Ces deux supports utilisent le même principe de base, le laser bleu qui vient se substituer au laser rouge employé par les lecteurs et graveurs de CD et DVD et dont la longueur d'ondes trop élevée ne permet plus d'augmenter significativement les capacités de stockage.

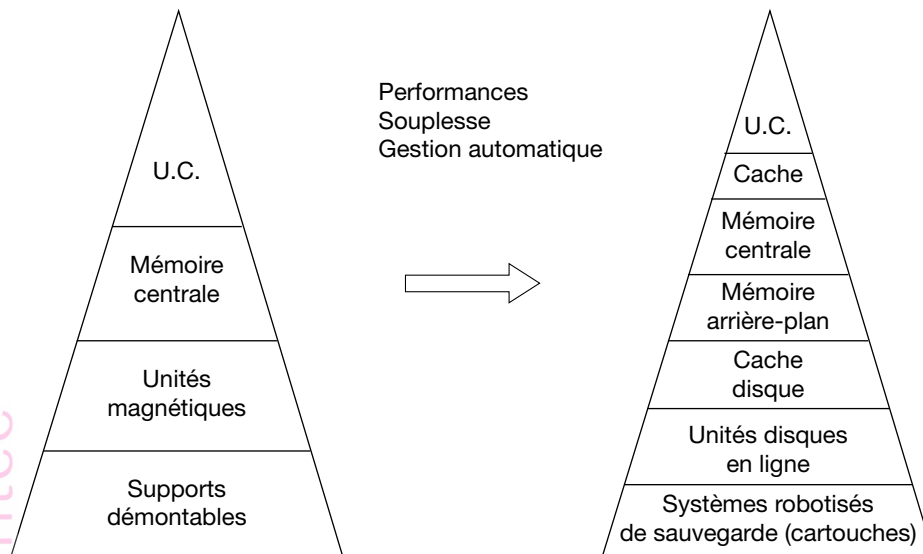
Le Blu-Ray stocke 23 Go de données par couche contre 30 Go pour le HD-DVD en double-couche. En revanche, celui-ci présente l'avantage d'assurer une compatibilité descendante avec les DVD actuels. Il a d'ailleurs été entériné par le DVD Forum, l'instance chargée de ratifier les normes en matière de stockage optique.

4. Un éternel compromis : capacité de stockage et rapidité d'accès

Ces évolutions techniques n'ont cependant pas permis de résoudre l'antagonisme entre capacité et vitesse. L'accès aux informations est devenu le goulet d'étranglement alors que les capacités de traitement des processeurs augmentent de manière considérable. Les unités de stockage sont aussi devenues les points les plus fragiles du point de vue de la fiabilité.

La mémoire cache est une autre approche pour l'amélioration des temps d'accès à l'information. Cette mémoire rapide sert de tampon entre les disques et l'unité centrale qui regroupe les circuits de traitement et de contrôle. Lorsqu'elle est bien utilisée, elle évite des accès aux disques en stockant les dernières informations utilisées. En effet, la statistique démontre que la probabilité d'avoir à nouveau besoin de ces informations est très élevée. Tout le problème revient à ne pas saturer cette mémoire rapide avec des données dont on n'aura plus l'usage. Les constructeurs ont développé plusieurs techniques, dont celle des « **caches** », pour atteindre cet objectif.

Figure 5 : la hiérarchie des mémoires



C. UNE COURSE PERPÉTUELLE

La technologie micro-électronique et quelques technologies annexes (mémoires magnétiques et optiques, batteries et alimentations, technologie de base des télécommunications) ont donc rendu possible cette fantastique course que nous avons commencé à retracer.

Cette évolution était une condition nécessaire, mais était-elle une condition suffisante ? Nous pouvons répondre clairement non car il fallait que les utilisateurs acceptent les contraintes liées à une remise en cause permanente et à une rapide obsolescence.

Ils ont accepté pour deux raisons :

- C'était moins cher !
- C'était « fun » !

La baisse des coûts a été le premier argument.

Le coût marginal de production d'un circuit est à peu près constant (une dizaine d'euros). La matière première, le silicium est disponible en abondance partout. Le prix unitaire d'un circuit est donc fixé par l'amortissement des études et de l'usine de fabrication. À performances constantes, le coût d'un microprocesseur ou de la mémoire est divisé par 10 tous les 4 ans.

Au début des années 1980, le super ordinateur CRAY 1, capable de traiter 100 millions d'instructions par seconde était vendu 10 millions d'euros. Il nécessitait une grande salle machine et des équipements de climatisation. En 1995, un micro-ordinateur de cette puissance, à base de Pentium 100, avec la même capacité mémoire est la machine multimédia de base pour le grand public. Le prix est d'environ 1 500 francs soit 6 000 fois moins que le CRAY 1. Ce micro-ordinateur fonctionne posé sur un bureau, sans précautions particulières.

Que pouvons-nous acheter avec 1 500 € ?

| Date | Offre |
|--------------|---|
| Juin 1991 | Processeur 386, 16 MHz, 1 Mo de RAM, 40 Mo sur disque, Écran Monochrome EGA, DOS. |
| Avril 1992 | Processeur 386, 25 MHz, 2 Mo de RAM, 80 Mo sur disque, Écran Monochrome VGA, DOS. |
| Octobre 1993 | Processeur 486, 33 MHz, 4 Mo de RAM, 170 Mo sur disque, Écran couleur 15" couleur 1024*768, DOS et Windows. |
| Octobre 1994 | Processeur 486, 50 MHz, 8 Mo de RAM, 320 Mo sur disque, Écran couleur 15" couleur 1024*768, Accélérateur vidéo en bus local avec 512 Ko de mémoire vidéo, DOS et Windows. |
| Octobre 1995 | Processeur Pentium 100 MHz, 8 Mo de RAM, 525 Mo sur disque, Contrôleur vidéo haute performances avec 1 Mo de mémoire vidéo, DOS/Windows. |
| Octobre 1996 | Processeur Pentium 166 MHz, 16 Mo de RAM, 1 Go sur disque, 2 Mo de mémoire vidéo, Écran couleur 17", Win 95. |
| Octobre 1997 | Pentium MMX 166 MHz, 32 Mo de RAM, 2 Go sur disque, Ensemble multimédia, CD ROM 12x, Win95, Office 97. |
| | |
| Octobre 2005 | Portable, Intel Pentium M725 1,60 GHz, 512 Mo de RAM et 60 Go, Graveur DVD, Bluetooth, infrarouge, Firewire. |
| Octobre 2007 | Portable, Intel Core 2 Duo T7500 2,2 GHz, 2 048 Mo de RAM et 160 Go de disque dur, Graveur DVD, Bluetooth, infrarouge. |
| Octobre 2008 | Portable, Intel Core 2 Duo T9500 2.6 GHz, 3 Go de RAM et 200 Go de disque dur, carte graphique 256 Mo, Écran 17" 1920*1200, Bluetooth, WiFi. |

Nous gagnons en 17 ans la portabilité, la connectivité à de multiples réseaux, une définition écran multipliée par 4,8 (800.600 à 1920.1200 une vitesse d'horloge multipliée par 162, une capacité RAM multipliée par 3 000, une capacité disque multipliée par 5 000.

Le deuxième argument a été le côté ludique. Lors d'une enquête menée auprès des utilisateurs aux États-Unis à la fin des années 1990 sur les nouvelles interfaces homme-machine à base de souris, fenêtres et menus déroulants, la réponse qui vient en tête est : *It's fun*.¹¹

D. BILAN

L'évolution des technologies et celle des architectures de machines sont indissociables. Elles peuvent se résumer ainsi :

- Plus petit ! (donc plus rapide, plus mobile, plus économe !)
- Plus puissant !
- Moins cher !

III. ARCHITECTURES DE SYSTÈMES

A. SYSTÈMES D'EXPLOITATION

Chaque ordinateur fonctionne sous le contrôle d'un système d'exploitation (OS pour *Operating System*), programme en charge de l'attribution des ressources pour les programmes utilisateurs.

Dans la phase de conception, le système d'exploitation décharge le programmeur de nombreuses tâches techniques fastidieuses et lui permet de se concentrer sur la finalité de son programme.

Nous rappelons les fonctions du système d'exploitation :

- allocation des ressources de la machine aux différents travaux en cours d'exécution ;
- gestion des tâches :
 - initiation et prise en compte fin opération (lecture/écriture sur disque, impression),

11. Mot de la langue anglaise que nous pouvons traduire par « plaisant ».

- prise en compte sollicitations du réseau (transactions),
- traitement coopératif ;
- gestion des travaux (ensemble des tâches qui vont s'effectuer une fois l'exécution du programme lancée) :
 - interprétation des commandes,
 - enchaînement des étapes ;
- gestion de la mémoire ;
- gestion des unités périphériques.

Trois familles d'OS subsistent aujourd'hui :

- La famille des systèmes IBM.
- La famille Unix avec la longue marche vers un noyau commun et l'arrivée de Linux.
- La famille Microsoft.

B. LES SYSTÈMES D'IBM

IBM est le seul « constructeur »¹² qui ait pu conserver sa gamme « propriétaire ». Bien qu'Unix, Linux et Microsoft Windows soient au catalogue d'IBM, celui-ci conserve des systèmes spécifiques :

- Pour sa gamme de gros ordinateurs :
 - z-OS est la désignation actuelle de l'OS des grands systèmes *IBM*. Cette famille naît avec l'OS 360 qui équipe la fameuse famille IBM 360 en 1964. Elle accompagne l'évolution de la gamme et reçoit les noms successifs d'OS/VS, de MVS et d'OS/390. Elle supporte les travaux batchs et transactionnels des grandes entreprises ;
 - z-VSE est l'aboutissement actuel d'une ligne de produit née aussi avec le 360, le *DOS* (rien à voir avec le *DOS* du PC), devenu *DOS/VSE*. Plus simple à mettre en œuvre que son grand frère, il devait disparaître mais ses clients, généralement des entreprises plus petites que celles utilisant l'OS 360, ont bataillé auprès d'IBM pour le conserver ;
 - z-VM est l'aboutissement du troisième système d'exploitation associé à la famille 360 : VM. Apprécié par les universités et les centres de recherche pour ces capacités conversationnelles, VM reposait sur le concept de machine virtuelle (VM = *Virtual Machine*), véritable ordinateur personnel virtuel. Le succès de VM a aussi été renforcé par sa bonne adaptation aux premiers services de bureautique collective (Profs) et d'informatique décisionnelle (AS).
- Pour sa gamme de minis :
 - OS/400 est lié à la famille AS/400 (aujourd'hui *iseries*, dédiée aux PME).

C. LES SYSTÈMES UNIX

La première version d'Unix a été développée sur PDP/7 en 1971 dans les Bell Laboratories d'AT&T par une équipe conduite par Ken Thompson et Dennis Ritchie, en reprenant certains des concepts de l'OS Multics du GE 645.

Tous les OS de l'époque étaient développés en Assembleur, donc spécifiquement pour un ordinateur. En 1973, Unix est réécrit dans un langage de 3^e génération conçu pour l'occasion : le langage C. Cette caractéristique est révolutionnaire puisque, pour la première fois, un OS devient portable sur plusieurs machines.

Outre l'indépendance de la plate-forme matérielle, Unix affiche les caractéristiques suivantes :

- un système multi-utilisateurs et multi-tâches ;
- un système modulaire, avec des sous-ensembles aux fonctions bien définies, aisés à maintenir ;
- un système intégrant un système complet d'Entrées/Sorties ;
- un système intégrant un système de fichiers hiérarchiques ;
- un système gérant des processus asynchrones et réentrants ;

12. Entre guillemets car nous avons vu qu'IBM reste un constructeur mais est surtout devenu une société de services.

- un système intégrant un mécanisme simple d'échange entre mémoire centrale et mémoires auxiliaires (disques) : le « *swapper* » ;
- un système offrant une interface utilisateur simple et interactif, non intégré dans le noyau : le « *shell* » ;
- un système assurant une maintenance et une évolution facile.

Des décisions de justice empêchent Unix de devenir un produit commercial. Il est donc mis à la disposition d'organismes à but non lucratif et d'universités. L'université de Berkeley distribue une version sous le nom de *Berkeley Software Distribution (BSD)*.

Le consortium Unix International (AT&T, Sun, Intel, Olivetti et Fujitsu) reprend le contrôle d'Unix avec Unix System V en 1983 et décide de le commercialiser.

Pour s'opposer au monopole d'Unix International, d'autres constructeurs (IBM, DIGITAL, HP, BULL) créent l'OSF (*Open Software Foundation*) en 1990.

Unix souffre de cette lutte jusqu'à la création d'un noyau commun entre Unix System 5 V4 et OSF/1 en 1993, alors qu'AT&T cède le contrôle d'Unix System Laboratories à Novell. Chaque grand constructeur met Unix à son catalogue (AIX pour IBM ; HP-UX pour HP, Solaris pour Sun, etc.). Ce sont les normes Posix de l'IEEE qui garantissent la portabilité des programmes d'un Unix à un autre.

Linux a été écrit par le Finlandais Linus Torvalds et a été amélioré par de nombreux développeurs du monde entier. C'est une version d'Unix entièrement nouvelle. Linux est protégé par le droit d'auteur conformément à GNU *General Public License (GPL)*. Le projet GNU a été lancé par Richard Stallman en 1984, alors au laboratoire d'intelligence artificielle du MIT, pour créer un système d'exploitation libre et complet et « *ramener l'esprit de partage qui prévalait autrefois dans la communauté informatique* ».

À ce jour, Linux est un vrai système 32 bits, multitâches et multi-utilisateurs, offrant le support des fonctions réseau. Il s'installe sur la plupart des PC (avec ou sans autre système d'exploitation). Il supporte une large gamme de programmes de protocoles, de langages et d'application GNU.

Linux est une libre implémentation des spécifications Posix, avec des extensions System V et Berkeley. Ceci accélère la propagation de Linux au sein de l'administration, qui exige la conformité Posix de la plupart des systèmes qu'elle utilise.

Rappelons la galaxie Unix aujourd'hui :

- GNU/Linux : un système d'exploitation libre s'appuyant sur le noyau Linux et les outils GNU. Distributions Debian, Gentoo, Mandriva (MandrakeLinux), Red Hat, Fedora, SuSE, Slackware, EduLinux...
- La famille BSD : un effort réussi pour rendre sa liberté au système de Berkeley comprenant : NetBSD, OpenBSD, FreeBSD et ses dérivés, PicoBSD et DragonFly BSD, Darwin (sur lequel est construit Mac OS X, semi-propriétaire).
- Les UNIX propriétaires : AIX (IBM, SystemV), A/UX (Apple, SystemV), BOS (Bull Operating System), Irix (Silicon Graphics, SystemV), HP-UX (Hewlett Packard, SystemV), NeXTSTEP (NeXT, BSD), Sinix (Siemens), Solaris (Sun, SystemV), SunOS (Sun, BSD), Tru64 (HP-Compaq).

D. LA FAMILLE MICROSOFT

La version 1 de MS-DOS, présentée au public le 12 août 1981, est en fait le 86-DOS (aussi appelé QDOS pour *Quick and Dirty Operating System*), une adaptation de CP/M pour processeur Intel 16 bits, réalisée par Tim Patterson pour la société Seattle Computer Products. Les droits sont rachetés 50 000 \$ par Microsoft pour le proposer à Philip Estridge, patron de la Data Entry System d'IBM qui cherche un OS pour équiper son PC¹³ (Version PC-DOS). Cette version ne dispose que de quelques commandes élémentaires de gestion de fichiers, d'un basic rudimentaire et ne supporte que les disquettes 5"1/4 simples faces de 160 Ko.

13. Le PC n'étant pas, à l'époque, un produit stratégique pour IBM, *Estridge* ne peut faire appel aux labos d'IBM. Il doit faire son marché auprès de fournisseurs extérieurs.

Les versions 2 et 3 apportent quelques services complémentaires mais rien de révolutionnaire au niveau de l'interface utilisateur. Or la demande se fait forte pour des interfaces graphiques plus conviviales. Les travaux fondamentaux réalisés dès 1973 par les équipes du *Xerox Palo Alto Research Center* (XPARC) ont permis l'invention de la souris et le développement des concepts de GUI (*Graphic User Interface*) et de WYSIWYG (« *What You See Is What You Get* »). Ces innovations ont donné naissance aux premiers produits commerciaux comme *LISA* en 1982. Chers et peu performants, ces produits ont été des échecs. En 1985, le Macintosh d'Apple a été le premier produit à réussir commercialement.

Beaucoup tentent de développer une interface graphique pour le PC, mais tous vont à l'échec : Vision de VisiCorp (Créateur de Visicalc), DesQ de Quaterderck, GEM de Digital Research (Créateur de CPM), Topview d'IBM.

En novembre 1983, Microsoft annonce Windows, mais on ne voit rien venir. Windows est devenu un « *Vaporware* » alors que les relations entre Microsoft et Apple se dégradent.

Windows 1.0 arrive enfin en novembre 1985. On ne sait pas vraiment quoi faire de cette surcouche à MS-DOS du fait de la lenteur et de l'absence de logiciel d'application.

Véritable OS à interface graphique, l'OS/2, fruit de la dernière collaboration IBM-Microsoft, sort alors qu'aucune configuration machine n'est réellement adaptée à sa lourdeur. Ce sera un échec pour IBM qui cherchait, au travers du couple PS/2-OS/2, mal positionné au plan marketing, à reprendre le contrôle du marché.

Il faut attendre 1992 et la conjonction du processeur 386, de Windows 3.1 et d'Office version Windows pour que le succès soit enfin au rendez-vous. C'est un remarquable succès. Il aura ses successeurs avec Windows 95, puis Windows 98 et enfin Windows XP qui s'affranchissent petit à petit de MS-DOS.

Windows NT reprend l'ambition d'OS/2 : être un véritable OS à interface graphique. Dave Cutler est le responsable du projet. Il a été, chez Digital Equipment, l'architecte du système d'exploitation VMS (*Virtual Memory System*) sur VAX. Son projet s'appellera donc WNT (Faites + 1 sur chaque lettre de VMS)¹⁴. Windows NT est décliné en version poste de travail et en version serveur (Windows NT Advanced Server). NT 3.x laisse la place à NT 4.x, puis à Windows 2000 et 2003.

Bill Gates a annoncé en septembre 1999 à Seattle la stratégie du *Digital Nervous System* (DNS) qui sous-tend depuis toutes les initiatives de Microsoft. Les bénéfices attendus pour l'entreprise cliente (selon Microsoft bien sûr) sont :

- agir plus rapidement ;
- réagir à tous les événements ;
- prendre des décisions documentées ;
- se rapprocher des clients ;
- se concentrer sur le business et non sur la technologie.

La stratégie a été précisée un an plus tard selon un ensemble de 6 points :

- architecture du traitement informatique (sur la base de Windows) ;
- toutes les informations sous forme numérique ;
- messagerie électronique universelle (sur la base d'Outlook) ;
- omniprésence de la connectivité (sur la base des sites intranet et Internet utilisant IIS) ;
- outils de productivité communs à tous les utilisateurs (sur la base d'Office) ;
- applications professionnelles spécifiques et intégrées (autour de SQL server).

Windows Distributed interNet Applications Architecture (DNA) a été la première couche d'implémentation de Microsoft pour ce système nerveux numérique, préfigurant .Net).

Le cœur de DNA est l'intégration du Web et des modèles de développement d'application via un modèle d'objet commun. DNA utilise un jeu commun de services : composants, langage HTML, navigateur et serveur web, bases de données... L'interconnexion entre les composants se fait par COM/DCOM (*Distributed Common Object Model*).

14. Les informaticiens adorent ces jeux sur les acronymes. N'oublions pas la machine HAL du film de S. Kubrick, 2001 : *L'Odyssée de l'espace* : Faites +1 sur chacune des lettres de HAL.

Microsoft annonce au Windows Hardware Engineers Conference 2005, la reprise du développement du successeur de XP, Longhorn sur la base de Windows Server 2003, auquel sont ajoutées les fonctions principales du Windows XP Service Pack.

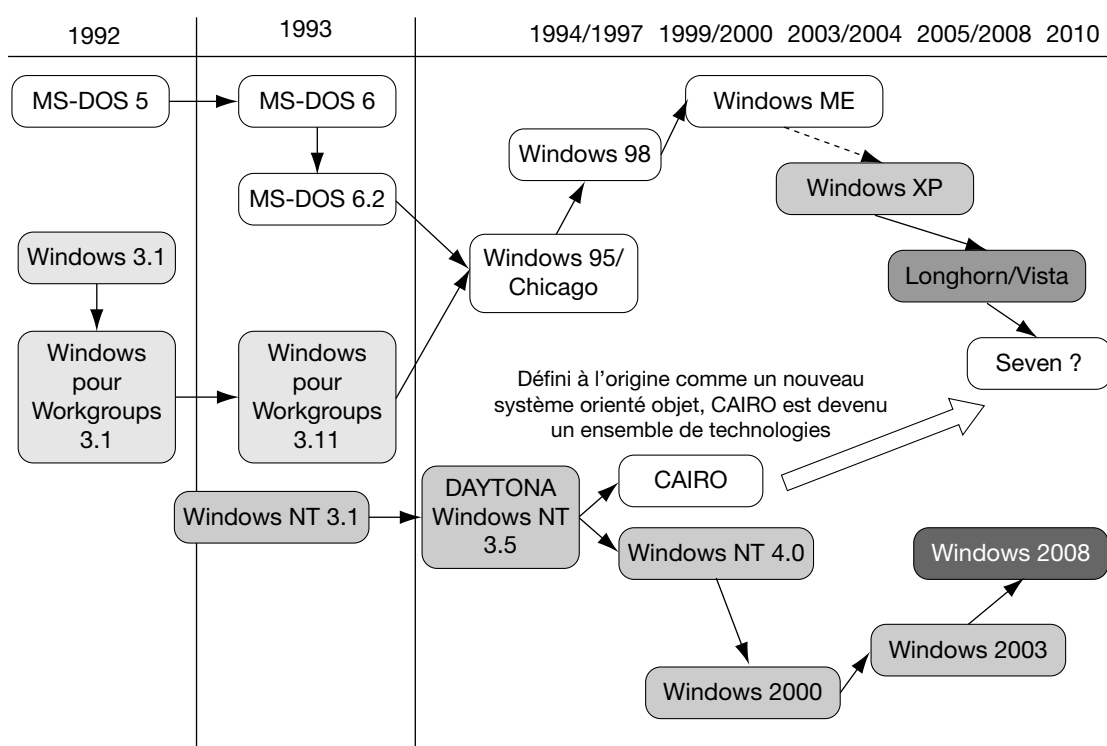
Longhorn devient Vista et sort en janvier 2007, 5 ans après XP. Cette version n'a pas apporté toutes les nouveautés attendues, comme le très critiqué NGSCB (*Next Generation Secure Computing Base*) et le service de recherche WinFS.

Vista est un succès mitigé qui conduit Microsoft à annoncer la nouvelle mouture, Seven, dès 2008.

Windows NT a l'ambition d'être véritable OS multi-tâches et multi-utilisateurs, adaptable sur plusieurs plates-formes matérielles, avec une interface graphique. Windows NT sera décliné en version poste de travail et en version serveur (Windows NT Advanced Server). NT 3.x laisse la place à NT 4.x, puis à Windows 2000, 2003 et 2008.

La figure ci-après rappelle quelques jalons de l'évolution de cette famille Microsoft.

Figure 6 : Famille des systèmes d'exploitation Microsoft



IV. ARCHITECTURES DE RÉSEAU

A. ASSURER LA CONNEXION DES POSTES DE TRAVAIL DISTANTS

Lorsque les ordinateurs sont apparus dans les entreprises, la mise en place d'applications (comptabilité, paie, etc.) a conduit à l'organisation de procédures de circulation des documents qui, bien qu'elles ne mettent pas en œuvre les techniques des télécommunications, dressaient déjà la carte d'un réseau.

La collecte de l'information était assurée dans les différents services au moyen de bordereaux qui étaient transmis à un atelier spécialisé, où de nombreuses employées, qualifiées en tant que « perfo-vérifs », saisissaient une nouvelle fois les informations consignées sur les bordereaux pour les transformer, selon un code précis, en petits trous dans une feuille de carton.

L'ordinateur savait lire ces cartes, décoder les perforations, et assurer les traitements correspondants. Ce cycle était entaché de nombreuses erreurs, le plus souvent humaines, qui imposaient un contrôle des données transmises et plusieurs allers et retours entre le service émetteur et l'atelier de saisie.

Ces procédures étaient longues et coûteuses. Les organisations mesuraient mal l'intérêt de disposer d'un programme assurant le calcul de la paie en quelques minutes alors que les travaux préliminaires de saisie, de contrôle et de correction exigeaient plusieurs jours. Les applications construites selon ce schéma étaient – sont toujours – dites « par lots » (« *batch processing* »).

Toutes les entreprises disposaient déjà d'un réseau de communication capable d'acheminer rapidement les informations d'un poste de travail à un autre poste de travail, d'un établissement à un autre établissement : le **Réseau Téléphonique Commuté (RTC)**. Ce réseau, conçu pour transporter la voix humaine, était cependant mal adapté au transport d'informations codées selon les exigences de la technologie informatique.

Ce défaut a été jugé provisoirement tolérable face à tous les avantages que pouvait présenter le mariage de la technologie informatique avec celle des télécommunications. La cérémonie a été célébrée à la fin des années 1960. Le fruit de cette union fut baptisé « Télénformatique ».

Le concept eut rapidement un grand succès. Indépendante des aléas de transmission des documents, la télénformatique assurait une collecte et une concentration rapides des données vers le centre de traitement. En permettant la consultation et la modification des fichiers à distance ainsi que le rapprochement permanent avec les bases de données de référence, la télénformatique contribuait à garantir une validation permanente des informations et à en assurer une plus grande fiabilité. La télénformatique permettait à l'ordinateur de collecter l'information **en tous lieux, en tout temps**, sous toutes ses formes. En supprimant le support papier fragile et dégradable, la télénformatique diminuait le risque de disparition d'informations vitales.

Pour pouvoir bénéficier de tous ces avantages, il fallait surmonter la contrainte d'inadéquation du réseau téléphonique au transport de données informatiques, ce qui revenait à résoudre deux problèmes.

Il fallait rendre le réseau téléphonique capable de transmettre des signaux numériques, alors qu'il avait été conçu pour assurer la transmission de signaux analogiques.

Il fallait rendre le réseau téléphonique capable de transmettre une information se présentant simultanément en parallèle sur plusieurs fils alors qu'il avait été conçu pour assurer la transmission de signaux émis sur un fil, les uns à la suite des autres.

Ces deux difficultés ont été surmontées par le développement d'un petit équipement électronique destiné à s'insérer entre tout matériel informatique et le réseau téléphonique : le **modem**¹⁵.

Grâce aux modems, les réseaux télénformatiques ont pu se développer, en s'appuyant sur l'infrastructure du réseau téléphonique (RTC).

Le marché du modem, devenu dans les années 1990 la clef des accès individuels à l'Internet via le RTC¹⁶, est toujours très actif.

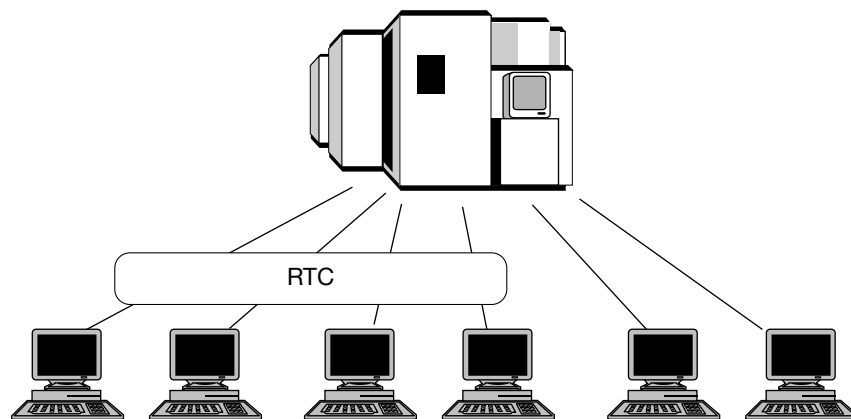
Les architectures de la décade 1970 étaient toutes organisées autour de l'ordinateur central, considéré en tant que nœud du réseau. Pour éviter la multiplication des connexions sur le réseau, des dispositifs appelés multiplexeurs et concentrateurs ont permis le regroupement de terminaux en grappes. Les premiers périphériques de dialogue, baptisés téléimprimeurs, ont rapidement laissé la place aux terminaux constitués d'un clavier et d'un écran cathodique.

De telles architectures techniques ont permis le développement de nouvelles applications et de refondre les applications anciennes comme la comptabilité et la gestion commerciale.

15. Modem pour modulateur/démodulateur, ce qui nous renvoie au chapitre précédent consacré aux technologies.

16. Avec aujourd'hui soit un modem classique, soit un « modem ADSL » (voir plus loin). Ce dernier n'est d'ailleurs plus tout à fait un modem au sens strict du terme.

Figure 7 : Accès transactionnel au site central en local et à distance via le RTC



Le Réseau Téléphonique Commuté permet le démarrage de la téléinformatique mais les performances restent limitées et les développements réclament des compétences très pointues.

B. FACILITER LE DÉVELOPPEMENT DES APPLICATIONS TRANSACTIONNELLES

La téléinformatique introduisait un nouveau mode de dialogue : le mode transactionnel, dans lequel l'utilisateur dispose d'une réponse quasi immédiate à sa requête.

Il faut souligner au passage que ce mode de fonctionnement est parfois improprement appelé « en temps réel ». Le terme « temps réel » doit être réservé à un mode de fonctionnement très particulier. C'est celui des applications comme la conduite de processus industriels, l'acquisition de données en télémétrie ou les simulateurs de vols professionnels. Alors que le mode transactionnel se contente d'envoyer une question qui vient s'insérer dans la file d'attente et d'attendre sagement la réponse (qui viendra heureusement assez vite), le mode temps réel envoie une interruption qui, en fonction du niveau de priorité qui lui a été affectée, peut conduire le système d'exploitation de l'ordinateur à répondre immédiatement à la sollicitation, toutes autres affaires cessantes.

La programmation du dialogue entre terminaux et ordinateur central est une tâche complexe. Pour simplifier le travail des programmeurs, les sociétés de logiciels, puis les constructeurs, ont rapidement proposé des systèmes prenant en charge la gestion de ce dialogue, autour d'une notion clef : la notion de **transaction**.

Une transaction regroupe la transmission d'une question depuis le terminal de l'utilisateur jusqu'à l'ordinateur central, le traitement qui permet d'élaborer la réponse à cette question, et la transmission de cette réponse vers le terminal d'origine. Les **Systèmes de Gestion de Transactions (SGT)** ont permis de libérer les programmeurs de toutes les tâches associées à la gestion de ces échanges en prenant en compte :

- La gestion des transmissions : Y a-t-il une station qui souhaite émettre un message ? Nous prenons en charge votre message ! Comment faut-il coder ce message ? Votre message est bien arrivé ! Vous avez une réponse à votre message !
- La gestion des traitements : À quel programme d'application dois-je délivrer ce message ? Merci de me prévenir lorsque vous aurez terminé d'élaborer la réponse !
- La gestion des tâches en assurant la prise en compte simultanée de plusieurs transactions en provenance de plusieurs utilisateurs (Initialisation, synchronisation et gestion des priorités, achèvement).
- L'interface avec les systèmes de gestion des fichiers.

Le représentant le plus connu de ce type de logiciel est probablement le produit CICS¹⁷, d'IBM, apparu sur le marché en 1969. Toujours présent, ce produit a su trouver sa place au milieu des nouvelles architectures, cohabitant sur le marché avec des nouveaux venus comme BEA Tuxedo et Transarc/IBM Encina.

17. CICS pour *Customer Information Control System* (Système de gestion des informations du client).

C. PROPOSER UN VÉRITABLE CONCEPT DE RÉSEAU

Puisqu'il était plus facile, grâce aux SGT, de développer des applications transactionnelles, celles-ci se sont multipliées et un autre besoin s'est fait jour très rapidement.

Imaginons une application transactionnelle de comptabilité, une autre de gestion commerciale et une troisième de gestion du personnel sur un même ordinateur central. Chacune avait son SGT et gérât son propre réseau de terminaux. L'utilisateur du système de gestion commerciale ne pouvait pas, à partir de son terminal dédié, consulter le compte d'un client sur l'application comptable, même si les procédures internes de l'organisation lui conféraient ce droit.

Pour ne pas reconstruire un réseau spécifique pour chaque nouvelle application transactionnelle, les constructeurs ont développé un concept unique pour :

- réaliser l'indépendance entre les utilisateurs et le réseau, c'est-à-dire permettre à tout poste de travail d'accéder à n'importe quelle application, sous réserve des droits nécessaires ;
- partager les ressources (gestion des lignes, gestion des terminaux) ;
- définir des formats et des protocoles d'échange communs à toutes les applications ;
- offrir une large flexibilité pour prendre en compte l'évolution des réseaux ;
- améliorer l'efficacité du réseau grâce à la distribution de l'« intelligence¹⁸ » dans les différentes unités de contrôle des communications.

Ce concept a débouché sur la réalisation de **Systèmes de Gestion de Réseau**. C'était une avancée considérable puisqu'elle a permis aux utilisateurs, à partir de leur terminal, d'accéder à n'importe quelle application, quel que soit l'ordinateur hôte, à condition bien sûr de posséder l'autorisation d'accès.

En déportant, répartissant et diffusant l'« intelligence » sur le réseau, ces systèmes ont eu un impact considérable sur l'architecture technique des systèmes d'information puisque l'ordinateur cessait d'être le point central du système informatique. C'est désormais le réseau qui assume ce rôle : l'utilisateur ne se connecte plus à un ordinateur mais à un réseau, dans le but de sélectionner un service. Cette évolution ouvrait la voie à la multiplication des services accessibles sur le réseau : l'ordinateur central unique pouvait être remplacé par une galaxie de serveurs. Tous les grands constructeurs informatiques de l'époque ont rapidement développé de tels systèmes. Les plus répandus ont été SNA chez IBM, dont la première version remonte à 1974, DSA chez Bull, Decnet chez Digital Equipment.

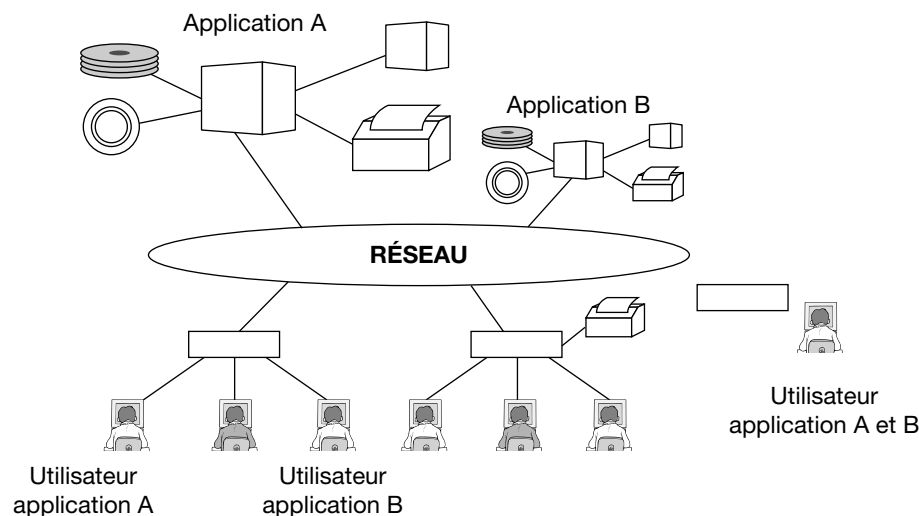
En complément de ces systèmes de gestion de réseau, qui rendaient possibles des réseaux vastes et complexes mais n'offraient que peu de services pour en faciliter l'exploitation, sont apparus les **Systèmes d'Administration de Réseaux** qui ont pris en charge l'attribution des ressources et des droits d'accès, l'enregistrement des incidents et l'aide au diagnostic, la mesure des performances et la gestion de la sécurité.

Netview (IBM), Netmaster (Cincom), Openview (HP) et Unicenter (Computer Associates) sont quelques produits phares en ce domaine.

18. Le terme d'« intelligence » n'est pas très heureux, mais c'est celui consacré par la profession. Il traduit simplement le fait que les unités de contrôle des communications du réseau sont capables de dérouler des programmes et de dialoguer avec l'utilisateur indépendamment de l'ordinateur central.

Figure 8 : Système de gestion de réseau

Applications accessibles sur « mainframes » et « minis »



Saisie et utilisation de l'Information

Systèmes de Gestion de Transaction, Systèmes de Gestion de Réseau et Systèmes d'Administration de Réseau facilitent le développement d'applications transactionnelles. Qu'en est-il de l'amélioration des performances des réseaux ?

D. ET PENDANT CE TEMPS-LÀ... LES OPÉRATEURS DE TÉLÉCOMS

En parallèle à cette évolution de l'offre chez les constructeurs, les opérateurs prenaient en considération sur la nouvelle donne relative au transport de données numériques. Ils n'étaient jusqu'ici que des spécialistes du transport de la voix transformée en signal analogique, mais ils ont rapidement vu tout l'intérêt qu'ils pourraient tirer des technologies numériques.

Le réseau téléphonique commuté a permis le démarrage de la téléinformatique. Malgré ses qualités, celui-ci conservait de nombreuses imperfections dues au fait qu'il n'avait pas été conçu comme réseau de transport de données informatiques. Divers défauts comme l'affaiblissement et le déphasage engendrés par l'impédance de la ligne, les bruits, les écarts de fréquence, les distorsions, les échos et les microcoupures engendraient une déformation des signaux de nature analogique.

Les défauts du RTC n'étaient pas suffisamment graves pour rendre incompréhensible une communication vocale pour laquelle nul n'exigeait pas la qualité « Haute-Fidélité ». Ils étaient par contre rédhibitoires pour la fiabilité d'une transmission de données. Le point faible dans la chaîne de communication se révélait toujours être « le dernier kilomètre ». Ce segment est le fil qui vous est propre et qui rattache votre combiné téléphonique au commutateur le plus proche. Les spécialistes appellent ce fil « boucle locale ».

La solution de connectivité fondée sur les modems classiques ne pouvait être que provisoire, surtout dans un contexte professionnel. Quatre solutions sont envisagées pour pallier ces insuffisances :

1. Améliorer la qualité du RTC, tout au long de la ligne de transmission.
2. Abandonner purement et simplement le RTC au profit d'un réseau mieux adapté au transport des données.
3. Court-circuiter la boucle locale en la remplaçant par un autre dispositif plus performant.
4. Trouver une solution technique pour tirer un meilleur parti de cette boucle locale, visiblement sous-employée.

Les quatre voies ont été explorées. Les solutions trouvées ont fait l'objet de réalisations industrielles qui sont aujourd'hui toutes exploitées. Vous avez probablement eu l'occasion d'être le bénéficiaire de ces technologies. Nous allons les exposer dans l'ordre chronologique de leur apparition.

1. Prendre en compte la révolution du numérique dans les réseaux conçus pour la voix

Les opérateurs nationaux, à l'époque en situation de monopole, ont démarré la numérisation du cœur de leurs réseaux téléphoniques. En France les PTT¹⁹ ont choisi une technologie dite MIC²⁰.

La numérisation a eu plusieurs conséquences. Elle a permis de relier les autocommutateurs (PABX)²¹ des entreprises aux centraux par des liaisons à haut débit (dans la gamme des performances de l'époque, à savoir 2 millions de bits par seconde). Elle a permis, dès 1987, d'offrir les services complémentaires dits « de confort » qui semblent aujourd'hui indispensables : Transfert d'appel, signal d'appel, facturation détaillée, etc.

Ces améliorations, couplées avec les progrès dans la technologie des modems, ont fait passer les débits possibles d'une liaison RTC classique de 9 600 bits par seconde à 56 000 bits par seconde. Ceci représente un facteur multiplicateur proche de 6.

2. Offrir des réseaux spécialisés pour les échanges de données

De nouvelles techniques spécialement adaptées à la transmission de données numériques ont vu le jour. Toutes sont fondées sur la commutation de messages (par opposition à la commutation de circuits qui est la règle sur le RTC). La première est la commutation par paquets : les messages sont découpés, étiquetés et transportés sur des chemins différents avant d'être réassemblés à l'arrivée. Le réseau fonctionne comme une entreprise de messagerie express.

Le réseau Transpac mis en place par ce qui était à l'époque une filiale éponyme des PTT (aujourd'hui de France Telecom) est caractéristique de ces réseaux spécialisés dans la transmission de données informatiques fondés sur la commutation par paquets. Les services de *Transpac* reposent sur le concept du circuit virtuel : le flux de paquets donne à l'abonné l'impression qu'il est connecté à son interlocuteur par un fil dédié alors qu'il n'en est rien.

Dès la fin des années 1980, Transpac comptait près de cent mille raccordements et transmettait plusieurs centaines de milliards d'octets chaque mois. Le succès a parfois entraîné des pannes qui sont restées célèbres dans les annales. Le débit des liaisons pouvait atteindre deux millions de bits par seconde. Le facteur multiplicateur est de 200.

Les systèmes de gestion de réseaux des constructeurs ont rapidement pris en compte ces réseaux spécialisés : SNA d'IBM, disponible en 1974, qui avait intégré le RTC en 1976, intègre le protocole associé à ces réseaux, baptisé X25, dès 1981.

Les technologies évoluant, X25 (commutation de paquets) va laisser progressivement la place à « *Frame Relay* » (commutation de trames) et ATM²² (commutation de cellules), plus performants et plus compatibles avec le nouveau protocole réseau qui va s'imposer, celui de l'Internet (IP pour *Internet Protocol*). Commutation de paquets, de trames et de cellules reposent toutes sur le principe de la commutation de messages. C'est la structure du message qui change.

Avec ATM l'offre commerciale, réservée aux grandes organisations, atteint plus de 700 millions de bits par seconde. Le facteur multiplicateur est de 73 000. On est fort loin des 9 600 bits de la téléinformatique mais les besoins ont évolué. Il ne s'agit plus de transférer un texte affiché sur un écran de 24 lignes de 80 colonnes (ce qui correspond à environ 19 200 bits sans compression, soit deux secondes de transmission à 9 600 bits par seconde). Il s'agit de transférer un fichier d'un million de caractères – donc de 8 millions de bits – attaché à un message ou de passer le flux continu (« *streaming* ») d'un clip vidéo. À 9 600 bits par seconde, il faut près d'un quart d'heure pour transférer le fichier d'un million de caractères.

19. L'administration des Postes et Télécommunication dispose alors du monopole des services de communication.

20. Pour Modulation par Impulsion et Codage.

21. Pour *Private Automatic Branch Exchange*.

22. Pour *Asynchronous Transfer Mode*.

3. Court-circuiter la boucle locale

Tout se numérise progressivement au cœur du réseau RTC. Il n'y a plus que la fameuse « boucle locale » qui s'accroche désespérément à la technique analogique, par souci des équipements de l'immense majorité des abonnés. Les opérateurs veulent pouvoir fournir à ceux qui ont des équipements numériques – en particulier des ordinateurs –, d'un bout à l'autre d'une chaîne de communication complètement numérisée, un accès unique, universel et public.

Ils prolongent la ligne numérique jusqu'à l'abonné chez qui ils installent une régie capable de connecter les équipements numériques aussi bien que les appareils analogiques, court-circuitant ainsi la boucle locale.

Cette offre va s'intituler **Réseau Numérique à Intégration de Services (RNIS** en anglais ISDN²³).

Le RNIS est un réseau universel qui permet de fédérer tous les terminaux et d'acheminer tous les types de communication. C'est aussi un réseau accessible à l'aide d'une prise unique, via une procédure unique. Le RNIS est une simple évolution du RTC. C'est un réseau à commutation de circuits mais il propose la continuité numérique de bout en bout. Ce n'est pas un réseau supplémentaire entrant en concurrence avec les autres réseaux. Ainsi que le souligne G. Pujolle²⁴ : « C'est plutôt un accès universel à ces réseaux. » Les PTT ont lancé leur RNIS, Numéris, en 1987. Numéris offre deux voies à 64 000 bits par seconde. Le projet Euro-ISDN assure depuis 1996 l'interconnexion des RNIS européens, dont Numéris, devenu en 1992 un réseau de France Télécom.

4. Tirer un meilleur parti de la boucle locale

C'est l'aboutissement du quatrième et dernier axe de recherche. La boucle locale dispose d'une bande passante dont seule la partie basse est utilisée par les signaux de la communication téléphonique. Les techniciens ont eu l'idée d'utiliser la partie haute de cette bande passante pour le transfert de données. Les deux trafics voix et données sont portés par le même fil mais sont aiguillés différemment au niveau de l'abonné (trafic voix vers le combiné téléphonique, trafic données vers l'ordinateur) et de son commutateur de rattachement (trafic voix vers le correspondant sur le RTC, trafic données vers le fournisseur d'accès Internet). La technologie ADSL²⁵, qui connaît aujourd'hui un grand succès, sait tirer parti de la boucle locale pour transmettre des données de manière asymétrique à haut débit (1 million de bits par seconde en réception, soit un facteur multiplicateur de 100 à la portée de – presque – tous les abonnés).

Les technologies des télécommunications offrent un éventail très large de solutions techniques pour améliorer les performances des applications. Les réseaux spécialisés X25, Frame Relay et ATM, les connections RNIS et ADSL contribuent à la généralisation des modes transactionnels.

23. L'acronyme ISDN (*Integrated Services Digital Network*) a donné lieu à quelques jeux de mots restés célèbres. Les uns ont vu dans le RNIS une offre technologique de plus, ne répondant à aucun besoin « business » (*Innovation Subscribers Don't Need!* – Les abonnés n'ont pas besoin d'innovation !), d'autres une belle opportunité d'affaires (*I Smell Dollars Now!* – Il y a de l'argent à gagner !).

24. [Les réseaux] chez Eyrolles.

25. ADSL pour *Asynchronous Digital Subscriber Line* (Ligne numérique asynchrone de l'abonné) est l'une des technologies de la famille xDSL.

E. RETOUR AU SEIN DES ORGANISATIONS : FÉDÉRER LES POSTES DANS DES GROUPES DE TRAVAIL

Au milieu des années 1980, le développement de la micro-informatique a introduit un nouveau concept, celui de **Réseau Local** (« *Lan Area Netwok* » – LAN). À l'origine, celui-ci avait pour unique ambition le partage de ressources locales alors encore onéreuses comme les imprimantes laser ou les supports de stockage de grande capacité. Le concept a évolué pour devenir celui d'un fédérateur de postes de travail, permettant les échanges et l'accès à de nombreux services communs touchant l'accès aux bases de données ou de documents, la connexion à d'autres réseaux, la sécurité ou la mise en œuvre de certains logiciels.

C'est avec le développement de ce mode de fonctionnement que se banalise le concept de serveur : serveur d'impression, serveur de fichiers, serveur de communication.

L'apparition des réseaux « Poste à poste » (« *Peer to peer* »)²⁶ a permis la mise en place de réseaux légers, regroupant cinq à dix utilisateurs, peu coûteux, intégrables dans des réseaux plus importants dont ils bénéficient des services d'administration. Il est intéressant de laisser le trafic local au niveau du réseau du Groupe de travail, sans le remonter au niveau d'un réseau central, car 80 % des informations manipulées par un groupe homogène n'ont d'intérêt qu'au niveau local.

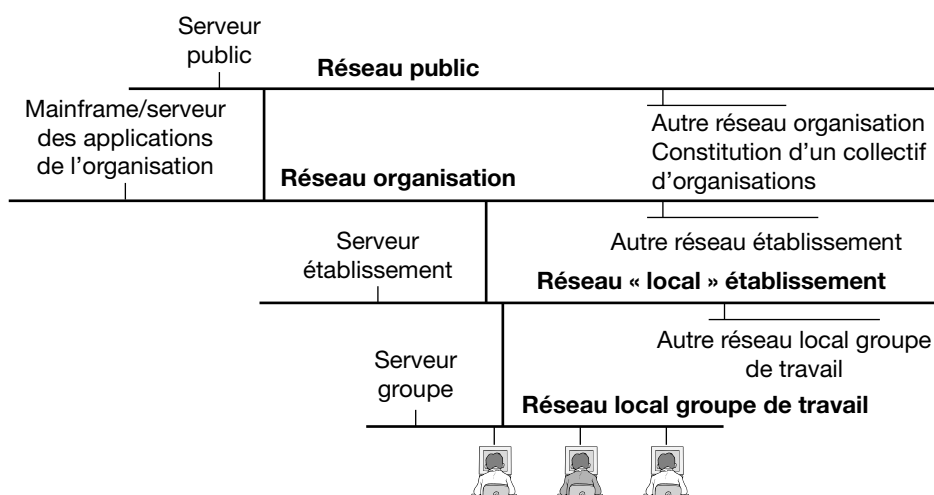
Des standards *de facto* s'imposent sur le marché. Novell crédibilise le concept en construisant un système d'exploitation réseau, donc par obligation multi-tâches et multi-utilisateurs, Netware, intégrant la tâche MS-DOS, alors que tous ses prédécesseurs avaient vainement et stupidement tenté de transformer le système d'exploitation du PC, MS-DOS, conçu comme mono-tâche et mono-utilisateur, en un gestionnaire de réseau, ce qu'il ne pouvait devenir par nature. Microsoft et IBM ont conçu Lan-Manager/Lan-Server autour du système d'exploitation multi-tâches OS/2, avant que Microsoft n'intègre sa solution d'exploitation de réseau local (Advanced Server) au sein de son nouveau système d'exploitation Windows NT.

Les standards Ethernet et Token Ring s'imposent au niveau de la gestion des accès sur le fil. Les systèmes de gestion de réseaux des constructeurs ont rapidement pris en compte ces réseaux locaux : SNA d'IBM, intègre les réseaux locaux à jeton (Token Ring) dès 1985.

F. METTRE EN PLACE UNE STRUCTURE DE RÉSEAU HIÉRARCHISÉE

À ce stade de l'évolution – dans la période 1990-1992 –, les organisations disposent de l'architecture réseau suivante figurée sur le schéma de la figure 9 :

Figure 9 : Un réseau hiérarchisé mais hétérogène



26. Le concept « peer to peer » connaît une nouvelle notoriété dans les années 2000 grâce à la diffusion de musique sur l'Internet (Sites de type *Napster*). À cette occasion, sans raison particulière, il se voit affublé d'une nouvelle traduction : « pair à pair ».

Le poste de travail standard est le micro-ordinateur.

Au niveau le plus bas sont les réseaux locaux « Groupe de Travail », où Novell et Microsoft imposent leurs solutions spécifiques, dites propriétaires, autour des protocoles IPX/SPX et NetBeui.

Les réseaux « Groupe de travail » sont fédérés dans un réseau d'établissement dont les serveurs sont alors des mini-ordinateurs. C'est un domaine conquis récemment par le système d'exploitation Unix au détriment de tous les systèmes propriétaires promus par les divers constructeurs concernés. Unix a choisi IP comme protocole réseau.

Les réseaux d'établissement sont fédérés dans un réseau d'entreprise où subsistent encore les protocoles propriétaires liés aux systèmes de gestion de réseau des constructeurs déjà cités tels SNA d'IBM, DSA de Bull et Decnet de Digital.

Au niveau le plus élevé, en réponse aux besoins liés à ceux de l'entreprise étendue, le besoin d'un fédérateur des réseaux d'entreprises s'impose. C'est l'Internet qui va jouer ce rôle. Ici règne naturellement le protocole IP puisqu'il est l'« *Internet Protocol* ».

Un utilisateur peut accéder aux divers serveurs de la hiérarchie des réseaux s'il a les droits d'accès adéquats. Les données n'intéressant qu'un niveau de la hiérarchie restent à ce niveau.

Cette architecture est caractérisée par son hétérogénéité. Des standards différents se déclinent aux divers niveaux de la hiérarchie. C'est IP, déjà présent à deux étages, qui va s'imposer tout naturellement comme protocole fédérateur de tous les niveaux. Les réseaux des entreprises vont dès lors pouvoir intégrer l'ensemble des technologies de l'Internet. C'est le concept « intranet ».

Nous verrons que certains acteurs du marché s'adaptent très vite à IP. Ceux qui tergiversent et sont trop lents pour rallier le nouveau standard perdent leurs positions sur le marché.

La constitution et l'interconnexion de réseaux locaux créent le besoin d'une nouvelle gamme d'équipements, les matériels actifs du réseau comme les concentrateurs (« *hubs* »), les commutateurs (« *switchs* »), les ponts, les routeurs, etc. De nouvelles sociétés se créent pour occuper ce marché. Cisco, créée en 1986 à San José en Californie par deux chercheurs de l'Université de Stanford, Sandy Lerner et Ben Bosack, s'affirme rapidement comme le leader, une fois que les deux créateurs passent sagement la main à un manager, John Morgridge, qui introduit la société en Bourse en 1990.

L'interconnexion des réseaux locaux distants engendre, par opposition au réseau local LAN, le concept de réseau étendu WAN (« *Wide Area Network* »).

Le protocole IP est le signe annonciateur d'une révolution qui se lève, celle de l'Internet bien sûr, mais surtout de toutes les technologies qui l'accompagnent.

G. LA RÉVOLUTION INTERNET

Défini comme le réseau des réseaux, Internet est un ensemble de moyens de communication qui permet à des ordinateurs d'être reliés entre eux. Les utilisateurs de ces ordinateurs peuvent proposer différents services sur ce réseau et utiliser l'ensemble des services offerts par la collectivité ainsi constituée. Ces services sont des services d'accès aux données comme le « Web », des services d'envoi de données comme la messagerie ou le transfert de fichiers.

