IDEC école supérieure d'informatique

Brevet fédéral en informatique

Module 176

Assurer la sécurité de l'information

Sommaire

Introduction

Le fameux an 2000 que l'on nous présentait vingt ans auparavant comme l'ère de toutes les technologies ne laisse finalement dans les mémoires des utilisateurs d'informatique que le vague souvenir d'un bug, avéré ou avorté selon les cas.

Cette année-là, le CLUSIF s'intéressait déjà depuis longtemps à la sécurité des systèmes d'information (SI) notamment en conduisant des études annuelles approfondies auprès d'entreprises françaises de tailles et de secteurs variés. Ces enquêtes, qui continuent d'être menées tous les deux ans, visent à identifier les usages que font les organisations de leurs SI et leur degré de protection.

L'une des premières questions posées lors de ces enquêtes concerne la dépendance de l'organisation à son SI.

Décryptage

Le CLUSIF, club de la sécurité de l'information français, est une association à but non lucratif dont la finalité est de promouvoir la sécurisation des SI. De nombreuses grandes entreprises françaises en sont membres ainsi que des organismes d'état.

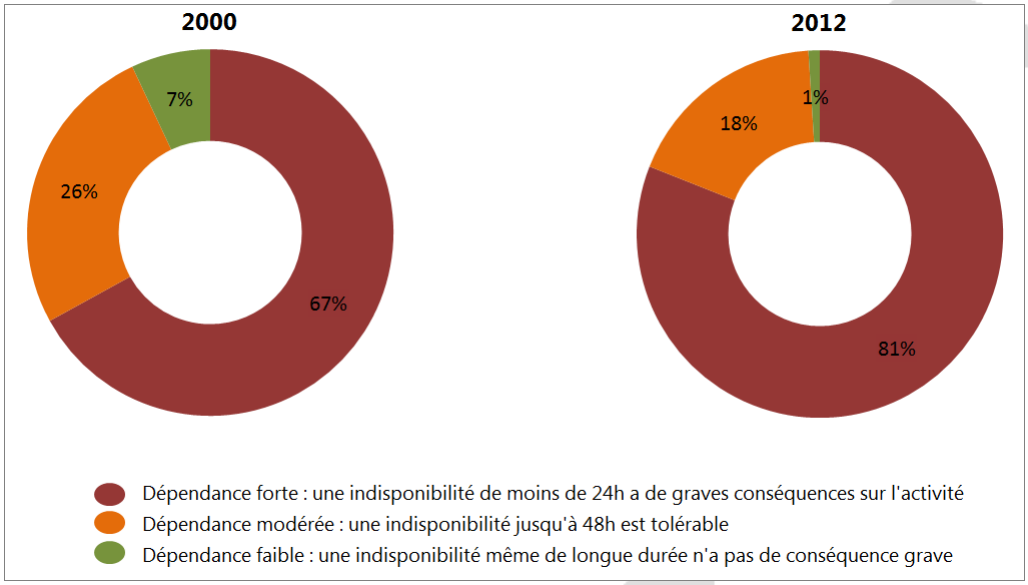

Figure 1 : évolution en 12 ans de la dépendance des entreprises à leur SI

Alors qu'un tiers des organisations pouvait supporter jusqu'à deux jours d'interruption de service de son SI en 2000, elles sont maintenant moins d'un quart à pouvoir se le permettre.

En 2000, le CLUSIF annonçait que seules 10% des entreprises vendaient sur Internet – 15% y faisant des achats – et que l'accès Internet et la messagerie n'étaient pas encore généralisés pour plus de la moitié d'entre elles.

Si l'on ajoute que seules 22% avaient mis en place un accès distant à leur SI, on constate qu'une grande partie des menaces actuelles était encore tenue en respect.

Douze ans plus tard, la situation a bien changé.