Nous ne revenons pas sur la structure et les services d'Internet, bien connus de tous nos lecteurs. Nous rappelons simplement qu'Internet permet à chaque station d'être identifiée par un numéro qui la différencie de toutes les autres stations dans le monde (Adresse IP) et à chaque service hébergé sur un serveur d'être identifié par une URL (« *Unique Resource Locator* ») à l'exemple de www.cnamintec.fr.

Nous évoquons aussi la genèse, qui fut dans une première période (1969-1995), plutôt lente, et dans une seconde (à partir de 1995) extrêmement rapide. Internet est né en 1969 sous l'impulsion de l'ARPA (*Advanced Research Project Agency*). Cette agence, créée en 1957 et placée sous la tutelle du Département de la Défense (DoD) avait pour mission de mettre à la disposition de l'armée américaine des technologies de pointe. La guerre froide faisait rage et il semblait

nécessaire de mettre au point des techniques efficaces et robustes pour assurer un échange fiable de données entre les ordinateurs dédiés aux missions opérationnelles des forces armées. L'université de Californie à Los Angeles (UCLA) a proposé à l'ARPA un modèle de réseau original par rapport à l'état de l'art de l'époque, basé sur la commutation de circuits. Le modèle proposé est celui du réseau à commutation de messages.

Dès l'instant qu'il existe un chemin entre deux ordinateurs, ceux-ci peuvent échanger des informations. Ce chemin n'a pas à être direct, il peut passer par un ou plusieurs ordinateurs intermédiaires. Chaque ordinateur intermédiaire est programmé pour router les informations qui ne lui sont pas destinées vers un ordinateur plus proche de la destination finale. De proche en proche, les données arrivent au destinataire. Si plusieurs chemins existent à un instant donné, ils constituent autant de solutions pour acheminer les données en transit. Cette redondance répondait aux attentes des militaires qui envisagent toujours que certains de leurs centres de calcul puissent être détruits suite aux actions de l'ennemi.

Arpanet fonctionnait mais des améliorations étaient souhaitables. Il était nécessaire de développer de meilleurs protocoles pour le transfert de fichiers, la connexion à distance, le routage et d'autres applications. L'ARPA créa donc un groupe de recherche : l'Inter Network Working Group avec Vint Cerf et Bob Kahn. Au cours des années 1972-1976, l'INWG propose un protocole de réseau : IP pour *Internet Protocol* et un protocole de transport : TCP pour *Transmission Control Protocol*.

Le couple TCP/IP, finalisé en 1982, auquel s'ajoutent progressivement d'autres protocoles spécialisés comme ICMP, IGMP, ARP et UDP, est adopté par Arpanet en 1983, alors que l'IAB (*Internet Activities Board*) prend officiellement la relève de l'Arpa pour la recherche, et se divise en deux groupes :

- IETF (Internet Engineering Task Force) ;
- IRTF (Internet Research Task Force).

Entre-temps, le rapprochement des travaux de développement de TCP/IP et ceux de XNS (*Xerox Network System*) conduisent au protocole RIP (*Routing Information Protocol*) implanté dans Unix BSD (1978-1980).

TCP/IP touchera le monde des réseaux locaux avec l'implantation de TCP/IP dans Novell Netware en 1987.

L'année 1983 marque aussi l'éclatement du réseau Arpanet en deux.

- Milnet, le réseau militaire, est confié à une autorité militaire.
- Arpanet, forme la partie civile, placée sous une autorité universitaire, celle de la *National Science Foundation* (NSF). La NSF possédait déjà un réseau similaire (NSFNet) pour ses propres besoins.

L'Internet n'est pas qu'un réseau. Il est aussi le vecteur de diffusion des technologies associées qui vont permettre le développement de concepts comme intranet et extranet. Elles vont conduire également à la refonte complète des architectures techniques des systèmes d'information.

Introduire les standards de l'Internet dans le réseau de l'organisation

Le schéma de la figure 9 souffrait de son hétérogénéité. Celle-ci disparaît avec l'introduction des technologies de l'Internet.

Le protocole réseau IP est généralisé, en compagnie de protocoles de transport associés comme TCP, d'où l'acronyme très courant TCP/IP. Tous les postes de travail sont équipés d'un navigateur, appelé à devenir le client universel d'accès à toutes les applications (Mozilla, Netscape Navigator ou Microsoft Explorer). Des serveurs de pages « web » (Protocole HTTP), de fichiers (Protocole FTP) et de messagerie (Protocole SMTP) sont déployés. Une passerelle sécurisée permet d'assurer l'interconnexion avec l'Internet.

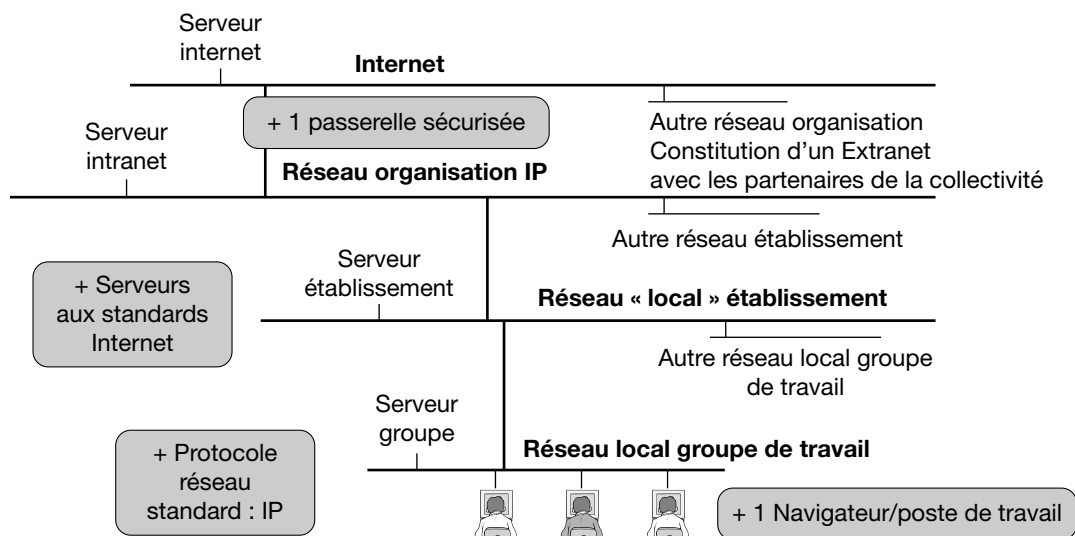
IP est choisi car :

- il est le protocole d'Internet et d'Unix ;
- il repose sur une technologie robuste et éprouvée ;

- il est un standard ouvert, développé et supporté par l'industrie ;
- c'est un protocole routable, administrable et adaptable ;
- il est le dénominateur commun d'environnements hétérogènes : connectivité à l'environnement UNIX, client-Serveur (RPC, *Windows Sockets*) et réseau Internet.

TCP/IP devient le réseau principal des entreprises.

Figure 10 : Un réseau hiérarchisé et homogène



Les systèmes de sécurisation sont des pare-feu, des antivirus, des sondes de détection et des proxys.

Les pare-feu (« *firewall* ») sont des dispositifs qui limitent, filtrent, séparent et analysent les entrées/sorties d'un réseau pour détecter une tentative d'attaque ou d'intrusion. Les antivirus réseau tentent d'éradiquer les virus transitant entre les réseaux extérieurs et le réseau protégé. Les sondes de détection d'intrusion écoutent le réseau et envoient des alarmes à une console d'administration dès qu'elle repère des flux jugés dangereux. Contrairement aux pare-feu, elles ne se contentent pas de détecter les attaques provenant de l'extérieur mais analysent aussi ce qui se passe sur le réseau local. Comme un antivirus, elles peuvent fonctionner avec des bases de signatures d'attaques connues ou analyser les comportements suspects. Les proxys n'interviennent dans la sécurité qu'indirectement. Leur fonction première est de jouer le rôle de mandataire pour un certain nombre de clients. Ceci signifie qu'ils émettent des requêtes pour le compte de tiers, les stations du réseau local qui de ce fait peuvent cacher leur identité – élément de leur vulnérabilité – à des observateurs extérieurs mal intentionnés.

Un intranet est un réseau privé construit pour les besoins d'une organisation (entreprise, administration, collectivité locale, hôpital, université, etc.) sur la base des technologies utilisées par l'Internet.

L'extranet est l'extension de cet intranet pour partager quelques-uns des services offerts sur le réseau avec la collectivité d'organisations (fournisseurs, partenaires, clients, etc.).

Extranet et intranet offrent les services classiques de messagerie, de forum et de base documentaire. Il offrira aussi demain la possibilité de partager des applications conçues selon les architectures orientées, service dont il sera question un peu plus loin. À l'opposé de l'Internet, intranet et extranet répondent à des exigences précises en matière de contrôle d'accès : il est impératif de prévoir un système d'authentification forte des utilisateurs et de protection des données. Ils sont réservés à un groupe identifié d'utilisateurs qui, selon les applications, ne bénéficieront pas de droits identiques.

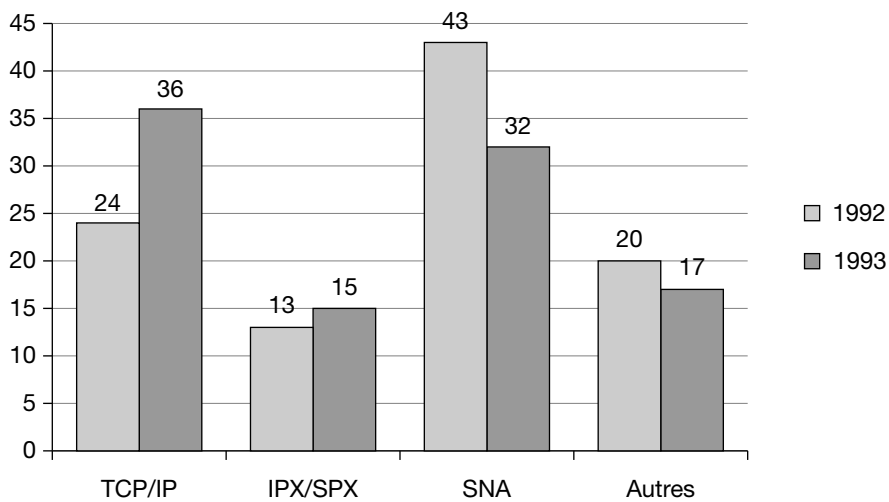
Ces concepts rencontrent un très fort succès du fait d'avantages très significatifs. Ils assurent une adaptation progressive et simplifiée du système d'information en éliminant les problèmes d'hétérogénéité du fait de l'adhésion à un ensemble de standards communs. Ils autorisent une plus grande simplicité de communication, de partage et d'accès à l'information.

Ils permettent une accessibilité plus large du système d'information grâce à des applications standards. Ils s'intègrent naturellement à l'univers de l'Internet.

Dans la perspective d'identification de la trajectoire, il est intéressant de dater le basculement. Il se situe très précisément de 1992 à 1993.

Figure 11 : Tout bascule entre 1992 et 1993

Protocoles primaires de transport en usage dans les entreprises



Source : DataMation Juin 93

Certains grands acteurs du marché prennent conscience de ce basculement : Microsoft, IBM, HP. Ils sont toujours présents aujourd'hui.

Les annonces Microsoft en 1993-1994 :

- Implantation 32 bits du protocole TCP/IP.
- DHCP : Gestion automatique des configurations.
- WINS : Gestion dynamique des noms.
- SLIP/PPP : Support des connexions distantes TCP/IP.
- PREP : Moteur d'impression directe via TCP/IP.

Les annonces IBM de 1993-1994 :

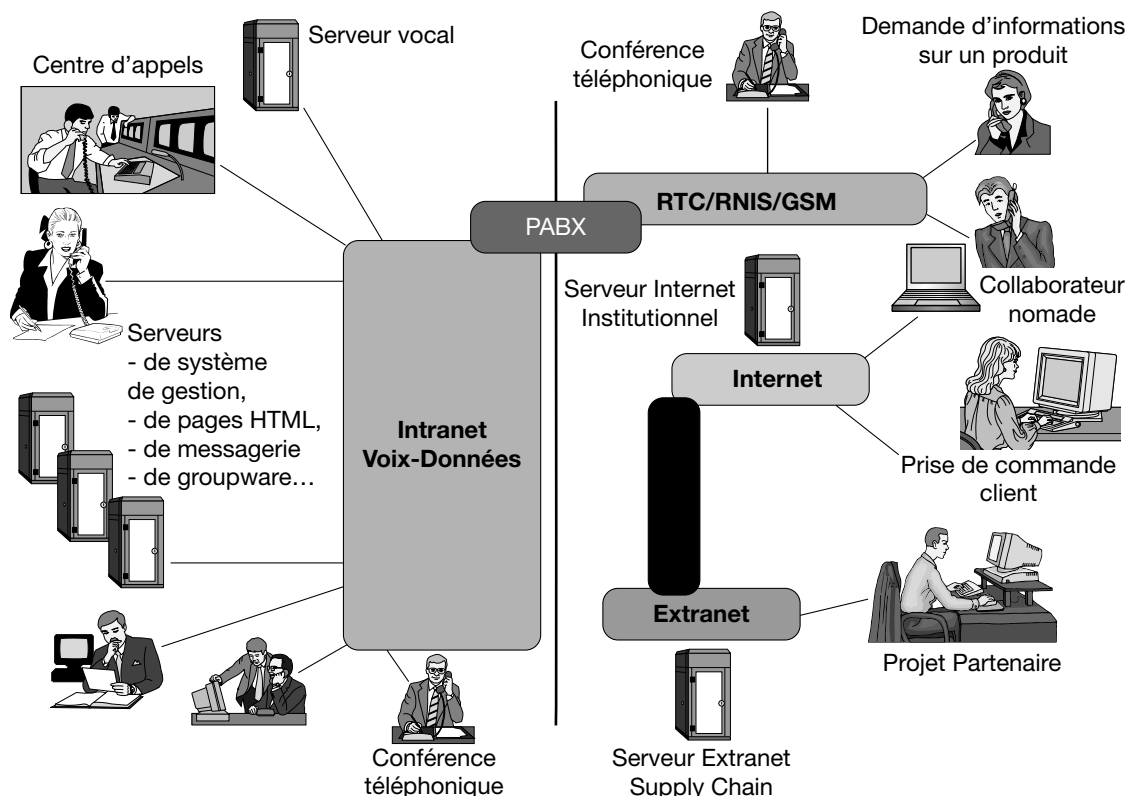
- Évolution de SNA vers APPN.
- Une architecture multi-protocoles qui veut répondre aux offres concurrentes et s'adapter à la construction d'applications client-serveur.

Ceux qui n'ont pas suivi (comme Digital, alors n° 2 de l'informatique, et Novell, alors n° 1 des réseaux) ont disparu ou ont perdu leur position.

À l'inverse, ce basculement offrira à certains nouveaux entrants l'opportunité de prendre une position clef. Les utilisateurs d'IBM ne suivront pas Big Blue sur le chemin d'APPN. Ils basculent en tout IP et plébiscitent un constructeur de routeurs qui leur permet de traiter les trames IP et les trames SNA : Cisco.

L'architecture globale de l'organisation à l'horizon 2005-2010 se construit comme le montre le schéma de la figure 12.

Figure 12 : Architecture complète du réseau de l'organisation



Sur ce schéma on reconnaît un intranet supportant les flux voix et données, connectant les postes de travail et les serveurs de l'entreprise. Cet intranet veut contribuer à l'efficacité des processus internes. L'extranet relie l'organisation à ses partenaires. Il veut contribuer à la bonne marche de l'organisation étendue. L'Internet abrite les services que l'organisation propose au monde et supporte les échanges avec tous ceux qui n'appartiennent pas à la communauté qui bénéficie des services de l'intranet et/ou de l'extranet.

L'intranet se connecte au réseau « voix » mondial par le biais d'un autocommutateur compatible avec les technologies IP. Les clients ou usagers peuvent contacter l'organisation par téléphone ou par l'Internet.

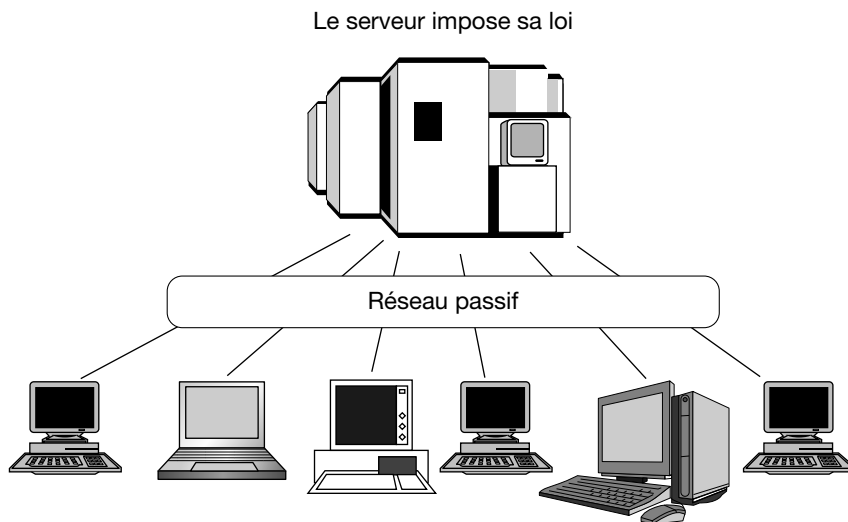
Le réseau intègre des dispositifs qui permettent aux membres de l'organisation en situation de mobilité de se connecter, soit pour une communication vocale, soit pour un échange de données.

Comment résumer cette extraordinaire évolution des technologies et des architectures de communication ?

H. ANALYSE DU PROCESSUS D'ÉVOLUTION ET BILAN

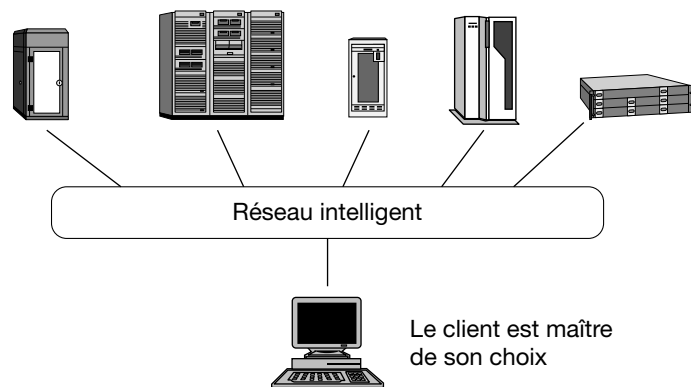
Ce qui frappe dans cette évolution qui marque la période 1970-2000, c'est le renversement quasi copernicien de l'architecture de base. Tout part d'une situation où le serveur – le « *main-frame* » – impose sa loi.

Figure 13 : Retour sur l'architecture « téléinformatique »



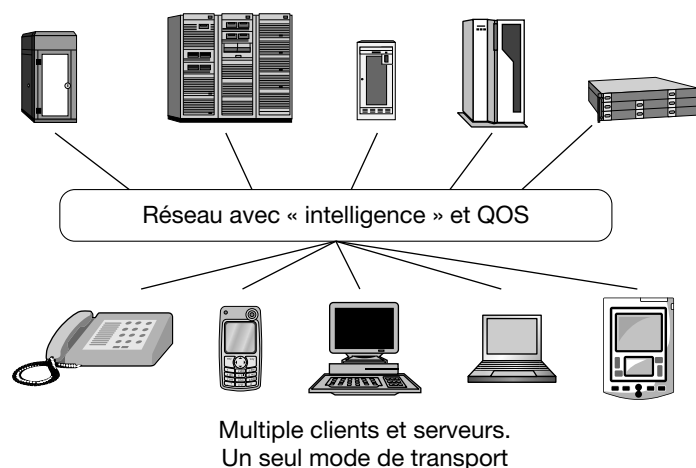
Trente ans plus tard, le client est devenu maître du jeu :

Figure 14 : Le client est devenu roi et dispose d'un vaste choix de services



La tendance 2005-2010 sera celle de l'introduction de la qualité de service (QoS : Quality of Service) et à la diversité au niveau des frontaux d'accès utilisables. Outre l'ordinateur personnel classique, l'utilisateur pourra utiliser son téléphone, son téléphone portable, un Assistant Numérique personnel (« *Personal Digital Assistant* » – PDA), voire d'autres outils que la technologie ne sera pas en peine de nous proposer. Certains laboratoires travaillent sur l'utilisation de lunettes qui permettraient de rentrer en communication visuelle et sonore avec divers serveurs et avec divers interlocuteurs par le biais de ces serveurs.

Figure 15 : Ce que nous pouvons attendre



Il n'y a pas de limites aux solutions offertes par les technologies mais il reste à compter avec le facteur humain. La perspective de voir le visage de son patron surgir inopinément en surimpression d'un magnifique coucher de soleil devrait ne séduire qu'un nombre limité de salariés !

De plus en plus d'utilisateurs nomades désirent accéder depuis l'extérieur aux ressources internes de l'organisation. Au début, c'était principalement pour accéder à leur messagerie ou à l'intranet. Ces besoins étaient relativement simples à satisfaire grâce à l'utilisation de protocoles sécurisés associés à des techniques d'identification comme les certificats numériques. Ils souhaitent aujourd'hui accéder à tout le système d'information de leur organisation. Ils souhaitent pouvoir accéder de l'extérieur aux services dont ils disposent à l'intérieur, quel que soit l'endroit d'où ils se connectent (domicile, hôtel, client) et quel que soit le matériel avec lequel ils se connectent (portable, poste fixe).

Pour répondre à ces besoins plus complexes, une réponse possible est la mise en place de réseaux privés virtuels (« *Virtual Private Network* » – VPN), qui créent des « tunnels » sécurisés, c'est-à-dire authentifiés et chiffrés, entre le nomade et son organisation.

Les solutions supportant la mobilité prennent ainsi une importance grandissante. Du côté des protocoles de communication des réseaux distants, les opérateurs font évoluer leurs réseaux GSM vers les technologies GPRS et UMTS.

Cette évolution est une parfaite illustration de l'accélération technologique. Dans le domaine de l'accès mobile à l'Internet, on a vu se succéder dans un intervalle de 5 ans les technologies GSM-WAP (9,6 kbps), HSCSD (57,6 kbps), GPRS (155 kbps), EDGE (384 kbps) et UMTS (2 000 kbps). Rappelons que le « kbps » représente un débit de 1 024 bits – soit 128 caractères – par seconde.²⁷

N'en déplaise à l'optimisme de certains opérateurs, il était inconcevable que les usages – et les usagers devenus des clients – suivent ce train d'enfer.

Le dernier facteur à considérer le long de cette trajectoire est l'importance de l'effectif concerné. En 1960, moins de 5 % des emplois de bureau étaient concernés par l'informatique. En 1992, ils étaient de 40 % à 80 % (banque) selon les branches. En 1995, ils étaient de 100 %. Ceci signifie que pendant les années du basculement vers IP et de l'arrivée de Windows 3, on a mis en place deux fois plus de postes de travail informatisés que pendant les trente années précédentes.

27. GSM : *Global System for Mobile* (Système global pour les mobiles).

WAP : *Wireless Application Protocol* (Protocole d'Application sans fil).

HSCSD : *High Speed Circuit Switched Data* (Circuit de Données Commutées à Haute Vitesse).

GPRS : *General Packet Radio Service* (Service Radio à commutation de Paquets).

EDGE : *Enhanced Data Rates for GSM Evolution* (Débits de données améliorés pour l'évolution du GSM).

UMTS : *Universal Mobile Telecommunications System* (Système Universel de Télécommunication pour les mobiles).

I. DES PROGRÈS TECHNIQUES CONTINUS

L'évolution scientifique et technologique du secteur des réseaux et des télécommunications est principalement commandée par trois faits incontournables :

- la constance des progrès de l'informatique, basés sur les gains de performances des micro-processeurs et des mémoires ;
- l'apparition après 1995 de la fibre optique à haut débit ;
- le développement explosif des systèmes de communication sans-fil avec l'utilisation des fréquences hertziennes numériques, satellitaires ou terrestres.

1. Loi de Moore

Le premier point est souvent décrit par la loi de Moore qui prédit un doublement de la puissance des microprocesseurs tous les 18 mois. Cette loi à l'œuvre depuis le début des années 1980 a conduit à diffusion sans précédent de ces « puces électroniques » dans tous les domaines de l'industrie et plus particulièrement dans celle des télécommunications. La « numérisation » des communications, qu'elles soient sons, images, textes en est la conséquence. Il est à noter que ces gains de performances se sont accompagnés de chutes de prix considérables.

2. Loi de Gilder

Le deuxième point, moins bien perçu par le grand public, car plus caché (et même enfoui !), est le développement de la fibre optique comme support de transfert de l'information numérique d'un point à un autre. On retrouve cette fibre aussi bien au fond des océans pour les lignes intercontinentales, que sous les trottoirs des grandes villes ou dans les « immeubles intelligents » câblés. La loi de Georges Gilder, qui avait prédit en 1993, dans le domaine de l'optique, pour les vingt-cinq prochaines années, un triplement des capacités de transmission des réseaux optiques, et ce à prix égal, tous les 12 mois, en est la prophétie réalisée.

3. Le développement du sans-fil

Le troisième point, est bien connu du public par son caractère spectaculaire. Le vecteur aérien de diffusion de l'information est en pleine croissance ces dernières années, satellites, GSM, WIFI... La communication numérique sans fil est partout présente, toutes les parties du spectre des fréquences sont sollicitées.

Ces phénomènes s'accompagnent de très fortes réductions des coûts et d'une multiplication des vitesses et des volumes transmis. En 2005, un câble en fibre optique peut à lui seul transporter, en une seconde, davantage de données que tout le réseau Internet ne le permettait en un mois en 1999. Le coût d'acheminement de mille milliards de bits d'informations de Boston à Los Angeles est passé de 150 000 dollars en 1970 à 0,04 dollar aujourd'hui.

En 1930, une conversation téléphonique de trois minutes entre New York et Londres coûtait plus de 300 dollars (aux prix actuels). Aujourd'hui, elle revient à moins de 0,20 dollar. Et, pour envoyer un document de 40 pages du Chili au Kenya, il faut moins de 0,10 dollar par courrier électronique, une dizaine de dollars par télécopie et 50 dollars par un service de messagerie.

Abaisser les coûts, multiplier les débits disponibles ne suffit pas à expliquer l'engouement des utilisateurs des réseaux numériques, encore fallait-il des moteurs puissants d'usages. Une approche théorique résume cette attitude des individus et des entités vers toujours plus de communications et donc de réseaux : la loi de Metcalfe.

4. Loi de Metcalfe

Cette loi constate que l'utilité d'un réseau augmente suivant le carré des utilisateurs qui y sont reliés. Pour Bob Metcalfe c'est la raison fondamentale du développement rapide de l'Internet. Plus de gens s'y abonnent, plus de gens ont envie de s'y abonner. Si le nombre d'utilisateurs est multiplié par deux, le nombre des moyens qui permettent de lier les gens entre eux et de conjuguer leurs talents et leurs idées se trouve multiplié par quatre. D'où la grande importance d'un accès sans entraves : moins on raccorde de gens au réseau, moins le réseau est utile.

Un exemple numérique simple permet de comprendre cette loi :

Supposons un réseau composé de deux amis, les échanges possibles entre eux sont au nombre de 2 : A vers B, et B vers A.

Ajoutons un nouveau membre dans le réseau avec l'entrée de C, nous avons alors les liaisons supplémentaires :

C vers A, C vers B et bien sûr les liaisons de sens inverse (A vers C et B vers C).

Soit au total 6 liaisons possibles.

Une autre manière de présenter les choses serait de dire que chaque membre du réseau peut se lier avec les autres membres (si le réseau compte trois membres, chacun peut obtenir 2 liaisons), puis de multiplier ce résultat par le nombre de membres du réseau. Dans notre exemple ceci fait 3×2 , soit bien 6 comme vu plus haut.

Donc, en généralisant, si on suppose que la valeur d'un réseau est proportionnelle au nombre de liaisons possibles entre ses membres, on obtient une valeur de $N(N-1)$. Pour un réseau de grande taille (exemple de l'Internet) le $N-1$ est réputé égal à N et donc la valeur globale du réseau dépend de N^2 .

La valeur d'un réseau croît en fonction du carré du nombre de ses membres.

Mais attention, cette définition de la valeur d'un réseau repose sur des liens possibles entre tous les membres du réseau. Un réseau hiérarchique (un émetteur et de multiples récepteurs, comme pour la télévision ou la radio) est d'une autre nature et sa valeur obéit à d'autres lois (cette valeur sera plutôt proportionnelle au nombre de ses membres).

Conclusion : les progrès de la technologie ont embrayé sur des lois économiques génératrices de valeur. La croissance qui en a résulté a provisoirement perturbé la Bourse (bulle spéculative de la netéconomie), mais fondamentalement les équipements produits et les nouveaux usages qui en découlent ont profondément transformé le système d'information des organisations. Le mouvement vers les mises en réseaux numériques des individus et des postes de travail est bien irréversible, aussi bien dans les organisations qu'à domicile (la rapide diffusion parmi les ménages du haut débit avec l'ADSL en est l'illustration).

V. ÉVOLUTION DES ARCHITECTURES DE DONNÉES

A. LES ENSEMBLES DE DONNÉES : DOCUMENTS, FICHIERS, BASES DE DONNÉES

L'étude d'une organisation conduit au recensement d'une multitude de données.

Ces données peuvent être regroupées en lots, de manière à constituer un ensemble cohérent : l'ensemble des données attachées à un client, à un produit, à une commande, à une facture, à un contribuable, à un patient, à un cursus de formation, etc.

Ces données peuvent être structurées (la place attribuée à une donnée élémentaire est définie une fois pour toutes) ou non structurées.

Un bilan est un ensemble de données structurées. Le rapport informant les actionnaires de l'entreprise sur les résultats et les objectifs de l'entreprise est un ensemble de données non structurées.

Le système d'information de l'entreprise va manipuler des ensembles de données non structurées (lettres diverses, rapports, notes d'organisation...) et des ensembles de données structurées (Compte de résultat, bilan, factures, fiches signalétiques des employés, gammes de fabrication...).

Les ensembles de données non structurées sont, le plus souvent, baptisés simplement Documents. Les images numérisées, les notes émises par les systèmes de messagerie, sont aussi des données non structurées.

À la notion d'ensemble de données structurées sont associés les concepts de Tableaux, de Fichiers et de Bases de Données.

B. ÉVOLUTION DU DEGRÉ DE STRUCTURATION

Le degré de structuration varie : une lettre de candidature est moins structurée qu'un CV, qui lui-même est moins structuré que le dossier de candidature qui va être exigé par le cabinet de recrutement, qui lui-même est moins structuré que la fiche de recrutement de l'entreprise, celle-ci servant à créer l'enregistrement du candidat recruté dans la base des données qui regroupe tous les dossiers individuels des employés.

Le développement des outils informatisés permettant la manipulation des documents (Traitement de Texte, Publication Assistée par Ordinateur, Gestion Électronique des Documents) conduit à augmenter le degré de structuration des documents, et à définir des normes (SGML).

1. Les tableaux

Un Tableau est un ensemble de données présenté de manière structurée, claire et ordonnée.

Il peut y avoir ou ne pas y avoir de relation entre les données présentées dans le tableau.

Chaque donnée est enregistrée dans une Cellule dont la localisation géographique se fait au moyen d'un numéro de Ligne (parmi n lignes) et d'un numéro de Colonne (parmi p colonnes). C'est la règle d'identification que les enfants utilisent lorsqu'ils jouent à la bataille navale.

L'apparition du tableur a constitué une véritable révolution. On parle souvent du phénomène PC mais il serait plus justifié de parler de phénomène tableur. C'est cet outil qui a supporté l'extraordinaire succès de la micro-informatique.

Nous avons évoqué au § II.A.6 la naissance du PC. Celui-ci était livré avec un système d'exploitation (DOS) et un compilateur Basic. Mais ce n'est pas celui-ci, réservé aux informaticiens, que mettront en œuvre les utilisateurs. Ils plébisciteront un nouveau logiciel appelé tableur. Aujourd'hui Microsoft Excel s'est imposé comme un standard de fait mais d'autres produits ont ouvert la voie : Visicalc, Multiplan de Microsoft, 1.2.3. et Symphony de Lotus.

2. Les tables simples

On rencontre deux types de tables.

Les tables sont des tableaux particuliers.

Le premier type de table est le plus simple. Il s'agit d'un tableau à 2 colonnes mettant en correspondance un code et le libellé associé. Ces tables sont très pratiques car elles permettent de réduire sensiblement les volumes de stockage : la répétition d'un code de trois lettres une centaine de fois entraîne une occupation moindre que celle d'un libellé de quarante caractères.

3. Les fichiers

Un Fichier est un ensemble de données structurées en sous – ensembles ayant tous la même structure.

Cette structure de base peut s'appeler Enregistrement, Fiche ou Article. Un Fichier est donc une collection de n Enregistrements (ou de n Articles, ou de n Fiches) : un Fichier « Clients », un Fichier « Produits ».

L'unité de base du Fichier est donc l'Enregistrement. Cet Enregistrement comporte p Rubriques (ou champs).

Il est possible de rapprocher la notion de Ligne de celle d'Enregistrement, et la notion de Colonne de celle de Rubrique.

Un Fichier peut donc s'inscrire dans un Tableau dont il va constituer un sous-ensemble. Cette caractéristique permet aux Tableurs d'offrir des fonctions de gestion de fichier.

Les vrais systèmes de gestion de fichiers sont apparus avec les grands systèmes d'exploitation et géraient les fonctions de base de lecture, d'écriture, d'indexation tout en offrant des interfaces de programmation aux compilateurs.

4. Les tables complexes

Il y a deux façons de définir une table complexe :

- soit on la considère comme une table simple à laquelle on a rajouté des colonnes ;
- soit on la considère comme un fichier auquel on a rajouté une ligne d'en tête.

Les fonctions de gestion d'ensemble de données qu'offrent les tableurs les plus courants, souvent un peu pompeusement baptisées fonction de gestion de bases de données, permettent en fait de gérer une table complexe.

5. Les bases de données

Il est souvent difficile de décrire une entité de l'organisation avec un seul fichier (ou une seule table complexe).

Décrire un produit c'est parfois définir simplement un code, un libellé et un prix, mais c'est le plus souvent décrire aussi une liste de x composants élémentaires (nomenclature), de y produits pouvant le remplacer, de z conditions tarifaires, etc.

L'ensemble des données décrivant le produit se présente donc sous la forme de plusieurs fichiers dont les enregistrements sont liés par des relations complexes.

Nous parlerons alors de **Base de Données**.

Une base de données est un ensemble de données modélisant les objets (entités) d'une partie du monde réel et servant de support à une application informatique.

Une base de données est un ensemble de données non indépendantes, interrogeable par le contenu (possibilité de retrouver toutes les entités qui répondent à un critère donné, tous les salariés ayant 10 ans d'ancienneté).

Les données sont stockées de manière permanente sur un support adressable (medium magnétique).

Le concept naît officiellement vraiment en 1969 avec une première publication du Codasyl qui crée à cette occasion un Data Base Task Group : « *A survey of General Data Base Management System* » qui analyse les logiciels Adam, GIS, IDS, ISL-1, Mark IV, NIPS/FFS, SC-1, TDMS et UL/1, noms aujourd'hui oubliés (sauf peut-être IDS de General Electric, conçu en 1964 par C. Bachman, qui peut être considéré comme le premier Système de Gestion de Bases de Données). Celui-ci a même, écrit, dans « *The evolution of storage structure* », que :

« Le monde des bases de données est né avec les enregistrements sur bande magnétique, bloqués ou non selon que l'on remonte à l'Univac I ou à l'IBM 702. »

6. Modélisation des données

Les bases de données doivent traduire physiquement les travaux de modélisation des concepteurs de systèmes d'information. De même que les programmes traduisent les modèles de processus, les bases de données traduisent les modèles de données.

Toutes les méthodes traitant de la modélisation des données partent du concept entité-association.

Une organisation regroupe des objets qui sont modélisés sous forme d'**entités**. Les DRH travaillent sur les entités Société, Direction, Service, Établissement, Employé, Poste de travail, Compétence, Formation. Les Directions logistiques travaillent sur les entités Commande, Client, Produit, Expédition, Bon de livraison, Devis de poids, Manifeste de chargement, etc.

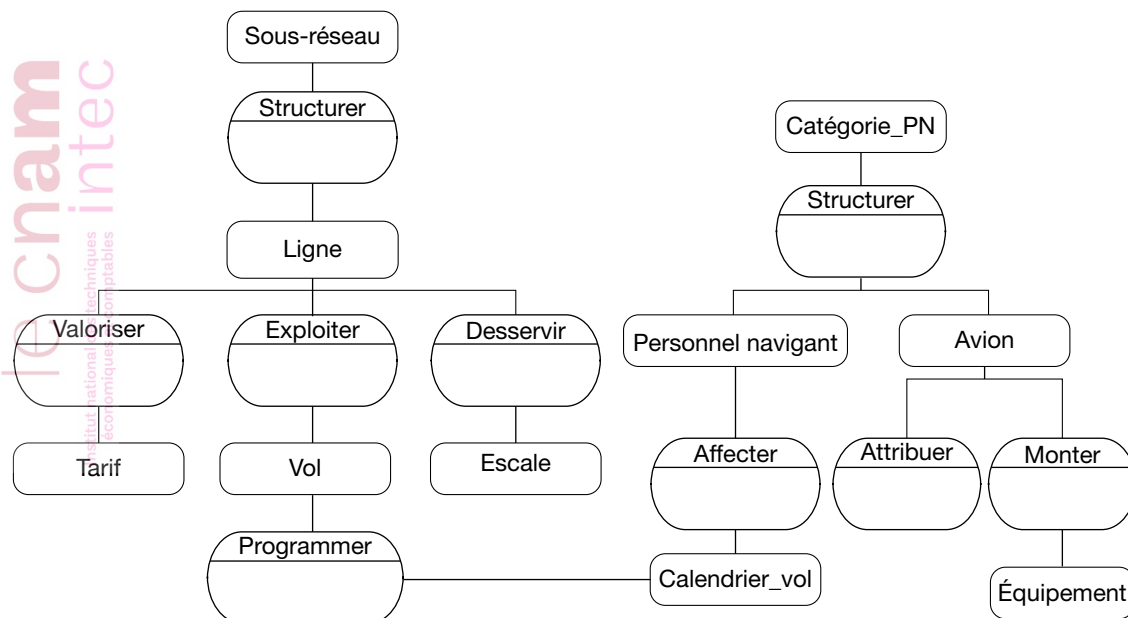
Considérons le cas d'une Compagnie Aérienne et de l'organisation de son réseau. Cet exemple est important car il va nous permettre d'illustrer comment les architectures de données vont évoluer vers le modèle quasi idéal.

Les **associations** relient les entités :

- Les Lignes sont structurées dans un Sous-réseau.
- Une Ligne dessert 2 Escales ou plus.
- La Ligne est valorisée par plusieurs Tarifs.
- La Ligne est exploitée par plusieurs Vols.
- Les vols sont programmés dans un Calendrier des vols.
- Le Calendrier des vols.

Le Modèle Conceptuel des Données décrit ces entités et ces associations.

Figure 16 : Modèle conceptuel des données



7. Passer d'un modèle conceptuel à un modèle physique

Pour pouvoir implanter physiquement une base de données, il faut disposer d'un **Système de Gestion de Bases de Données (SGBD)**. Un SGBD permet :

- **La description des données** : La description des données vise à la constitution du **référentiel** appelé **dictionnaire des données** ou encore méta-base – puisqu'organisé lui-même en base de données – qui regroupe les éléments descriptifs de la Base. Cette description s'appuie sur des outils de modélisation.
- **La création et la mise à jour des données** : Un ensemble de logiciels permettent aux utilisateurs d'insérer et de modifier efficacement des données spécifiques dans une grande masse de données partagée par de multiples utilisateurs.
- **La recherche de données** : Les requêtes d'un **langage de manipulation** sont d'abord prises en compte par l'**analyseur**. Celui-ci vérifie la conformité à la grammaire (analyse syntaxique) et la conformité par rapport au schéma et à la vue référencée (analyse sémantique). La requête est alors traduite au format interne. Celle-ci, référençant une vue, doit tout d'abord être traduite en

une ou plusieurs requêtes référençant des objets existant dans la Base, c'est-à-dire décrits au niveau du schéma. Cette fonctionnalité est accomplie au niveau du **traducteur** qui effectue aussi les contrôles de droit d'accès et d'intégrité.

- **Contrôle de l'intégrité** : Le SGBD doit assurer la cohérence des données par rapport aux différents schémas décrits dans le référentiel. On appelle contrainte d'intégrité toute règle implicite ou explicite que doivent suivre les données. Toute entité doit posséder un identifiant unique (contrainte d'unicité de clé). Certaines relations doivent associer des instances d'entité obligatoirement décrites dans la Base. Par exemple une vente ne peut être effectuée que par un vendeur et avec un ou plusieurs produits existant dans la Base (Contrainte référentielle). Tout attribut d'entité ou d'association doit posséder une valeur qui appartient à son type.
- **Gestion de transaction et sécurité** : Une transaction est un groupe de mises à jour qui fait passer la Base de Données d'un état 1 à un état 2. Les états successifs doivent être cohérents et respecter la contrainte d'intégrité. La gestion des transactions permet d'assurer qu'un groupe de mises à jour est totalement exécuté ou pas du tout. C'est la propriété d'atomicité des transactions.
- **Autres fonctions** : D'autres fonctions se sont progressivement intégrées aux SGBD. Par exemple, beaucoup savent déclencher des procédures cataloguées par l'utilisateur lors de l'apparition de certaines conditions sur les données ou lors de l'exécution de certaines opérations sur certaines entités ou certaines associations (trigger ou déclencheur ou réflexe). Les SGBD sont amenés à supporter des règles permettant d'inférer – c'est-à-dire de calculer de nouvelles données à partir des données existantes en suivant un raisonnement logique. Enfin, les SGBD sont amenés à gérer des objets complexes.
- Un ensemble intégrant aussi des fonctions utilitaires de sauvegarde, de partage, de sécurité, d'administration.

8. Architectures des bases de données

a. Évolution

Le modèle Hiérarchique (IBM IMS) et le modèle « Réseau » (Cullinet IDMS, Bull IDS2, Règles CODASYL) ont permis les premières réalisations de Bases de Données mais présentaient des limites importantes comme la difficulté pour respecter les objectifs de non-redondance et d'intégrité et le manque de flexibilité. Libre de ces contraintes, le modèle relationnel a fini par s'imposer dès que les performances du matériel ont su répondre à son exigence en matière de ressources.

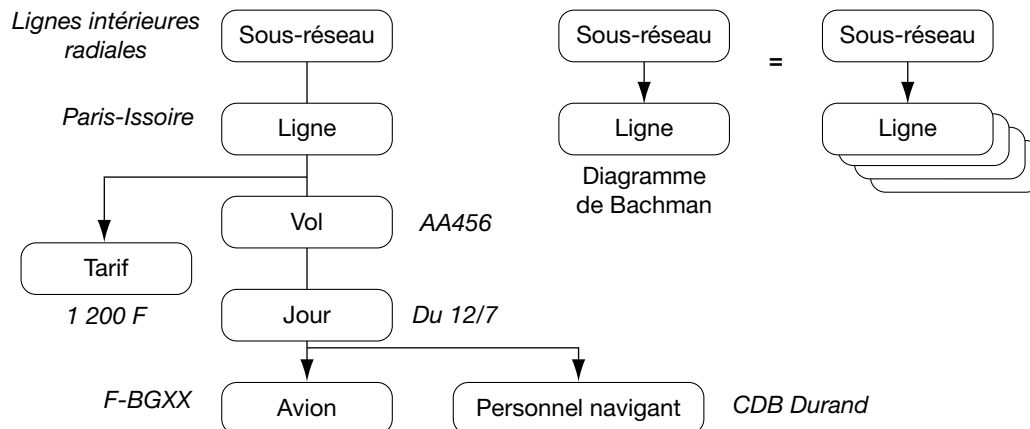
b. Le modèle hiérarchique

Le premier modèle mis en place n'offrait que la gestion d'une relation « Père-fils » classique.

Le produit représentatif de cette famille est IMS d'IBM. La première version d'IMS offrait deux organisations de base pour les fichiers : HSAM (*Hierarchical Sequential*) et HISAM (*Hierarchical Indexed Sequential*). Les enregistrements étaient constitués de segments pouvant comporter une relation père-fils et créer des enregistrements multi-niveaux selon une structure arborescente. L'interface de programmation est le DL/1 (*Data Language/1*) à une époque où IBM tente de promouvoir le PL/1 (*Programming Language/1*) face au COBOL et au Fortran. Viendra plus tard la génération des x/2 (PS/2, OS/2, DB/2).

Cette structure engendrait des limitations qui n'étaient franchissables que par l'introduction de certaines redondances dans le stockage physique comme le démontre le schéma ci-dessous, mais l'ensemble présentait une forte robustesse et de bons temps de réponse, adaptés aux capacités des machines de l'époque. Elle permet à Lockheed Aircraft de gérer ses nomenclatures dès 1970.

Figure 17 : Le modèle hiérarchique



Le schéma montre la hiérarchie :

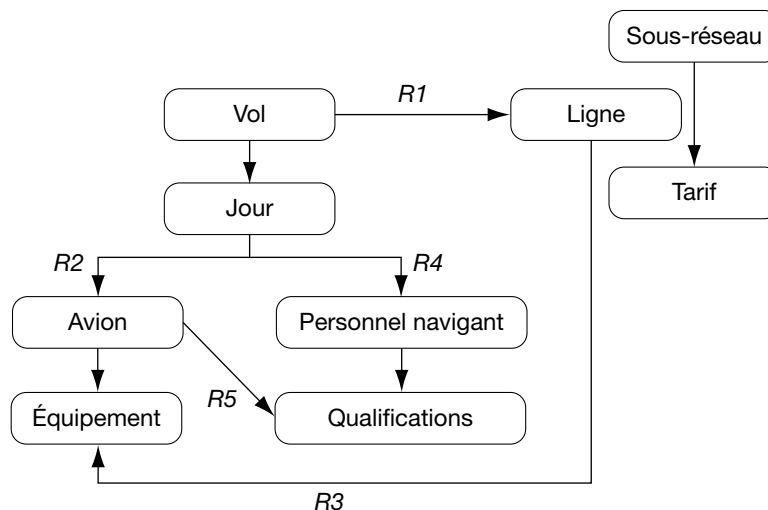
- Un sous-réseau comporte n lignes (les radiales intérieures au départ de Paris comme Paris-Issoire, Paris-Le Puy, Paris-Rodez).
- Une ligne exploite p vols (Paris-Issoire est desservie par le AA456 du matin et le AA457 du soir).
- Chaque vol est exécuté quotidiennement (le AA456 du 2/1, celui du 3/1...).
- Au vol du 3/1 sont affectés l'appareil F-BGXX et le Commandant de Bord M. Durand.

On mesure la redondance du segment Avion, chaque fois que celui-ci sera affecté à un vol.

c. Le modèle réseau

La structure réseau fait éclater la grosse structure hiérarchique en de petites structures hiérarchiques. Les occurrences des segments de ces structures sont reliées entre elles par des liens qui dessinent un réseau complexe.

Figure 18 : Le modèle réseau



Reprenons notre exemple. Nous identifions les petites hiérarchies :

- sous-réseaux avec leurs lignes et leurs tarifs ;
- vols avec leur calendrier ;
- membres du Personnel Navigant avec leurs qualifications ;
- avions avec leurs équipements.

Il suffit de réaliser des tables d'index couplant deux clefs pour affecter un vol à une ligne (R1), un avion au vol d'un jour donné (R2), un navigant au vol d'un jour donné (R4).

Le seul défaut de cette organisation est qu'il fallait tout prévoir à l'avance. Si l'on souhaitait un jour contrôler que le pilote que l'on affecte à un avion donné possède bien la qualification nécessaire (R5) ou que l'avion possède les équipements adéquats pour une escale de la ligne (R3), il fallait que ces liens aient été prévus lors de la définition de la base.

Dans le cas contraire, il fallait réorganiser la base, c'est-à-dire le remettre complètement à plat sur des fichiers de sauvegarde, redéfinir son schéma et recharger le tout. Il fallait aussi modifier les programmes qui assurent sa mise à jour et sa consultation. Tout ceci était extrêmement coûteux et pouvait entraîner l'indisponibilité de la base pendant plusieurs jours.

Les logiciels les plus caractéristiques de cette génération ont été IDS-II (Honeywell Bull reprenant le produit IDS de General Electric), Total de Cincom et IDMS de Cullinet.

d. Le modèle relationnel

Le modèle relationnel est à la base des principaux SGBD qu'offre le marché aujourd'hui.

Le modèle relationnel a été introduit au milieu des années 1970 par *EF Codd* qui travaillait au fameux centre de recherche d'IBM de San José. Le modèle théorique est contemporain des autres modèles mais il a fallu attendre que les machines aient la puissance nécessaire pour mettre en œuvre un système beaucoup plus flexible mais beaucoup plus gourmand en ressources. En France, il faut attendre la fin des années 1980 pour que BNP, Framatome, Renault et Michelin lancent leurs premiers grands projets DB/2 et/ou Oracle.

Le modèle relationnel résulte de la volonté d'offrir un modèle ensembliste simple, basé sur les concepts de **table** et de **relation**, aisément accessibles aux utilisateurs.

Une relation est une liaison entre 2 champs similaires de 2 tables différentes.

On créera la relation entre l'identifiant NoLigne dans la table des lignes (décrivant les lignes avec leurs itinéraires) et l'identifiant NoLigne dans la table des vols (décrivant les vols avec leurs horaires) pour accéder à l'ensemble des informations décrivant la ligne exploitée par le vol sans avoir à stocker cette information au niveau du vol lui-même.

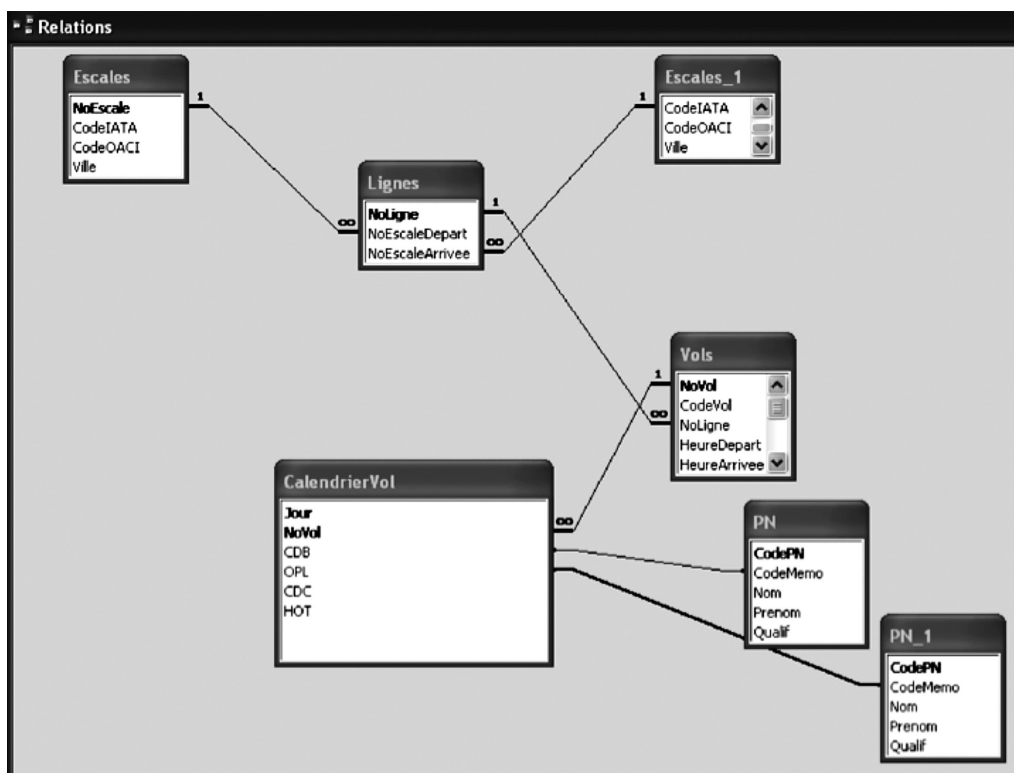


Figure 19 : Le modèle relationnel, notre exemple sous access

The screenshot displays the Microsoft Access interface with several tables and their relationships:

- Escales Table:**

| NoEscale | CodeIATA | CodeOACI | Ville |
|----------|----------|----------|------------------------|
| 1 | ORY | LLLL | Paris-Orly |
| 2 | CDG | MMMM | Paris-CDG |
| 3 | LYS | NNNN | Lyon-St EX |
| 4 | TUF | TTTT | Tours Saint Symphonien |
| 5 | MRS | BBBBBB | Marseille Marignane |
- PN Table:**

| CodePN | CodeMemo | Nom | Prenom | Qualif |
|--------|----------|--------|---------|--------|
| 1 | ADU | DUPONT | Albert | 1 |
| 2 | BMA | MARTIN | Bernard | 1 |
- CalendrierVol Table:**

| Jour | NoVol | CDB | OPL | CDC | HO |
|------------|-------|-----|-----|-----|----|
| 14/10/2002 | 1 | 1 | 3 | 5 | |
| 14/10/2002 | 2 | 2 | 4 | 6 | |
- Lignes Table:**

| NoLigne | NoEscaleDepart | NoEscaleArrivee |
|---------|----------------|-----------------|
| 1 | 1 | 3 |
| 2 | 1 | 4 |
| 3 | 1 | 5 |
| 0 | 0 | 0 |
- Vols Table:**

| NoVol | CodeVol | NoLigne | HeureDepart | HeureArrivee | ActifLu | ActifMa | ActifMe | ActifJe | ActifVe | ActifSa | ActifDi |
|-------|---------|---------|-------------|--------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 1 | U001 | 1 | 09:00 | 10:30 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | U002 | 1 | 09:45 | 11:15 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | U003 | 2 | 08:10 | 09:20 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | U004 | 2 | 08:45 | 09:55 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | U005 | 3 | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
- Requête1 : Requête Sélection:**

| Jour | CodeVol | Escale Depart | HeureDepart | Escale Arrivee | HeureArrivee | Nom CDB | Prenom CDB |
|------------|---------|---------------|-------------|------------------------|--------------|---------|------------|
| 14/10/2002 | U001 | Paris-Orly | 09:00 | Lyon-St EX | 10:30 | DUPONT | Albert |
| 14/10/2002 | U003 | Paris-Orly | 08:10 | Tours Saint Symphonien | 09:20 | MARTIN | Bernard |

Le modèle relationnel a pour objectifs :

- de permettre un haut degré d'indépendance des programmes d'application et des activités interactives vis-à-vis du schéma interne des données ;
- de fournir une base solide pour traiter les problèmes de cohérence et de redondance des données ;
- de permettre le développement de langages de manipulation ou procéduraux basés sur des théories solides ;
- d'être un modèle extensible permettant de modéliser et de manipuler simplement des données tabulaires mais pouvant être étendu pour manipuler des données complexes ;
- de devenir un standard pour la description et la manipulation des bases de données.

Le langage SQL, lui aussi fruit des travaux du milieu des années 1970, est aujourd'hui le standard d'accès aux bases de données relationnelles. La version 2 date de 1992. La version 3 de 1999.

SQL comporte quatre opérations essentielles.

- La recherche (SELECT) permet de retrouver les lignes (tuples) vérifiant les critères qualifiés en arguments.
- L'insertion (INSERT) permet d'ajouter des tuples dans une relation.
- La suppression (DELETE).
- La mise à jour (UPDATE).

SQL est normalisé par l'ISO.

Une requête SQL (Access) pour illustrer une dernière fois notre exemple permettant d'afficher les horaires après jointure entre les tables calendrier des vols, lignes et escales :

```
SELECT CalendrierVol.Jour, Vols.CodeVol, Escales.Ville AS [Escale Départ], Vols.HeureDepart, Escales_1.Ville AS [Escale Arrivée], Vols.HeureArrivee, PN.Nom AS [Nom CDB], PN.Prenom AS [Prénom CDB] FROM Escales INNER JOIN (((Lignes INNER JOIN Vols ON Lignes.NoLigne = Vols.NoLigne) INNER JOIN CalendrierVol ON Vols.NoVol = CalendrierVol.NoVol) INNER JOIN Escales AS Escales_1 ON Lignes.NoEscaleArrivee = Escales_1.NoEscale) INNER JOIN PN ON CalendrierVol.CDB = PN.CodePN) ON Escales.NoEscale = Lignes.NoEscaleDepart ;
```

L'offre SGBDR (SGBD relationnel) s'articule autour de quelques produits (nombreux au départ, mais la sélection a été drastique) dont les plus représentatifs sont :

- Oracle de Oracle Corp.
- SQL Server et son avatar « bureautique » Access de Microsoft, fruit du partenariat avec Sybas.

- DB/2 d'IBM.
- My-SQL et PostGres (héritier du fameux Ingres de Relational Technology) dans le monde de l'open source.

9. Le marché mondial des SGBD

En valeur, la taille du marché des systèmes de gestion de bases de données relationnelles dans le monde est estimée à 14,6 milliards de dollars en 2005. Le marché progresse de 9,3 % en valeur par rapport à 2004. (Source IDC).

Figure 20 : Le marché des SGBD relationnelles

Les cinq premiers éditeurs de SGBD selon IDC (en M\$)

| Fournisseurs | 2005 | En % | 2004 | En % | 05/04 (%) |
|---------------------|--------|-------|----------|-------|-----------|
| Oracle | 6 495 | 45,0 | 5 982 | 44,6 | 8,6 |
| IBM | 3 113 | 22,0 | 2 923 | 21,4 | 6,5 |
| Microsoft | 2 442 | 15,1 | 2 013 | 16,8 | 21,3 |
| Teradata | 503 | 3,5 | 471 | 3,5 | 6,7 |
| Sybase | 423 | 2,9 | 390,0 | 2,9 | 8,5 |
| Autres fournisseurs | 1 591 | 11,5 | 1 529 | 10,9 | 4,1 |
| Total | 14 564 | 100,0 | 13 308,1 | 100,0 | 9,4 |

Source : IDC (mai 2006)

REMARQUE

Les revenus des éditeurs proviennent de plusieurs sources (nouvelles licences, redevances annuelles, ingénierie...) et les chiffres publiés par IDC sont élaborés avec sa propre méthodologie. Une autre société d'études de marché peut aboutir à des résultats sensiblement différents. Il est à noter que, si l'on tient compte des SGBD navigationnels (les plus anciens), IBM devient alors le premier éditeur. Par ailleurs, Microsoft reste leader sur le marché des serveurs sous Windows avec ses produits SQL-Server et Access.

Le monde du logiciel libre (Linux) dispose de plusieurs produits diffusés selon d'autres modèles économiques qui rendent les comparaisons difficiles : MySQL le plus connu, mais aussi Postgres qui est plus puissant.

VI. ÉVOLUTION DES ARCHITECTURES DE TRAITEMENT

A. LE BESOIN : CLIENTS ET SERVEURS

À la terrasse d'un café, vous êtes le client. En tant que client, vous êtes en position d'exprimer vos requêtes à un serveur qui tentera de satisfaire tous vos désirs. C'est ce principe appliqué aux technologies de l'information qui a engendré l'**architecture client-serveur**.

Ceux qui ont vécu l'informatique des années 1980 ont été témoins d'un étrange phénomène : les utilisateurs avaient sur leur bureau deux postes de travail :

- un terminal en mode texte pour accéder aux applications centralisées type comptabilité, gestion commerciale, etc. ;
- un PC, rapidement en mode graphique, pour bénéficier des outils bureautiques.

Ces utilisateurs ont naturellement souhaité retrouver de la place sur leur bureau en regroupant les deux postes en un seul. Les cartes d'émulation de terminal ont rendu la chose possible en transformant, le temps d'une session, le PC en terminal clavier/écran connecté. Ce faisant, ces cartes court-circuitaient « l'intelligence » du PC, celle qui permettait de disposer de logiciels très conviviaux avec des icônes et des menus déroulants accessibles via la souris.

Les utilisateurs ont alors exprimé une deuxième insatisfaction : pourquoi les programmes de gestion accessibles sur le site central n'offraient-ils pas la même convivialité que les outils bureautiques présents sur le poste ?

Lorsqu'ils se connectaient, les utilisateurs subissaient la loi du « site central » (version « *corporate* » de *Big Brother*), qui leur imposait d'office une liste restrictive de services. Pour devenir des clients réellement satisfaits, ils ont exprimé un troisième souhait, avoir le choix et pouvoir se connecter, selon leur humeur du moment, au service jugé le plus pertinent.

B. LA RÉPONSE

Les informaticiens se sont alors mis au travail pour éclater les applications à deux niveaux :

- une partie interface homme-machine résidente sur le PC (avec toute la convivialité que sait fournir ce type de machine) ;
- une partie dédiée au traitement et à l'accès aux données sur la grosse machine centrale (avec toute la rapidité et la capacité de stockage que sait offrir ce type de machine).

La machine centrale devenait serveur. Elle était capable de répondre aux multiples sollicitations de divers PC devenus clients.

Dans la version la plus simple, le poste de travail (PC, Mac, ..), appelé client, ne prend en charge que la présentation des informations en mode graphique. Le serveur assure la logique applicative et l'accès aux données réunies dans une Base de Données.

L'essor de la première génération de l'architecture client-serveur est lié à la multiplication des PC et au développement des Systèmes de Gestion de Bases de Données Relationnelles (SGBDR) et du langage d'interrogation associé : SQL (pour *Structured Query Language*) que nous avons présentés au chapitre précédent.

La couche logicielle du PC propose une grille de saisie des données avec des boutons radios, des cases à cocher et des listes déroulantes. Dès que l'utilisateur clique le bouton OK pour valider la saisie, le PC transforme la grille de saisie en une requête qui est transmise au serveur. Celui-ci la soumet à la base de données. Le serveur envoie les résultats de la requête (une table de données extraite de la base en fonction des critères de sélection et des règles de jointure définis dans la requête) au PC qui les stocke et les met en forme dans un écran de réponse.

Le modèle est progressivement enrichi et décliné en de multiples variantes. Profitant des développements technologiques de l'époque (système d'exploitation multitâche pour les postes de travail, évolution des protocoles réseau) et d'autres touchant les architectures de traitement et de stockage des informations, les informaticiens transfèrent vers les clients une partie de la logique fonctionnelle et quelques données locales.

La complexité du réseau évolue aussi d'une structure de type « n clients vers 1 serveur » en une structure de type « n clients vers p serveurs », chacun des serveurs étant censé jouer un rôle particulier. Les experts parlent d'architecture distribuée et éditent des normes pour assurer l'interopérabilité (DCE de l'OSF, en clair *Distributed Computing Architecture* de l'*Open Software Foundation*).

Alors que les premières applications avaient ravi les utilisateurs du fait de la nouvelle convivialité (*it's fun* – c'est sympa – plébiscitent les utilisateurs aux USA), la complexité croissante va transformer les tâches de développement, de déploiement, d'administration et de maintenance en un véritable cauchemar pour les informaticiens. Les clients deviennent « gras » du fait de l'empilement des couches logicielles, chaque application apporte une nouvelle « couche client ».

Deux facteurs vont permettre de sortir de cette impasse : le développement du concept d'**objet** et l'explosion d'Internet.

Grâce au concept d'objet, le modèle client-serveur de la première génération évolue vers un modèle d'architecture à base de composants réutilisables et interopérables.

Un composant « client » est simplement celui qui émet une demande de services à destination d'un autre composant, le serveur, qui lui-même peut jouer le rôle de client vis-à-vis d'un autre objet. La tendance est donc de réduire la taille du client (qui devient un client léger) avec les composants strictement nécessaires à la gestion de l'interface utilisateur. Les postes clients peuvent être alors de simples terminaux Windows, sans disque ni disquette – donc plus fiables et sans souci de sécurité – ou de vieux PC à bout de souffle.

Tous donnent à l'utilisateur l'impression de travailler avec un PC classique dans sa forme et moderne dans sa puissance, y compris pour les outils bureautiques. Le serveur analyse les sollicitations clients (touches du clavier, opérations souris) et renvoie les images des écrans sous forme compressée à l'aide du protocole R.D.P. (solution Microsoft avec Terminal Edition) ou I.C.A. (solution Citrix avec Metaframe).

Avec le développement de l'Internet, une autre approche, qui vise elle aussi à réduire la taille du client, est d'utiliser le navigateur comme interface universelle d'accès. Il dialogue alors avec un serveur web au standard HTTP qui analyse les demandes client sous forme de formulaires HTML, construit des requêtes vers le serveur de base de données avec des scripts type ASP ou PHP²⁸, récupère les réponses et les formate sous forme de pages web pour les renvoyer vers le navigateur.

Dans les deux cas, l'architecture se structure à trois niveaux (3-tiers où il ne faut pas entendre *tiers* comme le français tiers, mais comme l'anglais *tier* : couche) :

- la couche du client léger sur le poste de l'utilisateur ;
- la couche intermédiaire (*middleware*) qui regroupe les logiciels assurant l'analyse des sollicitations clients et le dialogue avec le serveur de base de données (dans le cas d'une architecture type Internet/intranet « *web computing* » nous aurons un serveur web, un « serveur d'applications » pour orienter les requêtes et un moniteur transactionnel pour supporter le serveur web dans sa charge de dialogue avec les nombreux postes clients) ;
- la couche du serveur hébergeant les logiciels d'application (ceux que nous verrons dans le chapitre 4) traitant les processus de gestion et l'accès aux bases de données.

Ce retour de la charge vers le serveur implique un déploiement plus simple des applications en évitant la diffusion et le support de modules clients spécifiques.

Enfin, la conversion de l'ensemble aux règles du Web permet d'offrir à l'utilisateur un éventail de choix qui marque un renversement par rapport à la vision du terminal esclave du « site central ».

Le modèle client-serveur permet de réutiliser des composants au sein du système d'information, mais les liens très forts qui unissent ces composants nuisent à une parfaite flexibilité.

Ces limites – et le besoin de faire du « *business* » – conduisent les acteurs du marché à proposer de nouvelles offres qui passent du modèle client-serveur classique à base d'objets (*object-oriented distributed architecture*) à un modèle basé sur une architecture distribuée orientée services (*service oriented distributed architecture*).

Derrière ce jargon technique se cache une idée simple et séduisante, faire que chaque composant du système d'information soit clairement identifiable, capable de prendre en charge une liste d'actions parfaitement définies, autonome, doté d'un dispositif de sécurité efficace, documenté, indépendant des autres services et accessible sur l'Internet (ou sur un réseau IP privé).

Ces services pourront être techniques ou « *business* ». Le concept de « *web services* » dont Microsoft assure aujourd'hui la promotion se rattache à cette famille.

28. ASP : *Active Page Server* est la solution Microsoft pour construire des pages web dynamiques, où le code HTML est engendré au moment de l'appel de la page. *PHP* (*Personal Home Page Hypertext Processor*) est la solution issue du principe du logiciel libre (licence GPL).

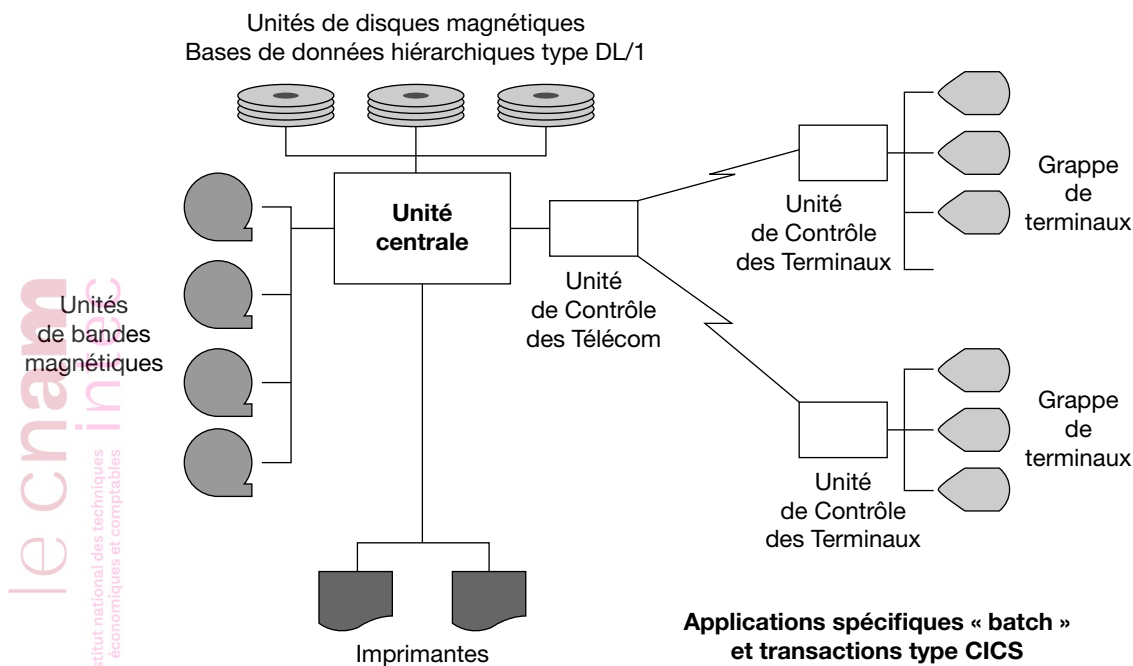
De même qu'un moteur de recherche nous permet aujourd'hui de trouver l'information pertinente, ces « *business and technical services* » devront nous permettre de trouver, intégrer et exploiter l'outil dont l'entreprise a besoin, là où elle en a besoin, quand elle en a besoin. C'est un projet ambitieux.

VII. ÉVOLUTION DES ARCHITECTURES GLOBALES

A. ÉVOLUTION DES ARCHITECTURES DE 1970 À 2010

L'architecture globale de la décennie 1970-1979 est la suivante :

Figure 21 : Architecture globale des années 1970-1979

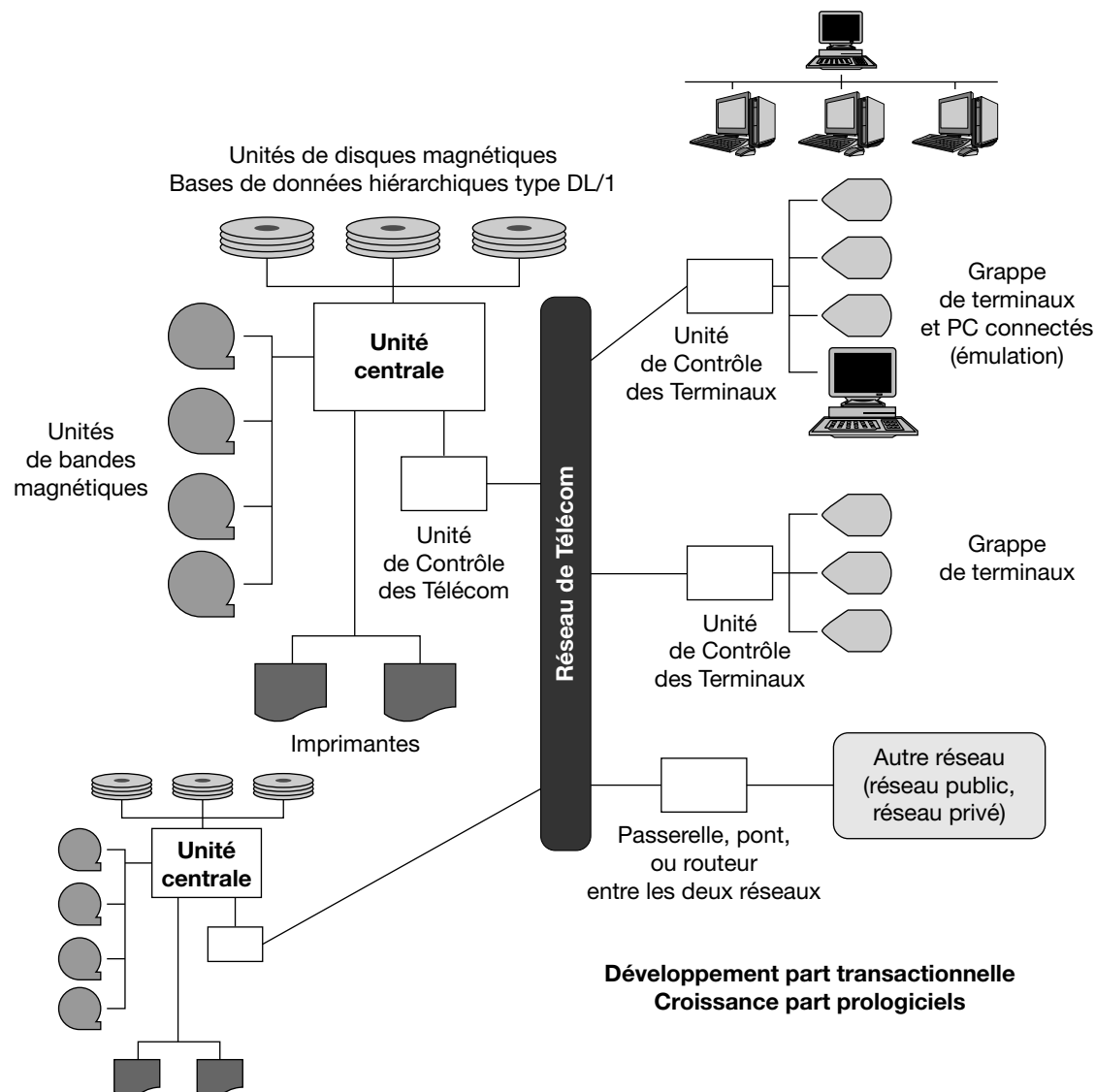


Tout s'articule autour de l'ordinateur central, le « *mainframe* ». Autour de l'unité centrale, les unités périphériques assurent la collecte des données, le stockage (disques fixes, disques amovibles, unités de bandes magnétiques) et la restitution (imprimantes).

La grande majorité des travaux s'opère en mode « par lots » (*batch processing*). Quelques applications transactionnelles exploitent les capacités d'un moniteur de télétraitement et l'utilisateur qui allume son terminal se trouve connecté directement à la machine.

L'architecture globale de la décennie 1980-1989 met le réseau comme nœud central :

Figure 22 : Architecture globale des années 1980-1989



Le réseau de l'entreprise repose sur une solution propriétaire constructeur (type SNA pour IBM ou Decnet pour Digital) et fédère plusieurs « *mainframes* » et minis.

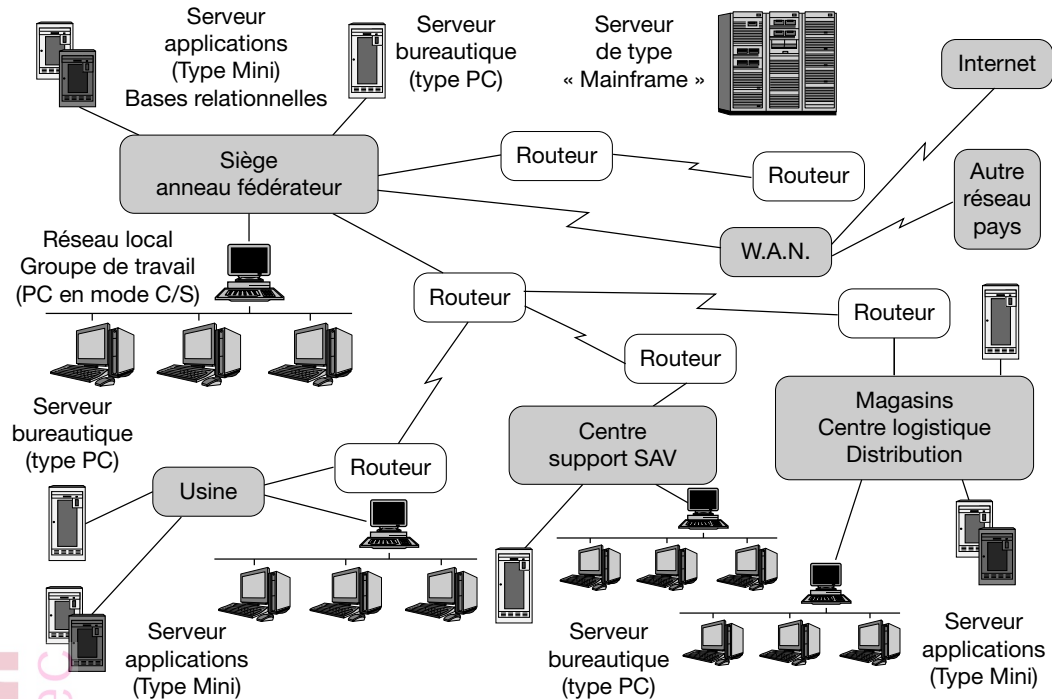
L'utilisateur qui allume son poste de travail se connecte au réseau. Il choisit alors un service qui se trouve hébergé par un des ordinateurs assurant une fonction de serveur.

La bureautique et les ordinateurs personnels constituent un monde à part. Les réseaux locaux qui se développent ne sont pas encore pris en compte.

Les applications transactionnelles se développent et les progiciels se généralisent (paie, comptabilité, gestion de production, gestion commerciale...). Chacun fait référence à une base de données.

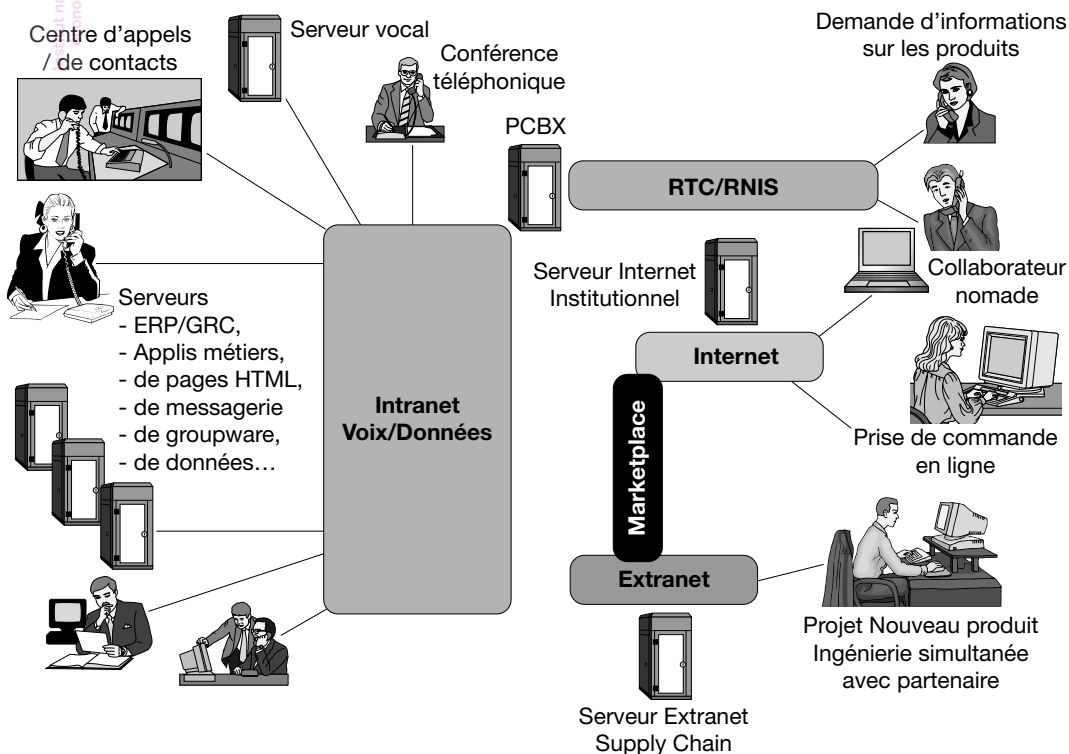
L'architecture globale de la décennie 1990-1999 voit les réseaux se hiérarchiser. Les réseaux d'établissement fédèrent les réseaux locaux. Le réseau d'entreprise fédère les réseaux d'établissement :

Figure 23 : Architecture globale des années 1990-1999



L'utilisateur dispose d'un ordinateur personnel regroupant les fonctionnalités bureautiques et jouant le rôle de station connectée au réseau. Il peut accéder à des services hiérarchisés : au niveau individuel (bureautique individuelle), au niveau du groupe de travail (travail collaboratif), au niveau de l'établissement (applicatifs métiers), au niveau de l'entreprise (PGI/ERP), au niveau d'une collectivité d'entreprise (Gestion de la « supply chain ») ou au niveau global (Internet). La décennie 2000-2009 se structure autour des concepts d'intranet, d'extranet et d'Internet.

Figure 24 : Architecture globale des années 2000-2009



Cette architecture globale, où l'on remarque l'impact très structurant des architectures de communication, est conçue pour répondre aux enjeux métiers et « business » des entreprises de la décennie.

L'intranet fédère les serveurs et les clients internes. Les technologies de voix sur IP ont permis d'intégrer le réseau voix, ses propres serveurs (l'autocommutateur PABX, devenu PCBX) et ses propres clients (les postes téléphoniques). Cette intégration permet d'offrir des services voix-données (Centre de contact).

L'extranet connecte les partenaires. Il va supporter des applications d'ingénierie concurrente pour mettre au point de nouveaux produits et les services de la chaîne logistique (« *supply chain* ») pour les distribuer. Ces services pourront passer par des places de marché électroniques (*marketplace*). La connexion à l'Internet permet les échanges avec les consommateurs, mais aussi avec les collaborateurs nomades.

Nous construisons un tableau récapitulant l'ensemble des besoins à satisfaire en fonction des enjeux. Répondre à ces besoins va conduire à mettre en place divers composants de l'architecture globale.

Éléments d'architecture

| Famille de besoin | Enjeux métiers et « business » | Architecture cible |
|--------------------|---|--|
| B2E ⁽¹⁾ | Mieux communiquer en interne entre collaborateurs | Construire un intranet |
| | Mieux communiquer en interne et partager des référentiels communs | Accéder à l'intranet dans une optique « Accès au référentiel d'information » |
| | Mieux communiquer en interne et partager des processus communs | Accéder à l'intranet dans une optique « Accès au référentiel applicatif » |
| | Mieux communiquer avec les collaborateurs physiquement éloignés de l'entreprise | Accéder hors entreprise à l'intranet au travers un portail de services |
| B2C | Mieux communiquer avec les clients | Accéder à l'Internet |
| | Fournir des informations aux clients | Être présent sur l'Internet |
| | Fournir des services aux clients | Devenir Fournisseur d'accès Internet |
| | Fournir des services aux clients | Offrir l'accès à un bouquet de services |
| | Donner aux clients la possibilité d'acheter en ligne | Offrir l'accès des services marchands |
| B2B | Mieux échanger avec les partenaires | Mettre en place et/ou accéder à des services web EDI |
| | Mieux travailler avec les partenaires | Mettre en place et/ou accéder à un extranet |
| | Mieux commercer avec les clients potentiels | Accéder à une place de Marché |
| | Mieux commercer avec les fournisseurs potentiels | Mettre en place une Place de Marché |
| Toutes | Bien conduire les projets | Intégrer l'ensemble des services dans une architecture cohérente |
| | Bien exploiter les systèmes | Animer les sites et développer les contenus |

(1) Un petit rappel : B2E = Business to Employee (l'entreprise vers ses collaborateurs), B2C = Business to Consumers (l'entreprise vers ses clients consommateurs, B2B = Business to Business (l'entreprise vers ses partenaires – fournisseurs, distributeurs).

B. ARCHITECTURES POUR LES SERVICES B2E

1. Construire un intranet

L'intranet est le réseau interne de l'entreprise aux standards de l'Internet. L'intranet va donc constituer la base des services B2E.

Pour construire cet intranet, l'entreprise peut :

- construire un réseau privé basé sur des solutions d'interconnexion de réseaux locaux via des liens de transport qu'elle va intégrer dans une architecture qu'elle conçoit elle-même avec des équipements actifs ;
- utiliser un Réseau Privé Virtuel (RPV, VPN – *Virtual Private Network* – en anglais) défini au sein du réseau d'un opérateur.

Dans cette phase, l'entreprise peut attendre du prestataire qu'il fournisse :

- des liens de transport ;
- des solutions IRLE (Interconnexion des Réseaux Locaux d'Entreprise) avec fourniture des routeurs ;
- le réseau support du RPV ;
- les services classiquement associés au concept d'intranet (messaging, serveur web interne, accès sécurisé à l'Internet), hébergés sur une ferme de serveurs administrés par l'opérateur.

Figure 25 : Intranet sur une base IRLE avec Liaisons spécialisées

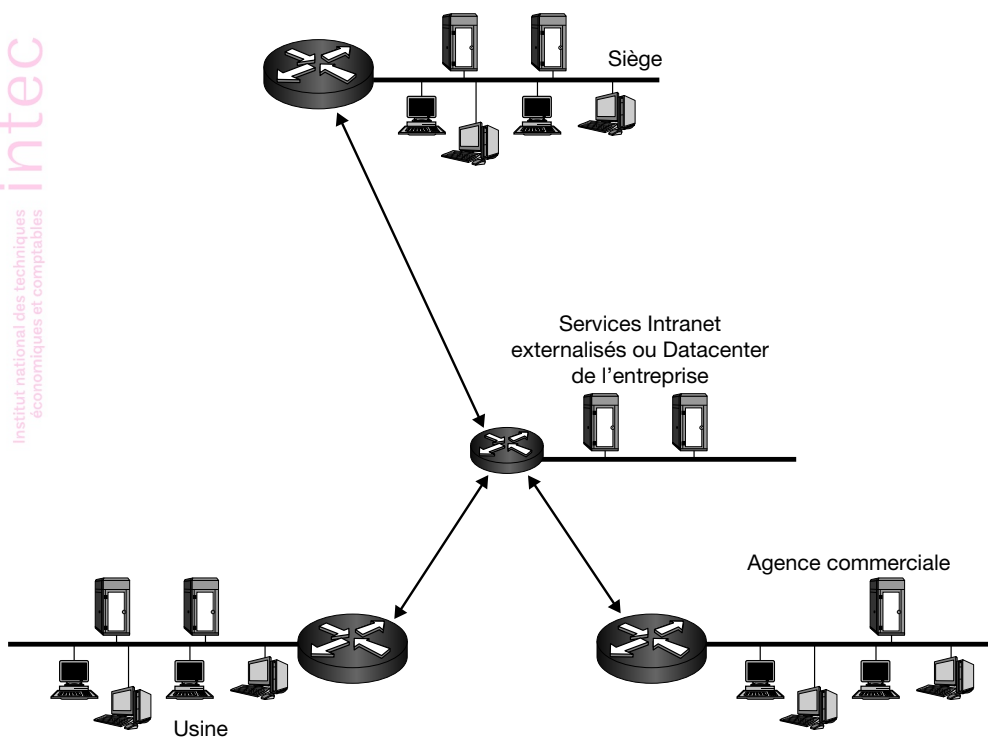
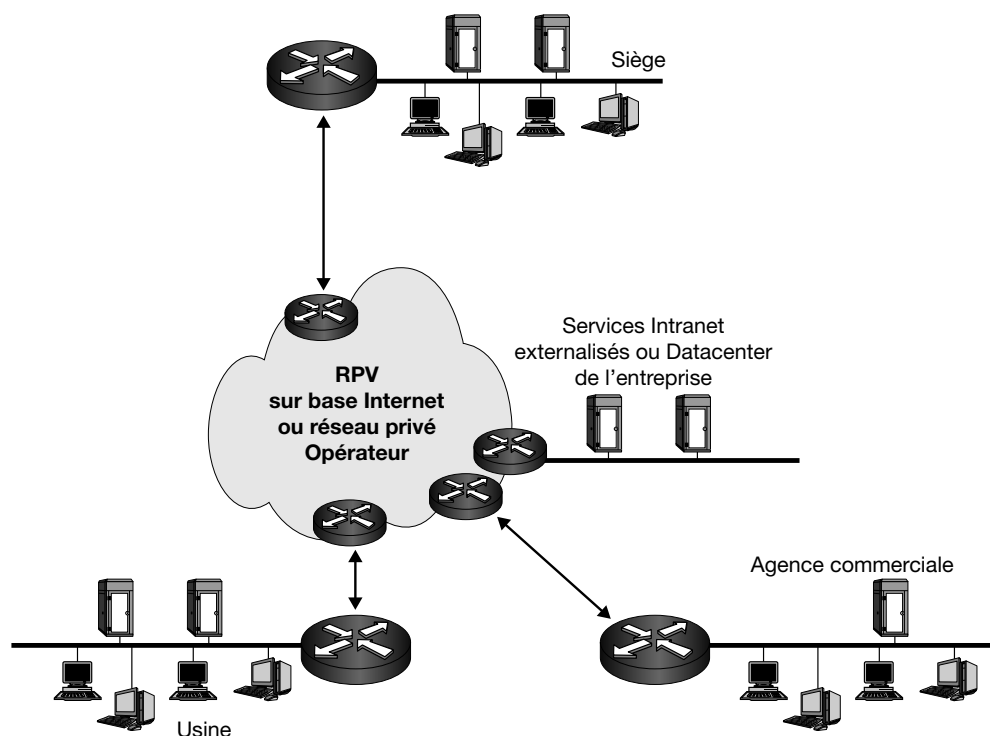


Figure 26 : Intranet sur une base RPV sur un réseau opérateur



La solution RPV via l'Internet est moins chère. La solution via un opérateur présente l'intérêt d'un engagement en matière de sécurité et de performance.

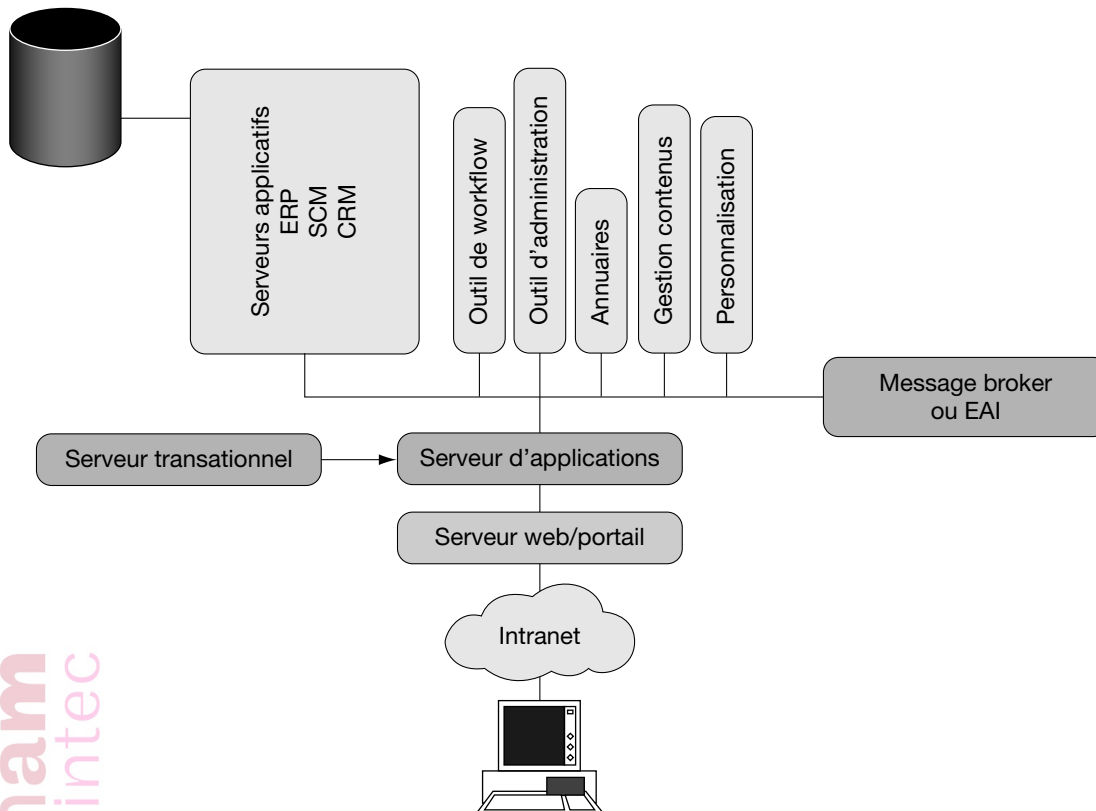
2. Accéder à l'intranet dans une optique « Accès au référentiel d'information »

Dans une première étape, la plate-forme des services intranet héberge des services de messagerie et des serveurs web sur lesquels l'entreprise va développer des contenus correspondant aux référentiels de l'entreprise (référentiel des procédures, des produits, référentiel qualité...).

3. Accéder à l'intranet dans une optique « Accès au référentiel applicatif »

Dans une deuxième étape, le poste de travail du collaborateur et le navigateur web (browser) va servir de client unique à l'ensemble des applications de gestion (ERP, MSC, CRM). Cette évolution, souvent baptisée *web computing*, conduit à des architectures assez complexes basées autour du concept de **serveur d'application**, qui, comme son nom ne l'indique pas, n'héberge aucune application mais assure l'interface entre les serveurs qui supportent effectivement des applications et le serveur web qui délivre les pages à l'utilisateur.

Figure 27 : Accès aux applications de gestion via l'intranet



Si le serveur d'application gère les échanges entre le serveur web et les applicatifs de gestion, l'ensemble EAI/Message Broker gère les échanges entre les applicatifs eux-mêmes.

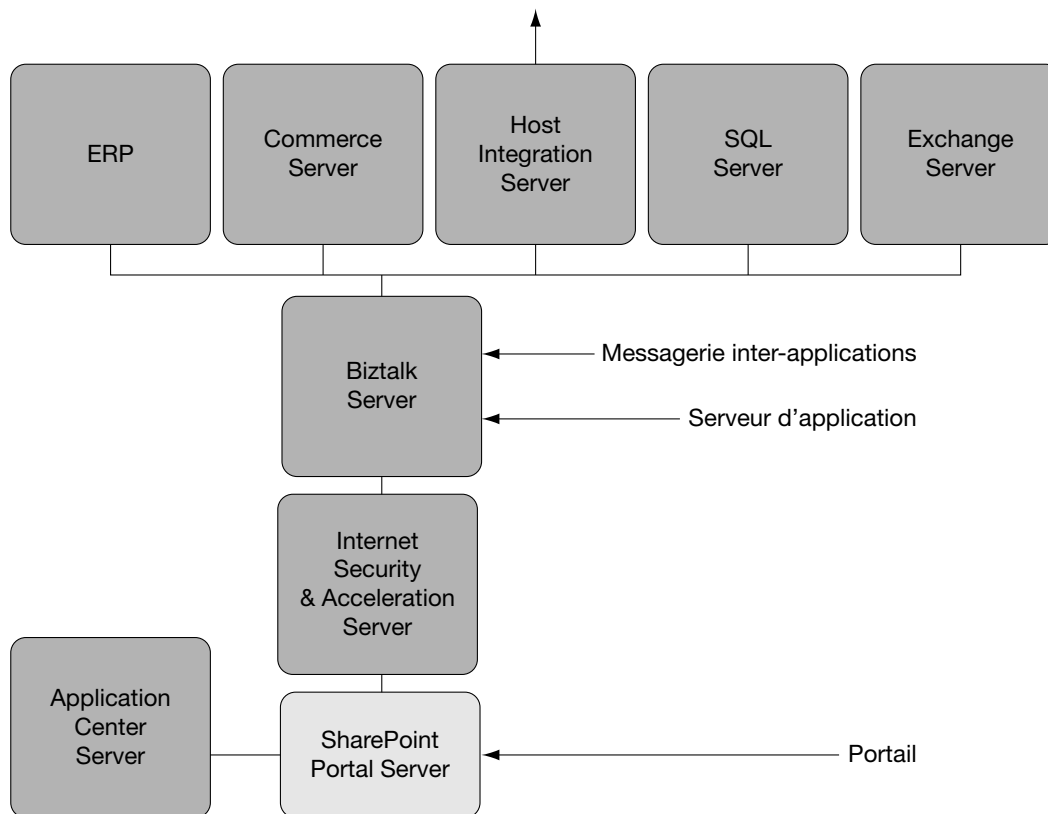
La solution Message Broker est simple (échange de messages) mais demande le développement d'interfaces.

La solution EAI (*Enterprise Applications Integration*) est beaucoup plus ambitieuse en visant une intégration horizontale des applications mais est très lourde à mettre en œuvre. Les technologies propriétaires de l'EAI se placent à l'opposé des principes d'urbanisation et les tarifs de licence sont élevés.

Parallèlement à l'essor des architectures orientées services (*Services Oriented Architectures* – SOA), un nouveau concept est apparu, réunissant l'ambition de l'EAI (et parfois son coût de possession) et la souplesse du Message Broker. L'ESB (*Enterprise Service Bus*) veut constituer un socle de déploiement pour les architectures SOA en mettant en œuvre certains de leurs principes fondateurs : réutilisation, couplage lâche et interopérabilité, en s'appuyant sur le langage XML et les web services.

À titre d'illustration, considérons l'architecture correspondante chez Microsoft :

Figure 28 : Positionnement des briques logicielles dans l'architecture Microsoft.Net



- Le Portail (SharePoint Portal Serve – aujourd'hui Office Sharepoint Server –, Mobile Manager Server) constitue le point d'entrée.
- Application Center Server assure la gestion et le déploiement des applications, l'évolutivité logicielle et la disponibilité critique.
- Internet Security & Acceleration Server assure la connectivité sécurisée à l'Internet, l'accès rapide web et la gestion unifiée des pare-feu.
- Biztalk Server est le serveur d'application qui assure la traduction des données entre application et organisation, la communication B2B et l'automatisation des processus business. Il assure la communication inter-applications.
- Commerce Server assure les fonctionnalités de la plate-forme e-commerce, l'analyse des activités sites et des comportements des internautes, ainsi que le ciblage des promotions.
- SQL Server assure les fonctions SGBD : le stockage des données, l'indexation et la recherche, l'audit et la sécurité.
- Exchange Server assure le support des communications et transactions ainsi que les services collaboratifs.

Si certains composants restent sur mainframe, Host Integration Server assure la passerelle mainframe, l'accès sécurisé aux bases de données et la communication inter-applications. Le marché offre d'autres architectures comme *WebLogic* de BEA ou *Websphere* d'IBM. Le monde du logiciel libre offre d'autres solutions (*Enhydra*).

Un portail peut jouer son rôle de porte d'accès aussi bien pour les intranetes (notre cas actuel) que pour les internautes (cas B2C). L'objectif d'un portail est d'offrir, sur un point d'entrée unique, différents contenus adaptés à des communautés d'intérêts, parfois restreintes, mais aux motivations fortes.

Basé sur le modèle de la télévision, il offre un bouquet de services. Ainsi, internautes et intranutes vont sur leurs portails pour retrouver leurs sources d'informations favorites, telles que les prévisions météo, les dépêches économiques, les cotations boursières ou les avis d'appel d'offres. Le portail est une interface universelle.

Pour être éligible au titre de portail, un **site** doit être doté d'un **moteur sémantique** capable de rechercher l'information en langage naturel et de la catégoriser automatiquement. Par exemple, lancer une requête sur **IBM** rapportera des articles sur Big Blue ou sur n° 1 de l'informatique même si le sigle **IBM** n'apparaît pas dans l'article.

Parce que chaque collaborateur et chaque client sont uniques, les entreprises souhaitent constituer un portail personnalisable sur Internet, intranet ou extranet.

Les utilisateurs de ce portail définissent leur profil et leurs centres d'intérêts afin de disposer de services personnalisés et d'une interface adaptée à leurs besoins à partir de n'importe quel navigateur ou périphérique Internet.

Le portail intègre aussi des techniques de personnalisation que nous étudierions plus précisément dans le cadre des portails marchands.

Un portail est donc constitué par :

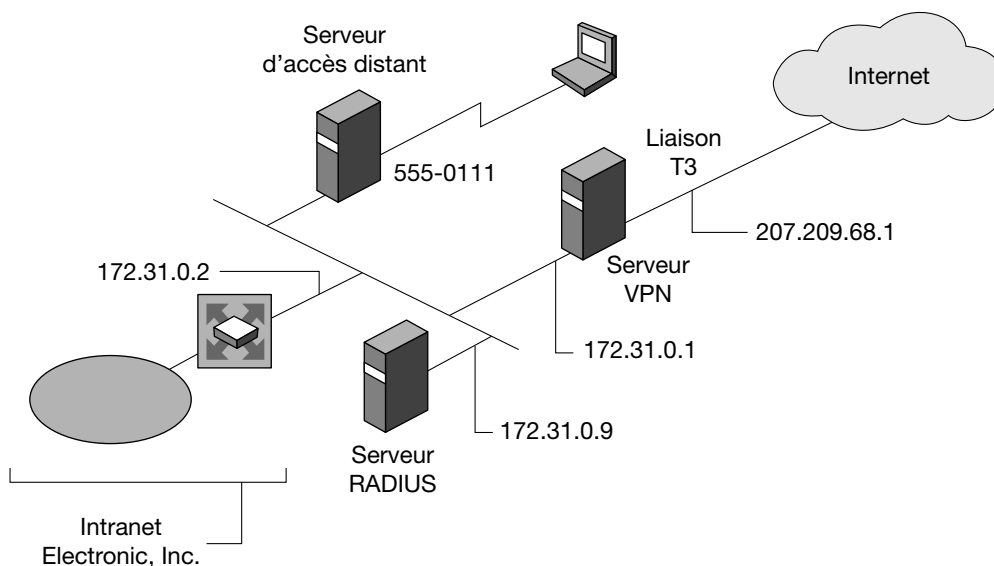
- une partie présentation : l'interface utilisateur ;
- des agents chargés de récupérer les informations, de gérer les envois de mails, SMS ;
- une partie traitement sur le serveur chargé de gérer les interactions utilisateurs ;
- les outils de personnalisation.

Le portail peut être géré en interne sur la base d'outils comme Corporate Yahoo, Mediapps Net. Portal, Share Point Portal Server de Microsoft.Net. Il peut aussi être hébergé chez un fournisseur de services. La mention multi-terminaux fait état de la possibilité d'accès par PC portable, par PDA ou par téléphone GSM/3G.

4. Accéder à distance à l'intranet

Le besoin d'accéder à l'intranet en dehors de l'entreprise intéresse tous les collaborateurs, mais tout particulièrement les nomades permanents que sont les commerciaux, les inspecteurs de maintenance, les chauffeurs-livreurs...

Figure 29 : Accès distant à l'intranet (source Microsoft)



Plusieurs types d'accès peuvent être envisagés (cf. figure 29). Tous sont basés sur le concept de **Serveur d'Accès Distant**. Le Serveur d'Accès Distant est le point d'entrée d'un intranet pour les salariés nomades.

Le rôle du serveur d'accès est de traiter les appels entrants dans l'optique de connecter un utilisateur au réseau interne. Son architecture dicte le nombre d'accès simultanés selon le nombre d'interfaces et les moyens de se connecter. Certains serveurs d'accès distants supportent un panachage de modems et de cartes RNIS. D'autres proposent des cartes numériques capables de traiter tous types d'appels.

C. ARCHITECTURES POUR LES SERVICES B2C

1. Accéder à Internet

La problématique de relation de l'entreprise avec ses clients implique :

- de pouvoir accéder à Internet ;
- de pouvoir être présent sur Internet en proposant des services de type web ;
- de pouvoir offrir à ses clients, s'ils ne possèdent déjà, un accès à Internet pour qu'ils puissent bénéficier de ces services ;
- de proposer à ses clients à un bouquet de services présélectionné pour eux ;
- de passer au niveau de la transaction commerciale directe via le réseau.

Pour que l'entreprise puisse accéder à Internet, il faut qu'elle soit connectée à l'épine dorsale (*backbone*) constituée par les nœuds de transit du réseau.

Le moyen le plus simple consiste à passer par un fournisseur d'accès Internet (FAI, IAP – *Internet Access Provider* – en anglais), devenu rapidement Fournisseur de services Internet (ISP – *Internet Services Provider*)²⁹. Ce FAI mutualise les trafics afin de justifier du débit d'une telle connexion.

Le métier d'ISP est devenu un des métiers de base des opérateurs. Ceux-ci proposent une offre extrêmement riche, soit à l'attention des particuliers – ce qui est intéressant dans le contexte B2C – soit à l'attention des entreprises – ce qui est intéressant dans les contextes B2E et B2B –. Selon les débits proposés, ces offres se déclinent en RTC, RNIS, xDSL ou liaison louée.

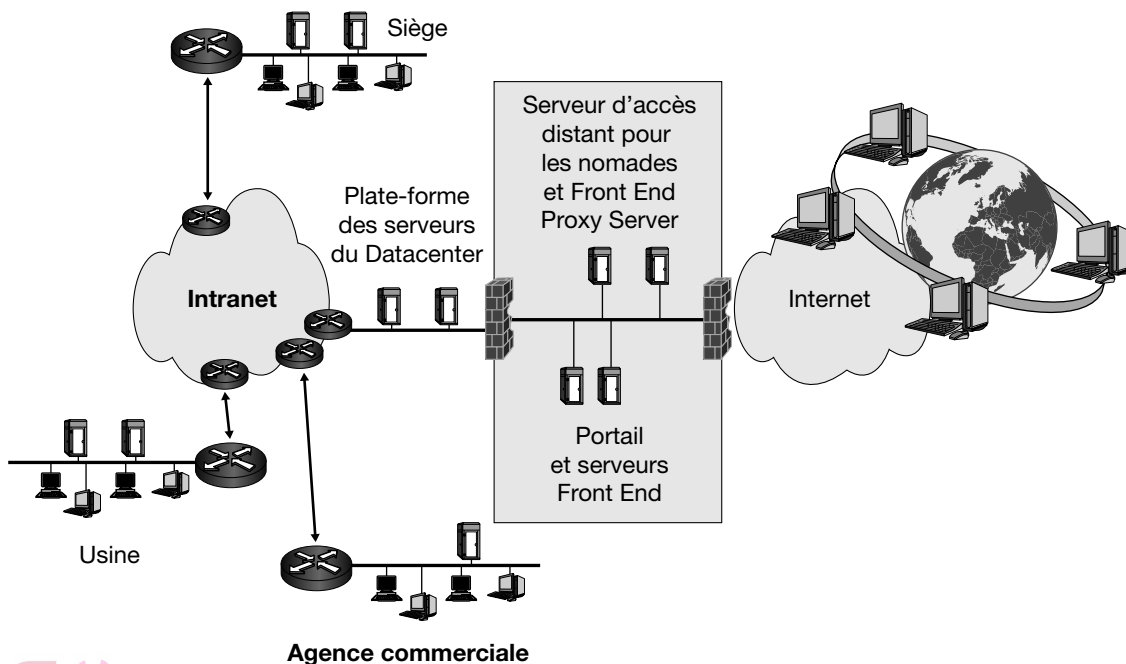
Les grands opérateurs sont des ISP disposant de leur propre « *backbone* ». D'autres ISP, exploitant des stratégies de niches, n'ont pas vocation de disposer de leur propre *backbone*. Ils peuvent alors utiliser l'infrastructure d'un opérateur possédant son propre *backbone*, devenant en quelque sorte revendeurs de bande passante.

L'entreprise a trois approches possibles de l'accès à Internet :

- Laisser les collaborateurs se connecter par eux-mêmes au moyen d'un modem sur le réseau téléphonique : c'est bien sûr la pire des solutions parce qu'elle constitue une faille énorme dans le dispositif de sécurité si les machines sont par ailleurs connectées à un réseau interne, mais c'est à coup sûr la solution qui risque de se développer si l'entreprise n'a pas pris d'autres mesures pour permettre l'accès au réseau des réseaux. Cette pratique a pratiquement disparu avec le remplacement des accès RTC par ADSL.
- Laisser l'indépendance aux sites qui vont connecter leur réseau local au point de présence du réseau de leur fournisseur d'accès via un routeur et devoir gérer la sécurité de cette interconnexion (firewall, proxy, anti-virus...).
- Établir une solution d'accès centralisée via une plate-forme sécurisée, elle-même connectée à l'intranet et à l'Internet, sous le contrôle d'un administrateur.

29. Nous reviendrons, dans le chapitre 6, sur cette évolution.

Figure 30 : Accès centralisé via intranet



2. Être présent sur Internet

Pour que l'entreprise soit présente sur Internet, il faut mettre en place des serveurs de ressources connectés à l'Internet.

Les ressources sont reconnues par l'Internet grâce à l'affectation d'une URL (*Unique Resource Locator*) qui intègre un nom de domaine attribué à l'entreprise. Ces ressources correspondent à des services définis selon les standards de l'Internet : pages web (standard HTTP), mails (standard SMTP), fichiers (standard FTP).

L'entreprise souhaite se faire connaître en créant un ou plusieurs sites web et communiquer en installant un ou plusieurs serveurs de messagerie.

Ces serveurs peuvent être hébergés dans l'entreprise (généralement sur la plate-forme sécurisée qui gère l'accès à Internet). Ils peuvent aussi être hébergés par un prestataire extérieur.

3. Devenir Fournisseur d'accès Internet

Une entreprise, dans un secteur d'activité quelconque, peut-elle devenir Fournisseur d'accès Internet.

Rien ne s'y oppose mais on peut se demander quel intérêt elle peut y trouver. En fait elle peut offrir des kits de connexion qui auront la particularité d'offrir le site de l'entreprise comme page d'accès standard (exemple d'une banque qui veut inciter ses clients à recourir à la banque en ligne).

C'est le principe de l'ISP blanc (*Virtual ISP*) : des opérateurs spécialisés gèrent le service pour le compte de l'entreprise et préparent des kits blancs sur lesquels celle-ci place son logo. Ce principe a eu un certain succès dans les années 1998-2000 mais a progressivement disparu avec le développement des équipements des consommateurs.

4. Offrir un bouquet de services

L'entreprise offre à ses clients un bouquet de services dans le cadre de son portail ou de son centre de contact.

Dans ce bouquet :

- boîte de courrier électronique ;
- informations générales ;
- informations financières ;
- agenda quotidien ;
- chat et FAQ.

5. Fournir des services marchands

Le dialogue étant établi avec un consommateur acquis à la marque, pourquoi ne pas profiter de l'opportunité pour passer à l'acte d'achat. Le portail devient alors un portail d'achat et le logiciel qui le gère une suite marchande.

Aux fonctionnalités du bouquet précédent, on ajoutera les services suivants :

- catalogue et promotions ;
- prise de commande et gestion du panier d'achat ;
- paiement sécurisé ;
- commandes en cours ;
- échos GRC, sondages et enquêtes ;
- recherche marques, produits et boutiques ;
- personnalisation ;
- publication ;
- affiliation.

Si l'entreprise ne souhaite pas faire évoluer son portail de cette manière, elle peut aussi se contenter d'insérer des liens vers un portail marchand multi-vendeurs, mutualisant les services.

D. ARCHITECTURES B2B

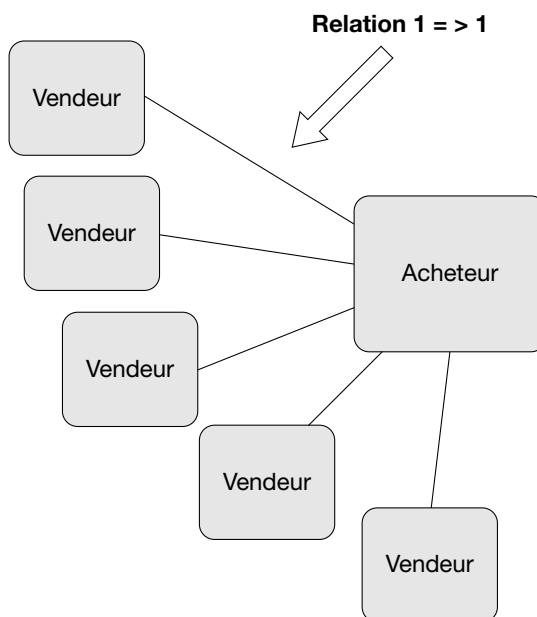
1. Mettre en place et/ou accéder à des services web EDI

Les réseaux EDI sont apparus dans les années 1980 pour permettre aux grands donneurs d'ordres de faciliter les relations avec leurs sous-traitants.

Les liens établis sont de type 1 => 1.

Des normes sont venues progressivement définir le cadre de ces échanges au niveau des conte-nants (EdiFact) et des contenus métiers (Galia-Odette, Allegro, ATA, Swift, Tedeco, EdiFret...).

Figure 31 : Les liens 1 => 1 de l'EDI



Les techniques de l'Internet ont bien sûr investi ce champ pour arriver au concept WebEDI, les liens étant supportés par le réseau Internet.

Un bon exemple est donné par un produit d'Orange Business Services dont le nom est justement WebEDI. WebEDI s'adresse aux PME clients-chargeurs de transporteurs pour environ 10 expéditions/jour, n'ayant pas les moyens d'une station EDI spécialisée.

Cette PME accède au service, en mode sécurisé, à partir d'un simple PC équipé d'un navigateur.

WebEDI permet :

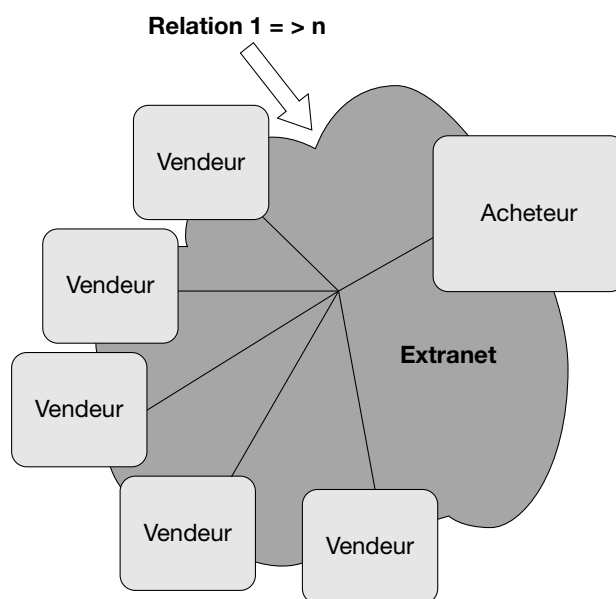
- la saisie contrôlée des expéditions à partir de formulaires Web ;
- l'édition, chez le chargeur, de l'étiquette code-barres transporteur ;
- l'édition du bordereau de remise ;
- le suivi des expéditions ;
- la sortie de statistiques sur les expéditions et les remontées d'informations livraison ;
- la gestion des bases de données annexes (communes, clients-destinataires) ;
- la diffusion d'informations générales et personnalisées.

2. Mettre en place un extranet pour les partenaires

La logique précédente de relation entre un acheteur et ses vendeurs conduit à la mise en place d'un groupe fermé d'abonnés au sein d'un réseau construit sur les technologies Internet : un extranet.

Cet extranet peut être vu comme une extension de l'intranet vers les partenaires, via des solutions commutées avec authentification des acteurs ou comme une réduction de l'Internet via un réseau privé virtuel.

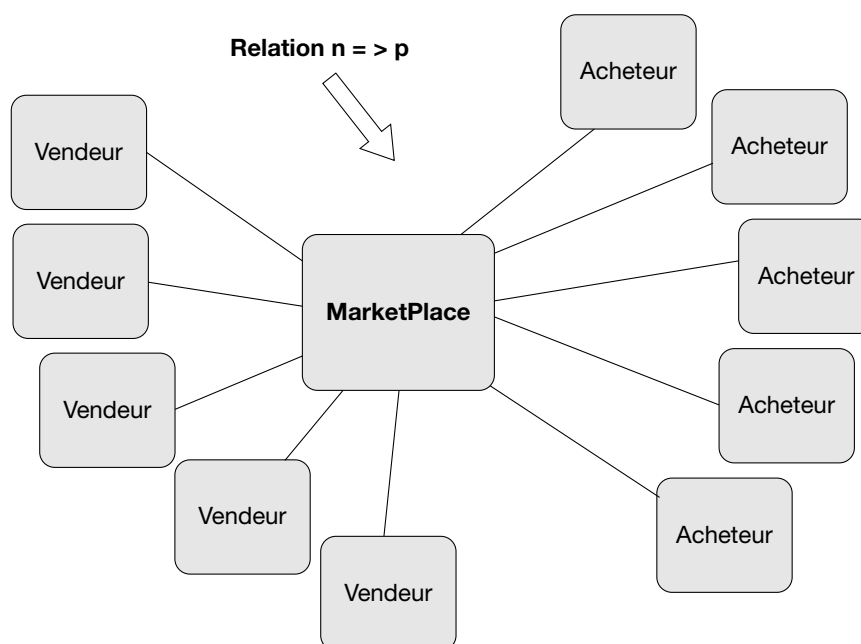
Figure 32 : Les liens 1 => n de l'extranet



3. Accéder à une place de marché

Étendre la logique précédente aux relations entre n acheteurs et p vendeurs conduit au concept de place de marché (*Market place*).

Figure 33 : Les liens n => p de la Place de Marché



E. ÉVOLUER VERS LE WEB 2.0

1. Le Web comme une plate-forme

Comme de nombreux concepts majeurs, le Web 2.0 n'a pas de frontière claire mais plutôt un centre de gravité.

On peut considérer le Web 2.0 comme un ensemble de principes et de pratiques que l'on peut suivre avec une grande souplesse, les uns respectant la totalité du corpus, les autres s'en inspirant plus ou moins librement.

La formule a été lancée par Netscape, qui n'a pas su vraiment en tirer parti. Les premières réalisations concrètes ont été les serveurs de publicité qui affichaient des fenêtres pop-up sur le site que vous visitiez, ils sont le premier exemple de « *mashup* » (service composite).

Akamai traite aussi le réseau en tant que plate-forme quand il élabore un cache ainsi qu'un système de distribution de contenu soulageant la bande-passante d'un réseau souvent congestionné. Sa plateforme mondiale, constituée de milliers de serveurs spécialement équipés, permet à Internet de résister à la pression des requêtes quotidiennes pour obtenir un contenu, des transactions et des applications riches, dynamiques et interactifs.

Netscape énonçait « *le Web en tant que plate-forme* » dans les termes du paradigme du logiciel d'autrefois : leur produit-phare était le navigateur web, une application cliente, et leur stratégie était d'utiliser leur domination sur le marché du navigateur pour s'ouvrir le marché des serveurs haut de gamme.

Le contrôle des standards d'affichage de contenu et des applications utilisant un navigateur aurait dû en théorie donner à Netscape le même genre de pouvoir sur ce marché que celui que possède Microsoft sur celui des PC.

Finalement, serveurs et navigateurs web devinrent de simples outils et la plus grande part de la valeur ajoutée du Web se concentra dans les services diffusés par les plates-formes web.

Google au contraire, commença son existence en tant qu'application web native, jamais vendue ou packagée mais délivrée en tant que service, avec des clients payant, directement ou indirectement, pour utiliser ce service.

Les avantages :

- aucun des pièges de la vieille industrie logicielle ne pouvait s'appliquer à son modèle ;
- aucun planning de sortie de différentes versions, juste une amélioration continue ;
- aucun système de vente ou de licence, simplement des utilisateurs ;
- aucun problème de portage sur différentes plates-formes de sorte que les clients puissent faire marcher le logiciel sur leur machine, uniquement une quantité massive de PC utilisant un système d'exploitation open source ainsi que quelques applications maison (que nul d'extérieur à l'entreprise n'a jamais pu voir...).

Le service offert par Google n'est ni un serveur – bien qu'il soit délivré par une quantité massive de serveurs web – ni un navigateur – bien que pour l'utiliser, un navigateur soit nécessaire. Son moteur de recherche bien connu n'héberge même pas le contenu qu'il permet à ses utilisateurs de trouver.

À la façon d'un coup de téléphone où la valeur n'est pas dans les téléphones mais dans le réseau qui les met en relation, Google place sa valeur dans l'espace situé entre le navigateur et le serveur de contenu, comme un opérateur entre l'utilisateur et son usage du Web.

Mais il y a une grande différence avec le modèle du RTC : Google n'est pas qu'un simple commutateur (la valeur ici est devenue faible), il est fournisseur de données pertinentes que l'utilisateur aurait mis des heures à compiler.

La gestion de bases de données est le cœur de métier des sociétés du Web 2.0, à tel point qu'on donne parfois à leurs applications le nom d'« *infoware* ».

2. Les règles du Web 2.0

La règle n° 1 du Web 2.0 est de mettre au point un service simple d'accès et une gestion algorithmique des données pour toucher l'intégralité du Web, jusque dans sa périphérie, pas seulement son centre, jusqu'au bout de sa longue traîne, pas seulement en son cœur.

D'autres réussites démontrent la pertinence de ce modèle comme base du business : Ebay, Napster, BitTorrent.

Une règle est commune à ces réussites : construire le service non grâce à un immense catalogue mais à travers la mise au point d'un système faisant de chaque client un serveur renforçant lui-même le réseau, d'où la conclusion : le service s'améliore automatiquement quand le nombre de ses utilisateurs croît.

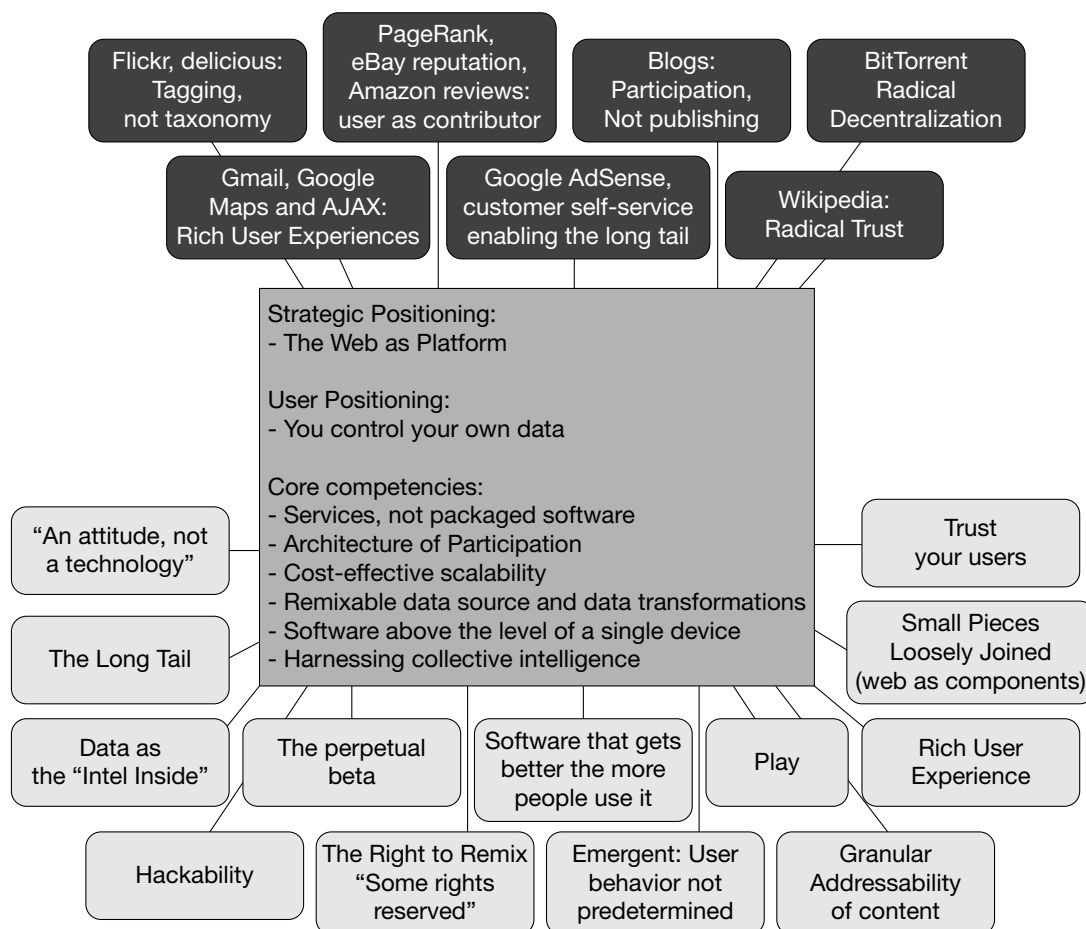
Il en découle la règle n° 2 qui est de tirer parti de l'intelligence collective :

- blogs et wikis (Wikipedia) ;
- développement du concept « mashup » sur la base des web services.

Exemple : Housingmaps.com, qui combine Google Maps avec les données de Craigslist pour créer un outil interactif de recherche de logement.

Google Maps a bouleversé cet univers du fait de sa simplicité. Alors que les expérimentations d'utilisation des web services demandaient jusque-là un contrat entre les intéressés, le fait de laisser les données aisément accessibles a permis à quelques « bidouilleurs » de réutiliser ces données de manière créative, à l'image des principes du « *mod* » dans le monde du jeu.

Figure 34 : La carte de référence du Web 2.0



3. Le management par le Web 2.0

L'influence de l'Internet sur l'entreprise n'est plus à démontrer. Cette dernière trouve sa source dans le besoin de communiquer au sens large (sur le plan institutionnel et commercial), d'obtenir et d'échanger des informations rapidement, d'établir des relations avec des partenaires, de faire du commerce en ligne, de faire de la veille technologique, etc. Mais jusqu'à une période récente, développer un intranet relevait plus d'une volonté de contrôle des individus dans l'organisation que d'émancipation. La révolution apportée par le Web 2.0 dans l'entreprise (parfois défini comme l'intranet où l'on peut écrire : Writable Intranet) est sans doute en train de modifier cet état de chose. En passant d'un modèle centralisé et maîtrisé, à un modèle non hiérarchique, le Web 2.0 est en voie de transformer profondément l'entreprise et l'ensemble des organisations.

L'arrivée du Web 2.0 en entreprise est tout d'abord celle de nouvelles générations dans le monde du travail. Ces générations ont grandi avec le Web et ont donc des attentes nouvelles dans le cadre des situations professionnelles. C'est l'occasion pour les entreprises d'innover en s'appuyant sur les compétences déjà acquises par leurs collaborateurs. C'est aussi une nouvelle forme de partage et de relations dans l'entreprise pour les professionnels de l'informatique qui doivent désormais composer avec de nouvelles demandes et des exigences accrues des personnels en termes de formation. Il devient en effet de plus en plus normal pour un salarié de s'approprier les outils mis à sa disposition et il attend même qu'on lui en donne la possibilité afin qu'il puisse travailler dans de bonnes conditions. C'est ainsi qu'il va configurer son courrier électronique, son téléphone mobile, sa messagerie, son wiki ou son blog.

L'apparition du thème de l'entreprise 2.0 ne peut donc se justifier par la seule justification de l'immersion dans une économie de la connaissance globale et dématérialisée où la compétitivité passerait par la capacité à innover et à travailler en réseau. Le modèle de management mis en œuvre par Google est sans doute un indice de ce changement. Il y a là la volonté de développer une nouvelle forme d'intelligence et d'innovation collective et d'avoir généralement une politique différente en termes de ressources humaines et des enjeux sur les recrutements à venir. Les entreprises ont bien compris qu'il y avait là une lame de fond et pas seulement un phénomène de mode devant le succès des réseaux sociaux professionnels comme Viadeo ou LinkedIn. Les grands éditeurs de solutions informatiques intègrent des fonctions Web 2.0 dans la plupart de leurs progiciels (PGI y compris). L'idée est de contourner une organisation pyramidale qui est un frein au développement des collaborations dans un contexte globalisé et un facteur de discontinuité. La complexité des organisations actuelle rend crucial le besoin de circuit court pour la circulation de l'information. La mise en commun et le partage sont les conditions de la maîtrise des risques et de l'augmentation de l'expertise associée à la qualité. On s'aperçoit en effet que les organisations doivent faire face à des plus en plus de problèmes difficiles à résoudre en bout de chaîne et à une gestion des exceptions qui suppose d'autres modalités de management. Avec des outils tels que les blogs et les micro-blogs, les flux RSS, les wikis, les mashup d'entreprise, les outils de réseaux sociaux à vocation interne, le Web 2.0 peut répondre à de tels besoins.

F. RÉPONDRE AUX ENJEUX DE LA MOBILITÉ

Le développement du nomadisme au détriment de la sédentarité implique d'être accessible n'importe où, n'importe quand, de n'importe quelle manière.

La mobilité représente un enjeu important pour un nombre sans cesse plus important d'organisations. Le déploiement de cette mobilité représente un véritable projet d'entreprise. Les opérateurs et fournisseurs de services doivent se remettre sans cesse en question et innover en la matière. Les nouvelles offres en matière de mobilité viennent aussi apporter une réponse à la saturation du marché.

Les entreprises sont prudentes car il est difficile d'évaluer le Retour sur Investissement ou la valeur créée par un projet « Mobilité ». Avant d'introduire des solutions de ce type, l'entreprise doit réfléchir sur ce qu'impliquent les qualificatifs « nomade » ou « mobile » sur ses processus.

Il y a trois motivations pour développer des solutions nomades :

- tirer avantage du mode interactif dans un plus grand nombre de situations ;
- homogénéiser ou sécuriser les processus pour qu'il n'y ait plus d'interruption dans la chaîne de traitement ;
- engendrer de nouveaux revenus.

Les solutions technologiques ne manquent pas mais le frein est souvent le facteur humain. La technologie Blackberry, qui permet de consulter et de répondre à ses courriels sur un petit terminal, restant ainsi sans cesse en contact avec son bureau, est née en 1998 au Canada et il a fallu une dizaine d'années pour qu'elle se généralise.

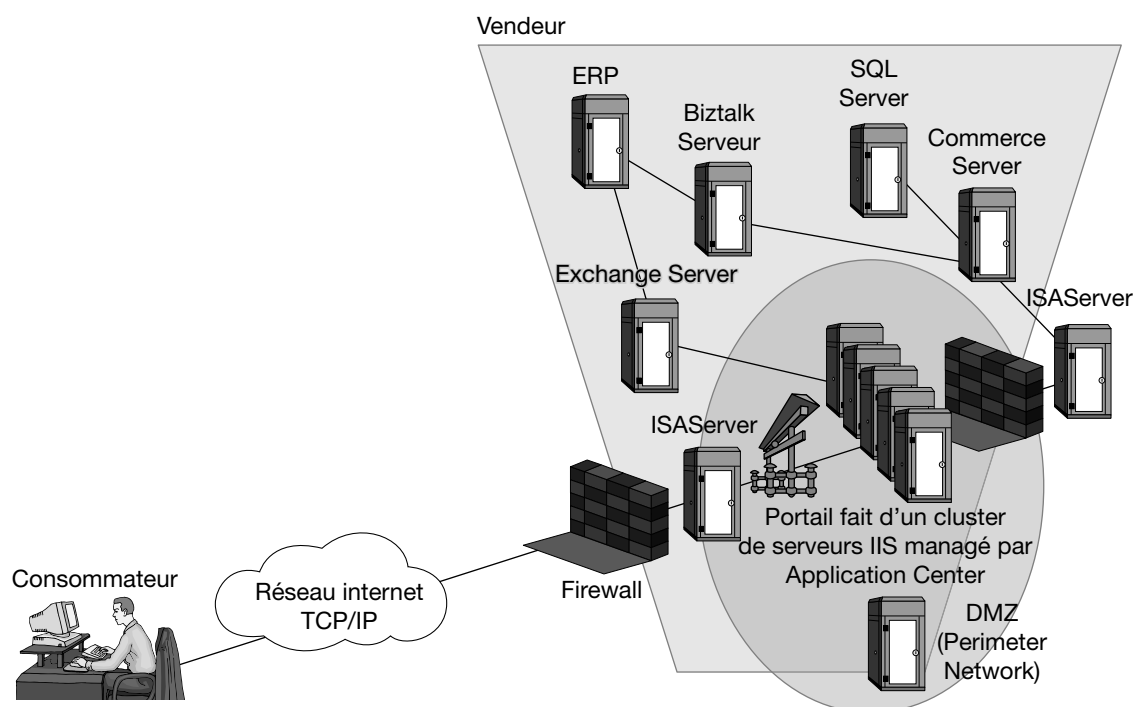
Selon une étude Ipsos, l'utilisation de cette technologie ou d'une technologie voisine type Windows mobile 5, dans différents segments de métiers et à différents niveaux hiérarchiques, engendre un gain de 54 minutes en moyenne par jour.

| Scénario d'utilisation | Terminal adapté | Application typique |
|---|--|--|
| Utilisation à plein temps pour ceux dont la fonction exige le nomadisme (commerciaux, inspecteurs de maintenance). | Ordinateur portable, téléphone et/ou PDA fournis par l'entreprise | Accès permanent aux applications de gestion (messagerie électronique, intranet, extranet, VOIP, visioconférence) |
| Utilisation occasionnelle pour les managers qui voyagent épisodiquement | Outil du même type que ci-dessus fourni par l'entreprise, outil personnel ou terminal public | Messagerie électronique, intranet et quelques applications |
| Travail à la maison | Outil personnel | Messagerie électronique, préparation et révision d'un rapport |
| Continuité des affaires (depuis l'indisponibilité temporaire d'un salarié jusqu'à la catastrophe paralysant l'entreprise) | Tout moyen de communication encore disponible | Permettre l'accès aux applications vitales pour garder les processus de gestion et les processus métiers opérationnels |
| Nouveau service à l'intention des clients | Toute innovation envisageable | Toute innovation envisageable |

G. UNE ARCHITECTURE DEVENUE TRÈS COMPLEXE

Pour conclure, les schémas qui suivent montrent comment ces architectures se mettent en œuvre dans le cadre du fonctionnement normal des affaires. À titre d'illustration, nous prenons l'exemple de Microsoft mais le principe reste le même avec les autres éditeurs.

Figure 35 : Transaction B2B



Une architecture devenue très complexe Qu'est ce qui caractérise les architectures globales d'aujourd'hui ?

- un coût en baisse pour les équipements ;
- mais une plus grande complexité, impliquant la traversée de multiples équipements et de multiples couches logicielles.

La transaction d'une application CICS classique partait du terminal pour aller au « mainframe » puis revenait au terminal en passant par quelques équipements réseau. (Unité de contrôle de communication, unité de contrôle des terminaux).

La transaction B2C d'aujourd'hui part du poste client, traverse les routeurs d'un réseau IP, se présente devant le pare-feu de la zone démilitarisée pour solliciter les serveurs de cette zone (serveurs web du portail, managé par un serveur en charge – entre autres tâches – d'assurer la disponibilité critique). La confirmation de l'intérêt du client pour un produit donné engendre une transaction qui va gagner l'intranet au travers d'un autre pare-feu, traverser le serveur garant de la sécurité et de la performance de la connectivité à l'Internet, pour atteindre le serveur d'application qui joue le rôle de connecteur entre les services aux normes Internet et les serveurs supportant les systèmes de gestion. La transaction reformatée sollicite alors les services d'un serveur e-commerce qui s'appuie sur un serveur de bases de données. Pour s'assurer de la disponibilité des produits, proposer une date de livraison et enregistrer la commande, le serveur e-commerce lance une requête vers le serveur supportant l'ERP, qui lui-même sollicitera un serveur de messagerie, toujours au travers du serveur d'application, pour envoyer un mail de confirmation qui retraversa le portail et le réseau pour atteindre le client.

La transaction B2B est tout aussi complexe. L'ERP n'enregistre que le montage de l'expédition vers notre client B2C conduit à un déstockage générateur d'une commande de réapprovisionnement vers le fournisseur. L'appel de livraison de l'ERP du vendeur est traduit en XML au niveau du serveur Biztalk (serveur d'application), puis transmis au réseau via ISA Server et la zone démilitarisée DMZ.

Cet appel de livraison transite via le réseau vers le *datacenter* du fournisseur où il va trouver une structure d'accueil équivalente qui va l'orienter vers un serveur d'application.

Ce serveur d'application traduit l'appel de livraison XML dans le format de l'ERP du fournisseur mais, pour attendre celui-ci, qui est hébergé sur un mainframe, il faut de plus traverser une machine supportant une passerelle « *Host Integration Server* ».

L'appel de livraison est traité par l'ERP qui renvoie en échange un avis prévisionnel d'expédition AVIEXP qui devra retraverser la même chaîne de serveurs que l'appel de livraison, cette fois dans l'autre sens, pour atteindre l'ERP du vendeur.

Cette complexité des architectures a pour corollaires :

- un coût en hausse des prestations humaines (compétences plus pointues) ;
- une complexité plus grande des processus de production ;
- un souci d'industrialisation et d'application de normes professionnelles pour essayer de maîtriser cette complexité ;
- un recours plus fréquent à l'externalisation pour tenter de baisser les coûts grâce à la mutualisation des moyens et de trouver les compétences nécessaires.

VIII. ARCHITECTURE TECHNIQUE D'AUJOURD'HUI

A. LES INFRASTRUCTURES ACTUELLES

L'**architecture technique (ou physique)** du système d'information s'intéresse aux divers composants techniques mis en place pour matérialiser l'architecture fonctionnelle : serveurs et systèmes d'exploitation associés, postes de travail, équipements de réseaux, support de bases de données et logiciels.

Ces composants exploitent les technologies de base : les postes de travail exploitent les technologies de collecte et de traitement, les serveurs exploitent les technologies de traitement, les supports des bases de données exploitent les technologies de stockage, les équipements de réseau exploitent les technologies de communication.

Les outils logiciels du système d'information se répartissent sur le poste de travail de l'utilisateur (considéré en tant que client) et sur des machines hébergeant les services auxquels l'utilisateur va accéder (considérées en tant que serveurs). Le client se connecte aux serveurs via des réseaux.

Même si l'organisation n'est présente que sur un site et que tous ses postes de travail sont reliés par un réseau dit local (les anglo-saxons parlent de « Local Area Network » – LAN), elle ne peut ignorer les télécommunications car elle est en liaison avec de multiples partenaires. C'est le concept d'entreprise étendue. Son réseau local est donc connecté à d'autres réseaux locaux par le biais de réseaux étendus (les anglo-saxons parlent alors de WAN – « Wide Area Network »).

Ces réseaux sont hiérarchisés en fonction du nombre d'individus qu'ils interconnectent. Le réseau « workgroup » relie les postes du groupe de travail. Le réseau « intranet » regroupe les postes de l'organisation. Le réseau « extranet » regroupe les postes de la collectivité d'organisations.

Sur le poste de travail sont installés un navigateur, divers « clients » d'applications hébergées à distance sur des serveurs et une suite bureautique (traitement de texte, tableur, gestionnaire de fiches, etc.).

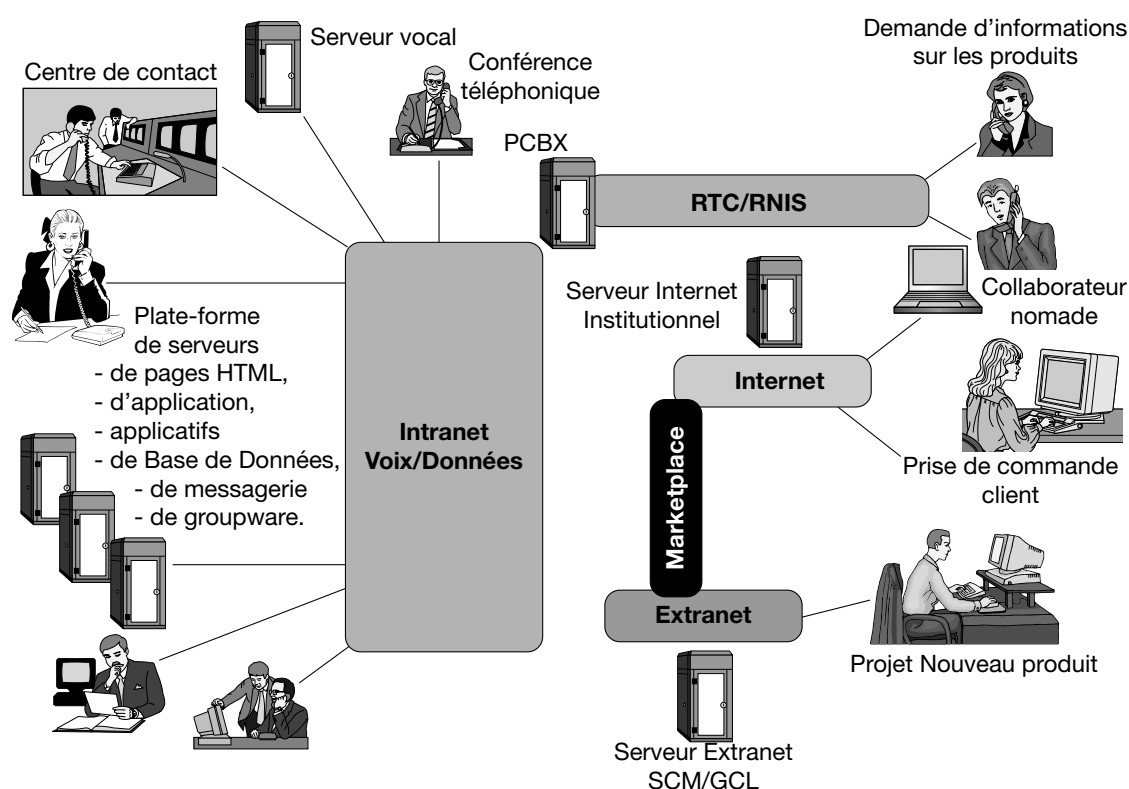
Sur les serveurs du groupe de travail, de l'organisation et de la collectivité d'organisations (extranet) sont installés des référentiels d'informations (sites « web intranet ») et des applications de gestion dialoguant avec les clients du poste de travail (ERP sur l'intranet, gestion de la chaîne logistique sur l'extranet).

Sur les serveurs de l'Internet sont installés aujourd'hui des référentiels d'informations (sites « web ») et demain des référentiels de services (« web services »).

Tout cet ensemble constitue **l'infrastructure**.

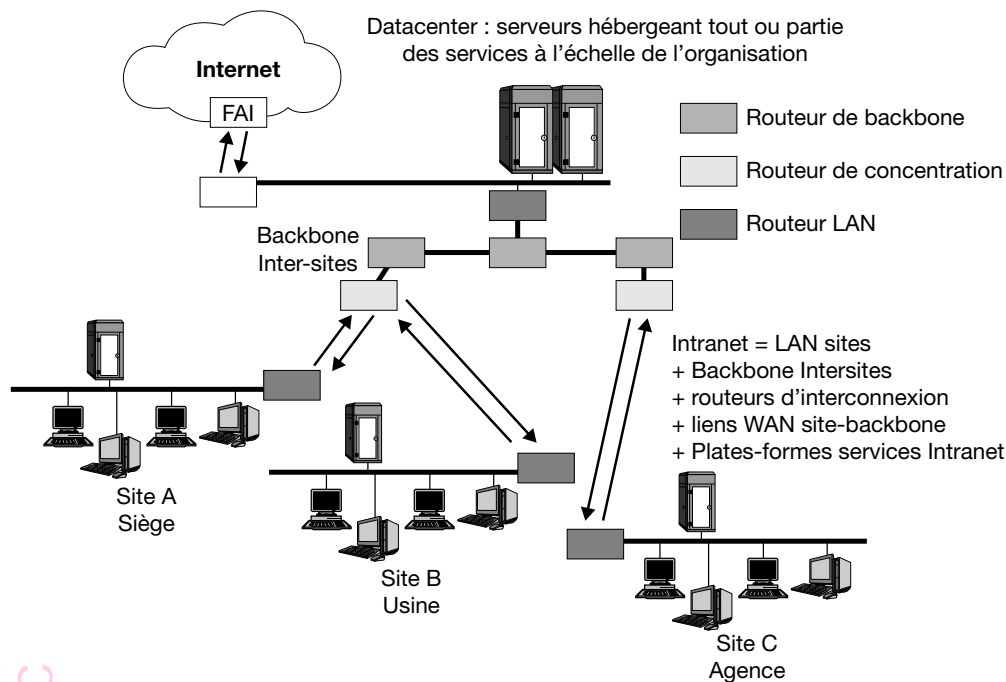
Au-delà des points spécifiques liés à chaque constructeur ou éditeur, il importe d'identifier les invariants et de dresser les contours généraux d'une infrastructure informatique. Au plus haut niveau, un schéma général basé sur la trilogie Internet/intranet/extranet, illustré par la figure 24, déjà rencontrée plus haut.

Figure 36 : Schéma général d'une infrastructure actuelle



Ce schéma général se précise par un ensemble de sites équipés de réseaux locaux, interconnectés entre eux par un *backbone*.

Figure 37 : Schéma général d'une infrastructure actuelle



Le centre informatique qui pilote cette infrastructure constitue un site à part, lui-même connecté au **backbone** par une artère à haut débit qui voit passer tous les flux. Ce centre est souvent désigné aujourd'hui en tant que **datacenter**.

Le datacenter est un centre de traitement considéré comme critique vis-à-vis de la continuité des affaires (*Business continuity*). Il comprend un contrôle sur l'environnement (climatisation, système de prévention contre l'incendie, etc.), une alimentation d'urgence et redondante, ainsi qu'une sécurité physique élevée.

Figure 38 : Le réseau, épine dorsale (*backbone*) de l'infrastructure

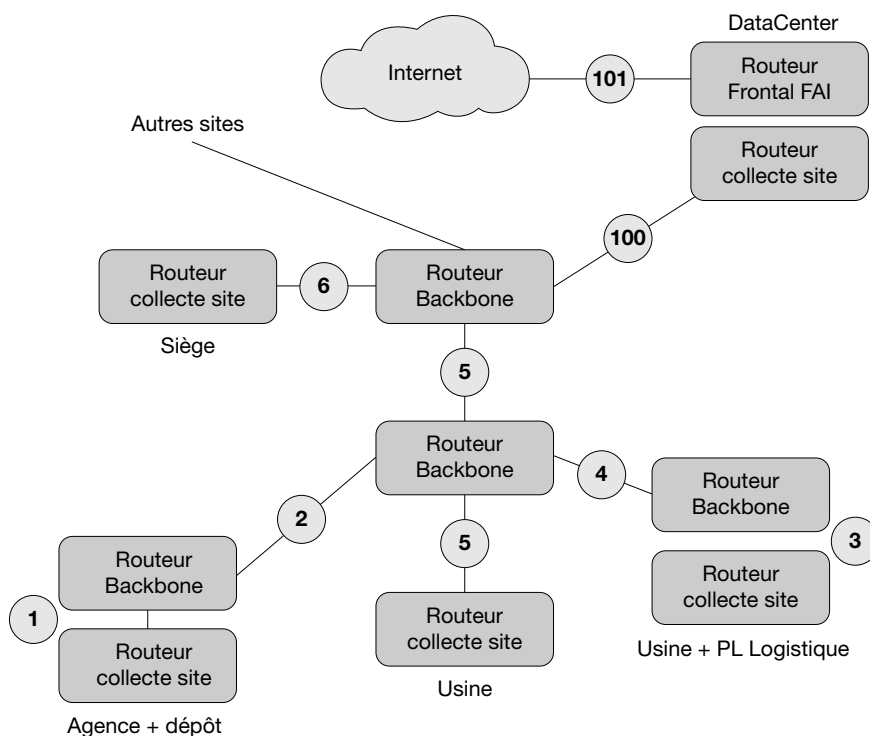
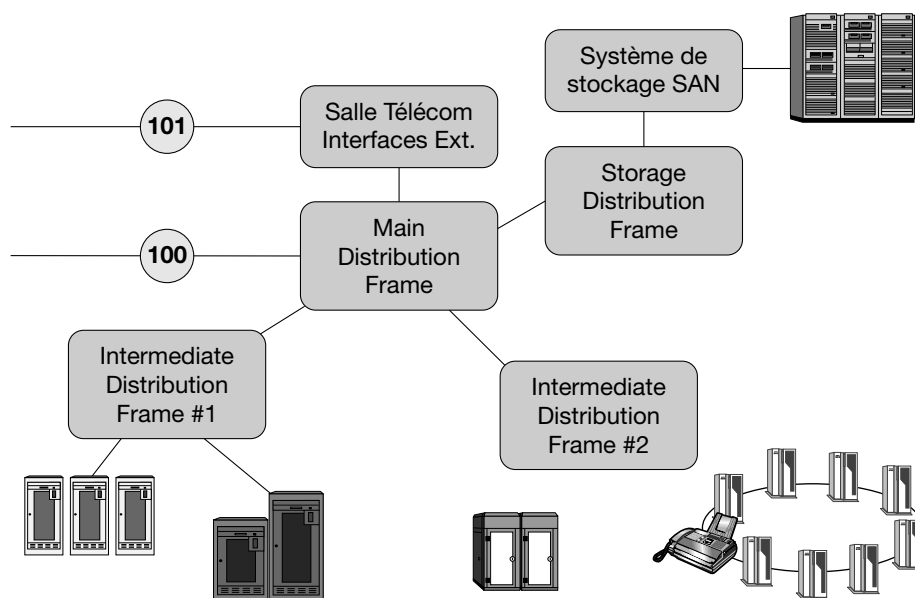


Figure 39 : Les composants du datacenter



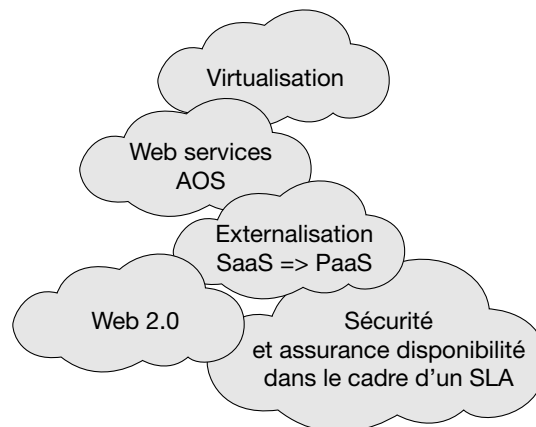
B. LE CLOUD COMPUTING

Littéralement « informatique en nuage », le *cloud computing* (CC) est une technique rendant possible l'utilisation des capacités de stockage et de traitement d'un groupe d'ordinateurs et de serveurs interconnectés. Elle apparaît comme particulièrement séduisante en ce qu'elle ouvre la possibilité de consommer les ressources informatiques comme l'on consomme l'eau ou l'électricité. Il s'agit en effet au travers de cette technologie de rendre possible l'accès pour des clients à des infrastructures collectives fournissant à la demande des services informatiques professionnels. Ceci suppose pour être viable, une très bonne bande passante pour l'accès et les communications entre les ordinateurs. En pratique, le CC fait référence à un nuage de machines accessibles par Internet et réparties dans le monde entier. Les utilisateurs du nuage peuvent donc en théorie disposer d'une puissance informatique considérable et modulable. En cela le CC présente certaines analogies avec le Grid (pour l'aspect technique de la mise en réseau de capacités de calcul) mais il s'en démarque fortement par l'ensemble des services associés.

On voit donc se dessiner derrière l'innovation technologique un véritable modèle économique. La flexibilité associée au CC est telle qu'elle permet de faire peser sur le prestataire l'interrogation sur le dimensionnement des infrastructures, et de passer de la possession de ressources à leur location. Le budget informatique en est clarifié par la signature de contrat d'abonnement avec des clauses de variabilité. L'inconnue principale de ce modèle repose sur les questions de confidentialité des données et la garantie contractuelle des niveaux de services. Par ailleurs le modèle économique du CC suppose le déplacement des expertises techniques vers les salles informatiques des prestataires, ce qui peut poser problème à terme pour les DSI des entreprises.

Les fournisseurs de services (de type « *Software as a service* » ou SAAS) s'orientent de plus en plus vers des offres globales avec proposition d'un système d'exploitation, de services d'infrastructure (stockage, authentification), d'applications professionnelles (CRM, PGI), d'outils de développement, voire de serveurs ou postes clients virtuels (« *Hardware as a service* » ou HAAS). Tout cela se marie facilement avec l'univers du Web 2.0 et les techniques de virtualisation. On parle alors de fournisseurs de plateforme ou « *Platform as a service* » (PAAS). Le premier problème que l'on rencontre actuellement sur ce type de solution est la grande hétérogénéité des propositions techniques qui se traduit par l'absence de portabilité d'une plateforme sur l'autre. Le deuxième est la timidité des engagements actuels des fournisseurs PAAS en termes de niveau de services (de type Service Level Agreement ou SLA) et des pénalités en cas de non-respect.

Figure 40 : Le cloud computing



Poussée à son terme, la logique économique du CC peut donc avoir pour conséquence l'externalisation totale du SI (Total Information Outsourcing). Dans ce cas, la clarté des coûts est parfaite et la charge du calcul de coût de possession (TCO) est déplacée chez le prestataire. Face au développement du CC, la Fondation pour une infrastructure informatique libre (FFII) recommande aux entreprises de s'assurer que leur fournisseur garantit l'accès intégral aux données, aux codes sources des applicatifs et n'entrave pas par ces pratiques la libre concurrence.

Le CC est le domaine des grands opérateurs. Si Amazon a été le premier à se lancer sur cette technologie et ce marché (avec S3 et EC2), il le partage maintenant avec des acteurs aussi importants que Google (Google 101), IBM (Blue Cloud) et Microsoft (Azure) entre autres.

En conclusion les caractéristiques principales du CC sont :

- des utilisateurs non propriétaires des serveurs ;
- des ressources consommées en fonction des besoins ;
- une absence de gestion par les utilisateurs de l'infrastructure sous-jacente ;
- des données et des applications délocalisées ;
- un accès aux services grâce à un simple navigateur.

LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises, et du mode de vie des citoyens. Les services qu'ils assurent nous sont tout aussi indispensables que l'approvisionnement en eau ou en électricité.

La croissance d'Internet a modifié considérablement la donne et conféré aux systèmes d'information une dimension incontournable au développement même de l'économie et de la société. C'est dire si la sécurité des systèmes d'information (SSI) est un enjeu à l'échelle de la nation tout entière.

Pour l'État, il s'agit d'un enjeu de souveraineté nationale. Il a, en effet, la responsabilité de garantir la sécurité de ses propres systèmes d'information, la continuité de fonctionnement des institutions et des infrastructures vitales pour les activités socio-économiques du pays, et la protection des entreprises et des citoyens.

De leur côté, les entreprises doivent protéger leur système d'information des dysfonctionnements et de la malveillance car il irrigue l'ensemble de leur patrimoine informationnel et supporte leur stratégie de développement, sans négliger le fait que leur responsabilité peut être mise en cause dans le cas d'utilisation abusive de données (nominatives, financières, etc.) qu'elles détiennent.

L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils ont renforcé la vulnérabilité des systèmes d'information.

Tous les utilisateurs sont sensibles à la menace constante des virus et des vers qui se propagent essentiellement par l'Internet, ciblant aussi bien les applications Web traditionnelles (sites Web statiques) que les applications Web 2.0 (réseaux sociaux, mondes virtuels, etc.). Le nombre de virus et vers a diminué au cours de ces dernières années, mais paradoxalement ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont aisément accessibles en ligne et il existe un échange constant d'information et de savoir-faire au sein des réseaux de pirates pour rendre ces attaques de plus en plus efficaces.

Susceptibles d'affecter un système d'information critique, les attaques ou les incidents majeurs pourraient avoir de graves répercussions, notamment sur les infrastructures qui fournissent des services à l'ensemble de la société civile.

Cependant, sécuriser les systèmes d'information requiert de mobiliser des ressources financières et humaines dont le retour sur investissement est souvent difficile à justifier. Les PME ont notamment du mal, du fait de leur faible taille, à disposer des ressources nécessaires.

Les entreprises attendent de l'État, des organisations professionnelles, mais aussi des entreprises de conseil (sociétés de services informatiques, cabinets d'expertise comptable, etc.) des services de support efficaces et accessibles, des préconisations de produits de sécurité, un soutien spécifique (notamment juridique) lorsqu'elles s'étendent au-delà des frontières nationales, des propositions de formation de leur personnel, etc.

Pour aborder la SSI de manière compréhensible et sans technicité excessive, nous proposons le plan suivant :

I. La protection des actifs

En premier lieu, il est nécessaire de comprendre ce qui est en jeu, c'est-à-dire quels actifs (au sens large du terme) sont éventuellement menacés. Ces actifs peuvent être composés de matériels, de logiciels, d'informations sensibles... mais aussi de savoir-faire, etc.

II. L'évaluation des risques

Une atteinte à la sécurité se traduit par un sinistre plus ou moins significatif. Dans ce contexte, il faut être capable de mesurer les conséquences d'une atteinte à un actif ou à un ensemble d'actifs. Cette démarche évaluative permet également de poser les bases d'une approche budgétaire de la mise en œuvre d'une politique de sécurité du système d'information (PSSI).

III. L'identification des menaces

L'environnement de l'entreprise évolue. Des menaces existent, qu'il est nécessaire d'identifier en s'appuyant sur des expertises reconnues (pouvoirs publics, organisations professionnelles, experts...) pour mettre en lumière les vulnérabilités existantes dans les systèmes d'information.

IV. La mise en œuvre d'une PSSI

La phase d'analyse et de réflexion terminée, il s'agit de passer à l'action, c'est-à-dire à la définition d'une PSSI et à sa mise en pratique au niveau opérationnel par toute une série de « contre-mesures » destinées à juguler les risques en réduisant les vulnérabilités et en assurant la continuité du fonctionnement du système d'information.

V. La sécurité opérationnelle

Cette section présente quelques aperçus techniques sur la protection des réseaux, serveurs et postes de travail, et sur la sauvegarde des données.

I. LA PROTECTION DES ACTIFS

La sécurité n'a de sens que par rapport à ce qu'on cherche à protéger. Le système d'information de l'entreprise est composé d'éléments matériels et immatériels. Les premiers sont en général bien recensés dans l'inventaire comptable de l'entreprise, mais pas toujours ! C'est donc un point préalable à vérifier. Le vol, la disparition ou le dommage à l'un de ces actifs devront être déclarés et justifiés par les personnels en charge de leur utilisation ou surveillance. Il faudra aussi étudier les polices d'assurance pour apprécier la pertinence du contrat.

Les biens immatériels composant le système d'information sont en général des logiciels. Certains sont inscrits à l'inventaire (les logiciels acquis). Pour ceux qui sont développés en interne, ce n'est pas toujours le cas, la procédure d'activation étant souvent jugée sans avantage économique et les commissaires aux comptes pas toujours très au faite de leur existence ou de leur importance dans la vie de l'entreprise.

En tout état de cause, les logiciels demandent une identification bien précise et une conservation sécurisée des codes sources (si disponibles), des supports originaux des éditeurs, des licences d'utilisation, des contrats de cessions de droits ou de maintenance, ou tout autre élément constitutif des droits possédés par l'entreprise sur les logiciels qu'elle utilise.

Les contenus des bases de données ou des fichiers ne sont généralement pas valorisés dans les actifs de l'entreprise, mais représentent parfois des valeurs vénales importantes susceptibles d'être valorisées à certaines occasions (cession ou fusion de l'entreprise, par exemple).

Les données concernant les clients, les contrats, les réponses aux appels d'offres, représentent souvent la valeur principale des entreprises, qui sont de plus en plus dépendantes des informations contenues dans leur « mémoire », constitutives de leur « savoir » et donc de leur capacité à « faire ».

L'importance de ces « actifs » est donc cruciale, et leur protection est impérative :

- de par la loi qui protège les informations nominatives (informatique et libertés) et rend responsable pénalement celui qui les détient sans protéger efficacement leur confidentialité ;
- de par la responsabilité du chef d'entreprise devant les propriétaires de l'entreprise ;
- de par la prise de conscience des salariés que leur emploi en dépend.

La prise en compte de la sensibilité de l'information

Dans certaines situations, la cible principale des convoitises est l'information, qu'il s'agisse de la manipuler ou de la détruire, de l'extraire ou d'en restreindre l'accès voire de la rendre inaccessible. La SSI a pour objet de proposer des solutions organisationnelles et/ou techniques susceptibles de protéger les informations les plus sensibles en priorité mais également les autres.

Les informations qui doivent demeurer confidentielles, c'est-à-dire celles qui doivent absolument être disponibles ou celles qui peuvent représenter un attrait pour une tierce partie, sont dites sensibles.

L'Afnor distingue trois types d'informations :

- « L'information aisément et licitement accessible » que certains appellent « l'information blanche » est ouverte à tous. Elle se trouve dans la presse, sur Internet, etc.
- « L'information licitement accessible mais caractérisée par des difficultés dans la connaissance de son existence et de son accès » est appelée « information grise ». Pour la trouver, il faut d'abord savoir la chercher ; les techniques de recherche à mettre en œuvre s'apparentent au renseignement.
- « L'information à diffusion restreinte et dont l'accès et l'usage sont expressément protégés. » On parle d'« information noire », habituellement protégée par un contrat ou une loi. Un nombre restreint de personnes est autorisé à y accéder.

Il est recommandé que les informations relevant de cette dernière catégorie reçoivent une mention rappelant leur sensibilité en considération de la gravité des conséquences qu'auraient leur divulgation, leur altération, leur indisponibilité ou leur destruction.

À cette fin, une distinction est opérée par deux mentions relativement au niveau de protection qu'il faut assurer à l'information : CONFIDENTIEL et DIFFUSION LIMITÉE.

Chacune de ces mentions de sensibilité peut être assortie d'une mention spécifique, caractéristique du domaine protégé : personnel (information nominative au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) ; professionnel (protégé par l'article 226-13 du Code pénal) ; industriel ; commercial ; nom d'une société ou d'un organisme ; noms de partenaires ; nom d'un programme.

La mention spécifique assure le cloisonnement de l'information en réservant son accès aux seules personnes ayant besoin de les connaître pour l'accomplissement de leur fonction ou de leur mission.

Après avoir défini le périmètre du système d'information de l'entreprise, il convient de mesurer les risques y relatifs.

II. L'ÉVALUATION DES RISQUES

A. GÉRER LE PARADOXE DE L'OUVERTURE ET DE LA PROTECTION

Le système d'information de l'entreprise est désormais déployé dans un contexte d'entreprise étendue permettant un travail en réseau avec ses partenaires (clients ou usagers, fournisseurs, donneurs d'ordre, administrations, etc.).

Ces échanges engendrent des vulnérabilités pour les systèmes d'information de l'entreprise vis-à-vis d'attaques potentielles contre lesquelles elle doit se protéger.

En outre, la généralisation des outils nomades (téléphones mobiles, PDA, ordinateurs portables, etc.) et le passage au tout numérique gommant progressivement la frontière entre espace professionnel et espace privé, accentuant très significativement les risques.

La sécurité n'est pas une fin en soi mais résulte toujours d'un compromis entre :

- un besoin de protection ;
- le besoin opérationnel qui prime sur la sécurité (coopérations, interconnexions, etc.) ;
- les fonctionnalités toujours plus tentantes offertes par les technologies (sans fil, VoIP, etc.) ;

- un besoin de mobilité (technologies mobiles) ;
- des ressources financières limitées ;
- des limitations techniques.

La gestion du risque et la SSI font partie d'une même démarche globale fondée sur l'identification des attaques potentielles, mais également sur l'idée qu'aucun système d'information n'est invulnérable. En effet, la sécurité repose sur des outils mais aussi sur le facteur humain ; concernant les outils :

- il n'est pas possible de se protéger à 100 % des codes malveillants (par exemple, les virus ou les chevaux de Troie) ;
- les algorithmes cryptographiques ne sont pas tous fiables ;
- les solutions de détection d'intrusion peuvent être trompées ;
- il n'est pas possible de tester les systèmes et les applications dans des délais raisonnables au regard de leur déploiement auprès des utilisateurs.

Concernant le facteur humain, la technique d'ingénierie sociale consiste à abuser de la crédulité (ou naïveté) de certains utilisateurs pour leur soutirer des informations confidentielles (par exemple, un mot de passe ou des renseignements permettant de préparer une attaque).

Néanmoins, la prise de conscience de l'impact des pertes possibles dues à un sinistre informatique est à mettre en balance avec les investissements souvent modestes qui pourraient protéger efficacement les actifs de l'entreprise. La loi de Pareto (ou loi des 80/20) est applicable à la gestion des risques informatiques ; dans ce contexte, elle postule que 80 % des risques peuvent être couverts par 20 % des investissements de sécurité.

B. QUANTIFIER LES PERTES DUES AUX SINISTRES

1. De nombreux incidents de sécurité identifiés dans les entreprises

Le rapport 2010 du Clusif, enquête intersectorielle auprès de 350 entreprises (200 à 499 salariés : 39,1 % ; 500 à 999 : 21,4 % ; 1 000 et plus : 39,4 %), met en évidence les principales menaces informatiques et pratiques de sécurité en France en passant en revue les onze thèmes de la norme ISO 27002. Cette étude révèle notamment que :

- le nombre d'incidents de sécurité augmente ;
- les facteurs déclenchants se répartissent comme suit : erreurs d'utilisation (dans 46 % des entreprises), perte de services essentiels (45 %), pannes d'origine interne (44 %), infection par virus (40 %), vol et disparition de matériel (37 %), erreurs de conception (24 %), événements naturels (9 %), intrusions (8 %), attaques logiques ciblées (6 %), accidents physiques (4 %), divulgations d'informations (4 %), sabotages physiques (4 %), actes de dénigrement ou d'atteinte à l'image (3 %), fraudes informatiques ou de télécommunications (3 %), actes de chantage ou extorsion informatique (0 %) ;
- 51 % des entreprises comprennent dorénavant une équipe chargée de collecter et traiter les incidents de sécurité du système d'information.

Il est à noter que la menace stratégique, par exemple d'espionnage industriel, n'apparaît jamais dans les enquêtes, sans doute pour des questions de confidentialité et d'image.

2. Des conséquences économiques importantes

Les incidents dus à une défaillance de la SSI peuvent affecter l'ensemble des activités et du patrimoine de l'entreprise, conduisant potentiellement à :

- des perturbations ou des interruptions des processus-clés de production de l'entreprise ;
- des pertes de parts de marché (vol de technologies, de bases clients/fournisseurs, etc.) ;
- des pertes financières directes :
 - coûts d'immobilisation des installations de production,
 - coût du temps passé à la restauration des systèmes,
 - coûts techniques de remplacement de matériels ou de logiciels, etc. ;
- une perte d'image et/ou de confiance des partenaires (clients, employés, etc.) ;

- des actions contentieuses ou de mise en responsabilité liées à la fraude informatique ;
- une remise en cause des assurances de perte d'activité.

De manière moins visible mais plus lourde de conséquences, les actions d'espionnage industriel, relayées parfois par des moyens étatiques, se traduisent pour les entreprises par une perte de substance ou de compétitivité, et au final par des incidences négatives sur l'emploi.

3. Des conséquences financières et sur l'emploi sous-évaluées

D'après une étude de l'institut américain en sécurité informatique CSI menée en 2009 en partenariat avec le FBI (*Federal Bureau of Investigation*), une société perdrait en moyenne 261 622 dollars par an consécutivement aux incidents de sécurité.

Mais la fiabilité de cette estimation est très relative car :

- de nombreux responsables de la sécurité des systèmes d'information (RSSI) ne connaissent pas le nombre d'attaques réussies survenues dans leur entreprise ;
- même concrétisées, les conséquences de ces incidents et leurs coûts demeurent difficiles à évaluer ;
- de nombreux incidents de sécurité sont tus par les entreprises pour des raisons évidentes de préservation de leur image.

S'agissant des pertes d'emplois, il n'existe pas de données statistiques permettant d'avoir une vision précise du phénomène.

4. Des protections encore insuffisantes

Selon le rapport 2010 du Clusif :

- 3 % (respectivement 5 %) des entreprises font un usage « partiel » de leur antivirus (respectivement de leur pare-feu) ;
- 54 % (respectivement 63 %) des entreprises n'utilisent pas ou ne connaissent pas les systèmes de détection (respectivement de prévention) d'intrusion ;
- 60 % des entreprises n'utilisent pas d'outil de chiffrement ; 33 % des entreprises n'ont pas de procédure formalisée de gestion de la continuité de l'activité ;
- 36 % des entreprises n'ont pas de procédure formalisée de déploiement de correctifs de sécurité ;
- 49 % des entreprises ne possèdent pas de cellule de collecte/traitement des incidents de sécurité.

Or, 99 % des entreprises sont fortement ou modérément dépendantes des systèmes d'information pour leur activité économique !

Ces éléments chiffrés montrent une bonne progression des entreprises en matière de SSI par rapport aux années précédentes, mais la perception des menaces pesant sur les systèmes d'information des entreprises reste encore insuffisante sur de nombreux points, en particulier dans les PME.

C. L'ANALYSE DES RISQUES

L'étape d'analyse des risques consiste à répertorier les différents risques encourus, à estimer leur probabilité de concrétisation et à étudier leur impact. La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait (par exemple, une attaque sur un serveur ou la détérioration de données vitales pour l'entreprise).

Sur cette base, il peut être intéressant d'établir un tableau des risques et de leur potentialité, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonnés selon un barème à définir, par exemple :

- sans objet (ou improbable) : la menace n'a pas lieu d'être ;
- faible : la menace a peu de chances de se concrétiser ;
- moyenne : la menace est réelle ;
- haute : la menace a de grandes chances de se concrétiser.

III. L'IDENTIFICATION DES MENACES

Le risque de sécurité est généralement caractérisé par l'équation (approximative) suivante :

Risque = menace × vulnérabilité × impact

De manière rigoureuse, on peut dire que le risque est fonction de trois facteurs : la menace, la vulnérabilité et l'impact. La menace représente le type d'action susceptible de nuire dans l'absolu, tandis que la vulnérabilité (appelée parfois faille, brèche ou trou de sécurité) représente le niveau d'exposition à la menace dans un contexte particulier. L'impact est le résultat de l'exploitation d'une vulnérabilité par une menace ; il se caractérise par les conséquences économiques, financières et sur l'emploi précédemment identifiées. En conséquence, le risque est d'autant plus élevé que les probabilités de menaces sur les actifs, les vulnérabilités et impacts potentiels sont importants.

Pour prévenir les menaces, l'entreprise peut mettre en place des contremesures. Celles-ci ne se résument pas uniquement à des solutions techniques, mais comprennent également des mesures de formation et de sensibilisation des utilisateurs, ainsi qu'un ensemble de règles et de procédures clairement définies.

Les sources de menaces effectives pesant sur les systèmes d'information sont de natures très variées, par exemple :

- l'utilisateur : il peut se retrouver face à une situation complexe à laquelle il n'a pas été préparé (tout individu ne disposant pas des connaissances et compétences d'un administrateur informatique). Un exemple typique de menace ciblant l'utilisateur est le *phishing*³⁰ ;
- les programmes malveillants : ces logiciels, destinés à nuire ou abuser des ressources du système d'information, sont installés sur celui-ci (par mégarde ou par malveillance), et ouvrent la porte à des intrusions ou modifient les données du système ;
- l'intrusion : situation dans laquelle une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès ;
- un sinistre : incident (vol, incendie, dégât des eaux, etc.) qui génère une perte matérielle et/ou de données.

La SSI fait partie intégrante de la sécurité globale de l'entreprise visant à se protéger des attaques :

- physiques : ces attaques (vols ou destructions, par exemple) visent les infrastructures physiques des systèmes d'information (telles que les câbles ou les ordinateurs) ;
- électroniques : il s'agit notamment de l'interception ou du brouillage des communications ;
- logicielles : ces attaques regroupent l'intrusion, l'exploration, l'altération, la destruction et la saturation des systèmes informatiques par des moyens logiciels ;
- humaines : l'homme est un acteur-clé du système d'information ; il constitue à ce titre une cible privilégiée et peut faire l'objet de manipulations (ingénierie sociale, corruption, etc.) ;
- organisationnelles : ici, l'attaquant cherche à exploiter les défauts de l'entreprise et de sa sécurité pour accéder à ses ressources sensibles. Ces attaques sont surtout mises en œuvre dans des contextes interorganisationnels (par exemple, l'attaque d'une entreprise pour en toucher une autre grâce à l'interconnexion de leurs réseaux).

Ces attaques diverses sont des éléments indissociables parfois utilisés simultanément pour mener une attaque sophistiquée (appelée attaque multi-étapes ou chaîne d'exploits), qu'il convient d'intégrer dans un plan de sécurité globale. Ne traiter qu'un seul de ces points pourrait être comparé à l'installation d'une porte blindée à l'entrée d'une maison dont les fenêtres sont ouvertes sur la rue.

30. Technique utilisée par les pirates en ligne, visant à usurper l'identité d'une personne ou d'une entité connue. Le principe est le suivant : un internaute reçoit un courriel non sollicité (*spam*) reprenant le logo et la charte graphique d'une entité connue (portail, banque, etc.). L'objectif est d'attirer l'internaute sur un site contrefait (ou site leurre) en lui demandant de mettre à jour ses informations personnelles (carte bancaire, numéro de téléphone, code d'accès, etc.). Ces informations, saisies dans un formulaire falsifié, sont ensuite utilisées à mauvais escient.

Pour sécuriser un système d'information, il est nécessaire d'identifier les menaces potentielles, et de connaître/prévoir la façon de procéder de l'ennemi. Il s'agit donc d'identifier les vulnérabilités afin de se défendre contre une intrusion.

A. LES MÉCANISMES DE L'INTRUSION

Le fait de s'introduire dans un système d'information sans y être autorisé tombe sous le coup du Code pénal (intrusions et « piratages » : articles 323-1 à -4 du Code pénal, ex-loi Godfrain).

Pour s'introduire dans un système d'information, l'intrus recherche dans un premier temps des failles, c'est-à-dire des vulnérabilités exploitables dans les protocoles, les systèmes d'exploitation, les applications voire le personnel de l'entreprise cible.

Une fois que l'intrus a établi une cartographie du système d'information, il est en mesure de mettre en application sa stratégie d'attaque. Un premier accès à une machine lui permet de récupérer d'autres informations et éventuellement d'étendre ses privilèges sur la machine. Son but ultime est d'accéder au niveau administrateur (*root*). L'intrus possède alors le plus haut niveau de droits sur la machine pour commettre son délit. La dernière étape pour l'intrus consiste à effacer ses traces afin d'éviter tout soupçon de la part de l'administrateur du réseau et de pouvoir garder le plus longtemps possible le contrôle des machines compromises.

En conclusion, pas d'intrusion sans faille de sécurité ; celles-ci peuvent être dues à la négligence des administrateurs du système, des « défauts » des logiciels utilisés, des imprudences des utilisateurs, etc.. Pour lutter sur le front des « défauts » des logiciels, encore faut-il en être informé et en connaître les remèdes. La question a été jugée suffisamment sérieuse pour que les gouvernements décident de créer des organismes chargés de centraliser ces informations et d'en assurer la diffusion auprès des RSSI des organisations publiques et privées.

L'action des CERT (*Computer Emergency Response Team*) en France est issue de cette volonté.

B. LES ORGANISMES DE SOUTIEN

1. Le réseau des CERT

Le Certe (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques, <http://www.certa.ssi.gouv.fr/>) a été créé en France en janvier 1999 afin de renforcer la protection des réseaux de l'État face aux risques informatiques, quelle qu'en soit l'origine.

Service du Premier ministre, rattaché à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au sein du Secrétariat général de la défense et de la sécurité nationale (SGDSN), le Certe est chargé d'assister les administrations dans la mise en place de moyens de protection et la résolution des incidents ou agressions informatiques dont ils sont victimes. Il participe au réseau mondial des CERT et constitue le complément indispensable aux actions préventives déjà assurées par l'ANSSI qui se situent plus en amont dans la démarche de sécurisation des systèmes d'information.

Afin de mener à bien ses missions, le Certe doit tout à la fois :

- assurer une veille technologique ;
- organiser la mise en place d'un réseau de confiance ;
- piloter la résolution des incidents (si besoin, en relation avec le réseau mondial des CERT).

Le Certe est relayé par d'autres CERT en France :

- **Renater**, Réseau national de télécommunications pour la technologie, l'enseignement et la recherche (<http://www.renater.fr/>), a été déployé au début des années 1990 pour fédérer les infrastructures de télécommunications pour la recherche et l'éducation. Afin de mener à bien cette action, le Groupement d'intérêt public Renater a été constitué en janvier 1993. Les organismes membres du Gip Renater sont de grands organismes de recherche tels que CEA, Cirad, Cnes, CNRS, Inra, Inria, Inserm, BRGM, Cemagref, IRD, ainsi que le Ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche. Pour information, c'est à travers Renater que le Cnam accède aux réseaux Internet.

La sécurité du réseau Renater est assurée par le CERT. En activité depuis 1995, le CERT Renater a pour rôle d'assister ses adhérents en matière de SSI, et notamment dans le domaine de la prévention, de la détection et de la résolution d'incidents de sécurité.

- Le **CERT-IST** (*Computer Emergency Response Team* - Industrie, Services et Tertiaire, <http://www.cert-ist.com/>) est une association de loi 1901 qui a pour vocation d'assurer à ses adhérents des services de prévention des risques et d'assistance au traitement des incidents. Le CERT-IST est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises françaises membres du FIRST et possédant un certain nombre de partenaires français et européens. Les activités principales du CERT-IST sont les traitements préventifs des risques et curatifs des incidents.

Sur le plan international, le Cerna est membre du FIRST (*Forum of Incident Response and Security Teams*) et participe à l'activité TF-CSIRT (*Computer Security Incident Response Team*) de coordination des CERT européens.

2. Le CLUSIF

Le Clusif (Club de la sécurité de l'information français, <http://www.clusif.asso.fr/>) est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie.

La finalité du Clusif est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques. Il entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion. Les groupes de travail traitent de thématiques variées en fonction de l'actualité et des besoins des membres : management des risques, droit, intelligence économique, etc.

Le Clusif a des relais régionaux, les Clusir, et des partenaires européens, les Clusi.

Le Clusif réalise, entre autres activités, une enquête annuelle sur l'état des lieux de la SSI dans les entreprises et les administrations françaises.



L'étude publiée en 2010 concernant l'année 2009 est disponible sur le site Internet du Clusif : <http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2010.pdf>.

3. Les autres organismes

Divers organismes publics et privés ont élaboré d'excellents guides à l'attention des entreprises.

Par exemple, l'**Ossir** (Observatoire de la sécurité des systèmes d'information et des réseaux, <http://www.ossir.org/>) est une association de loi 1901 existant depuis 1996 qui regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux.

HSC – Hervé Schauer Consultants (<http://www.hsc.fr/>) est un cabinet spécialisé dans la sécurité informatique et des réseaux.

IV. LA MISE EN PLACE D'UNE POLITIQUE SSI (PSSI)

La SSI fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité global du système est déterminé par le niveau de sécurité de son maillon le plus faible (rejoignant l'analogie de la porte blindée inutile dans un bâtiment si ses fenêtres sont ouvertes sur la rue).

Cela signifie que la sécurité doit être abordée dans un contexte global et prendre en compte tous les aspects suivants :

- la sécurité physique, c'est-à-dire la sécurité au niveau des infrastructures matérielles : lieux ouverts au public, espaces communs de l'entreprise, salles sécurisées, postes de travail des salariés, etc. ;
- la sécurité logique, c'est-à-dire la sécurité au niveau des données de l'entreprise, des applications et des systèmes d'exploitation ;

- la sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, accès, etc. ;
- la sensibilisation des utilisateurs aux problèmes de sécurité.

La diversité des questions soulevées et des réponses à y apporter en fonction des contingences (taille de l'entreprise, secteur d'activité, types de matériels et de logiciels informatiques, etc.) pourrait décourager d'aucuns. Quelles sont les priorités à dégager, les urgences à traiter ? Comment définir un programme d'investissement cohérent ? Et comment le faire avaliser par des directions d'entreprises qui n'ont pas forcément la « culture informatique » nécessaire pour appréhender les enjeux de la sécurité ?

Toutes ces questions, et bien d'autres encore, tout responsable SSI (RSSI) se les pose ! Heureusement, il existe des référentiels et des méthodes pour l'aider à y répondre et à convaincre sa direction générale de la pertinence de ses préconisations.

A. L'IMPÉRATIF D'UNE APPROCHE GLOBALE, SYSTÉMIQUE ET PRÉVENTIVE

La sécurité est certes liée à la fiabilité du système d'information, mais au-delà des équipements et des équipes en charge de la sécurisation, elle demande au dirigeant d'entreprise la mise en œuvre d'une réflexion globale sur la maîtrise des risques impliquant l'ensemble des personnels ainsi que des partenaires de l'entreprise sur le périmètre de ses activités.

Le déploiement de solutions de sécurité (produits, services) et des procédures associées doit s'inscrire dans une démarche préventive, les investissements nécessaires pour couvrir raisonnablement et efficacement les menaces potentielles étant en général sans commune mesure avec les conséquences d'une attaque majeure qui pourrait se traduire par des pertes économiques ou d'image considérables voire une perte d'indépendance ou une cessation d'activité.

1. Vers un référentiel commun de bonnes pratiques

Les pouvoirs publics, cabinets de conseil spécialisés en SSI, des SSII, des éditeurs de logiciels, des fournisseurs de matériels de sécurité, des organisations patronales, notamment le Medef, et des organismes privés et publics divers ont formalisé des recommandations convergentes pour une démarche de sécurisation des grandes entreprises et des PME/PMI. Dans son guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise (mai 2005), le Medef préconise dix actions :

- bâtir une PSSI ;
- connaître les législations, jurisprudences et usages en vigueur dans chaque pays où les activités s'exercent ;
- mettre en œuvre des moyens appropriés à la confidentialité des données ;
- mettre en œuvre des moyens de défense minimaux, y compris pour les connexions sans fil ;
- établir une barrière entre les données externes et internes ;
- sensibiliser et mobiliser les salariés par une charte d'utilisation, des campagnes régulières de formation et de sensibilisation ;
- mettre en œuvre un plan de sauvegarde ;
- alerter et activer les services compétents en cas de besoin ;
- gérer et maintenir la (ou les) PSSI.

2. À chaque entreprise, sa propre démarche d'implémentation

Si les entreprises sont toutes menacées, elles ne sont pas exposées au même niveau de risque. Il y a en effet des jeux de facteurs aggravants tels que :

- la taille de l'entreprise ;
- le déploiement international des implantations et des systèmes d'information ;
- la nature et la complexité des activités (nucléaire, défense, agroalimentaire, réseaux d'infrastructures, etc.) qui peuvent créer une attractivité pour des pirates, des terroristes, des concurrents voire des États ;
- la culture et l'expérience en matière de sécurité et de protection acquises par l'entreprise.

Chaque entreprise doit donc adapter sa démarche de sécurité à sa situation particulière.

B. DÉFINITION DE LA PSSI

La PSSI est le document de référence définissant les objectifs poursuivis par l'entreprise en matière de SSI et les moyens mis en œuvre pour les atteindre.

La PSSI édicte un certain nombre de règles, procédures et bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'entreprise.

L'élaboration d'un tel document doit nécessairement être menée comme un véritable projet, *i.e.* associant des représentants des utilisateurs et conduite au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous. Lorsque la rédaction de la PSSI est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner le maximum d'impact à la PSSI.

Il existe de nombreuses méthodes permettant de mettre au point une PSSI. Voici une liste non exhaustive des principales méthodes :

- **Mehari** (Méthode harmonisée d'analyse de risques, <http://www.clusif.asso.fr/fr/production/mehari/>) a été élaborée par la commission Méthodes du Clusif.

La méthode met à disposition des règles, modes de présentation et schémas de décision. Elle propose, au niveau d'une entreprise ou d'une activité, un plan de sécurité qui se traduit par un ensemble cohérent de mesures permettant de pallier au mieux les failles constatées et d'atteindre le niveau de sécurité répondant aux exigences des objectifs fixés.

- **Ebios** (Expression des besoins et identification des objectifs de sécurité, http://www.ssi.gouv.fr/site_article45.html) a été mise au point par l'ANSSI.

Depuis 2009, **la série de normes ISO 27000** est dédiée au management de la sécurité de l'information (de nombreuses normes sont encore en cours d'écriture). Les normes ISO 27001 et 27002 sont les deux principales normes de la série : la première décrit les exigences à satisfaire pour la mise en place d'un système de management de la SSI, et peut aboutir à plus long terme à une certification de l'entreprise ; la seconde (anciennement ISO 17799) constitue un guide de bonnes pratiques opérationnelles en matière de sécurité de l'information (en définissant onze domaines de SSI, abordant des aspects tant techniques qu'organisationnels, elle propose plus d'une centaine de mesures de sécurité).

Mais des freins et un manque de maturité s'opposent encore à la mise en œuvre d'une PSSI efficace dans les entreprises.

Selon une étude du cabinet Ernst & Young réalisée en 2005 auprès de 1 230 entreprises dans le monde dont 50 en France, les obstacles principaux à la mise en œuvre d'une PSSI efficace sont les suivants :

| Principaux obstacles à la mise en œuvre d'une PSSI efficace | Monde | France |
|--|-------|--------|
| Faible prise de conscience des utilisateurs | 45 % | 51 % |
| Rythme des évolutions informatiques | 31 % | 51 % |
| Limites ou contraintes budgétaires | 42 % | 49 % |
| Absence d'un processus formel de gestion de la SSI | 31 % | 45 % |
| Engagement et sensibilisation insuffisants ou inexistantes des cadres dirigeants | 30 % | 43 % |
| Communication inefficace avec les utilisateurs | 27 % | 40 % |
| Problème de cohérence entre les besoins en SSI et les objectifs métiers | 26 % | 37 % |
| Difficulté à justifier l'importance de la SSI | 35 % | 35 % |

Étude Ernst & Young.

Cette étude souligne par ailleurs les préoccupations majeures des grandes et moyennes entreprises, et met en évidence l'attitude particulière des entreprises françaises dans de nombreux domaines par rapport à leurs homologues étrangères :

- Un manque d'implication des directions générales.
La perception de l'importance de la sécurité par les directions générales reste faible. 90 % des RSSI considèrent que la SSI est directement liée à l'atteinte des objectifs généraux de l'entreprise mais seuls 20 % considèrent que la SSI est réellement une priorité de leur direction générale.
- Une prise en compte insuffisante des facteurs humains.

Seulement 49 % des entreprises françaises ont conscience des risques de complicité interne, contre 60 % au niveau mondial. Or, 35 % des incidents ayant provoqué un arrêt du système d'information ont pour origine la faute d'un salarié ou d'un ex-salarié. Dès lors, toute démarche efficace en matière de SSI doit s'accompagner d'un volet ressources humaines (sensibilisation, procédures, audits et contrôles).

Seules 20 % des entreprises françaises assurent à leurs salariés une formation régulière sur la sécurité et la maîtrise des risques, contre 47 % des entreprises dans le monde.

- Des freins organisationnels.

Peu d'entreprises, même parmi les plus importantes, ont une approche de sécurité globale dont la SSI serait un volet parmi d'autres. Si au plan mondial 85 % des RSSI jugent leur organisation de la SSI efficace par rapport aux besoins métiers, ils ne sont que 65 % à avoir cette opinion en France, et à peine un quart des responsables métiers sont capables d'apprécier la valeur ajoutée de la SSI à leurs activités.

Contrairement à leurs homologues étrangers, les RSSI français portent une attention accrue aux aspects technologiques et organisationnels, qui l'emportent sur l'efficacité opérationnelle. Il faut noter également la faible collaboration entre RSSI et auditeurs internes (en France 40 % des RSSI avouent n'avoir aucune coopération avec l'audit interne et seuls 29 % déclarent plus d'une coopération par an).

- L'intégration de la SSI dans le modèle culturel de l'entreprise demeure une exception.

Très peu d'entreprises ont intégré dans leur modèle culturel et leurs processus opérationnels la SSI comme une priorité stratégique, une fonction vitale pouvant s'imposer dans la prévention, la réaction ou le temps de crise à toutes autres considérations économiques, commerciales ou financières majeures.

- L'identification des données sensibles est insuffisante.

Certaines entreprises, par leurs activités, notamment liées à la Défense nationale, ont une pratique des données classifiées ou des données sensibles. D'autres entreprises se sont appuyées sur ces méthodologies afin d'identifier, de classer et de protéger de manière spécifique certaines informations sensibles.

Une réflexion préalable sur la nature des données sensibles de l'entreprise, au regard des menaces qui s'exercent sur elles, est indispensable. Or, dans l'étude menée, seuls 51 % des répondants français (contre 71 % au niveau mondial) ont répertorié les informations sensibles ou confidentielles de leur entreprise. Comment bien protéger quelque chose que l'on n'a pas identifié ?

- Le retour sur investissement en matière de SSI est difficile à justifier.

Pour de nombreux RSSI, la question du retour sur investissement n'est pas essentielle ou n'a pas nécessairement de sens. Cependant, les pertes financières consécutives à des attaques informatiques étant souvent difficiles à évaluer, peut-on et doit-on promettre aux directions générales un retour sur investissement concernant les dépenses en SSI ?

En ce sens, les rapports du Clusif des dernières années ont montré que, plus les dirigeants sont informés de leur responsabilité civile ou pénale, moins ils exigent de justifier une dépense en SSI par un rendement particulier. Ainsi, pour les RSSI, une justification essentielle des investissements en SSI est de se conformer aux réglementations (cet argument est plus avéré dans les grandes entreprises que dans les PME).

L'étude CSI/FBI de 2009 précise à ce sujet que le retour sur investissement est de plus en plus utilisé comme une métrique de sécurité (67,8 % des entreprises). Cependant, seules 44 % des entreprises ont pris en 2008 une assurance extérieure contre les risques de menaces informatiques ; les responsabilités civiles et pénales restent donc sous-estimées.

- Le budget SSI est souvent insuffisant.

Les RSSI considèrent que l'un des principaux obstacles à leur mission est la limitation des budgets notamment dans les PME/PMI (29,7 % contre 21,8 % dans les grandes entreprises). Selon le rapport 2010 du Clusif, le budget SSI représente plus de 6 % du budget informatique total pour 22 % des entreprises, de 3 à 6 % pour 16 % d'entre elles, de 1 à 3 % pour 15 % des entreprises, et moins de 1 % (ou non connu) pour 47 % des entreprises. La motivation à investir dans la SSI varie de manière considérable selon la taille de l'entreprise.

EXEMPLE

Bonne pratique : Le RSSI d'un grand groupe manufacturier est rattaché directement au PDG. Il anime et contrôle une structure transversale « sécurité » qui croise et s'impose à chaque grande unité opérationnelle ; cette structure matricielle est doublée d'une structure d'audit indépendante qui couvre également le domaine SSI. Le RSSI a tout pouvoir d'arrêter un dispositif opérationnel s'il juge que la PSSI n'est pas respectée, même si cette décision est susceptible de générer des pertes financières significatives.

C. LES QUALITÉS D'UN SYSTÈME D'INFORMATION SÉCURISÉ

La SSI repose sur plusieurs fondements. Pour rester dans une approche globale sans excès de technicité, on peut se rappeler l'acronyme « CIA » qui regroupe les trois qualités essentielles au maintien de la SSI, à savoir la confidentialité (*confidentiality*), l'intégrité (*integrity*) et la disponibilité (*availability*).

Les professionnels de la SSI ajoutent parfois à ces trois qualités de base, des objectifs complémentaires tels que l'authentification, l'autorisation, la non-répudiabilité, l'imputabilité ou encore la traçabilité.

1. Confidentialité

Alice envoie un message à Bob. Qu'est-ce qui garantit à Alice que personne d'autre que Bob n'a pu ou ne pourra consulter le message ?

La confidentialité regroupe tous les mécanismes permettant d'assurer qu'une information n'est accessible (et exploitable) que par les utilisateurs autorisés.

Ce principe peut être considéré de manière autonome, par exemple lorsque l'on traite de cryptographie sur un système de fichiers, ou de manière combinée au principe d'authentification.

2. Intégrité

Alice envoie un message à Bob. Qu'est-ce qui garantit à Bob que ce message n'a pas été modifié durant son acheminement ?

Le principe d'intégrité vise à assurer qu'une donnée est restée en l'état initial.

Des contrôles d'intégrité périodiques vérifient qu'une donnée n'a pas subi de modification ou de détérioration depuis le dernier contrôle.

3. Disponibilité

Alice envoie un message à Bob. Qu'est-ce qui garantit à Alice que Bob pourra consulter ce message dans les délais prévus ?

Le principe de disponibilité vise à fournir les données, les informations ou les services du système d'information lorsque les utilisateurs en ont besoin.

En clair : la disponibilité regroupe toutes les mesures visant à permettre un service sans interruption du système d'information ou, sinon, prévue et anticipée.

4. Authentification

Bob souhaite récupérer le message d'Alice. Comment peut-il prouver qu'il est bien Bob ?

L'authentification consiste à s'assurer qu'un utilisateur est celui qu'il prétend être.

Le principe d'authentification admet un sous-principe, l'identification, qui consiste à identifier un utilisateur de manière unique. L'identification permet donc de *connaître* l'identité d'une entité alors que l'authentification permet de *vérifier* cette identité.

Voici quelques exemples pour différencier l'identification de l'authentification :

- Système d'authentification « mot de passe » : vous insérez votre carte bancaire dans un distributeur de billets. La carte sert à identifier le client (et ses comptes) sur lequel le distributeur va effectuer les opérations. Le NIP (Numéro d'identification personnel, c'est-à-dire le code à quatre chiffres) vous permet de vous authentifier au distributeur : vous lui prouvez que vous êtes bien le titulaire de la carte.
- Système d'authentification « passeport » : votre carte d'identité porte votre nom. Elle vous identifie au sein du fichier de la population d'un pays. Sur votre carte d'identité se trouve votre photo. Lorsque vous montrez votre carte d'identité à une police des frontières, on vous identifie par votre nom et vous authentifier par deux facteurs : le fait que vous possédiez cette carte et le fait que vous soyez la personne représentée sur la photo. Bien évidemment, il est possible d'améliorer la fiabilité de l'authentification par d'autres méthodes (biométriques dans ce cas, comme l'empreinte digitale).

De manière générale, pour authentifier un utilisateur sur un système d'information, les critères utilisés peuvent être de trois types :

- la connaissance : information connue par l'utilisateur seul (mot de passe, code PIN, etc.) ;
- la possession : objet appartenant à l'utilisateur seul (carte à puce, token USB, etc.) ;
- la caractérisation : caractéristique physiologique ou comportementale spécifique à l'utilisateur (biométrie, signature).

Lorsqu'un seul de ces critères est utilisé, il s'agit d'une authentification faible (par exemple, le couple d'identifiants compte + mot de passe car seules des informations connues par l'utilisateur sont requises) ; on parle d'authentification forte lorsque deux de ces critères sont utilisés (par exemple, la lecture d'une carte à puce associée à la saisie d'un code PIN prend en compte les critères de possession et de connaissance).

5. Autorisation

Alice désire envoyer un message à Bob. A-t-elle le droit de le faire ?

L'autorisation (ou permission) consiste à déterminer si une opération est autorisée ou non par le système d'information. Le mécanisme d'autorisation doit normalement être en mesure de répondre aux questions suivantes :

- Quel acteur désire effectuer une opération ?
- Quelle opération souhaite-t-il effectuer ?
- A-t-il le droit d'effectuer cette opération, oui ou non ?

6. Non-répudiabilité

Bob a reçu un message d'Alice. Alice prétend qu'elle ne l'a pas envoyé. Qui a raison ?

Le principe de non-répudiabilité regroupe les mesures permettant d'affirmer avec certitude qui est l'auteur d'une opération.

Très utilisées dans le domaine boursier, les mesures de non-répudiabilité permettent par exemple d'empêcher que des opérateurs se dédient de leur acquisition (respectivement, de leur vente) en cas de chute (respectivement, de hausse) du cours.

Les mécanismes de non-répudiabilité sont également appréciés en audit (pour le fait de ne pas pouvoir nier que l'on a fait quelque chose) : « ça a eu lieu, c'est écrit ici », ou encore dans le cadre d'analyses statistiques, par exemple : « combien de personnes ont demandé telle ressource à telle date ? »

7. Imputabilité

Bob prétend n'avoir pas reçu le message d'Alice. Comment vérifier cette affirmation ? Et comment Alice peut-elle prouver qu'elle a bien envoyé le message ?

Conjuguant authentification et non-répudiabilité, le principe d'imputabilité permet de faire porter la responsabilité d'une action à un utilisateur.

Ce principe prend une place grandissante avec l'expansion du commerce électronique, notamment par l'utilisation de la signature électronique (voir section suivante).

8. Traçabilité

Alice a envoyé un message à Bob le 11 août à 18 heures 25 minutes et 8 secondes. Bob a consulté ce message 5 minutes plus tard, à savoir, le 11 août à 18 heures 30 minutes et 8 secondes précises. QUI a fait QUOI et QUAND ?

Le principe de traçabilité permet de répondre à cette question par un mécanisme de journalisation.

Les mécanismes de journalisation mettent en œuvre des techniques permettant de récupérer et stocker toutes les informations d'activité (ou événements) du système d'information de manière exploitable.

En conclusion de cette section, un système d'information ou une application, pour être considéré comme « sécurisé », doit au minimum disposer des qualités suivantes :

- empêcher la consultation de données par les personnes non-autorisées ;
- conserver et restituer les données dans l'état où elles ont été saisies ;
- fournir les données ou services requis lorsque les utilisateurs autorisés en ont besoin ;
- identifier et authentifier les utilisateurs sur le système d'information ;
- décider si une opération est autorisée pour un utilisateur identifié ;
- savoir de manière certaine quand, et par qui, a été effectuée une opération.

V. LA SÉCURITÉ OPÉRATIONNELLE

A. LA SÉCURITÉ DES RÉSEAUX

1. Les pare-feu

Les pare-feu (de l'anglais *firewall*) sont des dispositifs qui permettent de limiter, de filtrer, de séparer et d'analyser les entrées/sorties d'un réseau. Ils ont pour objectif principal de bloquer l'entrée sur un réseau interne lors d'une tentative d'attaque.

La fonction première d'un pare-feu est de réaliser un filtrage détaillé des sessions qui sont appelées à travers lui, en appliquant les règles d'état de connexion définies par l'administrateur. Pour ce faire, il utilise des filtres qui contrôlent les données en transit selon différents facteurs tels que l'identité de l'émetteur, la destination, le protocole utilisé, le contenu même des données, etc.

Il existe deux catégories de pare-feu : avec ou sans conservation des états de connexion. Les pare-feu avec conservation des états (ou à états) sont plus efficaces car ils vérifient la conformité des paquets de données analysés à une connexion en cours (en d'autres termes, ils vérifient la cohérence des échanges de données dans le cadre d'une session : ordre des paquets de données, réponse à une demande effective, etc.).

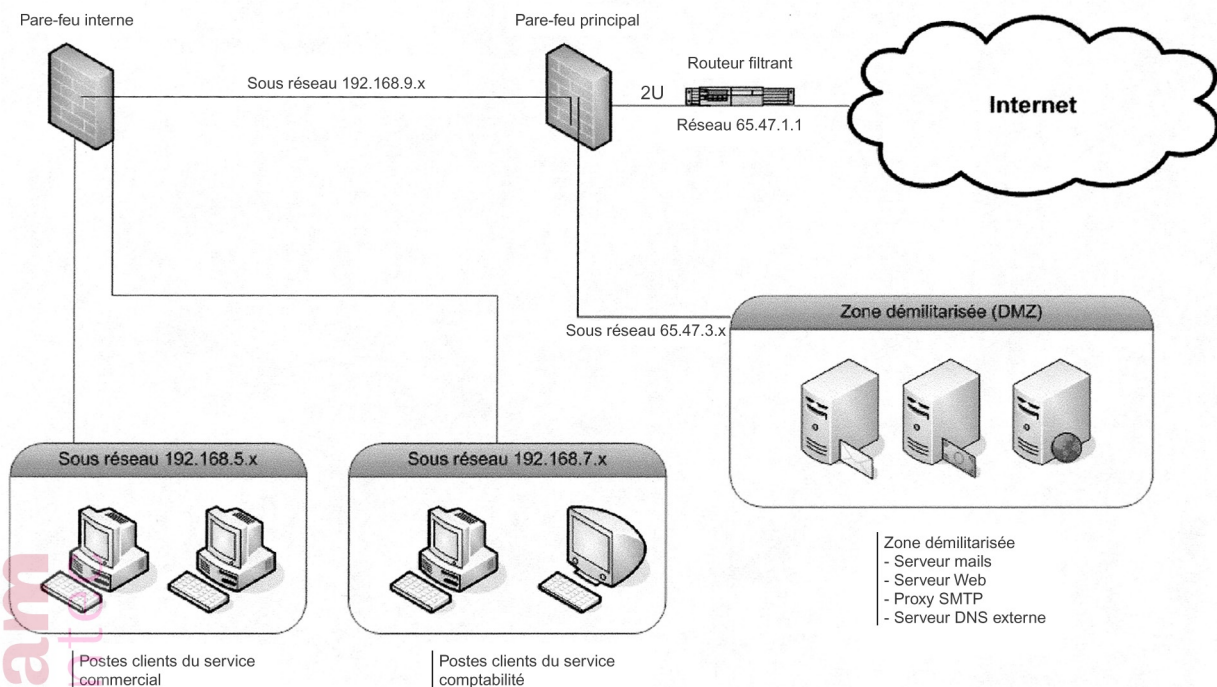
L'action d'un pare-feu touche donc différents points :

- restriction des accès sur une entrée précise ;
- restriction des sorties afin de limiter les émissions de données ;
- arrêt des agressions en cas d'attaque du réseau.

Un pare-feu est indispensable mais il ne constitue pas une protection sans faille. Lorsqu'un cambrioleur fracture une porte blindée, il a tout loisir de visiter tranquillement le local si le propriétaire n'a pas prévu d'autres dispositifs de protection. Il en est de même pour les pare-feu qui deviennent plus perméables du fait de l'évolution des protocoles réseau (ceux-ci visent toujours plus de souplesse, mais de ce fait offrent plus facilement une porte d'accès aux trafics malveillants).

Les pare-feu se présentent sous forme de logiciels spécialisés (par exemple, Check Point FireWall-1) et/ou de matériels (par exemple, CISCO Asa).

Figure 41 : Exemple d'architecture de réseau

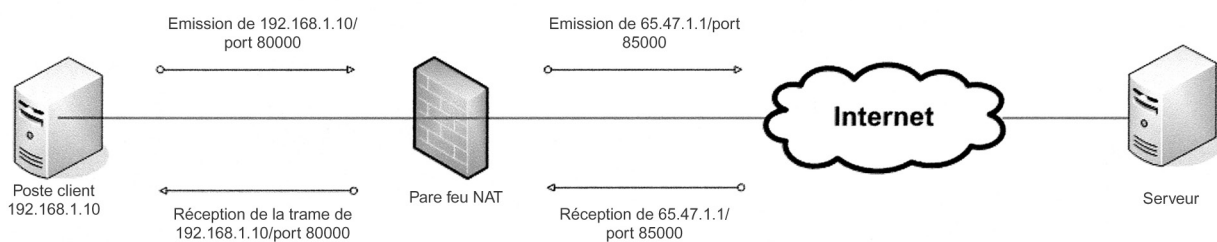


2. La translation d'adresses réseau (NAT)

Les pare-feu assurent souvent ce type de protection (*Network Address Translation*). Le principe est de masquer les adresses internes du réseau vis-à-vis de l'extérieur.

Le diagramme suivant explique le fonctionnement de la translation d'adresses :

Figure 42 : Principe du Nat



3. Les réseaux privés virtuels

Les réseaux privés virtuels (RPV, ou en anglais VPN pour *Virtual private network*) et le protocole IPSec (qui assure à la fois confidentialité, authentification et intégrité) fournissent un niveau de sécurité suffisant pour la plupart des transferts des entreprises.

Le RPV associe des algorithmes de cryptage à une technologie de tunnelisation (*tunneling*) de manière à établir une connexion sécurisée entre deux sites.

Une fois les deux interlocuteurs identifiés, il faut créer un « tunnel », c'est-à-dire un chemin logique entre les deux points à relier au sein du réseau.

B. LA SÉCURITÉ DES SERVEURS

1. La zone dématérialisée

Une architecture de sécurité à base de pare-feu conduit à dissocier les notions de zone militarisée et de zone démilitarisée (en anglais MZ et DMZ pour *Militarized Zone* et *Demilitarized Zone*).

La DMZ est une zone tampon, sorte de « no man's land » construit autour des systèmes d'information-clés de l'entreprise. Ceux-ci, par opposition, forment la MZ.

Les zones sont séparées les unes des autres par des pare-feu.

La DMZ contient les serveurs qui communiquent avec les zones de niveau de confiance inférieur, par exemple l'Internet. Aucune donnée ni application sensible n'est stockée ou exécutée dans cette zone.

Le contrôle d'accès système doit être le point de contention central du système d'information. L'idée générale est de mutualiser un maximum de fonctionnalités du système d'information en un point unique qui constituera le point de passage obligé entre les différentes zones du système d'information, y compris l'extérieur.

2. Les disques

La technique des « disques miroir », où l'information est écrite deux fois, augmente la sécurité, mais aussi le prix.

La recherche de la sécurité à moindre coût a conduit à la technologie RAID (*Redundant Array of Independent Disks*).

Il s'agit de répartir l'information sur un réseau de petits disques plutôt que sur une grosse unité, pour assurer une fiabilité complète et pour accélérer le processus en répartissant le travail entre plusieurs canaux et plusieurs têtes de lecture.

3. Les procédures

a. Désactivation des services superflus

Il est recommandé d'arrêter tous les services inutilisés sur le serveur. En effet, plus nombreux sont les services actifs, plus nombreux sont les risques d'intrusion.

De manière générale, il vaut mieux installer peu de services et les compléter au fur et à mesure des besoins, plutôt que d'en installer trop et devoir les retirer par la suite.

b. Administration des comptes utilisateurs

Dans un système sécurisé, chaque utilisateur doit disposer de son propre compte. Un mode d'organisation en groupes d'utilisateurs permet d'appliquer des règles de sécurité globales à une équipe, un service ou un ensemble d'utilisateurs souhaitant accéder aux mêmes ressources.

c. Administration des droits d'accès

Il faut attribuer aux comptes et groupes d'utilisateurs des droits d'accès à chaque répertoire ou fichier dont ils se servent.

Au moment d'attribuer ces droits d'accès, le principe des droits minimaux stipule que chaque utilisateur doit bénéficier uniquement des permissions nécessaires à son travail. Il est plus sûr d'assouplir des restrictions au fur et à mesure, que de supprimer des privilèges avec le temps.

d. Journalisation

Comme introduit dans la section précédente, la journalisation est le fait de garder une trace de tous les événements se produisant au sein d'un système donné. Ces informations sont regroupées dans un fichier accessible par l'administrateur ; ce dernier peut le consulter afin de détecter

des failles de sécurité, des échecs de connexion suspects, des tentatives de modification des droits d'accès de fichiers, etc.

e. Sauvegarde

La sauvegarde est un aspect fondamental de la sécurisation des serveurs. N'oublions pas que ceux-ci contiennent toutes les données de l'entreprise.

f. Vérification de l'intégrité des fichiers

Lorsqu'un pirate parvient à s'introduire dans un système d'information, il tente habituellement de remplacer certains fichiers par des chevaux de Troie ou de les infecter par des virus. Les RSSI doivent être capables de déceler rapidement les changements effectués sur un serveur compromis.

C. LA SÉCURITÉ DES POSTES DE TRAVAIL

Le piratage de serveurs devenant de plus en plus difficile, les attaquants se dirigent donc vers des cibles plus faciles : les postes clients.

De plus en plus de postes clients, contenant les identifiants et mots de passe de leurs utilisateurs, se connectent à distance à des réseaux d'entreprise. La prise de contrôle d'un tel poste permet l'accès à l'ensemble des applications et des fichiers utilisés par le titulaire du poste. Un seul poste client piraté suffit à court-circuiter toutes les barrières de protection d'un réseau d'entreprise (les pare-feu acceptant les connexions de ces postes).

Les versions récentes de Windows permettent l'enregistrement automatique de mots de passe. Cette pratique dangereuse permet à n'importe quelle personne ayant un accès physique à un ordinateur d'utiliser les ressources qu'il contient.

La sécurité des postes de travail passe donc souvent par la restriction des fonctionnalités, que ce soit au niveau des lecteurs de supports amovibles, sources d'infections (postes *diskless*, c'est-à-dire utilisant le serveur comme zone de stockage des programmes et des données), ou au niveau des systèmes d'exploitation.

Sous Windows, par exemple, si l'exécution des scripts n'est pas utile, mieux vaut retirer le *Windows Scripting Host*. Les postes seront ainsi immunisés contre les vers les plus courants. De même avec les navigateurs Internet : en neutralisant l'exécution de code (même signé), il est possible d'éviter bon nombre d'attaques communes ; même approche avec les macro-commandes des outils bureautiques.

Les mises à jour de sécurité disponibles, tant pour le système d'exploitation que pour les applications utilisées (Internet Explorer, Outlook, Office, etc.), doivent être installées par les administrateurs.

De même, l'installation d'un antivirus est indispensable, sa mise à jour, l'analyse régulière du système ainsi que de l'ensemble des documents téléchargés (courriers, fichiers, pages Web), sont indispensables.

La limitation des logiciels clients à une liste de logiciels autorisés contribue aussi à l'amélioration de la SSI.

D. LA SAUVEGARDE

La sauvegarde est une copie des données permettant une récupération en cas d'incident sur les systèmes utilisant ces données. C'est un pilier essentiel de la PSSI, quelle que soit la taille de l'entreprise, à partir du moment où les informations vitales sont stockées sous forme électronique.

1. Les risques de perte de données

Il n'est pas indispensable d'imaginer le pire, mais il est néanmoins rationnel de prendre en compte toutes les éventualités pouvant conduire à la perte partielle ou totale, temporaire ou définitive, des informations stockées sur les disques ou baies de disques du système d'information. Voici quelques exemples de risques susceptibles d'affecter un système d'information :

- dysfonctionnement du réseau électrique général ;
- virus ;
- dommages matériels (incendie, inondation, etc.) ;
- suppression accidentelle de fichier ;
- écrasement ou modification d'informations à mauvais escient ;
- vol de matériel ;
- erreurs dans le traitement des données, etc. (*liste non limitative*)

2. Les méthodes de sauvegarde

Pour mettre les données à l'abri, il est possible de faire appel à un prestataire spécialisé dans le domaine de la sauvegarde. Mais d'autres possibilités existent, notamment avec l'utilisation de supports spécifiques. En outre, pour ne pas entraver l'activité de l'entreprise, il convient d'effectuer l'opération de sauvegarde pendant la nuit et, bien sûr, de l'automatiser.

Traditionnellement, les sauvegardes utilisent des supports de type bandes ou cartouches (cassettes) magnétiques qui sont régulièrement réécrites (chaque jour, semaine, mois ou trimestre).

De petite taille, elles offrent pourtant une capacité de plusieurs dizaines de Go et une longévité beaucoup plus importante que les supports optiques.

Les cartouches se présentent sous une multitude de formats différents, en fonction des besoins (petits serveurs à grosses architectures).

La fréquence des sauvegardes est fonction du caractère critique et du volume des données modifiées par période.

Conserver les supports de sauvegarde dans un lieu différent de l'entreprise est recommandé, ainsi, en cas de sinistre ou de vol, les données seront épargnées.

REMARQUE

Ne pas confondre la sauvegarde avec l'archivage qui consiste à déplacer des données qui ne sont plus utilisées régulièrement, sur un support amovible pour gagner de la place et s'organiser. On utilise en général pour l'archivage des supports directement lisibles tels que CD-ROM, DVD, etc.

3. L'utilitaire de sauvegarde de Windows

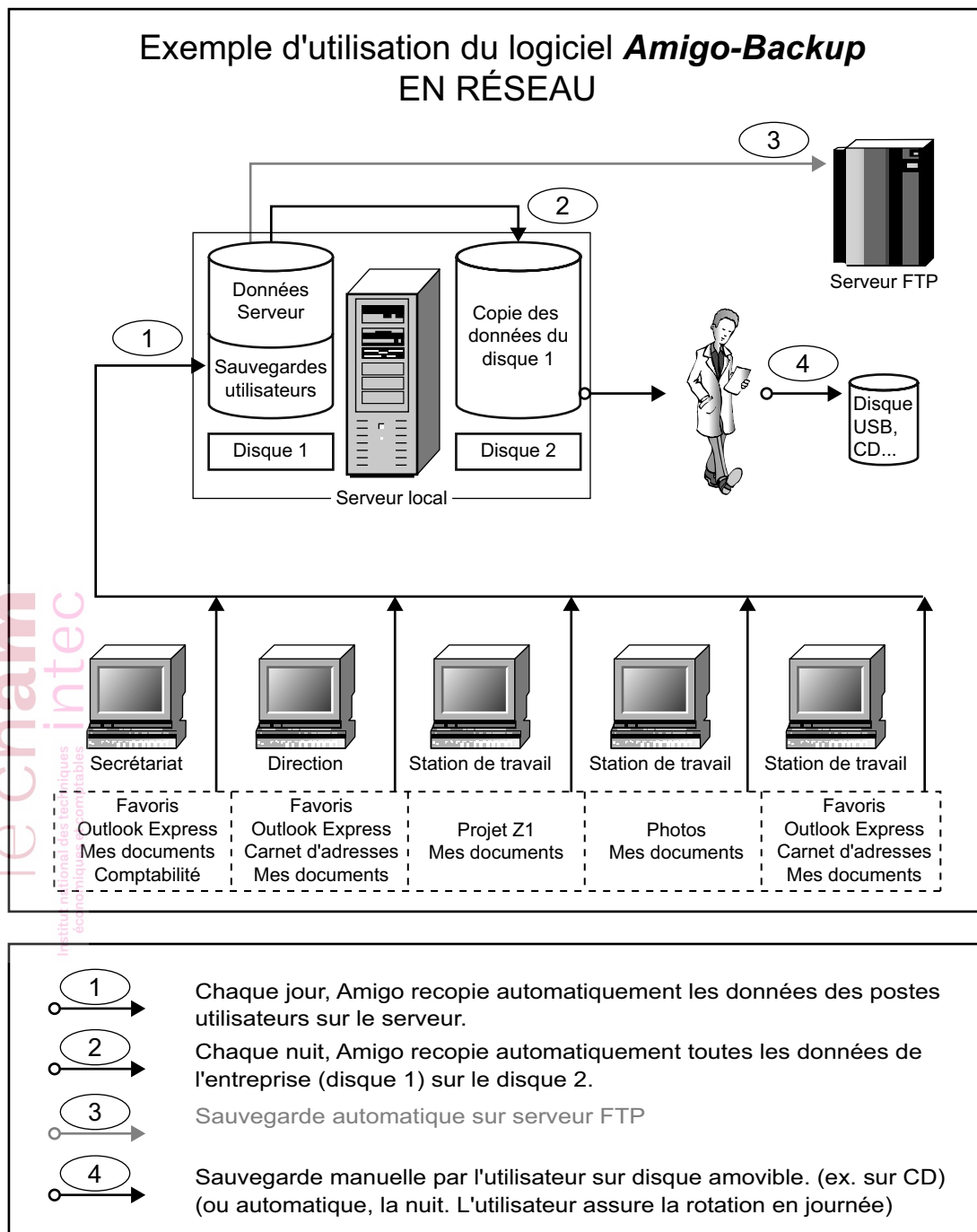
Depuis sa version 2000, Windows propose un utilitaire de sauvegarde efficace pour protéger les données. Celui-ci crée une copie exacte du contenu du disque dur (y compris des fichiers ouverts et en cours d'utilisation par le système) à un moment précis.

Un fichier de sauvegarde peut être enregistré sur un disque dur, une disquette ou tout autre support fixe ou amovible permettant l'enregistrement d'un fichier.

Un assistant permet de récupérer le contenu de la sauvegarde en cas de besoin.

Pour disposer de fonctionnalités plus évoluées, il est recommandé de se tourner vers des éditeurs qui proposent des offres adaptées aux besoins.

Figure 43 : Exemple de la solution de l'éditeur Amigo (pour petites structures)



Les phases 1, 2 et 3 protègent l'entreprise automatiquement, en recopiant chaque jour les données à d'autres emplacements du réseau. Si le disque 1 ou 2 du serveur, ou celui d'une station, tombe en panne, il reste toujours une copie des données (les pannes de disque dur représentent le risque le plus important de perte d'informations).

La phase 3 : en utilisant le protocole FTP (*File Transfer Protocol*) il est possible de copier le fichier de la sauvegarde sur un serveur distant à travers le réseau Internet. Ce serveur peut, par exemple, être celui d'un prestataire spécialisé dans les sauvegardes pour garantir une meilleure protection des données.

La phase 4, par l'intervention d'un utilisateur, protège des risques de virus, malveillance, incendie ou vol.

Il existe désormais des disques durs externes USB, Firewire ou Sata à des prix modiques : de 8 Go (env. 90 euros) à 2 To (env. 140 euros) pour des formats de disque de 1" à 3,5". Vitesse, fiabilité, aucune dépense de consommables !

Autres bonnes solutions :

- la clé USB de capacité atteignant les 256 Go à ce jour pour env. 700 euros ;
- les cartes mémoire (Compact Flash, SD, SDHC, SDXC, MicroSD, etc.) allant jusqu'à 64 Go pour env. 200 euros (le standard SDXC permettra d'aller jusqu'à 2 To dans un futur proche).

4. Critères d'appréciation des solutions logicielles et matérielles

Les solutions de sauvegarde sont nombreuses et reposent sur des techniques sensiblement différentes.

Le choix d'une technique de sauvegarde se fera en prenant en compte :

- la capacité de stockage du support (le volume d'informations) ;
- la vitesse de sauvegarde ;
- la fiabilité du support (notamment après une longue période de stockage) ;
- la simplicité de classement ;
- la facilité à restaurer les données ;
- et bien sûr le coût de l'ensemble.

Intervient également la possibilité de sélectionner les données à sauvegarder. Enfin, pour les grands systèmes de sauvegarde, il faut tenir compte de critères physiques : volume physique des supports de stockage, poids, sensibilité à la température, à l'humidité, à la poussière, à la lumière, etc.

5. Sauvegarde totale, différentielle ou incrémentale ?

Pour des serveurs, même de moyenne importance, les volumes de données à sauvegarder peuvent excéder les capacités des supports physiques amovibles utilisés (cartouches ou DVD-ROM) ou la durée impartie à l'opération (la nuit). La sauvegarde totale est alors réalisée selon une périodicité plus éloignée. Entre deux sauvegardes totales sont effectuées des sauvegardes incrémentales ou différentielles. L'idée est de copier seulement les éléments nouveaux ou ayant été modifiés depuis la dernière sauvegarde.

Dans la sauvegarde incrémentale, ne sont copiés que les éléments modifiés depuis la dernière sauvegarde incrémentale.

Dans la sauvegarde différentielle, ne sont copiés que les éléments modifiés depuis la dernière sauvegarde totale.

La différence est importante car en cas de restauration des fichiers, dans le premier cas (incrémental) il faudra repartir de la dernière sauvegarde totale, puis ajouter dans l'ordre toutes les sauvegardes incrémentales réalisées pour obtenir une restauration satisfaisante. Dans le second cas (différentiel), il suffira de disposer de la sauvegarde totale et de la dernière sauvegarde différentielle pour aboutir au même résultat.

Il est à noter que ces méthodes doivent être combinées avec le versionnage (*versioning*) qui est le processus permettant d'enregistrer les instances (différentes versions) d'un fichier chaque fois qu'il est enregistré. De la sorte, il est possible de récupérer une version précédente d'un fichier, ce qui peut être fort utile en cas d'attaque virale ou de corruption de fichier suite à un incident sur le disque dur.

Le choix entre les méthodes sera conditionné par les volumes à traiter et les contraintes techniques des supports.

6. Le recours à un prestataire extérieur

Le développement de l'ADSL a popularisé les offres de sauvegarde sur Internet pour des petites structures qui n'ont pas en interne les compétences pour assurer des sauvegardes dans les « règles de l'art ». Les avantages sont multiples :

- minimisation du risque de perte des données puisque le site est géré par un professionnel qui fait lui-même des sauvegardes avec du matériel adapté et dans un environnement protégé ;
- accès aux données à partir de n'importe quel ordinateur connecté à l'Internet ;
- souvent le coût de cette prestation est modique, parfois même gratuit pour les petites sauvegardes.

L'inconvénient majeur réside dans le fait de laisser ses données à disposition d'un tiers qui pourrait les consulter, les modifier ou en faire commerce, ce qui, reconnaissons-le, est peu vraisemblable mais reste inquiétant pour l'entreprise soumise à des obligations légales de confidentialité. Le risque d'indisponibilité des données qui deviendraient indisponibles (cas d'une faillite, d'un rachat du site par un concurrent, ou différend commercial avec l'hébergeur) est aussi peu rassurant. Évidemment, des dispositions contractuelles ou la notoriété de l'hébergeur viennent mitiger ces risques. En tout état de cause, il est indispensable d'exiger une garantie de confidentialité des données par le recours à leur chiffrement, ainsi l'hébergeur ou quiconque qui intercepterait les fichiers serait dans l'incapacité de les lire en clair. Pour un professionnel, expert-comptable, commissaire aux comptes ou avocat, c'est un critère impératif à imposer.

Un autre inconvénient vient de restrictions contractuelles sur le stockage ou la récupération des données : pour maîtriser l'usage de ses disques et de sa bande passante, un hébergeur peut limiter contractuellement l'entreprise à un volume de stockage ou de données consultées au-delà duquel il bloquera l'accès aux données. En général, ce souci s'élimine en choisissant un prestataire sur la base d'une tarification réaliste des flux et des volumes stockés. La concurrence est vive sur ce marché et les prix sont plutôt en chute libre ; ces deux facteurs devraient faciliter le choix du prestataire.

E. LA SIGNATURE ÉLECTRONIQUE

Le passage à l'« économie numérique » est souvent présenté comme le devenir de nos sociétés. Les échanges d'information entre les personnes, au sein des entreprises comme vers l'extérieur, reposent de plus en plus sur des documents au format numérique dit « dématérialisé ». Néanmoins, les contraintes de sécurité viennent freiner ces usages, soit par le refus du risque encouru en cas de mauvais usage, soit par les difficultés matérielles induites par des procédures mal maîtrisées, soit enfin par les coûts de la mise en œuvre de la SSI.

Or, les enjeux des échanges de documents numériques sont décisifs :

- engendrer des gains de productivité ;
- permettre une communication interpersonnelle plus fluide et plus réactive avec pour objectif d'aller vers un usage des outils collaboratifs de partage des connaissances et des savoir-faire ;
- favoriser le passage d'une culture papier à une culture numérique pour les échanges de documents à valeur juridique (relations clients-fournisseurs, entre professionnels, avec les administrations, etc.).

Pour toutes ces raisons, est très vite apparue la nécessité de créer un environnement technique et juridique de confiance dans les échanges numériques.

1. L'approche juridique

Sur le plan juridique, un imposant arsenal a été élaboré depuis dix ans. La directive du 13 décembre 1999 du Parlement européen définit un cadre communautaire pour les signatures électroniques.

Son objectif, rappelé dans l'article 1^{er} de la directive, est de :

« Faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique. Elle institue un cadre pour les signatures et certains services de certification afin de garantir le bon fonctionnement du marché intérieur. »

La transposition française de cette directive s'est effectuée en plusieurs étapes par :

- **la loi n° 2000-230 du 13 mars 2000** portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ;
- **le décret n° 2001-272 du 30 mars 2001** pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, modifié par le décret n° 2002-535 du 18 avril 2002 ;
- **le décret n° 2002-535 du 18 avril 2002** relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- **la loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique, notamment son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés ;
- **l'arrêté du 26 juillet 2004** relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation ;
- **la loi n° 2004-801 du 6 août 2004** relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui transpose dans son article 5 l'article 8 de la directive relatif à la protection des données (nouvel article 33 dans la loi du 6 janvier 1978 modifiée).

Plusieurs décrets et ordonnances ont ensuite étendu le champ d'application de cette directive à divers domaines professionnels :

- **le décret n° 2004-1397 du 23 décembre 2004** relatif à la carte de professionnel de santé et modifiant le code de la Sécurité sociale ;
- **le décret n° 2005-77 du 1^{er} février 2005** modifiant le décret n° 84-406 du 30 mai 1984 relatif au registre du commerce et des sociétés et le décret n° 58-1345 du 23 décembre 1958 relatif aux agents commerciaux ;
- **le décret n° 2005-973 du 10 août 2005** modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires ;
- **l'ordonnance n° 2005-1516 du 8 décembre 2005** relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives ;
- **le décret n° 2007-284 du 2 mars 2007** fixant les modalités d'élaboration, d'approbation, de modification et de publication du référentiel général d'interopérabilité ;
- **le décret n° 2009-1150 du 25 septembre 2009** relatif aux informations figurant au registre du commerce et des sociétés ;
- **le décret n° 2010-112 du 2 février 2010** pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives ;
- **le décret n° 2010-434 du 29 avril 2010** relatif à la communication par voie électronique en matière de procédure civile.

a. La modification du Code civil

La modification principale est l'insertion de l'article 1316-4 dans le Code civil par l'article 4 de la loi n° 2000-230 du 13 mars 2000.

Ainsi, le premier alinéa de l'article 1316-4 du Code civil définit la signature comme suit :

« La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. »

Le deuxième alinéa de l'article 1316-4 définit plus particulièrement la signature électronique, posant ainsi l'équivalence entre la signature électronique et la signature manuscrite sous certaines conditions :

« Lorsqu'elle [la signature] est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. »

Dès lors, toutes les signatures électroniques sont recevables en justice à partir du moment où elles assurent, à l'aide d'un procédé fiable, l'identification du signataire et la garantie de l'intégrité de l'acte signé.

Sous certaines conditions, la fiabilité du procédé de signature électronique est présumée :

« La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées en Conseil d'État. »

b. Effets juridiques de la signature électronique

La loi prévoit donc deux niveaux de validité juridique pour les signatures électroniques, dont les caractéristiques sont définies dans le décret 2001-272 du 30 mars 2001 :

- La signature électronique « simple » : à ce niveau, le procédé de signature électronique n'est pas présumé fiable mais l'écrit signé sous forme électronique ne pourra être refusé en justice au titre de preuve dès lors que le procédé permet d'identifier le signataire et de garantir le lien avec l'acte signé. En cas de contestation, il est nécessaire de prouver la fiabilité du procédé de signature électronique utilisé. Dans la pratique, cela suffit si l'utilisation du système de signature est conforme aux « règles de l'art ».
- La signature électronique « présumée fiable » : l'article 4 de la loi 2000-230 du 13 mars 2000 précise que la charge de la preuve peut être inversée, en cas de contestation, sous certaines conditions définies par décret. Or, étant donné la complexité du dispositif organisé par le décret n° 2001-272 du 30 mars 2001, renforcé par le décret n° 2002-535 du 18 avril 2002 et par l'arrêté du 26 juillet 2004, les praticiens se sont contentés d'implémenter la signature « simple » de premier niveau, laissant la signature « présumée fiable » dans les limbes.

2. La confiance dans les échanges numériques

Les mots-clés de cette confiance sont :

- intégrité des données stockées ou transmises ;
- authentification des entités participant à la communication ;
- confidentialité des données et de l'échange.

a. Intégrité des données

Ensemble de moyens et techniques permettant de vérifier ou de prouver la non-altération d'un ensemble de données (cela peut être un document, une image, un programme informatique, etc.).

- technique traditionnelle : comparaison entre l'original et la copie du document ;
- technique informatique : comparaison octet par octet des deux fichiers, l'intégrité sera respectée si aucune différence n'est constatée.

Mais comment faire si on ne dispose pas de l'original ? Des clés et empreintes sont alors utilisées.

Qu'est-ce qu'une clé ? Une clé est une valeur numérique unique qui, appliquée à une suite de caractères (chiffres, lettres, etc.) suivant une méthode mathématique précise (on utilise le terme d'algorithme), donne un résultat appelé « empreinte ». L'idée est d'appliquer la clé sur le document initial, d'obtenir l'empreinte, et de transmettre le document et l'empreinte au destinataire. Ce dernier, en possession de la clé et de la méthode, doit retrouver l'empreinte transmise avec le document pour être certain de son intégrité.

Un exemple simple est le nombre à 2 chiffres associé au numéro d'identification dit « numéro de Sécurité sociale » qui permet de détecter un numéro invalide (le numéro en lui-même comporte 13 chiffres et la clé 2). De même, des clés sont associées aux numéros de comptes bancaires. Il est à noter que le vocabulaire utilisé par ces organismes nomme « clé » ce que nous avons appelé « empreinte » ! Mais l'idée reste la même.

L'utilité d'un contrôle d'intégrité des données avec une clé est évidente.

La validation d'un fichier de numéros de Sécurité sociale (NIR : Numéro d'inscription au registre) par la clé permet de réduire le temps consacré à la vérification d'une base de données.

EXEMPLE

La clé de contrôle du NIR est un nombre à 2 chiffres dont la valeur est le complément à 97 du reste de la division du nombre formé par le NIR par 97 (une adaptation est prévue pour les départements corses 2A et 2B). Soit le numéro 2 64 03 99 001 087, sa clé (au sens courant) est 36. En fait, il faudrait dire que la clé est 97 et l'empreinte 36.

Une fois effectuée cette vérification qui met en évidence les erreurs, il suffit de corriger les quelques fiches erronées pour être sûr de l'intégrité des données d'un fichier. Attention, intégrité dans cette acception ne veut pas dire pertinence ou sincérité. D'autres erreurs peuvent exister : substitutions de numéros, fausses déclarations, etc.

b. Authentification des entités

Pour rappel, l'authentification est la procédure qui consiste, pour un système d'information, à vérifier l'identité d'une entité (personne, ordinateur, etc.), afin d'autoriser son accès à des ressources (systèmes, réseaux, applications, etc.). L'authentification permet donc de valider l'authenticité de l'entité en question.

L'authentification peut inclure une phase d'identification, au cours de laquelle l'entité indique son identité. Cependant, cela n'est pas obligatoire ; en effet, des entités peuvent être munies de droits d'accès tout en restant anonymes.

c. Confidentialité des données et de l'échange

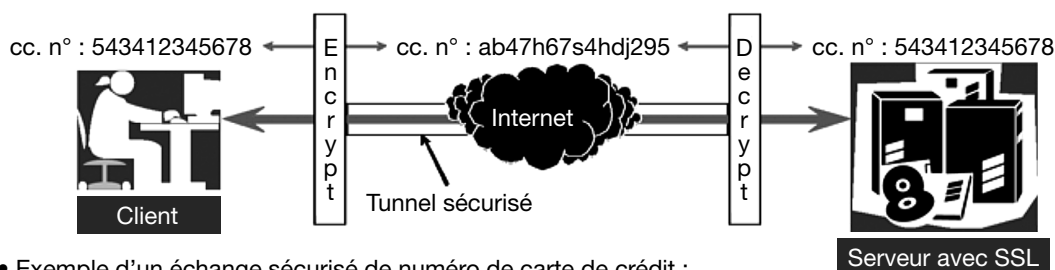
Comme introduit dans la section précédente, la confidentialité est la propriété d'un document ou d'une communication assurant la préservation de son contenu voire de son existence au regard des tiers non habilités expressément à en être destinataires.

Suivant les besoins, ces trois éléments constitutifs de la confiance seront définis de manière plus ou moins rigoureuse.

EXEMPLE

En matière de commerce électronique, un achat sur Internet avec paiement par carte bancaire nécessite la confidentialité de la transaction durant la transmission des informations d'identification de la carte pour éviter qu'un tiers ne capture ces données sur le réseau. Sur le plan technique, les sites de paiement en ligne prévoient un chiffrement de l'échange avec SSL (*Secure Socket Layer*). Les autres données de la commande en ligne ne sont en général pas chiffrées, les pertes de performances dues au chiffrement ne se justifiant pas par la protection d'informations non sensibles (les produits mis dans le panier de la commande).

Paieement avec une carte de crédit et SSL



- Exemple d'un échange sécurisé de numéro de carte de crédit :
 - **identification du serveur auprès du client et acceptation par celui-ci du certificat du serveur ;**
 - **chiffrement des données du client et envoi du message ;**
 - **déchiffrement du message par le serveur.**
- Il n'est pas nécessaire d'identifier le client.
- Cette technique permet aussi d'échanger des clés et donc des certificats ou tout autre message.

Il est à noter, dans cet exemple, que l'identité de la personne qui effectue la commande n'est pas toujours vérifiée, le commerçant se contentant de disposer d'une adresse réelle en cas de livraison d'une marchandise sous forme matérielle. La personne qui passe la commande n'est donc pas authentifiée.

3. Certificat électronique (appelé aussi certificat numérique)

Le décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique définit le certificat électronique ainsi :

« Un certificat électronique est un document sous forme électronique attestant du lien entre les données de vérification de signature électronique et un signataire. »

avec cette autre précision :

« Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique. »

On le voit dans ces définitions, le certificat électronique remplit un double rôle : il permet le chiffrement avec des clés et atteste de l'identité du signataire.

Un autre point à noter est l'indication de « clés cryptographiques publiques », signifiant que le système de chiffrement doit être asymétrique.

Le certificat électronique renforce aussi la sécurité des échanges effectués par courrier électronique.

De manière générale, l'usage du certificat électronique de signature permet :

- l'authentification de l'émetteur (confirmation que le document est bien envoyé par la personne identifiée) ;
- l'intégrité des données transmises (cohérence entre les données envoyées et celles reçues) ;
- la non-répudiabilité des messages (l'ensemble de ces fonctionnalités offre l'assurance que, ni la transaction elle-même, ni les informations transmises lors de cette transaction, ne pourront être contestées ultérieurement par l'émetteur) ;
- la confidentialité des échanges (palliant ainsi toute tentative de piratage).

a. Autorité de certification

Lors d'une authentification à clé publique, le récepteur du message doit connaître la clé publique de son interlocuteur et pouvoir en vérifier la validité auprès d'un tiers de confiance, dans la mesure où une usurpation d'identité serait possible. Pour ce faire, le vérificateur doit s'adresser à une autorité de certification, c'est-à-dire une instance fiable et indépendante chargée de gérer les clés publiques des interlocuteurs de confiance.

L'autorité de certification procure un certificat numérique contenant le nom de l'interlocuteur et la clé publique de confiance.

La norme gérant les certificats numériques est appelée X.509.

b. Infrastructure à clé publique

Le chiffrement des données est complexe à mettre en œuvre. Il nécessite des boîtiers spécialisés et/ou des logiciels de chiffrement à toutes les extrémités du réseau, ainsi que des échanges de clés. Ces échanges reposent sur une infrastructure technique et des procédures d'exploitation et d'administration qui permettent de délivrer et de stocker des certificats numériques de manière sécurisée : on parle d'infrastructure à clé publique (ICP ou PKI en anglais pour *Public key infrastructure*). Les certificats délivrés permettent d'accéder aux clés publiques.

Les infrastructures à clé publique assurent une prise en charge intégrale de la gestion des clés.

Elles nécessitent une approche organisationnelle très attentive à la formation des utilisateurs et à leur appropriation des mécanismes de protection de la confidentialité des échanges. Ce type d'infrastructure peut servir de base robuste à un déploiement de la signature électronique dans une entreprise ou un réseau.

VI. INFORMATIQUE ET LIBERTÉS

A. CONTENU DE LA LOI

La loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés a été préparée par les travaux de la commission informatique et libertés créée en 1974 ; cette loi marque une évolution notable dans les relations entre la société et l'informatique.

La loi :

- crée un organe veillant à son application : la Commission nationale de l'informatique et des libertés (Cnil) ;
- assujettit à diverses formalités l'utilisation d'un fichier informatisé concernant les personnes ;
- institue un droit d'accès en faveur des personnes concernées par un fichier.

Après de nombreuses péripéties, la mise en conformité de la loi française avec les directives européennes de 1995 et de 2002 est effective.

La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été publiée au Journal officiel du 7 août 2004.

Si la France était le premier pays européen à mettre en place une loi pour la protection des données, elle a été le dernier à transposer la directive européenne. Toutefois, si l'objectif assigné à l'origine visait à simplifier les procédures et alléger les formalités, force est de constater que les entreprises sont dorénavant confrontées à des textes touffus, peu évidents à analyser et qui, au contraire, conduisent à une multiplication des procédures.

1. Une refonte des procédures de notification

La loi était censée mener à un allègement des procédures, ce qui est plutôt réussi en ce qui concerne les traitements publics. Il en va autrement pour le secteur privé qui peut constater un effet inverse : bien que la déclaration ordinaire, telle que les entreprises la connaissaient auparavant, existe toujours et qu'une déclaration simplifiée à effectuer en ligne ait vu le jour, il faut savoir que certains traitements autrefois soumis à déclaration sont aujourd'hui soumis à autorisation par la Cnil.

Doivent faire l'objet d'une autorisation par la Cnil :

- les traitements liés à des données sensibles (telles que les appartenances religieuses, les données biométriques) ou à des condamnations ;
- les traitements susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, qui conduisent, par exemple, à la création de listes noires ou de *scorings* ;
- les traitements comportant des appréciations sur les difficultés sociales des personnes, comme l'exploitation marketing d'une information précisant que tel client est bénéficiaire du RMI, par exemple ;
- les traitements d'interconnexion entre fichiers publics ou entre fichiers privés ayant des finalités principales différentes, le terme est tellement vaste qu'il ramène dans le giron de la Cnil toutes sortes de traitements (liés notamment aux systèmes de pilotage, aux ERP et à tous les outils permettant d'identifier les clients).

En ce qui concerne les traitements fréquents et banals, une autorisation unique pour la famille de traitements peut être délivrée : pour un système d'information géographique à destination des collectivités locales, pour le cadastre ou l'urbanisme, par exemple. En revanche, s'il s'agit de traitements pour obtenir une gestion fine de la population à destination d'autres acteurs, une autorisation de la Cnil est obligatoire.

Des exonérations légales de déclaration sont accordées aux traitements concernant les membres d'associations ou de partis politiques, ainsi qu'aux traitements ayant pour objet la tenue d'un registre public destiné à l'information du public (listes électorales, RCS, etc.). Toutefois, des exonérations de déclaration peuvent être prononcées par la Cnil par le biais de normes : par exemple, les traitements de paie anciennement soumis à déclaration simplifiée sont exonérés de déclaration depuis le 7 janvier 2005.

Les traitements mis en œuvre par l'État comportant des données sensibles (fichiers de police et de justice) ou numéros de Sécurité sociale sont en revanche soumis à autorisation par le Conseil d'État. Une autorisation par « soi-même » peut être émise pour les traitements publics de police et de justice qui ne comportent pas de données sensibles, ou ceux qui intéressent la sûreté de l'État et la Défense.

2. Des contraintes nouvelles sur les transferts de données hors de l'Union européenne

L'interdiction de transferts de données personnelles vers les pays tiers qui n'assurent pas un niveau de protection adéquat a été levée : le *Safe harbor* et les transferts vers les États-Unis visent à remédier à cette interdiction. La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat en raison d'engagements internationaux dont le respect est vérifié chaque année.

Un contrat de transfert de données personnelles doit être conclu entre celui qui envoie les fichiers et celui qui les reçoit pour procéder au transfert de données. Le destinataire doit respecter la finalité, la non-transmission à des tiers sans l'accord de l'expéditeur, et désigner un représentant en charge de la protection des données.

En revanche, aucune condition particulière n'est imposée lorsque l'internaute a donné sans ambiguïté son consentement au transfert (lors d'une inscription en ligne sur un site américain, par exemple, dans laquelle il laisse son adresse électronique). Il en va de même lorsque le transfert de données personnelles est nécessaire à la réalisation d'un contrat (tel que l'achat d'un livre sur un site américain).

Les transferts vers un État tiers n'assurant pas un niveau de protection adéquat demeurent possibles sous réserve d'une décision de la Cnil. Un décret d'application décrit la procédure de décision de la Cnil en matière de transferts de données hors de l'Union européenne.

3. Un renforcement des pouvoirs de la Cnil

La Cnil bénéficie d'un pouvoir d'investigation qui peut passer par des contrôles sur place, ce qui n'est pas foncièrement nouveau. Elle peut également dénoncer au procureur de la République les infractions à la loi Informatique et libertés qu'elle constate.

En revanche, le pouvoir de prononcer des sanctions administratives en cas de violation de la loi constitue une innovation majeure. La Cnil peut, en effet, après une procédure contradictoire mais sans préjudice des sanctions pénales encourues, ordonner la cessation d'un traitement et prononcer des amendes administratives jusqu'à un montant de 300 000 euros. Néanmoins, les sanctions restent limitées, la procédure de sanction (comprenant les délais, les allers et retours, les mises en demeure, etc.) visant plutôt à inciter les entreprises à se mettre en conformité qu'à aller jusqu'à la sanction.

Des sanctions pénales pouvant aller jusqu'à cinq ans d'emprisonnement et 300 000 euros d'amende peuvent être prononcées en cas d'absence de notification préalable d'un traitement, de non-respect des conditions de traitement posées par la Cnil dans une norme simplifiée, ou de non-respect des conditions d'exonération de déclaration. Le fait de ne pas prendre toutes les mesures utiles pour préserver la sécurité, l'intégrité et la confidentialité des données peut également être sanctionné pénalement, ce qui signifie que, dans le cadre d'un piratage d'un site ou d'un système d'information, la victime d'une attaque peut agir contre l'entreprise propriétaire des données.

Des peines contraventionnelles pour défaut d'information des personnes peuvent atteindre 1 500 à 3 000 euros par infraction constatée : il peut, par exemple, s'agir d'une collecte de données personnelles par une entreprise sans avoir informé la personne sur les éléments prévus par la loi.

4. Le Cil : un vecteur de diffusion de la culture informatique et libertés

La publication au Journal officiel du 20 octobre 2005 du nouveau décret d'application de la loi Informatique et libertés permet notamment la nomination d'un correspondant à la protection des données, baptisé correspondant informatique et libertés (Cil). Les responsables de traitements qui disposent d'un Cil sont exonérés de l'obligation de déclaration ordinaire ou simplifiée.

La désignation du Cil, qui reste facultative, permet un allègement non négligeable de certaines formalités déclaratives auprès de la Cnil. Mais l'apport essentiel du Cil est son rôle de conseil et de pédagogie pour assurer une meilleure application de la loi Informatique et libertés.

Le rôle du Cil est de devenir le relais de la Cnil dans l'entreprise, en prodiguant des conseils en amont, en assurant une certaine pédagogie, et en réalisant des audits et une certaine médiation, en plus du rôle d'alerte de la Cnil s'il constate des violations ou des irrégularités.

Du point de vue du statut, le Cil peut être salarié du responsable de traitement, ou mutualisé (soit désigné également pour d'autres entités du groupe de sociétés auquel appartient ce responsable de traitement, soit salarié du groupement d'intérêt économique auquel appartient le responsable de traitement, soit désigné par un organisme professionnel ou un organisme regroupant les responsables de traitement dans un même secteur d'activité). Le Cil peut aussi être externe à l'entreprise, mais ce choix n'est possible que si moins de 50 personnes ont accès aux traitements concernés ou sont chargées de leur mise en œuvre.

B. LES FORMALITÉS REQUISES

Tout traitement automatisé d'informations nominatives doit être déclaré auprès de la Cnil ; cette déclaration recouvre ce qu'on appelle les formalités préalables. Pour ce faire, il est prévu des bordereaux de déclaration que l'on trouve soit au siège de la Cnil, soit dans les préfectures et les chambres de commerce et d'industrie. Toute modification ou suppression de traitement doit être déclarée. La Cnil est supposée détenir de la sorte un « fichier des fichiers » actualisé en permanence.

Cette loi s'applique aussi bien aux entreprises privées qu'aux organismes publics. La mise en œuvre de tout traitement doit être précédée d'une déclaration qui donne lieu à l'émission d'un récépissé faisant foi.

Le déclarant peut être soit la personne qui met en œuvre le traitement, soit celle pour le compte de laquelle il est mis en œuvre, cette dernière étant, dans tous les cas, considérée comme juridiquement responsable.

Un traitement est considéré comme nominatif s'il porte sur des personnes physiques soit identifiées, soit identifiables. Il est interdit de détenir ou de gérer certaines informations jugées trop sensibles faisant apparaître directement ou indirectement la race, la religion, les opinions politiques ou philosophiques, l'appartenance syndicale de toute personne physique.

Néanmoins, les groupements religieux, philosophiques, politiques ou syndicaux peuvent tenir un registre de leurs membres ou « correspondants » libres de tout contrôle de la Cnil à ce sujet.

La Cnil attache beaucoup d'importance à la durée de conservation des informations, qui ne peut excéder celle prévue initialement par le déclarant dans sa déclaration.

Il faut, enfin, informer toute personne auprès de laquelle sont recueillies des informations nominatives, du caractère obligatoire ou facultatif de chaque réponse, des conséquences d'un défaut de réponse, des destinataires prévus d'informations et de l'existence du droit d'accès. Ceci doit être notamment stipulé par écrit sur tout questionnaire à caractère nominatif au sens de la loi.

C. SIX QUESTIONS ESSENTIELLES (SOURCE : CNIL)

1. Où trouver le formulaire de déclaration et la notice explicative ?

Vous pouvez demander gratuitement le formulaire Cerfa n° 99001 ainsi que la notice explicative :

- aux préfectures ;
- aux chambres de commerce et d'industrie ;
- à la Cnil, en les téléchargeant sur le site Internet www.cnil.fr.

2. Quelle est la procédure ?

Une fois le formulaire rempli, les annexes et les justificatifs fournis, vous devez adresser à la Cnil l'ensemble de ces documents en 3 exemplaires :

- soit par envoi recommandé avec demande d'avis de réception postal ;
- soit par dépôt auprès de la Cnil contre reçu.

Ensuite, lorsqu'un traitement est déclaré, la Cnil vous adresse un récépissé indiquant le numéro sous lequel celui-ci est enregistré.

Dans le cas où vous ignorez si un traitement a été ou non déclaré à la Cnil, vous avez la possibilité d'interroger ses services qui vous donneront toutes les informations utiles (numéro de récépissé, finalité du traitement déclaré, etc.).

En cas de perte de votre récépissé, vous pouvez, par écrit, en demander un duplicata au service informatique de la Cnil.

3. Quand le traitement peut-il être mis en œuvre ?

La mise en œuvre du traitement est subordonnée :

- pour le secteur public, à la *publication* de l'acte réglementaire (pris après avis de la Cnil) portant création du traitement ; en cas de déclaration simplifiée, à la délivrance du récépissé de déclaration à la Cnil ;
- pour le secteur privé (déclaration ordinaire ou simplifiée), à la *délivrance du récépissé* de déclaration à la Cnil.

4. Qui doit signer ?

Celui qui a décidé de mettre en œuvre un traitement nominatif (par exemple, le maire, le PDG d'une entreprise, le directeur d'un hôpital par délégation, etc.) doit signer. Attention, le signataire est considéré comme juridiquement responsable du contenu de la déclaration.

5. Qu'est-ce qu'une annexe ?

C'est un papier libre dactylographié où sont portés :

- soit les renseignements supplémentaires, exigés pour les rubriques du formulaire marquées d'un astérisque ;
- soit la suite des énumérations quand la place sur le formulaire ne suffit pas ;
- soit les documents que vous devez joindre à votre déclaration, par exemple : textes de loi, statuts d'association, projet d'acte réglementaire (Par), etc.

6. Quels traitements sont exonérés de déclaration ?

Sous certaines conditions, certains traitements sont exonérés de déclaration. Il s'agit :

- des registres des membres ou des correspondants des églises ou des regroupements à caractère religieux, philosophique, politique ou syndical (article 31 de la loi du 6 janvier 1978) ;
- de certains traitements conformes à une norme rédigée par la Cnil.

Par exemple, la gestion informatisée de la paie des personnels par un employeur est sujette à déclaration à la Cnil, du fait des données nominatives indispensables à l'établissement des bulletins de paie.

Mais si les fichiers de l'application sont conformes à la norme n° 28 du 14 septembre 1985, alors il y a dispense de déclaration.

Ce principe de dispense est valable pour beaucoup de traitements. Pour prendre connaissance des normes, consulter le site de la Cnil (www.cnil.fr). Se référer à l'annexe 3 qui présente la norme pour l'établissement de la paie.

D. LE DROIT D'ACCÈS ET DE RECTIFICATION

Toute personne physique a le droit de consulter l'intégralité des données (en langage clair et non sous forme codée) la concernant, et de les faire rectifier en cas d'inexactitude, ou supprimer en cas d'illégalité. C'est ce que l'on appelle le droit d'accès direct. Il faut pour cela justifier de son identité.

Pour les traitements intéressant la sûreté de l'État, la Défense et la sécurité politique, c'est la Cnil qui exerce le droit d'accès, appelé alors « indirect » pour le compte de l'intéressé.

Pour permettre à chacun d'exercer son droit d'accès, la loi fait obligation à la Cnil de mettre à disposition du public la liste des traitements dont elle a enregistré la déclaration.

E. LA CNIL

La Commission nationale Informatique et libertés est une autorité administrative indépendante, ne rendant compte à aucun ministre. Seul un contrôle financier est exercé a posteriori par la Cour des comptes. Elle remet chaque année un rapport public au président de la République.

Elle se compose de 17 commissaires nommés pour 5 ans : aucun d'entre eux ne peut être membre du gouvernement, ni exercer des fonctions dans les branches de l'informatique ou des télécommunications, ni y avoir des intérêts.

Elle dispose de services et de conseillers. La commission délibère, rend des avis et émet des recommandations. Elle met à disposition, non seulement des membres et des agents de la Cnil mais encore du public, un service de documentation comportant ouvrages, textes juridiques, dossiers de presse et documents divers. Un service vous permet aussi de consulter la liste des traitements.

La Cnil est particulièrement sensible aux interconnexions de fichiers et à la transmission d'informations qu'elle juge plus dangereuses pour les libertés individuelles et collectives que la simple détention d'un seul fichier ; ceci explique ses réticences en matière d'utilisation du numéro d'identification au répertoire (Nir) qui peut être assimilé au numéro Sécurité sociale. En effet, ce numéro comporte la codification de données personnelles (sexe, âge, lieu de naissance) et permettrait une interconnexion massive du fait de son rôle d'identifiant et de sa large diffusion. En conséquence, l'utilisation du Nir doit être réservée aux fichiers pour lesquels sa conservation est nécessaire (par exemple, pour son impression sur un bulletin de paie) et ne doit en aucun cas servir d'identifiant pour des traitements.

F. LA SANCTION

Les sanctions prévues par le Code pénal sont lourdes : emprisonnement (jusqu'à 5 ans !), amendes (jusqu'à 300 000 euros). Mais il faut bien le dire, la sévérité de la loi est tempérée par une application plus que parcimonieuse de ces sanctions pénales. Est-ce à dire que la peur inspirée par cet impressionnant arsenal effraie suffisamment les contrevenants potentiels pour que ceux-ci s'abstiennent d'actes répréhensibles ? Ou que la faiblesse des autorités répressives laisse dans l'ombre les infractions à la loi ? Au lecteur de se faire une opinion sur cette question. Mais pour le professionnel qui engage sa responsabilité (commissaire aux comptes, par exemple), la non-dénonciation de ces délits est un risque important qu'il vaut mieux apprécier avec une bonne connaissance de cette loi.

On notera, outre la sévérité des sanctions de ces délits, le fait que la matérialité du délit puisse résulter de la mauvaise organisation d'un centre informatique ou d'un centre de saisie de l'information. Le personnel informatique, déjà soumis à une obligation de discrétion, est quasiment astreint à un secret professionnel par cette loi.

Toute personne peut s'adresser à la Cnil pour faire état d'une réclamation, d'une pétition collective, d'une plainte ou d'une dénonciation. Un service spécialisé peut conseiller la formulation d'une saisine.

La Cnil est habilitée, afin de faire respecter la loi, à toute mission d'investigation ou d'inspection sur place qu'elle juge utile. Ses représentants peuvent venir effectuer un contrôle à tout moment.

Adresse :

Cnil

8, rue Vivienne

CS 30223

75083 PARIS CEDEX 02

Tél. : 01 53 73 22 22

Télécopie : 01 53 73 22 00

@ Le site Internet : <http://www.cnil.fr> contient des informations et des documents qui permettent de mieux appréhender les obligations issues de la loi.

le cnam intec
Institut national des techniques
économiques et comptables

LES NORMES ET LES RÉFÉRENTIELS DES AUDITS DES SYSTÈMES D'INFORMATION

Dans la vie des organisations privées ou publiques, les audits des systèmes d'information recouvrent des situations très différentes :

- dans un cadre légal d'audit des comptes (la mission du Cac) pour lequel l'audit du système d'information de l'entité est nécessaire ;
- dans un cadre d'expertise judiciaire, sur la requête d'un tribunal (juridictions pénales, civiles, commerciale...) ;
- dans un cadre administratif, sur la demande d'une autorité administrative qui souhaite contrôler des entités évoluant dans son périmètre de contrôle (AMF, ART...) ;
- à la demande d'une autorité de tutelle sur l'entité dont elle a la charge (établissement public national, local, hôpital...) ;
- à la demande des dirigeants de l'organisation (direction générale, mais aussi direction des systèmes d'information) ;
- à la demande des propriétaires pour contrôler leurs mandataires (les dirigeants) ;
- au sein d'une mission d'audit qui concerne l'ensemble des filiales d'un groupe international...

Les éléments qui donnent à un audit son caractère spécifique sont :

- la nature du cadre juridique de l'audit : insertion dans un cadre légal ou réglementaire ou bien purement contractuel ;
- la nature du lien entre l'auditeur et l'audité : appartenance à la même entité ou non-appartenance ;
- le destinataire du rapport ;
- le financeur de la mission ;
- la technicité informatique de la mission.

Il est à noter que la formation initiale et le parcours professionnel de l'auditeur donnent aussi une orientation à la mission.

Pour ne pas céder aux délices de la combinatoire qui pourrait transformer chaque audit d'un système d'information en une espèce unique, il est bon d'observer que les professionnels se sont naturellement regroupés en instances nationales et internationales suivant ce qui apparaît comme les grandes frontières séparant ces audits.

La première ligne de séparation est apparue entre le point de vue de l'intérieur de l'organisation (audit interne) et l'intervenant extérieur (audit légal ou contractuel) :

- le premier point de vue est représenté par l'Institute of Internal Auditors (IIA) et son chapitre français : l'Institut français de l'audit et du contrôle internes (IFACI) ;
- le second par l'Information Systems Audit and Control Association (ISACA) et son chapitre français : Association française de l'audit et du conseil informatiques (AFAI).

La seconde ligne de démarcation est plus difficile à tracer car elle est très contingente au cadre légal des pays dans lequel peut s'exercer l'audit, elle a trait au caractère encadré ou non par les pouvoirs publics de la mission de l'audit elle-même.

Dans le cas de la France, sous la tutelle du ministère de la justice, c'est la Compagnie des commissaires aux comptes qui est en charge de ces audits particuliers que sont la certification des comptes des entités ayant certaines caractéristiques (forme juridique, mais aussi seuils d'activités économiques). Pour ces audits financiers, le lien avec le système d'information est évident, puisque c'est le système d'information automatisé qui alimente la confection des

comptes et leur agrégation dans des indicateurs de performances financières. Dans d'autres pays, la tutelle peut être différente, par exemple aux États-Unis elle s'exercera plutôt à travers l'autorité de contrôle des places boursières (la *Securities and Exchange Commission*).

De fait, l'ensemble de ces organismes, dotés d'un pouvoir de régulation dans le cadre national, se sont concertés pour trouver une solution internationale à leur besoin d'harmonisation et ils ont choisi l'*International Federation of Accountants* (IFAC) pour remplir ce rôle.

Pour compléter ce tableau, il serait malvenu d'oublier les professionnels de l'informatique et des télécommunications qui sont souvent en position de « subir » les audits et qui, en général de culture « technique » ou « ingénieur », veulent voir prises en compte les « règles de l'art », c'est-à-dire souvent les contraintes de leur métier. Pour eux, le modèle est à rechercher chez les grands instituts de normalisation technique qui font avancer l'industrie tous les jours : l'*Institute of Electrical and Electronics Engineers* (IEEE) en est un exemple. L'Union internationale des télécommunications (UIT) toujours aussi active malgré son grand âge (elle fut créée en 1865 sous le nom de l'Union télégraphique internationale), est certainement l'exemple le plus abouti d'une coopération internationale qui débouche sur des normes qui sont utilisées tous les jours par tous sur tous les continents.

Mais l'informatique ce n'est pas seulement du « hard » (matériel) ou des échanges de messages électroniques, c'est aussi, et de plus en plus, du service et, dans ce domaine, le leadership de la normalisation a été pris depuis de nombreuses années par l'*International Organization for Standardization* ou Organisation internationale de normalisation (ISO), par exemple avec les célèbres normes ISO 9000 et suivantes.

Pour clarifier ce panorama qui se révèle très touffu et qui, de plus, est sujet à des modifications rapides, nous essaierons, dans un premier temps, de clarifier le vocabulaire utilisé par les différents acteurs de ces audits, puis nous reviendrons sur le contexte international dont les évolutions récentes donnent un cadre général de compréhension des enjeux, enfin nous passerons en revue les différentes sources d'inspiration qui peuvent guider la réalisation d'une mission d'audit des systèmes d'information.

I. DÉFINITIONS ET VOCABULAIRE

Ce qui nous intéresse ici, ce n'est pas tellement le déroulement de la mission d'audit, que nous aborderons plus loin dans ce cours, mais plutôt les « fondations » : comment séparer le bon grain de l'ivraie, c'est-à-dire, qu'est-ce qui, dans les activités de l'entité auditée ou dans les comportements de ses membres, présente des risques de non-conformité avec les règles de l'art, met en danger certains actifs ou pire encore enfreint la réglementation ou la loi ?

Les termes qui expriment ce qui doit être fait, avec une signification « normative » plus ou moins forte sont les suivants : **norme ou normalisation, standard ou standardisation, référentiel, règles et usages de la profession, certification, conformité, label, code, exigences, principes, déontologie, règles de l'art, règlement ou réglementation ou régulation, loi ou législation.**

A. CONTEXTE

Ces termes se retrouvent dans des contextes différents, mais avec des significations qui sont toutes connotées comme :

- exprimant le bon chemin à suivre (la norme, c'est ce qui est jugé « normal ») ;
- émanant d'une « communauté » ou d'une organisation dépositaire d'un « savoir », et même dans certains cas, d'un pouvoir ;
- pouvant être sanctionné pour leur non-respect.

Si l'on prend comme exemple la conduite automobile, nous retrouvons bien le Code de la route comme exprimant la « bonne conduite », sa rédaction est une transposition dans chaque pays de règles définies par une coopération internationale, son respect dépend de la vigilance des pouvoirs publics. Mais l'auditeur dans cet exemple ? En fait, son rôle est assez mince, il ne serait présent

que lors du contrôle technique du véhicule dont il assurerait la conformité avec un certain nombre de qualités techniques. Pour le conducteur, il n'est pas encore prévu, en France, de contrôle périodique de ses capacités de conduite, mais dans le futur les choses peuvent évoluer...

En revanche, dans l'exemple du commissariat aux comptes, le rôle de l'auditeur est plus affirmé. Les organisations soumises à son contrôle doivent lui fournir toutes les informations nécessaires à l'accomplissement de sa mission, cette dernière suivant un ensemble de règles définies par des instances professionnelles sous la tutelle de la puissance publique. L'auditeur doit fournir son opinion sur le respect par l'organisation auditée des règles comptables et financières qui lui sont applicables.

Ainsi, on peut constater sur ce dernier exemple la coexistence de deux niveaux de règles :

- les règles qui s'appliquent à la publication des comptes financiers par une entité ;
- les règles qui s'appliquent à la conduite de la mission d'audit.

Chaque « corpus » de règles émanant d'instances distinctes et obéissant à des principes propres.

Le même schéma pourrait s'appliquer au contrôle fiscal :

- le Code général des impôts s'appliquant aux contribuables ;
- le contrôle fiscal obéissant à un Livre des procédures fiscales que doit respecter le contrôleur.

Évidemment, assimiler un contrôle fiscal à un audit peut paraître exagéré, puisque, dans ce cas, le contrôleur dispose du pouvoir de sanction (le redressement), ce qui n'est en général pas le cas pour un auditeur. Encore qu'avec son devoir de révélation de faits délictueux, le commissaire aux comptes français dispose bien, de fait, d'un droit et même d'un devoir de sanction.

Dans le domaine des systèmes d'information, nous allons retrouver ces mêmes distinctions, certaines règles à respecter par les utilisateurs ou les concepteurs des systèmes d'information ayant une assise légale forte (par exemple en France la loi Informatique et libertés ou la loi Godfrain), ou d'autres une application de bonnes pratiques recommandées par des organismes *ad hoc*.

La mission elle-même est aussi encadrée par des « usages » professionnels qui émanent des organismes professionnels déjà évoqués plus haut.

Comme promis, nous allons d'abord présenter la terminologie utilisée dans ces référentiels.

B. DÉFINITIONS

1. Norme (source : Afnor)

C'est un référentiel élaboré en **consensus** par l'ensemble des acteurs d'un marché : producteurs, utilisateurs, laboratoires, pouvoirs publics, consommateurs etc., et reflétant l'état de la technique et des contraintes économiques à un moment donné.

La **norme** est un document **d'application volontaire** et **contractuelle**.

La **Directive 98/34/CE** indique que la **norme** est « *une spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire* ».

2. Normalisation (source : Afnor)

Le processus de **normalisation** a pour objet la publication de normes et documents normatifs, aussi bien à l'échelle nationale, européenne ou internationale.

En France, le **décret n° 84-74 modifié** du ministère de l'industrie et de la recherche, fixant le statut de la **normalisation**, précise que :

« La **normalisation** a pour objet de fournir des documents de références comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux. »

Ce texte définit le système de normalisation français et en confie la gestion à l'Afnor (Association française de normalisation).

Afnor est le membre français des structures de normalisation internationale (ISO – Organisation internationale de normalisation) et européenne (CEN – Comité européen de normalisation).

3. Standard ou standardisation

Ces termes sont souvent utilisés comme synonymes de norme et normalisation du fait de l'origine anglo-saxonne de ces termes.

En revanche, pour beaucoup d'auteurs francophones, le « standard » n'a pas la reconnaissance officielle de la « norme ». Il doit être envisagé comme une « norme » de fait, qui a vocation à être validée par l'organisme en charge de la normalisation.

Pour les anglophones, seul le terme « standard » existe et recouvre les deux sens.

4. Référentiel

Un référentiel contient des informations de référence. Toute information identifiée comme information de référence doit obligatoirement faire l'objet d'une définition explicite permettant notamment :

- d'apporter une vision claire et précise du contour de cette information de référence (aucune ambiguïté ne doit exister sur les limites et le contenu de cette information de référence) ;
- une adhésion de tous sur la définition et le contour qu'elle porte (partage de la définition).

5. Certification

La certification est une reconnaissance écrite, par un organisme indépendant du fabricant ou du prestataire de service, de la conformité d'un produit, service, organisation ou personnel à des exigences fixées dans un référentiel. La certification doit être effectuée dans le cadre européen par un organisme accrédité. En France c'est le Comité français d'accréditation (Cofrac) qui délivre les accréditations.

Les accords multilatéraux dont le Cofrac est signataire facilitent les échanges des produits et des services : une accréditation obtenue en France est reconnue dans tous les pays signataires en Europe et dans le monde. L'État français reconnaît le Cofrac comme « instance nationale d'accréditation ».

@ Pour plus de détails, consulter le site : <http://www.cofrac.fr/>.

L'Afaq Afnor certification est un des principaux organismes de certification accrédités en France. En particulier, il propose des certifications suivantes dans le domaine de l'informatique :

- la certification ISO 20000-1 : 2005. Étroitement associée à ITIL, cette offre a été conçue avec l'ITSMF France ;
- l'évaluation CMMI dédiée au développement de systèmes, de produits ou de logiciels, qui permet de qualifier une entreprise selon le niveau de maturité de ses processus, de son organisation ;
- l'évaluation issue de l'ISO 17799 : 2005 qui détermine le niveau de maîtrise du système de management de la sécurité de l'information d'une entité ;
- la certification ISO 10006 : 2003, complémentaire à l'ISO 9001 : 2000, qui prouve la maîtrise de la conduite de projets dans les meilleures conditions de coûts et de délais ;
- la certification Tick-it, complément de l'ISO 9001 : 2000 et adaptée à la conception d'outils informatiques, présente les garanties d'une qualité de prestations et de produits/services ;
- la certification Webcert, référentiel de certification de services, orienté commerce électronique.

@ Pour plus de détails, consulter le site : <http://www.afaq.org/>.

6. Usages de la profession, état de l'art, règles de l'art...

Tous ces termes font référence à des pratiques professionnelles qui sont reconnues comme correctes et qui doivent assurer dans les métiers de services un niveau de prestation conforme aux attentes du client. Il est à noter que les tribunaux peuvent avoir à apprécier la conformité de cette « obligation de moyens » dans le cas d'un conflit client-fournisseur. Le rôle des instances professionnelles est donc important pour fixer ces usages. Le législateur confie d'ailleurs à certaines d'entre elles le soin de les rédiger (par exemple pour la profession réglementée d'avocat).

« Dans le respect des dispositions législatives et réglementaires en vigueur, le Conseil national des barreaux unifie par voie de dispositions générales les règles et usages de la profession d'avocat. »

C. trav., art. 22.

7. Code de déontologie

Document écrit qui regroupe l'ensemble des règles et devoirs qui régissent une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public. Désormais, de nombreuses professions se sont dotées, avec ou sans l'aval des pouvoirs publics, d'un tel code. Par exemple, les commissaires aux comptes : décret n° 2005-1412 du 16 novembre 2005 portant approbation du Code de déontologie de la profession de commissaire aux comptes.

@ À consulter sur <http://www.admi.net/>.

REMARQUE

Il est possible de rencontrer le terme équivalent « code d'éthique », traduction littérale de « *code of ethics* ».

II. LE CONTEXTE INTERNATIONAL ET LES ENJEUX

Les systèmes d'information se trouvent au confluent de plusieurs préoccupations de la communauté internationale, ce qui explique que le thème des normes techniques d'utilisation des équipements et des réseaux informatiques, a priori confinées à un cercle restreint de professionnels, soit parvenu à mobiliser l'attention des organismes de décision les plus importants du monde économique et financier. Plusieurs chocs aux répercussions mondiales expliquent ce phénomène :

- les crises financières qui ont frappé certains pays émergents dans la seconde moitié des années 1990 ;
- les affaires Enron, Worldcom et autres, qui ont jeté le discrédit sur le rôle régulateur des professionnels de l'audit comptable ;
- des diffusions massives de virus et autres codes malicieux pouvant provoquer des perturbations plus ou moins graves dans les systèmes économiques et sociaux ;
- la montée en puissance de l'Internet et de la mise en réseau des systèmes d'information au niveau mondial qui en augmentent la vulnérabilité ;
- enfin, après le 11 septembre 2001, les impératifs de la lutte contre le terrorisme dont le volet « renseignement électronique » est non négligeable.

Pour comprendre le lien entre tous ces événements et le cadre institutionnel dans lequel s'est développée l'évolution des normes d'audit, nous présenterons un rapide descriptif des principaux événements de la dernière décennie.

A. FORUM DE STABILITÉ FINANCIÈRE (FSF)

Suite aux crises financières qui ont secoué certains pays émergents dans la seconde moitié des années 1990, une orientation vers des standards reconnus à l'échelle planétaire est apparue comme une mesure réaliste et susceptible de recueillir un consensus international. Les ministres des finances et les gouverneurs des banques centrales des pays du G7 ont décidé de créer un Forum de stabilité financière (FSF). Le FSF a notamment pour objectif de renforcer le fonctionnement des marchés financiers et de réduire le risque systémique par une meilleure circulation de l'information et une collaboration accrue entre les autorités chargées de veiller à la stabilité financière. Il se compose de 42 membres, parmi lesquels on compte des responsables de onze pays dotés d'importantes places financières et des représentants d'organismes internationaux (FMI, OCDE, Banque mondiale, BRI, Comité de Bâle, OICV, AICA...).

Le travail du FSF a permis d'identifier douze familles de normes dont l'application semblait étroitement liée aux enjeux systémiques.

| DOMAINE | NORME | INSTITUTION RÉDACTRICE |
|--|---|---|
| Politique macroéconomique et transparence des données | | |
| Politique monétaire | Code de bonnes pratiques de politique monétaire | Fonds monétaire international |
| Transparence de la politique budgétaire et fiscale | Code de bonnes pratiques de politique budgétaire et fiscale | Fonds monétaire international |
| Diffusion des données économiques essentielles | Diffusion de données particulières (<i>système de diffusion de données générales</i>) | Fonds monétaire international |
| Infrastructure institutionnelle et de marché | | |
| Faillite | Principes et orientations applicables au régime de l'insolvabilité | Banque mondiale |
| Gouvernement d'entreprise | Principes relatifs au gouvernement d'entreprise | Organisation de coopération et de développement économique (OCDE) |
| Information financière et comptable | Normes comptables internationales | Comité des normes comptables internationales (IASB) |
| Audit | Normes internationales d'audit | Fédération internationale des comptables (IFAC) |
| <i>Payment and settlement</i> | Principes fondamentaux pour les systèmes de paiement d'importance systémique | Comité sur les systèmes de paiement et de règlement (CPSS) |
| Blanchiment | Les quarante recommandations du groupe d'action financière sur le blanchiment | Groupe d'action financière internationale (GAFI) |
| Régulation financière | | |
| Régulation bancaire | Les principes fondamentaux de la supervision bancaire | Comité de Bâle |
| Régulation des marchés financiers | Les objectifs et principes de la régulation financière | Organisation internationale des commissions de valeurs (OICV) |
| Régulation des assurances | Les principes fondamentaux de l'assurance | Organisation internationale des contrôleurs d'assurance (IAIS) |

Ainsi, dans ce contexte, on constate que l'Ifac est en charge de la normalisation de l'audit, la question de son étendue étant posée vis-à-vis des systèmes d'information ainsi d'ailleurs que le lien avec la gouvernance de l'entreprise, qui repose sur l'organisation d'un contrôle interne et sur le partage des informations pertinentes, et dont la définition est pilotée par l'OCDE.

Le bilan du FSF et de l'impulsion qu'il a donnée à la définition de nouvelles normes à vocation mondiale est impressionnant ; les normes d'audit ISA, les assurances, le monde bancaire avec Bâle II... Mais cela n'était pas suffisant pour éviter le « choc » des affaires Enron et autres en 2002 !

B. ENRON ET LA SUITE

Une deuxième vague est venue ébranler le système économique mondial par le doute que les affaires Enron, Worldcom et autres ont suscité envers les normes et les standards que doivent faire respecter les grands réseaux d'auditeurs financiers.

1. Sarbanes-Oxley Act

Votée par le Congrès des États-Unis en juillet 2002 suite aux scandales des affaires Enron et Worldcom, la loi Sarbanes-Oxley exige que les dirigeants des entreprises cotées sur une place financière aux États-Unis certifient leurs comptes auprès de la *Securities and Exchanges Commission* (SEC), l'organisme de régulation des marchés financiers.

a. Que contient la loi ?

On peut distinguer six grandes mesures :

1. La mesure la plus significative est celle qui concerne la « responsabilité » des dirigeants d'entreprises (le CEO, c'est-à-dire le directeur général, et le CFO, c'est-à-dire le directeur financier). Toute irrégularité volontaire ou consciente est pénalisée. Les dirigeants pris en faute encourrent des peines de prison.
2. Afin d'améliorer l'accès et la fiabilité de l'information, les entreprises devront fournir à la SEC des informations complémentaires (principes comptables guidant la présentation des comptes, transactions hors bilan, changements dans la propriété des actifs détenus par les dirigeants, codes d'éthique de l'entreprise...).
3. Depuis le 26 avril 2003, les entreprises doivent avoir mis sur pied des comités d'audit indépendants pour superviser le processus de vérification des comptes. Ceux-ci sont habilités à recevoir des plaintes venant des actionnaires ou encore des employés concernant la comptabilité de l'entreprise et les procédures de vérification.
4. Il est aussi prévu d'imposer la rotation des vérificateurs externes.
5. Un nouvel organisme de réglementation et de surveillance, le *Public Company Accounting Oversight Board*, doit superviser les cabinets comptables, établir des standards, enquêter et sanctionner les personnes physiques et morales qui ne respectent pas les règles.
6. Les sanctions sont considérablement renforcées. La sentence maximale pour fraude passe par exemple à 25 ans de prison !

b. Sa mise en place

Les investisseurs et la plupart des entreprises ont réagi favorablement aux mesures annoncées. Mais les entreprises ont fait valoir les délais de mise en conformité avec les nouvelles règles, ainsi que les coûts induits. De fait, il faudra attendre 2006 pour que la loi Sarbanes-Oxley soit appliquée, sans être tout à fait certain qu'elle le soit avec toute la sévérité qui en marque l'esprit. De plus, le budget de la SEC, qui est le bras armé de cette loi, apparaît très limité pour disposer des moyens d'accroître les contrôles préventifs.

De plus, la loi reste controversée de par sa portée extraterritoriale... notamment par l'Europe et le Canada dont les sociétés cotées aux États-Unis doivent se soumettre aux règles établies par la loi Sarbanes-Oxley.

Néanmoins, un rapide bilan démontre le fort impact de cette loi sur les systèmes d'information des sociétés qui lui sont soumises. Les reportings doivent être plus détaillés, les remontées d'information qui ont un impact sur les résultats de la société sont sous la responsabilité des dirigeants des filiales. Il est avéré que d'importants investissements informatiques sont venus conforter et fiabiliser les systèmes d'information des entités relevant du Sarbanes-Oxley Act (souvent désigné par l'acronyme SOX).

2. Loi sur la sécurité financière

Le Parlement français a adopté le 17 juillet 2003 la loi sur la sécurité financière (LSF) pour répondre à la crise de confiance des investisseurs née Outre-Atlantique avec les affaires Enron et Worldcom et relayée en Europe par des affaires comme Parmalat ou Vivendi.

Comme souvent en France, cette loi touche à beaucoup de domaines qui sont regroupés sous le vocable de « sécurité financière » :

- la création de l'Autorité des marchés financiers (AMF) ;
- la réforme du démarchage bancaire et financier et la création d'un statut pour les conseillers en investissements financiers ;
- la modernisation du régime des organismes de placement collectif en valeurs mobilières (OPCVM) et de divers instruments de financement ;
- la réforme du contrôle légal des comptes ;
- et enfin des mesures touchant au droit des sociétés et au renforcement du gouvernement d'entreprise.

La volonté du législateur est double : une information plus complète à destination des investisseurs et une plus grande vigilance dans le processus d'arrêté des comptes de la part des dirigeants. Le président d'une Société anonyme (SA) devra donc, dans un rapport joint au rapport de gestion sur les comptes sociaux et les comptes consolidés, rendre compte des procédures de contrôle interne mises en place par la société et le groupe.

Un Haut Conseil du commissariat aux comptes vient d'être mis en place comme organisme de régulation des normes d'exercice professionnel.

Une convergence ou un effet de calendrier ?

La LSF a été présentée par certains comme une loi Sarbanes-Oxley à la française. Effectivement, les deux textes traitent les thèmes de l'audit et du gouvernement d'entreprise : la LSF se montre à certains égards plus contraignante, puisqu'elle touche toutes les sociétés anonymes et pas seulement les sociétés cotées. Mais il est incontestable que les effets d'annonce de la loi Sarbanes-Oxley ont eu un impact médiatique beaucoup plus fort avec un volet pénal qui implique directement les dirigeants. Par ailleurs, la portée extraterritoriale de la loi Sarbanes-Oxley qui contrevient à un principe fondamental du droit, a beaucoup agité les milieux financiers hors des États-Unis mais il est à noter que le renforcement des contraintes, pour des émetteurs étrangers, constitue en quelque sorte une contrepartie du bénéfice qu'ils peuvent tirer de leur cotation sur une place financière aux États-Unis.

La LSF a elle-même un impact extraterritorial lorsqu'elle fixe les pouvoirs de l'AMF (Autorité des marchés financiers) qui s'exercent aussi à l'encontre des sociétés étrangères cotées sur la place de Paris.

Au total, il apparaît bien que l'interconnexion des marchés financiers imprime sa marque aux influences réciproques qu'exercent les régimes juridiques nationaux. De véritables convergences s'affirment, tout en s'insérant dans des traditions juridiques nationales qui persistent.

Mais, parallèlement à ces évolutions, dont les préoccupations économiques et financières sont prioritaires et dont les réponses sont essentiellement contenues dans le triptyque normes-contrôles-sanction, sont venues se greffer les inquiétudes liées à des menaces de toute nature (terrorisme, piratage, vol...) à l'encontre des grands systèmes d'information.

C. LA PROTECTION DES SYSTÈMES D'INFORMATION

L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'ouverture des réseaux et leur complexité croissante associant des acteurs aux multiples profils ont renforcé la vulnérabilité des systèmes d'information.

Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises, et du mode de vie des citoyens. Les services qu'ils assurent nous sont tout aussi indispensables que l'approvisionnement en eau ou en électricité.

La croissance d'Internet a modifié considérablement la donne et conféré aux systèmes d'information une dimension incontournable au développement même de l'économie et de la société. C'est dire si la Sécurité des systèmes d'information (SSI) est un enjeu à l'échelle de la Nation tout entière.

Pour l'État, il s'agit d'un enjeu de souveraineté nationale. Il a, en effet, la responsabilité de garantir la sécurité de ses propres systèmes d'information, la continuité de fonctionnement des institutions et des infrastructures vitales pour les activités socio-économiques du pays et la protection des entreprises et des citoyens. Mais l'État ne peut envisager le plein succès dans sa mission dans un cadre purement national, la coopération internationale doit être mise au premier plan.

De leur côté, les entreprises doivent protéger des dysfonctionnements et de la malveillance leur système d'information qui irrigue l'ensemble de leur patrimoine (propriété intellectuelle et savoir-faire) et supporte leur stratégie de développement, sans négliger le fait que leur responsabilité peut être mise en cause dans le cas d'utilisation abusive de données (nominatives, financières...) qu'elles détiennent.

Tous les utilisateurs identifient au quotidien la menace constante des virus et des vers qui se propagent désormais essentiellement par Internet. Leur nombre a explosé au cours de ces dernières années et ceux-ci deviennent de plus en plus sophistiqués. Les outils nécessaires aux pirates sont aisément accessibles en ligne et il existe un échange constant d'information et de savoir-faire au sein des communautés de pirates pour rendre ces attaques de plus en plus efficaces.

Le paradoxe est que les réponses ne peuvent que s'appuyer sur une dimension internationale, comme la nature de certaines menaces y conduit, alors que le cadre de la sécurité est essentiellement national avec des organismes dédiés à cette lutte dans ce périmètre restreint.

Par exemple aux États-Unis, après les attentats du 11 septembre 2001, qui ont ébranlé l'image de marque de la NSA (*National Security Agency* : Agence nationale de la sécurité, notamment en charge de la surveillance des menaces par des moyens informatiques), la cybersécurité est devenue un enjeu de sécurité nationale fondé sur la définition de la stratégie nationale de sécurisation du cyberspace. Diverses organisations gouvernementales ont ainsi été regroupées pour lutter contre la cybercriminalité.

De nombreux autres pays disposent ou sont en cours de création de telles structures. En France, l'État dispose de la **DCSSI** (Direction centrale de la sécurité des systèmes d'information) qui dépend du Secrétariat général de la défense nationale, service du Premier ministre, pour coordonner les actions de prévention et de protection des systèmes d'information du pays.

L'Union européenne a suscité, au début de 2004, la création d'une agence européenne chargée de la sécurité des réseaux et de l'information (ENISA). Son principal objectif est de promouvoir le développement d'une culture de la sécurité des réseaux et de l'information au sein de l'Union européenne.

Coopération internationale entre les CERTs

Sur le plan opérationnel, la mise en place de dispositifs d'alerte tels que les CERTs (*Computer Emergency Response Teams*) afin de pouvoir faire face à des attaques de virus ou à toutes sortes de nouvelles vulnérabilités nécessite de nombreux échanges entre les équipes aux niveaux national, régional et international. Pour la France, ces échanges ont lieu à l'échelle internationale au sein du FIRST (*Forum of Incident Response and Security Teams*) et à l'échelle européenne au sein de la TF-CSIRT qui contribue également à la formation des nouvelles équipes.



Pour plus d'informations, consulter le site du CERT français, le Certa : <http://www.certa.ssi.gouv.fr/>.

Pour replacer ces politiques de sécurité dans un cadre plus global, l'OCDE a émis en juillet 2002 des lignes directrices sur la sécurité des systèmes d'information et des réseaux qui ont donné naissance à un nouveau concept : la promotion de la culture de la sécurité.

@ Document à télécharger sur le site de l'OCDE :
<http://webdomino1.oecd.org/COMNET/STI/lccpSecu.nsf>.

D. CONCLUSION

Face à ces trois menaces : le dérèglement du système financier international, les dysfonctionnements des marchés financiers et les attaques de la cybercriminalité, nous avons vu qu'un des éléments de réponse des instances internationales est le renforcement des contrôles des normes de comportement des agents économiques. Dans ce contexte, les organismes rédacteurs de ces normes voient leur rôle s'accroître, de même les contrôleurs ou auditeurs qui en assurent la surveillance.

Mais une autre conséquence de la globalisation des menaces est la nécessaire articulation des réponses à y apporter. Un audit comptable et financier doit intégrer l'évaluation du contrôle interne, de son système d'information et mesurer les capacités de réponse de l'entité face à des menaces, souvent des formes nouvelles qui prennent leur source dans l'utilisation des technologies de l'information et de la communication.

Cela sera le but de la partie qui suit de clarifier l'expression de tous ces organismes qui tentent d'apporter des réponses aux praticiens en quête de référentiels et de bonnes pratiques.

III. LES SOURCES DES NORMES ET RÉFÉRENTIELS

Comme nous l'avons déjà indiqué, les organisations qui produisent des référentiels et des normes dans le domaine de l'audit sont nombreuses et leurs compétences se chevauchent dans de nombreux cas. Elles existent en général au niveau international et sont souvent relayées par des correspondants nationaux.

| Organisme international | Correspondant(s) en France |
|---|---|
| ISO : Organisation Internationale de Normalisation http://www.iso.org/iso/fr | Afnor : http://www.afnor.fr |
| IFAC : International Federation of Accountants http://www.ifac.org | CNCC : http://www.cncc.fr OEC : http://www.experts-comptables.fr/ |
| IIA : The Institute of Internal Auditors http://www.theiia.org/ | IFACI : https://www.ifaci.com |
| ISACA : Information System Audit & Control Association http://www.isaca.org/ | AFAI : http://www.afai.asso.fr/ |

Par ailleurs, les autorités de contrôle des bourses de valeurs mobilières et les tutelles du système bancaire sont regroupées dans des organisations internationales, coordonnées par le FSF (Forum pour la stabilité financière) créé en 1999, avec notamment :

- CBCB : Comité de Bâle sur le contrôle bancaire qui a produit les normes dites « BÂLE II » ;
- OICV : Organisation internationale des commissions de valeurs, qui regroupe les autorités de contrôle des marchés boursiers : <http://www.iosco.org/> ;
 – L'AMF assure cette mission en France : <http://www.amf-france.org/> ;
- AICA : Association internationale des contrôleurs d'assurance, ou IAIS : International Association of Insurance Supervisors qui regroupe les autorités de réglementation des sociétés d'assurance : <http://www.iaisweb.org/> ;
 – Le correspondant français est la Commission de contrôle des assurances, des mutuelles et des institutions de prévoyance (CCAMIP) qui a changé de nom, depuis la loi du 15 décembre 2005, et devient désormais l'Autorité de contrôle des assurances et des mutuelles (ACAM) : <http://www.ccamip.fr/>.

Sans oublier des normalisations américaines qui pèsent d'un poids très lourd :

- référentiel COSO : base de la définition du contrôle interne des entreprises (1992) : <http://www.coso.org> ;
- SOX : Sarbanes-Oxley Act, voté après les scandales financiers Enron, Worldcom... en 2002 ;
- DOD : *US Department Of Defense* qui, en définissant les normes techniques que doivent respecter ses fournisseurs, a toujours joué un rôle important dans l'évolution de l'informatique : <http://www.dodssp.daps.mil/>.

Mais aussi les Britanniques et les Allemands qui gardent des points forts dans la normalisation :

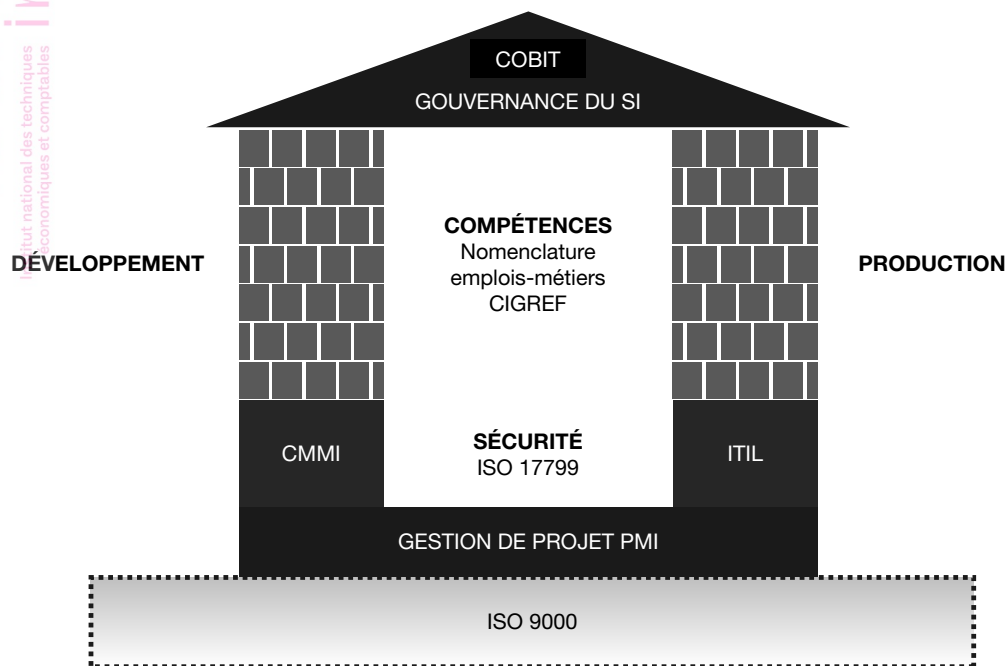
- BSI : British Standards Institution, l'équivalent de l'Afnor français mais avec un budget nettement plus significatif et une production de normes qui est reprise par l'ISO (sur la sécurité informatique en particulier) : <http://www.bsi-global.com/index.xalter> ;
- DIN : Deutsches Institut für Normung, Institut allemand de normalisation, très actif en électronique et en mécanique. Correspondant de l'ISO : <http://www2.din.de/>.

Nous allons maintenant présenter quelques-uns des référentiels les plus significatifs dans l'audit des systèmes d'information.

REMARQUE

Les présentations qui suivent sont volontairement sommaires, il s'agit dans une première approche de donner les traits essentiels de ces référentiels qui ont des objectifs et des origines très différents. Seuls quelques-uns d'entre eux seront étudiés de manière plus approfondie dans la suite de ce cours.

Pour clarifier les rapports que peuvent entretenir entre elles ces différentes approches, le schéma qui suit, proposé par le CIGREF et l'AFAI, est utile.



Source : CIGREF/AFAI

Seront définis pour la suite du cours :

- COBIT, le référentiel de l'ISACA ;
- ISO 17799, devenue ISO 27000 depuis 2005 pour le management de la sécurité informatique ;
- ITIL, une création britannique, désormais devenue une norme ISO 20000 ;
- CMMI, la rationalisation du développement informatique, référentiel développé par l'Université Carnegie-Mellon.

En revanche nous ne traiterons pas de :

- la nomenclature des métiers de l'informatique élaborée par le CIGREF (version 2005) : <http://www.cigref.fr/cigref/livelink.exe?func=ll&objId=401471&objAction=ViewNews> ;
- la PMI : la gestion de projet définie par le Project Management Institute : <http://www.pmi-fr.org> ;
- la famille des normes ISO 9000 qui traite principalement du « management de la qualité » http://www.iso.org/iso/fr/iso9000-14000/understand_selection_use/selection_use.html.

Ces référentiels sont par trop éloignés des objectifs de ce cours. Le lecteur qui s'intéresse à ces sujets pourra s'en informer sur les sites Internet respectifs des organisations qui supportent ces référentiels.

Mais, de plus, nous traiterons de référentiels qui ont un impact fort sur les systèmes d'information et qui ne peuvent pas être ignorés des auditeurs informatiques :

- les normes ISA élaborées par l'IFAC qui est en charge des normes internationales d'audit financier et comptable ;
- le SAC Report qui émane de l'IIA, concepteur des standards de l'audit interne.

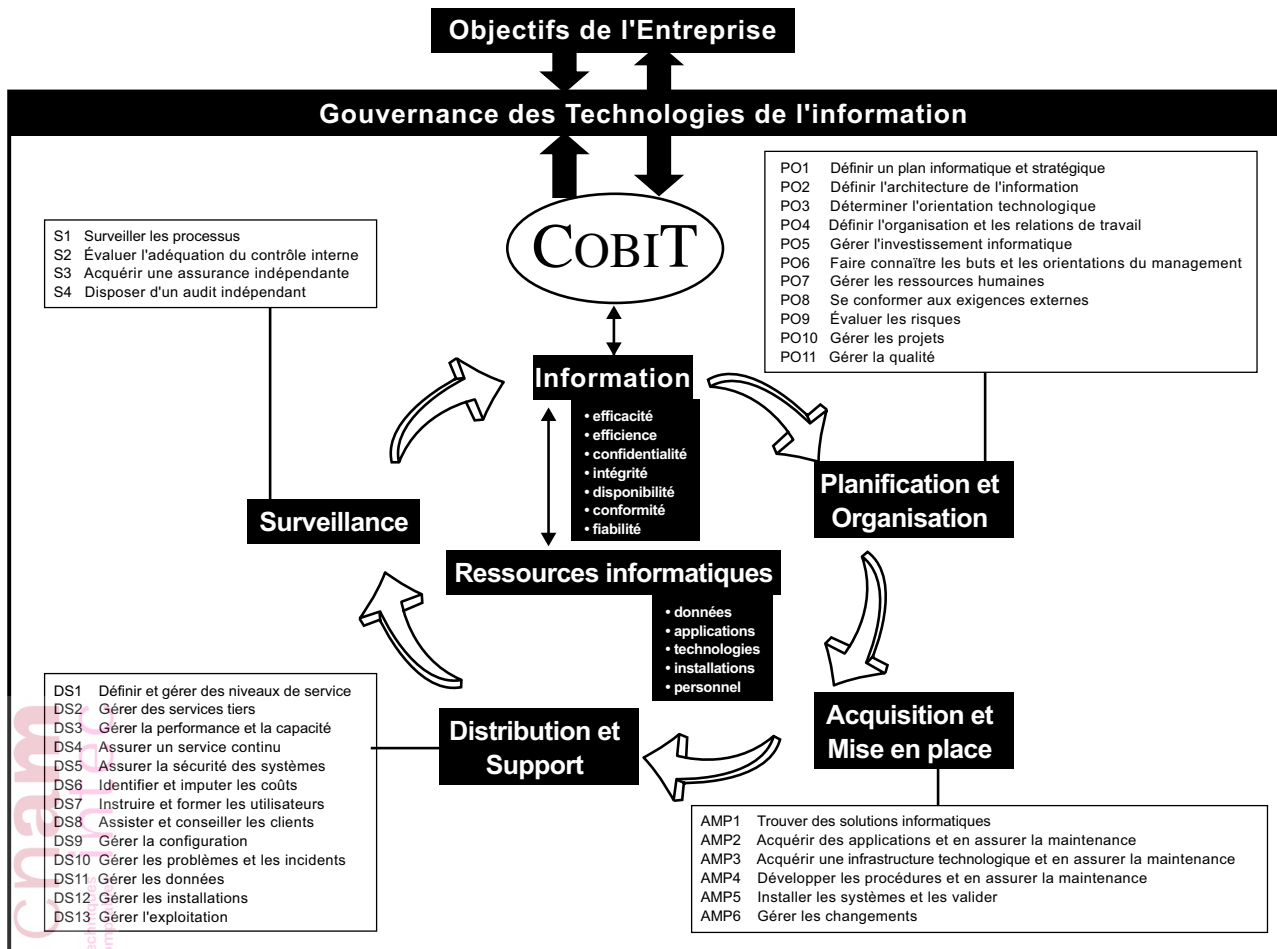
A. COBIT, LE RÉFÉRENTIEL DE L'ISACA

Comme nous l'avons déjà constaté, le fonctionnement des grandes organisations repose complètement sur le traitement de l'information. Un enjeu crucial, face à cette dépendance, est de savoir si les technologies de l'information sont en cohérence avec les objectifs et la stratégie de l'organisation. Le COBIT (*Common Objectives for Business Information Technology*) se veut l'outil de cet alignement.

1. Qu'est-ce que le COBIT ?

Développé par l'ISACA (*Information System Audit & Control Association*) dont l'AFAI (Association française de l'audit et du conseil informatique) est le correspondant en France, COBIT est un référentiel de gouvernance des systèmes d'information qui couvre 34 processus (voir la liste en annexe), répartis en quatre grands domaines :

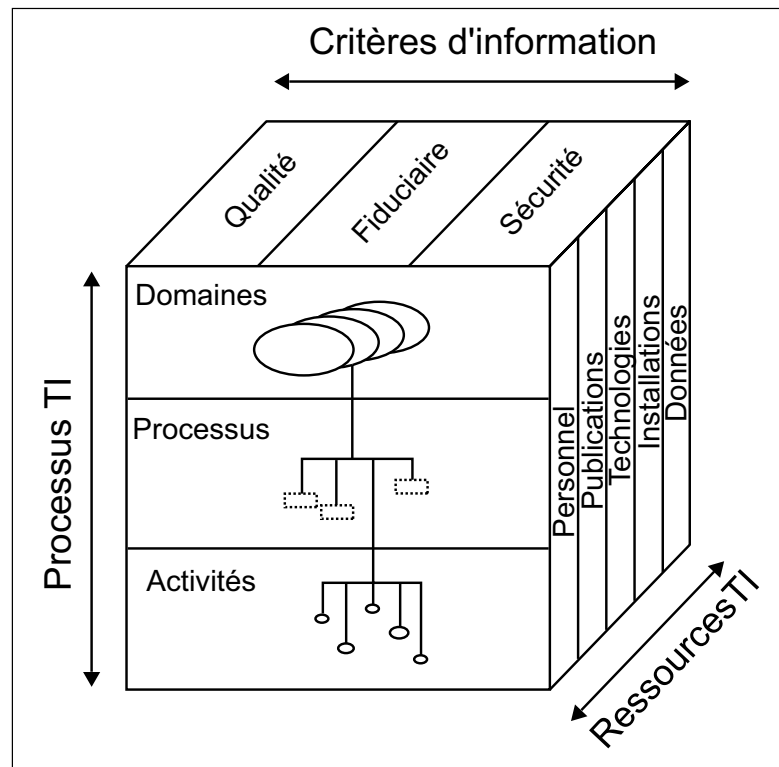
- planning et organisation ;
- acquisition et mise en place ;
- fourniture du service et support ;
- surveillance.



COBIT.

2. COBIT, un référentiel pour l'auditeur en système d'information

À l'origine, les premières versions de COBIT ont été développées par l'ISACA dans le but d'accompagner au mieux la profession des auditeurs des systèmes d'information. Dans cette logique, COBIT peut être utilisé pour mener toute forme d'investigation. Le schéma ci-après illustre l'organisation du référentiel selon un cube permettant d'auditer un processus, un critère d'information et une ressource.



COBIT.

3. Comment est utilisé le COBIT ?

À partir de ce référentiel général, COBIT donne une liste détaillée de plus de 300 objectifs de contrôle qui permettent à l'auditeur de cadrer son investigation. COBIT est utilisé comme une base solide de points de contrôles, il aide à la sélection des zones critiques et à leur évaluation. Même s'il est parfois nécessaire de le compléter en fonction des spécificités du sujet (pour un audit de sécurité il conviendra, par exemple, d'ajouter les aspects propres aux dispositifs de sécurité existants ; il en sera de même pour tout ce qui a trait au domaine légal et réglementaire), COBIT permet de prendre en compte des points qui n'auraient pas été évoqués, faute d'y songer ou par manque de connaissance.

Le référentiel d'audit et/ou de contrôle établi à partir de COBIT permet à des auditeurs non informaticiens de mener de façon professionnelle des audits informatiques intégrés aux audits généraux. Il sert aussi à établir les questions à dérouler lors des entretiens. Le COBIT apparaît de l'avis général comme une bonne base pour construire un référentiel métier dans une organisation. Ceci n'exclut pas pour autant de le compléter par d'autres référentiels que nous présentons plus loin dans ce cours.

4. COBIT un outil de dialogue entre Direction générale et DSI

Pour la DSI (Direction des systèmes d'information), COBIT est fréquemment utilisé comme un outil d'auto-évaluation. C'est un moyen, pour elle, de démontrer à la direction générale que son niveau de maîtrise des systèmes d'information est bon, sur tous les aspects relevant de sa responsabilité. Ainsi, il est plus facile à la DSI de faire face à des auditeurs qui disposent du même référentiel. Cette approche est un moyen de justifier l'importance de mener des projets d'amélioration du système d'information et d'en obtenir le financement.

Par ailleurs, COBIT va servir dans le cadre de l'évaluation de la maturité des processus. Cette approche met en lumière le niveau d'homogénéité des processus des systèmes d'information de l'entreprise.

5. Ce qu'apporte le COBIT sur la gouvernance des systèmes d'information

Ainsi, à partir du référentiel COBIT, l'organisation peut bâtir ses standards pour mettre sur pied un modèle de gouvernance des systèmes d'information (IT Gouvernance). Cette approche permet d'identifier les pistes de progrès que le management doit prendre en charge :

- adéquation des compétences aux enjeux ;
- allocation des ressources ;
- définition claire des processus ou réduction des risques en matière de sécurité des systèmes d'information.

Pour chacune des activités, COBIT propose une série de facteurs clés de succès, des indicateurs cibles, des indicateurs de performance et un maillage entre processus et un modèle de maturité dont les stades sont détaillés pour chaque processus. COBIT est aussi utilisé pour faire un benchmark de différentes entités de l'organisation. Il permet, avec les restrictions d'usage, de se comparer avec d'autres organisations. Plus facilement, il conduit à la définition de ses propres objectifs et à leur évaluation périodique. Les membres de l'ISACA utilisent COBIT dans beaucoup de secteurs d'activité, partout dans le monde. Les spécificités culturelles, les différences au plan technologique, ne semblent pas limiter l'adéquation de COBIT pour l'alignement des systèmes d'information aux objectifs stratégiques de l'organisation.

6. COBIT et le changement

COBIT est encore utilisé dans le cadre de refonte de l'organisation ou des méthodes de travail. C'est un outil d'accompagnement au changement. Il apporte une structure qui permet de clarifier les problèmes. Il contribue à faire travailler ensemble différents départements. Enfin, en cas d'externalisation de tout ou partie de l'activité informatique, ce référentiel aide à déterminer ce qu'on attend du prestataire. Il permet également d'établir les mesures qui, à l'avenir, permettront de s'assurer que le contrat est correctement exécuté.

7. En conclusion

COBIT est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information tout en intégrant les apports d'autres référentiels comme l'ISO 9000, ITIL, CMMI ou, de façon plus générale, les spécificités de l'entreprise. Il a l'avantage d'avoir été conçu pour une approche globale et le désavantage, pour le pilotage, d'être issu de l'audit, ce qui fait que son volet guide de management est moins développé. Enfin, un COBIT Quickstart permet un démarrage encore plus rapide et une bonne appropriation du référentiel.

ANNEXE LISTE DES PROCESSUS DU COBIT

Planification et organisation

- PO1 – Définir un plan informatique stratégique
- PO2 – Définir l'architecture de l'information
- PO3 – Déterminer l'orientation technologique
- PO4 – Définir l'organisation et les relations de travail
- PO5 – Gérer l'investissement informatique
- PO6 – Faire connaître les buts et les orientations du management
- PO7 – Gérer les ressources humaines
- PO8 – Se conformer aux exigences externes
- PO9 – Évaluer les risques
- PO10 – Gérer les projets
- PO11 – Gérer la qualité

Acquisition et mise en place

- AMP1 – Trouver des solutions informatiques
- AMP2 – Acquérir des applications et en assurer la maintenance
- AMP3 – Acquérir une infrastructure et en assurer la maintenance
- AMP4 – Développer les procédures et en assurer la maintenance
- AMP5 – Installer les systèmes et les valider
- AMP6 – Gérer les changements

Distribution et support

- DS1 – Définir et gérer des niveaux de service
- DS2 – Gérer des services tiers
- DS3 – Gérer la performance et la capacité
- DS4 – Assurer un service continu
- DS5 – Assurer la sécurité des systèmes
- DS6 – Identifier et imputer les coûts
- DS7 – Instruire et former les utilisateurs
- DS8 – Assister et conseiller les clients
- DS9 – Gérer la configuration
- DS10 – Gérer les problèmes et les incidents
- DS11 – Gérer les données
- DS12 – Gérer les installations
- DS13 – Gérer l'exploitation

Surveillance

- S1 – Surveiller les processus
- S2 – Évaluer l'adéquation du contrôle interne
- S3 – Acquérir une assurance indépendante
- S4 – Disposer d'un audit indépendant

B. LE RÉFÉRENTIEL ITIL

ITIL (*Information Technology Infrastructure Library* – Bibliothèque de l'infrastructure des technologies de l'Information) est en fait une série de documents portant sur la gestion des services liés aux technologies de l'Information, dont la totalité constitue un référentiel de meilleures pratiques (*best practices*).

1. Historique d'ITIL

ITIL est née en Angleterre à la fin des années 1980, à la suite de la politique de *market testing* – mise en concurrence systématique des prestations internes, notamment informatiques, avec l'offre du marché – imposée par le gouvernement Thatcher aux administrations et entreprises publiques britanniques.

Ce référentiel a été élaboré par des groupes de travail réunissant des responsables opérationnels, des experts indépendants, des consultants spécialisés et des formateurs, sous l'égide de la *Central Computer & Telecommunications Agency* (CCTA), agence gouvernementale anglaise chargée d'améliorer l'efficacité et la qualité des services informatiques centraux des ministères, devenue depuis l'*Office Government of Commerce* (OGC).

ITIL a connu un essor rapide en Angleterre, a été adoptée par plusieurs départements ministériels et par de grandes entreprises publiques et privées aux Pays-Bas et a poursuivi son développement dans de nombreux pays à travers le monde, devenant ainsi un standard de facto, sous l'impulsion de l'ITSMF (*IT Service Management Forum, association des utilisateurs d'ITIL*). Ce développement est assuré aujourd'hui conjointement par l'OGC, l'ITSMF, l'ISEB (*Information*

Systems Examination Board, anglais) et l'EXIN (*EXamination Institute*, hollandais). Ces deux derniers étant des organismes publics ayant pour principales responsabilités :

- la définition de programmes de certification pour les professionnels ;
- l'accréditation des organismes de formation habilités à délivrer des certifications ITIL.

On retrouve ainsi les trois niveaux :

- l'organisme qui fixe les normes ;
- l'organisme (différent du précédent) qui est accrédité pour délivrer une certification ;
- le professionnel certifié qui opère en respectant les normes.

2. Les objectifs d'ITIL

La raison d'être d'ITIL est de constituer un référentiel des meilleures pratiques pour la gestion des services fournis par les technologies de l'information. Les professionnels de l'informatique peuvent trouver ainsi une aide particulièrement intéressante pour aborder cette gestion des services. En particulier les directions informatiques trouveront avec ITIL une approche pour atteindre leurs objectifs de qualité et de maîtrise des coûts puisqu'ITIL a pour objectif la définition de la manière efficace et rentable de fournir, par les technologies de l'information, des services aux métiers de l'entreprise.

3. Trois idées importantes

Pour répondre à cette adéquation entre le métier de l'entreprise et les services fournis par les technologies de l'information, on peut retenir trois idées importantes qui inspirent les concepteurs d'ITIL :

- **l'orientation client** : l'utilisateur-client est positionné au centre des préoccupations de la direction informatique et toutes les activités de l'informatique doivent s'inscrire dans une relation client-fournisseur ;
- **les services s'appréhendent à travers un cycle de vie** : la gestion des services pour être efficace doit être prise en considération en amont des projets informatiques, dès les phases d'étude et de conception ;
- **l'approche par les processus** : la qualité de service repose sur un modèle d'activités se déclinant dans la mise en place de processus informatiques appropriés en étroite corrélation avec les processus métiers.

4. Domaines couverts par ITIL

ITIL définit un service lié aux technologies de l'information comme un ensemble de fonctions assurées par un système d'information pour répondre aux besoins d'un utilisateur dans la réalisation des activités propres à son métier ; un service s'appuie en général sur plusieurs éléments :

- matériels ;
- logiciels ;
- documentation.

Le tout constitue l'infrastructure informatique.

5. Structure d'ITIL

ITIL se présente sous la forme d'un ensemble de livres regroupés en sept domaines, chacun couvrant un aspect particulier de la gestion des services liés aux technologies de l'information :

- *Business Perspective*, consacré aux questions d'organisation et de structure (organisation de la production, relations entre les différentes fonctions, rôles et responsabilités, relations avec les fournisseurs et prestataires externes) ;
- *Application Management*, consacré à la gestion des relations entre études et exploitation (support logiciel, mise en production) ;
- *ICT³¹ Infrastructure Management*, consacré au cycle de vie de l'infrastructure et aux opérations associées (automatisation, maintenance, installation) ;

31. Information and Communication Technologies.

- *Security Management*, consacré à la mise en place et au pilotage de la sécurité informatique de manière générale ;
- *Planning to Implement Service Management*, consacré à la mise en place d'une « approche service » au sein de la DSI.

Mais les deux domaines qui ont fait le succès d'ITIL et qui font l'objet des certifications individuelles sont :

- *Service Delivery* (en français Fourniture des services), concerne la planification et l'amélioration à long terme de la fourniture de services liés aux technologies de l'information et comprend cinq disciplines :
 - gestion des niveaux de service ;
 - gestion financière ;
 - gestion de la capacité ;
 - gestion de la continuité de service informatique ;
 - gestion de la disponibilité.
- *Service Support* (en français Soutien des services), se concentre globalement sur les opérations au jour le jour et le support aux services liés aux technologies de l'information et comprend une fonction et cinq disciplines, le Centre de services (*Service Desk*) et :
 - gestion des incidents ;
 - gestion des problèmes ;
 - gestion des configurations ;
 - gestion des changements ;
 - gestion des mises en production.

Pour chacune de ces disciplines, ITIL propose de couvrir les meilleures pratiques par la description plus ou moins variable des points suivants :

- les objectifs ;
- le périmètre ;
- les concepts ;
- les bénéfices et les difficultés ;
- la mise en place ;
- les activités dans le détail ;
- les indicateurs ;
- et un certain nombre de détails sous forme d'annexes selon les disciplines traitées.

6. Utilisation d'ITIL

La philosophie de l'ITIL est d'adopter une démarche s'appuyant sur des processus suffisamment souples pour s'adapter à toutes les organisations, petites ou grandes. Elle part du principe que la gestion des services est constituée d'un certain nombre de processus étroitement liés et fortement intégrés.

Pour que les principaux objectifs en matière de gestion des services puissent être atteints, ces processus doivent utiliser les ressources humaines et les produits de manière efficace, rentable et économique de sorte que les services liés aux technologies de l'information soient innovants, de haute qualité et adaptés aux processus de l'entreprise.

Les organisations ne doivent pas être trop ambitieuses lors de la mise en œuvre de la gestion des services. La plupart d'entre elles possèdent déjà des éléments d'organisation déployés et opérationnels. L'activité de mise en œuvre de la gestion des services concerne donc plutôt l'amélioration des processus existants.

Pour ce faire, il est nécessaire de bien connaître son point de départ en évaluant la maturité de ses processus existants par exemple, ainsi que de s'assurer de l'implication du management pour engager une telle démarche et que les conditions d'un changement culturel sont satisfaites pour modifier le comportement de l'organisation dans la fourniture des services.

Les processus de gestion des services peuvent être mis en œuvre les uns à la suite des autres ou simultanément et chaque processus peut être décomposé en une série d'activités. L'utilisation

de ces meilleures pratiques est soutenue par un éventail de formations et de certifications qui est utilisé dans le monde entier pour reconnaître les compétences professionnelles nécessaires en matière de gestion des services liés aux technologies de l'information.

7. Intérêt d'ITIL

L'indéniable succès d'ITIL, en progression constante depuis plusieurs années auprès des entreprises et des organismes publics, en Europe, aux États-Unis et en Orient s'explique par plusieurs raisons :

- ITIL permet aux entreprises de capitaliser sur une expérience pratique de bientôt 20 ans sur la gestion des services informatiques, et de gagner du temps en évitant de réinventer la roue et en utilisant des éléments déjà testés et éprouvés (processus, règles de gestion, descriptions de postes, etc.) ;
- ITIL offre les avantages d'une méthode publique, standard de facto dans certains pays avec plus de 10 000 livres vendus chaque année, des groupes d'utilisateurs très actifs et à l'écoute des DSI ;
- le marché se développe autour d'ITIL (formation, conseil, progiciels) permettant aux professionnels du domaine de disposer de repères et de formalisme au-delà des frontières de leurs propres organisations.

8. Un cadre de référence commun

On retrouve les avantages des référentiels pour faciliter le dialogue entre les différents acteurs à partir d'un cadre de référence commun :

- entre DSI et DG ;
- entre DSI et utilisateurs/clients ;
- entre DSI et équipes informatiques ;
- entre DSI et prestataires externes.

La définition du référentiel ainsi que la gestion de la certification est sous la responsabilité de l'IT Service Management Forum, qui définit les critères pour les sociétés certificatrices.

L'ITSMF France forme le chapitre français de l'ITSMF (IT Service Management Forum), association regroupant les principaux utilisateurs d'ITIL et représentant plus de 1 000 sociétés dans le monde.

L'ITSMF France a vocation à mettre en place un forum permettant aux adhérents d'échanger leurs idées ou leurs expériences autour des meilleures pratiques, et de les faire évoluer. Plus de 50 sociétés ont d'ores et déjà manifesté leur intérêt en adhérant à l'association.

@ Site Internet : www.itsmf.fr.

Le *British Standards Institution* (BSI) a défini un standard, BS 15 000, basé sur ITIL. Cette norme est devenue la base d'une norme ISO/IEC³² 20 000 publiée en novembre 2005. Aujourd'hui, une organisation peut donc être certifiée BSI 15 000 et elle serait certifiable ISO 20 000 en 2006 au plus tôt.

C. CMMI : LA RATIONALISATION DU DÉVELOPPEMENT INFORMATIQUE

Les normes de management de la qualité et de gestion des processus sont nombreuses. La non-qualité dans le domaine des technologies de l'information a un coût, et il est élevé ! Projet débouchant sur l'abandon de développements coûteux, mise en production d'applications ne répondant pas aux attentes des utilisateurs, pannes à répétition... Pour lutter contre ces dérives, des propositions de normes existent ; dans le cadre de l'ISO, elles se définissent dans les déclinaisons de la norme ISO 15504 « Technologies de l'information – Évaluation de processus de logiciel ».

32. IEC : Commission électrotechnique internationale.

Pour mettre en œuvre ces normes, une méthode, le CMMI (*Capability Maturity Model Integrated*), est construite comme un référentiel pour mesurer la maturité et la capacité de l'organisation de mener à bien les processus nécessaires dans le domaine du génie logiciel. Il est à noter que CMMI n'a pas le statut de norme ISO, mais est maintenu et développé par le SEI (*Software Engineering Institute*) qui est un institut de l'université américaine Carnegie-Mellon.

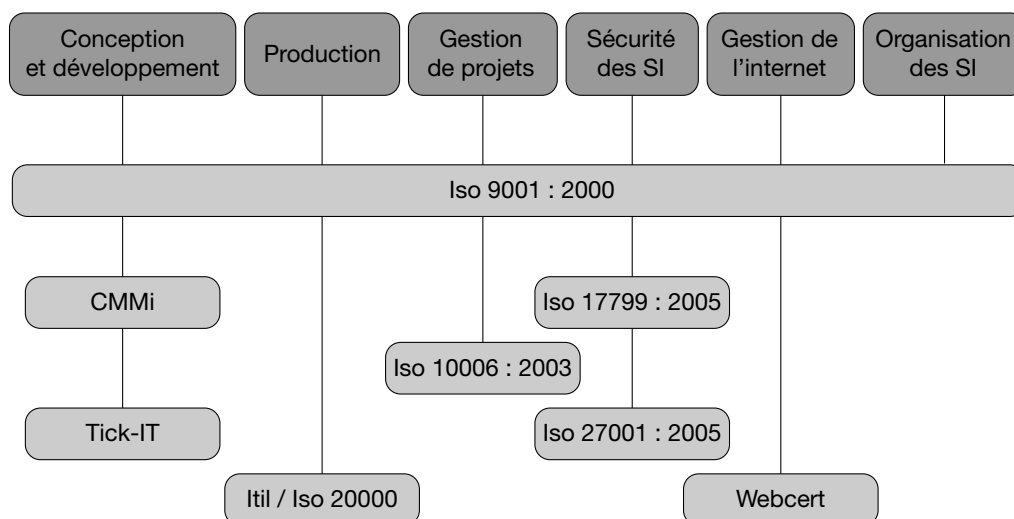
@ Pour plus de détails sur cette méthode voir le site du SEI : <http://www.sei.cmu.edu>.

Du fait que CMMI n'est pas une norme, il n'est pas possible d'obtenir une certification, mais en revanche une évaluation de la maturité suivant le référentiel CMMI est possible. Cette évaluation est connue sous le nom de SCAMPI (*Standard CMMI Appraisal Method for Process Improvement*). Les résultats définitifs indiquent la notation obtenue (niveau de maturité) ainsi que la description des forces et opportunités d'amélioration de chaque domaine de processus du périmètre évalué. Cette évaluation peut être menée par des auditeurs internes formés sur ce référentiel.

D. ISO 27000 : 2005 NORMES POUR LE MANAGEMENT DE LA SÉCURITÉ INFORMATIQUE

L'ISO supporte différentes normes qui couvrent divers aspects des métiers de l'informatique. Le schéma qui suit positionne les référentiels en regard des métiers.

Positionnement des Référentiels selon les métiers du Secteur de l'Informatique



AFAQ / AFNOR
CERTIFICATION

Afaq-Afnor.

La famille ISO 27000 recouvre donc les normes de la sécurité informatique. Actuellement, ces normes sont reprises des travaux de normalisation du BSI britannique (les standards BS 7799 depuis 1995).

En fait, la norme initiale avait été séparée en deux par le BSI, la BS7799-1 qui a été adoptée par l'ISO sous le numéro ISO 17799 en 2001, et qui deviendra en 2007 ISO 27002. Cette norme comprend la politique de sécurité, l'organisation de la sécurité, la sécurité du personnel, le contrôle d'accès, le développement, la maintenance, etc. Une version contenant des évolutions significatives a été publiée en 2005 contenant entre autres un chapitre sur l'analyse de risques.

Parallèlement, la BS7799-2 est devenue l'ISO 27001 en 2005 pour initier une nouvelle famille de normes consacrée à la sécurité des systèmes d'information.

1. La norme ISO 27001 : Système de management de la sécurité de l'information (SMSI)

Cette nouvelle norme permet aux entreprises et aux administrations d'obtenir une certification qui atteste de la mise en place effective d'un système de management de la sécurité de l'information (SMSI). Cette norme garantit aux parties prenantes (clients, actionnaires, partenaires, etc.) que la sécurité des systèmes d'information a été sérieusement prise en compte et que l'entreprise s'est engagée dans une démarche d'amélioration constante.

Comment mettre en place un système de management de la sécurité de l'information conforme à la norme ISO 27001 ?

- définition d'un responsable projet ;
- définition des budgets ;
- analyse de risques ;
- implication de la direction ;
- politique de sécurité ;
- construction du système de management ;
- sensibilisation ou formation des collaborateurs ;
- audits internes ;
- mise en œuvre du PDCA (Préparer, Développer, Comprendre, Agir).

2. Certification en ISO 27000

Comment auditer un SMSI selon les critères de l'ISO 27001 ?

Un organisme de certification vient vérifier la conformité du système de management au référentiel ISO 27001. À l'issue de cet audit, et si l'entreprise répond aux exigences de la norme, l'organisme de certification délivre un certificat valable pour une durée de trois ans.

Principes équivalents à tout audit :

- analyse du SMSI selon un plan d'audit préétabli ;
- analyse des pratiques de l'entreprise en fonction des procédures et des exigences du référentiel ;
- détection des écarts significatifs (non-conformité ou remarque) ;
- deux audits de suivi durant la période de 3 ans.

Quels sont les organismes accrédités pour délivrer une certification ISO 27000 ?

@ Tous les organismes accrédités sont répertoriés sur le site : <http://www.xisec.com>.

E. LES NORMES ISA ÉLABORÉES PAR L'IFAC

Comme nous l'avons déjà indiqué, le FSF a confirmé en 1999 la responsabilité confiée à l'IFAC (*International Federation of Accountants*) d'élaborer et de maintenir les normes de l'audit sous l'appellation ISA (*International Standard on Auditing*).

Pour être plus précis, indiquons que c'est un « board » spécifique qui, au sein de l'IFAC, est chargé de cette mission : l'*International Auditing and Assurance Standards Board* (IAASB).

@ Ces normes sont disponibles sur le site de l'IFAC : <http://www.ifac.org/Guidance/>.

Vous pouvez ainsi télécharger gratuitement un document au format PDF de 1 098 pages en anglais qui regroupe sous la dénomination de « *handbook* » ou « manuel » l'ensemble des normes de l'audit financier en application pour les années 2006 et suivantes. Tous les auditeurs du monde entier seront amenés à se référer à ce corpus impressionnant ; en France certaines de ces normes ont déjà été transposées. Voyons maintenant le contenu de cet ensemble.

Après une rapide introduction qui présente l'IFAC et qui évoque certaines informations qui ne sont pas dans le « *handbook* », la première partie est consacrée à l'« *Ethics* » que nous traduisons en français par Code de l'éthique ou de déontologie.

En fait, l'année 2006 voit s'appliquer la nouvelle déontologie des professionnels comptables. Le « *handbook* » présente les deux codes, l'ancien de 2002 et le nouveau de 2005 qui s'applique à partir du 1^{er} juillet 2006.

La nouveauté essentielle consiste dans l'accent mis par ce Code éthique sur la notion d'indépendance du professionnel en matière d'audit. Ce code prend en compte les observations importantes et les exigences de la SEC américaine (*Securities and Exchange Commission*). Une nouvelle version spécifique, adaptée aux besoins des sociétés cotées en Bourse, prévoit explicitement l'obligation de mettre au point des mécanismes permettant de sauvegarder l'indépendance des auditeurs. Le code décrit des situations dans lesquelles aucune protection ne saurait suffire et dans lesquelles il faut dès lors renoncer à exécuter le contrôle ou à exercer la mission proposée. C'est toute la question des autres missions que celle d'audit légal qui est posée. Les grands réseaux d'audits et de conseils se montrent peu enthousiastes pour ces prescriptions qui sont d'ailleurs reprises dans le cadre de la huitième directive.

La seconde grande partie de l'ouvrage est consacrée aux normes professionnelles qui encadrent l'exercice du métier d'auditeur : approche par les risques, attitude à observer face aux fraudes, etc.

Les anciennes normes qui spécifiaient le comportement du professionnel dans un environnement informatisé sont pratiquement toutes abrogées : le contexte étant toujours celui de l'informatique, toutes les normes sont supposées s'appliquer dans cet environnement. La transposition de ces normes en France est effective depuis l'été 2006 qui a vu le ministère de la justice faire paraître les arrêtés nécessaires.

F. L'IIA, CONCEPTEUR DES STANDARDS DE L'AUDIT INTERNE

http://www.theiia.org/index.cfm?doc_id=123

Définition

« L'**audit interne** est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée.

Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. »

Version française de la définition internationale, approuvée le 21 mars 2000
par le conseil d'administration de l'institut de l'audit interne.

L'IIA est représenté en France par l'IFACI. L'intérêt porté par les instituts de l'audit interne aux systèmes d'information est ancien, à preuve la rédaction en 1977 d'un document, le « *SAC Report* » servant de guide aux auditeurs. Une nouvelle version est parue en 1991 (traduite en français en 1992). Il n'existe pas de version numérique disponible librement du *SAC Report* (à notre connaissance). À consulter uniquement en bibliothèque.

Le SAC Report

Le *SAC Report* ou Rapport sur l'audit et le contrôle des systèmes d'information, dans sa version 1991, est le fruit de travaux menés en commun par de nombreux consultants, appuyés par de grandes entreprises qui en ont supporté les coûts.

Le *SAC Report* est structuré en dix modules organisés de la sorte :

- un module de pilotage général :
 - management de l'audit et du contrôle interne ;
- un module d'outils génériques :
 - les outils informatiques de l'audit ;

- cinq modules opérationnels :
 - gestion des ressources informatiques,
 - gestion de l'information et développement des systèmes,
 - audit des systèmes applicatifs,
 - informatique départementale et individuelle,
 - technologies nouvelles ;
- trois modules d'infrastructures :
 - télécommunications,
 - sécurité,
 - plan de secours.

L'absence de nouvelle version fait du *SAC Report* un document de référence mais qui reste un peu confiné parmi les membres de l'IIA. Il a le grand mérite de bien structurer le champ d'intervention de l'auditeur en se calant sur les grandes fonctions et l'organisation généralement rencontrée dans les organisations de grande taille. Pour les PME, il sera nécessaire de l'adapter.

IV. LE CONTRÔLE FISCAL DES COMPTABILITÉS INFORMATISÉES

La loi de finance 1990 a défini les modalités de contrôle des comptabilités informatisées. La mise en œuvre de ces contrôles impose l'existence d'une documentation du système d'information ainsi que la disponibilité des données de gestion élémentaires couvrant le délai de reprise de l'administration.

Après un rappel de ce dispositif, notre objectif est d'étudier **les impacts de la nouvelle instruction publiée le 24 janvier 2006** et de distinguer les principales recommandations qui résultent de la pratique constatée en entreprise.

A. RAPPEL DU DISPOSITIF RÉGLEMENTAIRE

L'article L. 13 du Livre de procédures fiscales stipule :

« Lorsque la comptabilité est tenue au moyen de systèmes informatisés, le contrôle porte sur l'ensemble des informations, données et traitements informatiques qui concourent directement ou indirectement à la formation des résultats comptables ou fiscaux et à l'élaboration des déclarations rendues obligatoires par le Code général des impôts ainsi que sur la documentation relative aux analyses, à la programmation et à l'exécution des traitements. »

Alinéa complémentaire issu de l'article 103 de la loi de finance 1990.

Le terme comptabilité ne doit donc pas être interprété restrictivement à la comptabilité générale et clients mais bien au contraire comme faisant référence au « système comptable étendu » qui englobe les systèmes opérants (appelées aussi applications métiers ou de gestion) qui détiennent les pièces comptables dématérialisées dans leurs bases de données.

Ce droit d'accès s'applique donc :

- aux données élémentaires prises en compte par le système d'information (cf. Bulletin officiel des impôts (BOI) n° 245 du 24 décembre 1996) sur la période contrôlée ;
- à la documentation et aux programmes sources (L.102B du LPF).

Trois modalités de mise en œuvre sont prévues par l'article 47A du LPF pour chaque point contrôlé :

- réalisation des traitements par l'entreprise sous contrôle de l'administration (option la plus utilisée) ;
- fourniture de copies des fichiers à l'administration (Brigade de vérification des comptabilités informatisées) ;
- utilisation des moyens informatiques de l'entreprise.

Dans la pratique, l'administration s'appuie sur la réglementation comptable et fiscale pour exiger une traçabilité (i.e. piste d'audit) entre les transactions de gestion et leur traduction comptable. À défaut de pouvoir réconcilier ces éléments, elle peut mettre en œuvre un rejet de comptabilité et une évaluation d'office (art. L. 74 al 2 du LPF).

La mise en œuvre de la piste d'audit dans un contexte de contrôle fiscal suppose :

- l'archivage des données détaillées appréhendées par le système d'information durant le délai de reprise de l'administration (6 ans) ;
- la possibilité de restaurer des supports de stockage et de les mettre en œuvre (serveur, OS et base de données) pour disposer du choix de l'article 47 A.

B. LE BULLETIN OFFICIEL DES IMPÔTS N° 12 DU 24 JANVIER 2006

Ce nouveau texte apporte des contraintes lourdes et pas nécessairement justifiées. Il devrait donner lieu à de multiples réactions et son interprétation mérite d'être suivie.

REMARQUE

Les renvois aux paragraphes du BOI sont signalés entre parenthèses dans le texte.

1. Les dispositions rappelées

- Rappels de principes fondamentaux du PCG 1999 :

« Les documents comptables [informatiques] doivent être identifiés, numérotés et datés dès leur établissement par des moyens offrant toute garantie en matière de preuve. »

§ 15, décret 83-1020 modifié par le 2002-312.

« Une documentation décrivant les procédures et l'organisation [...] en vue de permettre la compréhension et le contrôle du système de traitement. Cette documentation est conservée aussi longtemps qu'est exigée la présentation des comptes auxquels elle se rapporte. »

§ 16, PCG art 410-2.

« Tout enregistrement comptable doit préciser l'origine, le contenu et l'imputation de chaque donnée ainsi que les références de la pièce justificative qui l'appuie. »

§ 17.

Le caractère intangible des écritures comptables impose aux logiciels de comptabilité une procédure de validation. Ce traitement « volontaire » consiste à verrouiller toute possibilité de modification des écritures (§ 21 et 22).

Il en résulte que (§ 23) :

- toute fonction permettant de modifier ou supprimer une écriture **validée** est prohibée ;
- un logiciel ne permettant pas une telle validation des écritures conformément à l'article 420-5 du PCG conduira à s'interroger sur le caractère régulier et probant de la comptabilité.

La clôture d'une période comptable, et à plus forte raison d'un exercice, impose la validation des écritures concernées (§ 25 à 27) qui restent consultables ou éditables (§ 28). La réouverture d'un exercice clos à des fins de modification est interdite (§ 29).

L'article 420-6 du Plan comptable général énonce de même :

« Une procédure de clôture destinée à **figer la chronologie** et à garantir l'intangibilité des enregistrements est mise en œuvre au plus tard avant l'expiration de la période suivante. »

§ 26.

Il reste à définir la date servant à cette chronologie : saisie, opération, validation comptable, traitement ?

L'esprit de ce texte conduit à considérer que l'administration souhaite qu'il y ait une clôture raisonnablement rapide des périodes comptables afin de garantir leur intangibilité.

Il faut toutefois pouvoir revenir exceptionnellement sur une période pour constater une opération rétroactive (fusion ou acquisition).

Le PCG (art. 410-3) prévoit un « chemin de révision » permanent :

« Permettant de reconstituer à partir des pièces justificatives appuyant les données entrées, les éléments des comptes, états et renseignements, soumis à la vérification, ou, à partir de ces comptes, états et renseignements, de retrouver ces données et les pièces justificatives. »

§ 30.

Cette fonctionnalité est communément appelée piste d'audit ascendante et descendante.

Le périmètre du CFCI concerne les logiciels de gestion (tels : gestion commerciale, de production, des achats, des stocks, du personnel), quand leurs informations, données et traitements, permettent d'élaborer ou de justifier indirectement tout ou partie des écritures comptables ou des déclarations soumises à contrôle (§ 36).

2. Les mesures préparatoires à la charge des entreprises

Le fait d'utiliser un progiciel fonctionnant sur un ordinateur « interne » ou « externe » (ASP, extranet, service bureau, système d'une société mère...) ne doit pas limiter l'accès à sa documentation dont le programme source fait partie. Des modalités contractuelles doivent permettre l'accès à ces fichiers (dépôts des programmes sources notamment) (§ 57).

Cette mise en garde figurait déjà en première page du BOI du 24 décembre 1996. Nous constatons régulièrement que les entreprises de toutes tailles négligent l'accès aux codes sources des progiciels.

Pour autant, le dépôt de ces derniers auprès d'un tiers archiveur répond à la contrainte fiscale tout en contribuant à pérenniser le logiciel en cas de disparition de l'éditeur.

La documentation doit être disponible (§ 55 et 60) et si nécessaire traduite « rapidement » en français (§ 61 et 62).

L'entreprise devra dissocier la sauvegarde régulière des données de l'archivage fiscal (§ 98) réalisé à date de clôture comptable (PCG art. 420-6) (§ 99).

Nos interventions nous donnent régulièrement l'occasion de souligner cette différence en termes d'objectif et d'organisation.

La sauvegarde a pour objet de pallier une défaillance technique. Sa durée de vie est courte. Bien au contraire, l'archive est initiée par les utilisateurs pour figer les données de manière atemporelle.

L'archivage des données concerne les fichiers (ou tables) d'en-têtes et de lignes (exemple d'une facturation) ainsi que tous les fichiers liés à la facture (code TVA, article facturé...).

« Il en sera de même pour les autres pièces justificatives, telles que les commandes et bons de livraisons, qui obéissent aux mêmes règles d'archivage. »

§ 106.

L'administration illustre le principe du système comptable étendu et la nécessaire traçabilité des données depuis les différentes étapes d'un processus de gestion jusqu'à sa comptabilisation. Le périmètre de l'archivage des données en découle logiquement.

3. Mise en œuvre du CFCI

« Lorsque, en application de l'article L. 47 A, alinéa 1 du livre des procédures fiscales, les agents effectuent la vérification sur le matériel utilisé par le contribuable, ce dernier doit prendre toute mesure utile permettant la préservation de l'intégrité des données et la sécurité du matériel et des logiciels. »

§ 145.

Cette mesure conservatoire demandée par l'administration laisserait-elle supposer que ses contrôleurs, qui sont des informaticiens aguerris, seraient exempts de responsabilité en cas de négligence voire de non-respect des articles 323-1, 2, 3 du Code pénal relatifs aux intrusions et altérations des systèmes d'information ?

Il est à noter que ce paragraphe figurait à l'identique dans l'instruction du 14 octobre 1991.

Si l'entreprise met à disposition des ressources informatiques pour la mise en œuvre des contrôles (art. 47A al. 1), elle doit tout particulièrement « cloisonner » l'environnement de travail des contrôleurs ainsi que leur profil d'accès aux divers serveurs, applications et bases de données.

4. Les éléments nouveaux

a. Nouveautés – archivage des traitements

À des fins de tests ou d'analyse, l'instruction demande explicitement l'archivage de chaque version de traitement (i.e. programme) durant le délai de reprise (§ 48).

Ou encore :

« L'attention est toutefois appelée sur l'intérêt pour les contribuables de conserver les versions antérieures de logiciels et de progiciels, lorsque cela sera nécessaire à la bonne compréhension des traitements aboutissant à la formation des résultats. »

§ 91.

« La procédure d'archivage du progiciel ou logiciel comptable pourra permettre de réaliser une simulation ultérieure des traitements en conservant les données, programmes et environnement nécessaires. »

§ 103.

Cette contrainte maintenant explicite est particulièrement lourde puisqu'elle impose de conserver des équipements sans objet et d'en assurer la maintenance et le coût d'utilisation.

L'organisation de ce BOI permet de considérer que l'obligation porte sur le logiciel comptable *stricto sensu* et non sur ceux du domaine de gestion.

Un « environnement » permettant de réaliser des « simulations » sur des données archivées sous-entend que l'on peut mettre en œuvre des traitements. Il faut donc disposer des serveurs, système d'exploitation, base de données et enfin du logiciel et des données.

Il ne faut pas mésestimer les conséquences financières, techniques et organisationnelles induites.

« Techniquement, l'utilisation de fichiers images "PDF", "print", par exemple, ou tout autre format image standard compatible avec les micro-ordinateurs de type PC, peuvent être valablement utilisés par les entreprises, afin de remplir leur obligation de présentation [dans le cadre de l'article 54 du LPFR]. »

§ 118.

L'administration reconnaît explicitement la possibilité de présenter les documents comptables sous forme de documents numériques. Cette option ne dispense pas de l'archivage des données (§ 119).

b. Nouveautés – accès à la documentation

Un distinguo apparaît en matière de documentation ; si le logiciel est un produit standard (progiciel), la documentation utilisateur est un minimum requis pour comprendre le fonctionnement du système (§ 53 à 56).

A contrario, si le logiciel a nécessité un paramétrage significatif ou une interface en amont ou aval du logiciel, une documentation complémentaire est nécessaire à sa compréhension. Plus le système est complexe et intégré, plus la documentation doit se rapprocher de celle attendue pour un logiciel spécifique.

Selon le BOI n° 12 du 24 janvier 2006 § 55, lorsque le logiciel est spécifique, la documentation attendue est la suivante :

- le dossier de conception générale ;
- le dossier des spécifications fonctionnelles ;
- les dossiers technique, organisationnel et d'architecture ;
- le dossier de maintenance ;
- le dossier d'exploitation ;
- le dossier utilisateur.

Il est à noter que la description de la documentation est sensiblement différente de celle du BOI du 24 décembre 1996... elle-même différente de celle du BOI du 14 novembre 1991.

« Lorsque la documentation informatique est créée ou détenue par un tiers, celui-ci est tenu de la mettre à disposition de l'administration fiscale en cas de contrôle. »

§ 135.

Il est difficile d'imaginer comment ce texte peut trouver à s'appliquer. Il est à noter qu'il n'existe aucune contrainte réglementaire et a fortiori de sanction applicable au tiers concerné.

c. Nouveautés – archivage des données

Il est observé qu'un archivage réalisé en format « propriétaire » impose à l'entreprise de pouvoir relire le support informatique et accéder au fichier archive (§ 88).

Cette situation sous-entend une surveillance de l'obsolescence technique et fonctionnelle des supports de stockage, des périphériques de lecture-écriture et des logiciels de sauvegarde-restauration.

L'administration entend prévenir des difficultés par ailleurs rencontrées.

L'impossibilité technique d'accéder aux données ou de pouvoir les utiliser prive l'entreprise du choix de l'article 47 A, voire l'expose à l'évaluation d'office (art. L. 74 al. 2) si in fine les données ne sont pas disponibles (§ 163).

En cas de déclaration rectificative, les comptes doivent traduire les modifications intervenues par des écritures complémentaires permettant de tracer l'évolution des soldes (§ 109).

Dans le même esprit, les données de gestion éventuellement modifiées doivent être « *clairement identifiées et tracées* » une archive reflétant la déclaration rectificative doit être réalisée (§ 110). Si cette traçabilité est réalisée par un fichier « log », ce dernier fait partie du périmètre de contrôle [et donc de l'archivage].

« Les solutions d'archivage et de traçabilité retenues par les entreprises pourront s'accompagner, par exemple, d'une sécurisation des documents dématérialisés et des données, notamment comptables au moyen d'une signature électronique fiable. »

§112.

Cette évocation de la signature électronique ressemble plus à une piste de réflexion qu'à une disposition applicable.

En effet, le texte ne précise pas si la signature est applicable aux pièces comptables émises ou reçues, ni à la documentation du système ou encore aux archives de données. De surcroît, on peut se demander si la signature aurait pour objet d'authentifier l'auteur d'une écriture, de sceller un état voire de l'horodater.

Au regard des coûts et des complexités de mise en œuvre technique et organisationnelle, la sagesse devrait conduire à ne rien faire.

« Conformément à l'article R. 102 C-1 III du même livre [LPF], le contribuable s'assure que les factures et données détenues par lui-même ou en son nom et pour son compte, par un client ou par un tiers sont accessibles, en cas de contrôle, dans le meilleur délai, depuis son siège ou son principal établissement, quel que soit le lieu de détention de ces documents. »

§ 137.

Il en résulte que le sous-traitant doit s'assurer de la bonne conservation des données qu'il détient pour le compte de ses clients. On privilégiera en la matière un contrat circonstancié définissant les obligations des parties.

d. Nouveautés – comptabilité non régulière ou non probante (§ 157 et 158)

« En présence de comptabilités informatisées, l'attention est attirée sur le fait qu'une apparence de régularité peut être aisément obtenue par certaines fonctions du logiciel justifiant les écritures comptables en permettant :

- l'utilisation de brouillards permanents avec des éditions conformes aux journaux clôturés ;
- la suppression ou la modification d'enregistrements génériques sans laisser de trace ;
- la clôture apparente d'un exercice pour établir les comptes annuels. »

« Les exemples ci-après illustrent, sans être exhaustifs, les situations qui peuvent conduire à considérer que la comptabilité informatisée est irrégulière et/ou non probante :

- la présentation sous des formats non recevables (illisibles, propriétaires) des documents comptables et pièces justificatives dématérialisés, visés à l'article 54 du code général des impôts ;
- le défaut de validation des écritures comptables ou des pièces justificatives ;
- le défaut de clôture des exercices comptables ;
- le défaut de traçabilité ;
- l'absence de chronologie dans les enregistrements ;
- l'absence de permanence du chemin de révision ;
- l'insuffisance des données archivées : échantillons de données ou uniquement données agrégées (centralisation mensuelle par exemple). »

e. Nouveautés – mise en œuvre du CFCI

« La proposition de rectification visée à l'article L. 57 du livre des procédures fiscales précise la nature et le résultat des traitements effectués par ou à la demande de l'administration fiscale, lorsque ces traitements donnent lieu à rectification. Un exposé clair de la démarche suivie doit permettre au contribuable d'être en mesure de formuler ses observations ».

§ 132.

On peut s'étonner que l'administration ne soit pas tenue à une information plus circonstanciée notamment lorsqu'elle réalise elle-même les traitements. Dans un tel cas de figure, le seul principe du « droit à la défense » et du débat contradictoire devrait la conduire à présenter les objectifs de contrôle, la démarche de traitement et les programmes sources mis en œuvre.

À défaut, le contribuable ne connaît pas la « formule de calcul » réellement appliquée ce qui lui interdit d'en contester le bien-fondé comme la programmation.

C. IMPACTS

Cet article L. 13 présente les trois grands domaines impliqués que sont la documentation, l'archivage des données et celui des traitements.

1. Documentation requise

L'administration précise ainsi les éléments de documentation attendus dans l'instruction du 14 octobre 1991 annexe II (BOI n° 207 du 28 octobre 1991) :

- Le dossier des spécifications fonctionnelles définit de façon précise les entrées et sorties du système, les règles de fonctionnement et l'ensemble des contraintes.
- Le dossier de réalisation informatique définit de façon détaillée la conception et la construction de la solution informatique répondant aux spécifications fonctionnelles et notamment :
 - le découpage en chaînes de traitement ;
 - la description des unités de traitement ;
 - la description organique des fichiers et les schémas des bases de données ;
 - la codification et la normalisation des données ;
 - le code source des programmes.
- Le dossier d'étude de l'organisation a pour objet la définition au niveau le plus fin de l'organisation administrative et des procédures d'information.
- Le dossier de maintenance reprend l'historique des mises à jour effectuées sur tout ou partie d'une application, en vue de reconstituer les procédures ayant concouru à la détermination des résultats déclarés.
- Le dossier d'exploitation contient l'ensemble des informations nécessaires à l'implantation et à l'exploitation du système. Il est complété par des procédures internes du service exploitation (planning et journal des incidents notamment).
- Le dossier utilisateur constitue le mode d'emploi du système, rédigé à l'initiative des responsables opérationnels, à l'attention du personnel d'exécution.

Il est intéressant de constater ci-dessus que les exigences de l'administration se sont « recentrées » avec le BOI du 24 décembre 1996 puis celui du 24 janvier 2006.

Autant de BOI que de descriptions de la documentation attendue. À l'évidence, ce sont les objectifs de la documentation qui doivent être poursuivis.

Il est rarissime qu'un système d'information soit documenté d'une manière aussi parfaite que théorique. Sans chercher à atteindre un tel niveau de complétude, il est indispensable de créer un niveau minimal de documentation tant pour les raisons fiscales déjà évoquées que dans un souci de pérennité et « d'auditabilité » du système d'information.

En outre, l'administration accepte toutes les formes de documentation (y compris les sources des programmes) si l'ensemble des éléments qui lui sont présentés apporte une description suffisamment précise et explicite des règles de gestion appliquées (cf. instruction fiscale du 24 décembre 1996).

Cette documentation doit être disponible lors du contrôle. Il est admis qu'elle soit rédigée en langue étrangère. Dans un tel cas de figure, une traduction doit pouvoir être faite rapidement pour tout ou partie de la documentation.

2. Conservation des données élémentaires

L'article L. 102B du LPF instaure une obligation de conservation des données élémentaires pour l'ensemble des applications concernées (cf. art. L. 13 du LPF).

Cette conservation doit être faite sur support informatique durant le délai de reprise. Les données conservées doivent être celles qui sont en entrée du système d'information et non celles qui résultent d'une agrégation ou d'une quelconque transformation informatisée, interface par exemple. L'instruction du 24 décembre 1996 précise confusément comment conserver les données relatives aux interfaces.

Si l'environnement informatique de l'entreprise est modifié durant le délai de reprise, il convient de procéder à une sauvegarde de ces mêmes données sur un support informatique répondant aux normes fixées par l'arrêté du 13 septembre 1991.

3. L'archivage des traitements

Le contrôleur des impôts diligente ses contrôles comme un auditeur en choisissant une approche par la procédure et le contrôle interne ou encore par le contrôle exhaustif. Dans le premier cas, il peut inspecter le programme qui matérialise la règle de gestion contrôlée (calcul de TVA, de provision, etc.) ; dans le second cas, il valide la bonne application de cette règle en recalculant le résultat obtenu sur la base des données de l'époque (technique de l'analyse de données). Il peut combiner les approches et ainsi demander un accès aux traitements pour s'assurer de sa bonne compréhension de la règle de gestion qui lui a été décrite.

Compte tenu de ces objectifs, l'entreprise doit conserver les programmes sources de ses applications de gestion et s'assurer d'une possibilité d'accès à ceux qu'elle utilise au travers de progiciels. En effet, pour ces derniers, l'entreprise ne dispose que d'une version exécutable (ou objet).

La règle de gestion peut varier durant un exercice et le contrôleur doit pouvoir s'assurer de la permanence de la règle observée dans un programme en prenant connaissance des différentes modifications intervenues sur chaque traitement et de la date d'application de celles-ci.

Lorsqu'un système opérationnel a été remplacé, l'entreprise peut choisir de le conserver dans l'éventualité de tests requis par l'administration (BOI du 24 janvier 2006 § 91 et 103). Il s'agit là d'un choix fiscal, compte tenu des impacts financiers et techniques induits.

D. RECOMMANDATIONS

Cette réglementation fait encore l'objet de zones d'ombre qui disparaissent au fil des retours d'expérience des entreprises. Il est possible qu'il faille attendre l'arbitrage du juge de l'impôt sur certains points précis qui sont les suivants :

1. Organisation de l'archivage

- informer les acteurs (financiers et informaticiens) ;
- nommer un responsable de l'archivage fiscal en fixant des objectifs et des moyens ;
- analyser le contexte actuel (système d'information et fiscal).

2. Conservation exhaustive des « éléments » du système d'information

La seule conservation des données et des traitements peut ne pas suffire car leur utilisation suppose l'archivage de logiciels (OS, SGBD, langages, logiciel de sauvegarde, etc..) et parfois de matériel (unité centrale, dérouleur de bande, lecteur de cartouche, unité de disque, etc.). L'archivage fiscal doit donc être conçu de manière large.

- Mettre en place des procédures d'archivage de fin d'année :
 - initiées par les utilisateurs ;
 - basées sur 2 copies de fichiers, sur des supports fiables, en format logique et non propriétaire avec test de relecture (croisé si possible ; cela veut dire que la copie est faite sur une unité de sauvegarde et testée sur une autre) ;
 - sécurisées en termes de stockage ;
 - documentées.
- Gérer les versions de programmes sources (origine des modifications et conservation du programme source).
- Évaluer les impacts liés aux évolutions de matériel, d'OS, de base de données (sauvegarde de la version remplacée et si nécessaire retraitement des archives constituées).
- Archiver spécifiquement les applications devenues sans objet ou remplacées (archivage d'ensemble).
- S'assurer de la traçabilité et de l'intégrité des interfaces (piste d'audit).

- Valider l'accès aux programmes sources, aux documentations et aux compétences (→ aspect contractuel, tout particulièrement pour les progiciels).
- Valider la disponibilité d'une documentation d'ensemble en français (de préférence).

Certaines de ces remarques ne sont pas exclusivement liées au respect de la réglementation fiscale mais contribuent aussi à améliorer la sécurité du système d'information.

Enfin, il importe de s'assurer du périmètre des archives afin qu'elles prennent bien en compte l'intégralité des fichiers nécessaires.

3. Qualité des documentations techniques

L'administration exige une autre documentation technique dans le cadre de ses contrôles.

Il n'est pas possible de connaître avec précision le niveau de documentation exigé par l'administration. En effet, d'une part, la liste des documents qu'elle exige est impressionnante et n'existe que très rarement, d'autre part, sa non-présentation ne porte à conséquence que « *lorsque l'attitude du contribuable est assimilée à une opposition au contrôle* ».

Ce point constitue un espace d'interprétation très vaste. Il convient donc de trancher en respectant des principes de pragmatisme et de bon sens.

L'objectif du contrôleur est d'assimiler les règles de fonctionnement du système qui lui est présenté. Il nous semble donc nécessaire de pouvoir fournir *a minima* :

- une documentation fonctionnelle globale précisant les principales tables et relations (souvent appelée MCD) ;
- un dictionnaire des données permettant de comprendre le contenu des fichiers et la codification retenue pour chaque zone ;
- une description technique et fonctionnelle des principaux traitements.

Il importe de vérifier la qualité des documentations au regard de ce qui précède.

4. Disponibilité des programmes sources

Ici encore, il convient de contrôler la situation selon deux axes :

- Pour les progiciels, il peut s'agir d'un dépôt des programmes de la part de l'éditeur auprès d'un notaire, d'un huissier ou de l'APP (Agence pour la protection des programmes), ce qui garantit la disponibilité des sources dans le cas de la cessation d'activité du fournisseur ou de contrôle fiscal.
- Pour les logiciels spécifiques, il faut s'assurer de la conservation des sources et des différentes versions successives.

E. LES AMÉNAGEMENTS

L'administration fiscale a commenté dans une instruction (BOI n° 30 du 6 mars 2008), les aménagements apportés par la loi de finances rectificative pour 2007 concernant le contrôle des comptabilités informatisées.

La novation essentielle consiste en la possibilité pour les contribuables de satisfaire à l'obligation de représentation des documents comptables prévue par le premier alinéa de l'article 54 du Code général des impôts en **remettant sous forme dématérialisée une copie des fichiers des écritures comptables dans le respect des indications du plan comptable général**. Dans ce cas, l'administration peut effectuer des tris, classements ainsi que tous calculs sur ces fichiers.

Lorsqu'elle envisage de réaliser des traitements informatiques, l'administration doit indiquer **par écrit la nature des investigations envisagées** et le contribuable doit formaliser par écrit son choix pour l'une des options inchangées prévues au II de l'article L. 47 A par écrit.

Option à choisir :

| | | |
|---|---|--|
| Mise à disposition du vérificateur dans l'entreprise du matériel et des fichiers nécessaires aux opérations de contrôle sur place | Remise des résultats à l'administration des traitements réalisés par l'entreprise | Remise des copies de fichiers à l'administration pour lui permettre de réaliser elle-même les traitements. |
|---|---|--|

Le contribuable a l'obligation, lorsqu'il effectue lui-même les traitements demandés, **de remettre les résultats de ces derniers sous forme dématérialisée.**

Lorsque le contribuable choisit de remettre les copies de fichiers au service vérificateur afin qu'il effectue lui-même les traitements en application de la troisième option, la remise des fichiers peut s'effectuer **sur tous supports informatiques** y compris ceux fournis par l'administration, et l'administration doit, avant la mise en recouvrement, restituer les copies de fichiers et n'en conserver aucun double.

ANNEXES

ANNEXE 1 CHAMP D'APPLICATION ET CARACTÉRISTIQUES DE LA SINE

1. Préambule

Suite à une étude de faisabilité effectuée par son groupe de travail SINE, le CS-OEC/CNCC a décidé de s'appuyer sur la technologie de la signature électronique.

Tout en tenant compte de la définition de la signature selon la norme ISO 7498-2 [ISO/IEC7498-2] : Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple).

La synthèse de l'étude de faisabilité a énoncé les fonctions de base que la SINE peut couvrir, à savoir :

- protéger la signature institutionnelle de l'EC/CC ;
- assurer l'identification du signataire « EC/CC » ;
- vérifier la qualité de la signature de l'EC/CC et donc son appartenance à l'Ordre/CNCC ;
- garantir la réalisation d'une opération de signature, ainsi que les objectifs stratégiques de la profession ;
- diffuser dans le monde Internet la « présence » de l'EC/CC ;
- préparer l'EC/CC à l'audit des informations signées ;
- ouvrir la profession d'EC/CC vers de nouveaux marchés.

La SINE est la signature électronique d'un document lui-même sous forme électronique, qui est toujours générée par l'EC/CC responsable des travaux, et par laquelle :

- dans le cadre de ses missions, il indique avoir effectué les diligences prévues par les normes définies par le CS-OEC pour obtenir les informations figurant dans le document sur lequel s'applique sa signature ;
- dans un cadre plus général, réglementaire ou contractuel, il s'engage sur les informations contenues dans le document sur lequel s'applique sa signature (ex. : lettre, vote, etc.).

Cependant, la SINE ne peut être déléguée à une autre personne même si celle-ci est elle-même EC/CC car elle est attachée à la personne physique, quelles que soient sa fonction et sa position hiérarchique dans le cabinet.

2. Valeur juridique de la SINE

La signature électronique est reconnue comme moyen de preuve lorsqu'elle est apposée sur des actes juridiques dématérialisés, depuis la modification du Code civil (mars 2000) intégrant la signature électronique dans les moyens de preuve.

Cette signature s'appuie sur les techniques de la cryptographie asymétrique (plus communément appelée cryptographie à clé publique) et sur l'utilisation de certificats.

Afin d'être reconnue juridiquement, la signature SINE doit respecter les exigences de l'article 1322-2 nouveau du Code civil. D'une part, « La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. »

De plus, en ce qui concerne l'utilisation de la technologie : « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».

.../...

.../... Sur le plan de l'identification que doit garantir la signature électronique, la directive européenne sur le cadre de la reconnaissance de la signature électronique donne des précisions utiles dans son article 2.2.

Définitions

La signature doit :

- être liée uniquement au signataire ;
- permettre d'identifier le signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.

La SINE n'a pas vocation à mettre fin à la valeur juridique de la signature manuscrite existant dans l'environnement professionnel des EC, mais au contraire à s'intégrer dans le monde des documents dématérialisés utilisés par les EC/CC tout en ayant la même valeur légale.

Afin d'obtenir la reconnaissance juridique optimale, la SINE devra s'appuyer sur l'utilisation de certificats « qualifiés ». La directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques donne la définition suivante pour « certificat qualifié » : un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II.

L'annexe I de la directive énonce les mentions que doivent contenir les certificats qualifiés, alors que l'annexe II énumère les exigences auxquelles doivent satisfaire les prestataires de services de certification qui émettent les certificats.

Pour être reconnue par les administrations, la SINE devra encore être conforme au prochain schéma national d'accréditation dont le principe est fixé par la directive européenne.

Enfin la SINE devra faire apparaître la qualité du signataire (EC/CC).

Extrait du cahier des charges émanant du CSOEC et de la CNCC, fourniture d'un système de signature électronique (SINE), le 30 mars 2000.

REMARQUE

Il est à noter que cet appel d'offres est resté infructueux, le marché de la signature électronique manquant de maturité à cette date. La CNCC a depuis relancé un nouvel appel d'offres qui s'est traduit par le déploiement d'un dispositif de signature électronique chez les commissaires aux comptes.

EXERCICE AUTOCORRIGÉ

Ne pas envoyer à la correction

TEST DE VOCABULAIRE ET DE COMPRÉHENSION

QUESTIONS

1. **Architecture de système** : La liste ci-dessous veut recenser les **systèmes d'exploitation** utilisés dans l'entreprise. Cherchez l'intrus.
 - a. Unix.
 - b. Linux.
 - c. FiatLux.
 - d. Microsoft seven.
 - e. Mac OS.
 - f. Windows server.
2. **Protocole Internet** : La liste ci-dessous veut recenser les **principaux protocoles utilisés sur Internet**. Cherchez l'intrus.
 - a. HTTP.
 - b. FTP.
 - c. SMTP.
 - d. PPTT.
3. **Protocole Internet** : La liste ci-dessous veut recenser les **principales lois observées sur les progrès techniques**. Cherchez l'intrus.
 - a. La loi de Moore.
 - b. La loi de Gilder.
 - c. La loi de Murphy.
 - d. La loi de Metcalfe.
4. **Architecture des bases de données** : Dans cette liste qui recense les **modèles utiles pour la réalisation de bases de données**, qui n'a pas sa place ?
 - a. Le modèle hiérarchique.
 - b. Le modèle réseau.
 - c. Le modèle relationnel.
 - d. Le modèle confidentiel.
5. **Cloud computing** : Dans cette liste qui recense les **plateformes compatibles avec le cloud computing**, qui n'a pas sa place ?
 - a. Le HAAS.
 - b. Le PAAS.
 - c. Le SAAS.
 - d. Le SLA.
6. **Processus-clés de la sécurité des SI** : La liste ci-dessous veut recenser quelques étapes d'une **démarche de sécurisation des SI** de l'entreprise. Cherchez l'intrus.
 - a. Recensement des actifs à protéger.
 - b. Évaluation des risques.
 - c. Identification des menaces.
 - d. Réalisation d'un devis par un assureur.
 - e. Mise en œuvre d'une PSSI.
 - f. Déclinaison opérationnelle de la PSSI.

- 7. Protection des actifs :** La liste ci-dessous veut recenser les niveaux de **sensibilité de l'information** distingués par l'Afnor. Cherchez l'intrus.
 - a. Information blanche.
 - b. Information verte.
 - c. Information grise.
 - d. Information noire.
- 8. Évaluation des risques :** En quoi consiste la technique d'**ingénierie sociale** ?
 - a. À concevoir des outils et équipements destinés aux utilisateurs des SI.
 - b. À formaliser les besoins des utilisateurs des SI.
 - c. À créer des réseaux (sociaux) rassemblant des individus autour d'un même centre d'intérêt.
 - d. À mettre en œuvre des actions sociales dans l'entreprise, soutenues par les SI.
 - e. À soutirer des informations confidentielles à des utilisateurs en abusant de leur crédulité.
- 9. Identification des menaces :** Dans cette liste qui recense les facteurs intervenant dans l'« **équation du risque** », qui n'a pas sa place ?
 - a. La menace pesant sur les SI.
 - b. La vulnérabilité des SI.
 - c. Le nombre de SI.
 - d. L'impact sur les SI et/ou l'entreprise.
- 10. Mise en place d'une PSSI :** La liste ci-dessous veut recenser les principaux **critères de sécurité** des SI. Cherchez l'intrus.
 - a. Confidentialité.
 - b. Intégrité.
 - c. Disponibilité.
 - d. Authenticité.
 - e. Autorisation.
 - f. Non-répudiabilité.
 - g. Imputabilité.
 - h. Traçabilité.
- 11. Sécurité opérationnelle des réseaux :** Quel dispositif utilise-t-on pour **filtrer les entrées/sorties** d'un réseau ?
 - a. Un pare-feu.
 - b. Un réseau privé virtuel (VPN).
 - c. Une zone démilitarisée (DMZ).
 - d. Un antivirus.
 - e. Un mécanisme de journalisation.
 - f. Un utilitaire de sauvegarde.
 - g. Un mécanisme de chiffrement.
- 12. Sécurité opérationnelle des serveurs :** Quel dispositif utilise-t-on pour **isoler les SI-clés** de l'entreprise, des réseaux moins sécurisés tels que l'Internet ?
 - a. Un pare-feu.
 - b. Un réseau privé virtuel (VPN).
 - c. Une zone démilitarisée (DMZ).
 - d. Un antivirus.
 - e. Un mécanisme de journalisation.
 - f. Un utilitaire de sauvegarde.
 - g. Un mécanisme de chiffrement.
- 13. Sécurité opérationnelle des postes de travail :** La liste ci-dessous veut recenser quelques bonnes pratiques de **sécurisation des postes de travail**. Cherchez l'intrus.
 - a. La restriction des fonctionnalités.
 - b. L'enregistrement automatique des mots de passe.
 - c. L'installation systématique des mises à jour de sécurité des systèmes d'exploitation et applications.

- d. L'analyse régulière des SI à l'aide d'un antivirus à jour.
- e. La limitation des logiciels clients.

14. Sécurité opérationnelle – sauvegarde : La liste ci-dessous veut recenser quelques bonnes pratiques de **sauvegarde des données**. Cherchez l'intrus.

- a. Automatiser l'opération de sauvegarde.
- b. Pour ne pas entraver l'activité, effectuer l'opération de nuit.
- c. Conserver les supports de sauvegarde hors de l'entreprise.
- d. Déplacer les données anciennes sur un support amovible.
- e. Si les volumes de données sont trop importants, effectuer des sauvegardes incrémentales ou différentielles entre deux sauvegardes totales.
- f. Si l'on ne dispose pas de moyens et compétences internes suffisants, recourir à un prestataire externe.

15. Sécurité opérationnelle – chiffrement : Dans cette liste qui recense un certain nombre de termes relatifs au **chiffrement**, qui n'a pas sa place ?

- a. La signature électronique.
- b. L'algorithme symétrique.
- c. La clé asymétrique.
- d. Le certificat numérique.
- e. L'infrastructure à clé publique.

RÉPONSES

1. c. FiatLux n'est pas un système d'exploitation.
2. d. Le protocole HTTP est celui du Web, le FTP est utilisé pour le téléchargement, le SMTP est utilisé pour la messagerie, le PPTT n'existe pas.
3. c. La loi de Murphy « Tout ce qui peut aller mal, ira mal » est l'intrus même s'il est légitime d'avoir une vision pessimiste sur l'évolution du progrès technique.
4. d. Le modèle confidentiel n'existe pas.
5. d. Le SLA ou Service Level Agreement n'est pas une plateforme mais une mesure d'un niveau de service.
6. d. L'assureur n'est à contacter qu'en cas d'établissement d'un nouveau contrat d'assurance, de demande d'assurance particulière d'un actif ou de sinistre. Il n'est pas un acteur systématique d'une démarche de sécurisation des SI.
7. b. L'Afnor distingue à ce jour l'information « blanche » aisément et licitement accessible, l'information « grise » dont la connaissance et l'accès sont plus difficiles, et l'information « noire » à diffusion restreinte et accès protégé. L'information « verte » n'existe pas.
8. e. L'ingénierie sociale consiste, pour un attaquant, à abuser de la naïveté d'un ou plusieurs individus dans le but d'obtenir des informations auxquelles il n'a pas accès (mot de passe, etc.).
9. c. Le risque est fonction de trois facteurs : la menace, la vulnérabilité et l'impact ; le nombre de SI n'intervient pas dans cette équation.
10. d. Il s'agit de l'*authentification* et non de l'*authenticité*.
11. a. La réponse correcte est le pare-feu. Ce dispositif permet, en effet, de restreindre les accès sur une entrée précise du réseau (et donc de bloquer une éventuelle attaque), ainsi que de restreindre les sorties de certaines données. Les autres propositions sont inadaptées à cette question.
12. c. La zone démilitarisée (DMZ) sert de « tampon » entre une zone de confiance et une zone de sécurité de niveau inférieur. Les autres propositions sont inadaptées à cette question.
13. b. L'enregistrement automatique des mots de passe est dangereux car un intrus ayant accès au SI n'aurait aucun mal à les retrouver !
14. d. Déplacer des données qui ne sont plus utilisées régulièrement sur un support amovible pour gagner de la place et s'organiser, est une pratique d'*archivage* et non pas de sauvegarde. Ne pas confondre ces deux notions !
15. c. Il n'existe pas de « clé asymétrique » en tant que telle ; les algorithmes de chiffrement asymétriques utilisent la clé *publique* du destinataire, qui déchiffre ensuite le message chiffré (ou cryptogramme) à l'aide de sa clé privée.

INDEX

Architecture de données 44
Architecture de réseau 93
Architecture de système 24
Architecture de traitement 52
B2B 66
B2C 64
B2E 59
CERT 85
CLUSIF 86
CMMI 129
Cnil 108
COBIT 122

Contrôle fiscal 133
FSF 116
IFAC 131
IIA 132
ISACA 122
ISO 130
ITIL 126
Sécurité des postes de travail 95
Sécurité des réseaux 92
Sécurité des serveurs 94
Système d'exploitation 24

À envoyer à la correction

Auteur : Philippe LOUDENOT

Le cabinet d'expertise-comptable Bonzamis souhaite revoir l'ensemble de ses systèmes d'information et mettre en place d'un véritable réseau informatique.

Les missions du cabinet sont notamment :

- L'établissement des **comptes** annuels (bilan, comptes de résultats), comptes consolidés, situations comptables périodiques, comptes prévisionnels.
- Production de **tableaux** de bord (journaux, grand livre, balance).
- **Audits** contractuels/légaux, commissariat aux comptes, **certification** de comptes, **actes** sous seing privé, assistance en cas de contrôle.
- Élaboration d'information comptable et financière à destination de **tiers** (salariés, actionnaires, banquiers).
- **Conseil** en matière financière, juridique, fiscale : droit du travail, droit fiscal, création d'entreprise, rachat ou fusion d'entreprise, ouverture de capital.

Les **clients** du cabinet sont des sociétés (20 à 50 salariés) du secteur immobilier : syndics immobiliers et entreprises de services aux copropriétés, architectes et entreprises du bâtiment.

Ces systèmes d'information ne doit pas simplement se limiter au partage de données entre collaborateurs et aux gains de productivité. Il doit permettre, en outre, de partager et de mutualiser les « périphériques » du cabinet, évitant ainsi la multiplication d'achats de matériels annexes. Imprimantes, scanners, graveurs de CD ou de DVD sont, grâce au réseau, mis à la disposition de tous en un point de connexion centralisé. De même, le réseau doit permettre l'accès à Internet sur l'ensemble du réseau, quel que soit le mode de connexion (ex. : mode wifi pour les salles de réunions) ; tous les postes peuvent se connecter simultanément. Il en est de même pour le fax ou encore le photocopieur. C'est ainsi qu'en plus des gains de productivité, la mise en place d'un réseau doit diminuer considérablement la ligne budgétaire informatique, notamment en matière de périphériques. Cette logique d'évolution est également vraie pour les applications « métier ». La centralisation des applications sur un réseau informatique doit permettre d'y accéder sans limitation. Cela doit permettre à chaque collaborateur de gérer son information, ses messages et son emploi du temps à partir du cabinet mais également depuis l'extérieur.

La base de données fait partie intégrante de ce projet et doit être accessible via le réseau du cabinet par toute personne ayant les droits d'accès.

L'utilité d'une base de données réside dans la gestion et l'utilisation rationnelle des informations. Elle permet de faire :

- des tris (tous les clients qui ont la TVA au trimestre, toutes les clôtures 31/03, etc.) ;
- des extractions (liste des adresses pour les cartes de vœux, mailing, etc.) ;
- des courriers personnalisés à chaque client sélectionné ;
- des tableaux de synthèse, des listes, etc.

TRAVAIL À FAIRE

1. Définissez les enjeux d'une architecture B2C. (2 points)

Un système d'informations sécurisé est un système protégé de manière efficace des agressions, qu'elles proviennent de l'extérieur comme de l'intérieur, qu'elles soient délibérées ou accidentelles. Des règles de sécurité doivent être définies et mises en œuvre sur l'ensemble du réseau.

Il est essentiel de concevoir une infrastructure sécurisée et d'appliquer des consignes de protection sur l'intégralité du réseau. Il ne s'agit pas en effet de surprotéger un serveur alors que les bases de données sont en libre accès. La sécurité du réseau passe par les protections mises en place mais aussi par le respect de règles d'utilisation.

Les contraintes et valeurs propres de l'activité du cabinet d'experts-comptables sont notamment :

- **exactitude** des rapports ;
- **conformité** aux règlements, normes et règles comptables ou fiscales ;
- respect des **délais** (fisc, banques, fournisseurs, etc.) ;
- respect du Code de **déontologie** de l'ordre des experts-comptables ;
- indépendance, sincérité.

2. Décrivez en un mot les métiers du cabinet d'experts-comptables puis le risque majeur immédiatement identifiable. (1 point)

- _____ d'une comptabilité pour des clients.
- _____ de documents de synthèse (rapports comptables annuels, tableaux de bords, statistiques, rapports juridiques).
- _____ de documents papier.
- _____ de conformité aux normes comptables ou fiscales.
- _____ avec les clients.
- _____ du cabinet (ressources humaines, ressources informatiques, etc.).

La contribution du système d'information doit se traduire par des **calculs comptables**, des **consultations de bases de données** (normes comptables, référentiels juridiques, bases de données techniques), une production **bureautique** (traitement de texte, PAO, impression, etc.), des **échanges électroniques** avec les partenaires, la **gestion** du cabinet lui-même (RH, planning, commercial, finance, etc.).

3. Parmi les items ci-après, discriminez-les en « biens essentiels » ou « biens support ». Pour un bien essentiel, illustrez par sa valeur métier. Pour un bien support, illustrez par une vulnérabilité potentielle. (3 points)

- Logiciel professionnel de comptabilité
- Locaux du cabinet
- Base de données juridiques
- Rapport d'audit comptable d'un client
- Réseau local sans fil
- Un expert-comptable employé du cabinet
- Tableau de bord comptable d'un client
- Imprimante

| Bien essentiel | Valeur métier |
|----------------|---------------------------|
| | |
| Bien support | Vulnérabilité potentielle |
| | |

Une échelle de besoin (cf. annexe) sur les critères de disponibilité, intégrité et confidentialité a été définie et validée par l'ensemble des acteurs de l'étude de sécurité (direction et maîtrise d'ouvrage). Le libellé des échelons est explicite pour tous les personnels de l'organisme, et suffisamment générique, car l'échelle doit être réutilisable pour d'autres SI de l'organisme.

Par exemple, le besoin en disponibilité du bien essentiel « Tableau de bord d'un client » sera évalué au niveau **2** car une indisponibilité plus longue provoquerait une **dégradation sérieuse** de son image commerciale vis-à-vis de ses clients. Ce besoin n'est sûrement pas de niveau 1, car ce n'est pas une demande des clients. Par ailleurs, une disponibilité de niveau 2 est comparable avec celle d'opérations bancaires usuelles.

Le besoin en confidentialité du bien « Tableau de bord d'un client » est évalué au niveau **2** car la perte de confidentialité provoquerait une **dégradation sérieuse** de l'image commerciale du cabinet et sa **responsabilité professionnelle** serait mise en cause. Ce besoin n'est pas du niveau 1 car les employés du cabinet doivent pouvoir coopérer voire se substituer mutuellement (en cas de congés ou absence maladie par exemple). Par ailleurs, ils sont soumis au devoir professionnel de réserve.

4. Dans le tableau ci-après, classez les 9 biens essentiels suivants en fonction de ce qui vous semble convenable eu égard aux activités d'un cabinet d'experts-comptables. (2 points)

1. L'accès au bien essentiel est réservé aux membres du cabinet et au client concerné.
2. Le bien essentiel doit être disponible dans la journée.
3. Le bien essentiel doit être parfaitement intègre.
4. Le bien essentiel doit être disponible dans la semaine.
5. Le bien essentiel peut être rendu public.
6. Le bien essentiel peut être aucunement intègre.
7. Le bien essentiel peut ne pas être disponible pendant plusieurs semaines.
8. L'accès au bien essentiel est réservé au directeur du cabinet et au client concerné.
9. Le bien essentiel doit être au moins partiellement intègre.

| Niveau | Disponibilité | Intégrité | Confidentialité |
|--------|---------------|-----------|-----------------|
| 1 | | | |
| 2 | | | |
| 3 | | | |

5. Indiquez et justifiez quel est le niveau de besoins en intégrité du bien essentiel « Tableau de bord comptable d'un client ». (2 points)

Le guide EBIOS fournit un référentiel complet de 42 menaces. Le libellé de la menace n° 36 est le suivant :

Altération des données

Type : Humain.

Cause délibérée : Personne accédant aux moyens de communication du système d'information et altérant la transmission des informations (par interception, insertion, destruction...) ou sollicitant ces accès jusqu'à trouver un point autorisé.

Exemples :

- La destruction, insertion, modification de messages (modification de l'information ; réagencement de l'information à l'intérieur des messages ou réagencement de la suite des messages).
- Refus de service (décalage dans le temps d'un message).
- Balayage depuis l'extérieur des adresses IP jusqu'à trouver une adresse accessible du système d'information.

Type de conséquences : Intrusion, altération des communications.

Critères de sécurité : Intégrité/Confidentialité.

Une menace est un *modus operandi* exercé par une source de menace et applicable à des biens support via des vulnérabilités. La décision de retenir ou d'écarter une menace résulte notamment du profil retenu de la source de menace (en particulier de ses ressources techniques, financières, et motivations), du contexte de l'entreprise, mais aussi des accidents de sécurité qu'ont déjà connus l'entreprise ou le secteur d'activité.

La menace n° 36 est retenue parce que le cabinet d'experts comptables a déjà été dans le passé victime de modifications inexplicables de données comptables.

La source est plutôt externe car, selon les experts comptables du cabinet, les ententes entre sociétés du secteur (marchés publics, contrats de maintenance pour des copropriétés, etc.) seraient monnaie courante. Ces sources externes seraient d'abord motivées par l'enrichissement (fraude fiscale, pots de vin, etc.). Elles pourraient facilement mobiliser des ressources financières suffisantes pour acheter des compétences techniques nécessaires.

Par ailleurs, une source interne est considérée comme très peu vraisemblable car la taille du cabinet favorise le respect de la **déontologie** professionnelle. Enfin, le cabinet dispose d'un réseau local ouvert sur l'internet, sans fil et sans protection

6. Indiquez dans le tableau quelles sont les vulnérabilités, parmi celles proposées ci-après, qui permettent l'exercice de la menace n° 36 : altération des données. (2 points)

1. Absence de protection contre l'écoute passive du réseau wifi du cabinet.
2. Absence de pare-feu sur les machines.
3. Utilisation d'une imprimante obsolète.
4. Utilisation de mots de passe de taille faible et donc d'entropie faible.
5. Matériel disposant d'interface de communication sans-fil wifi.
6. Pas de mise à jour des anti-virus.

| Vulnérabilités applicables | Vulnérabilités non applicables |
|----------------------------|--------------------------------|
| | |

Lors de la construction de scénarios de risque, il est émis l'hypothèse suivante :

Un client motivé par la fraude fiscale, disposant de ressources financières importantes pénètre le réseau local du cabinet en exploitant la liaison wifi non protégée et l'absence de pare-feu. Il en résulte un rapport comptable annuel faux et non conforme mais cependant certifié par le cabinet. La responsabilité professionnelle du cabinet est alors engagée.

Toutes les composantes d'un scénario de risque sont présentes :

- sources de menace : client, motivé par la fraude fiscale, ressources financières importantes ;
- menace : pénètre le réseau local via la liaison wifi pour altérer des données ;
- vulnérabilités exploitées : wifi non protégé, absence de pare-feu ;
- biens support : réseau + serveur ;
- bien essentiel : rapport comptable annuel ;
- besoins de sécurité impactés : intégrité ;
- impact potentiel sur l'organisation : responsabilité professionnelle.

7. Indiquez un ensemble de mesures appropriées pour couvrir l'objectif suivant : « Un client du cabinet ne doit pas pouvoir pénétrer dans mon réseau via la liaison sans-fil, et puis profiter de l'absence de filtrage pour y altérer des données comptables. » (2 points)

Une fois les objectifs de sécurité énoncés, la maîtrise d'œuvre propose alors des mesures pour le traitement des risques conformément aux options indiquées dans les objectifs de sécurité. Dans les objectifs, il est souhaité pouvoir garantir de façon formelle l'ensemble des documents émis par le cabinet.

8. Quel moyen présumé fiable peut être mis en place pour permettre de garantir les documents qui seront réalisés par le cabinet ? Quels en sont les aspects et avantages ? (2 points)

Face à des technologies toujours plus complexes et des interfaces informatiques pas toujours évidentes à installer dans un cabinet, le recours au cloud apparaît pour beaucoup pour la direction comme une opportunité séduisante. Elle donc a exprimé la possibilité de s'affranchir de la gestion et de l'administration du réseau informatique et d'accéder à un service « *quand je veux, où je veux* ».

9. Cloud : donnez la définition du Cloud et les différents types de Cloud identifiables. (4 points)

ANNEXE ÉCHELLE DES NIVEAUX DE BESOINS SSI

| Niveau | Disponibilité | Intégrité | Confidentialité |
|---|---|--|---|
| 1 Le niveau d'indisponibilité ne gêne pas l'activité | Indisponibilité inférieure à une semaine. | Les données peuvent être altérées. | Les données sont publiques. |
| 2 Le niveau d'indisponibilité perturbe l'activité | Indisponibilité doit rester inférieure à 96 heures. | Les altérations doivent être détectées. | Les données sont internes au cabinet. |
| 3 Le niveau d'indisponibilité nuit fortement à l'activité | Indisponibilité doit rester inférieure à 24 heures. Responsabilité professionnelle du cabinet engagée | Les altérations doivent être détectées et corrigées. Responsabilité professionnelle du cabinet engagée | Les données ne doivent être connues que par un nombre très limité de personnes. Responsabilité professionnelle du cabinet engagée |

Disponibilité : Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées. [EBIOS 2010]

Intégrité : Propriété d'exactitude et de complétude des biens essentiels. [EBIOS 2010]

Confidentialité : Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisées. [EBIOS 2010]