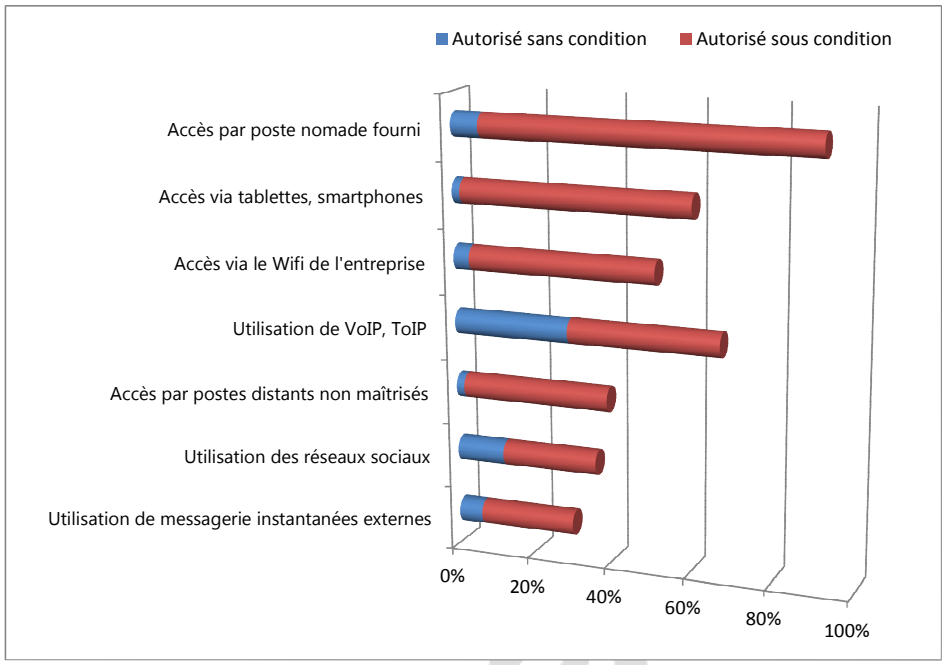

Figure 2 : ouverture des SI sur l'extérieur en 2012

En fait, les promesses de l'an 2000 de la légende n'ont pas été oubliées, elles ont simplement été tenues avec un peu de retard, pour une part, et pour l'autre part, elles sont en passe d'être tenues, le frein principal résidant dans l'acceptation des nouvelles technologies par les utilisateurs.

Le SI des entreprises a considérablement évolué en dix ans : généralisation de l'usage d'Internet dans toutes les activités, accès distants et mobiles, réseaux sans fil et BYOD ouvrent autant de failles de sécurité que de nouvelles manières de travailler.

Pour que les solutions n'amènent pas autant de problèmes qu'elles n'en résolvent, la sécurisation du système d'information est indispensable.

Ce manuel a pour vocation d'aider les responsables informatiques à élaborer une politique de sécurité de l'information (PSI) appropriée à l'activité de l'organisation pour laquelle ils œuvrent.

Comme toute solution informatique, une PSI se construit à l'aide d'outils et de méthodes relativement standardisés mais qui aboutissent à des résultats différents pour chaque organisation, car elle doit être parfaitement adaptée à ses besoins, ses contraintes et ses objectifs.

Sous-titrage

Bring Your Own Device (BYOD), soit « apportez votre propre matériel » est le nom donné à la tendance consistant à confondre matériel personnel et professionnel quand il s'agit d'appareils mobiles comme les smartphones ou les tablettes.

Les enjeux de la sécurisation du SI et les pratiques actuelles des entreprises seront présentés, puis les principes et les acteurs principaux de la sécurité des systèmes d'information (SSI).

Nous aborderons ensuite l'élaboration de la PSI sous l'angle des méthodes qui peuvent l'accompagner, avant d'entrer dans son élaboration concrète, par le biais des inventaires et des évaluations de risques qui permettent de déterminer les mesures nécessaires.

Enfin, nous terminerons sur les moyens de vérifier l'efficacité de la PSI et sur son cycle de révision.

Analogie

Nous reprenons dans ce manuel l'analogie de la maison pour illustrer certains aspects quelque peu abstraits de la SSI.

1. Les enjeux

L'activité de toute entreprise ou administration s'appuie sur des personnes qui elles-mêmes dépendent d'une infrastructure pour accomplir leur travail. L'informatique est une composante vitale de cette infrastructure : dans l'industrie, elle contrôle et pilote l'infrastructure de production, dans le secteur tertiaire, elle représente à elle seule la quasi-totalité de l'infrastructure.

Pour que l'entreprise puisse fournir sa clientèle ou que l'administration puisse servir ses administrés, leur infrastructure doit être fiable et disponible.

En outre, les actifs informatiques ont une importance croissante dans la « richesse » de l'entreprise. Aujourd'hui, quand un ordinateur portable est

volé, c'est moins son prix que les données qu'il contenait qui pose problème.

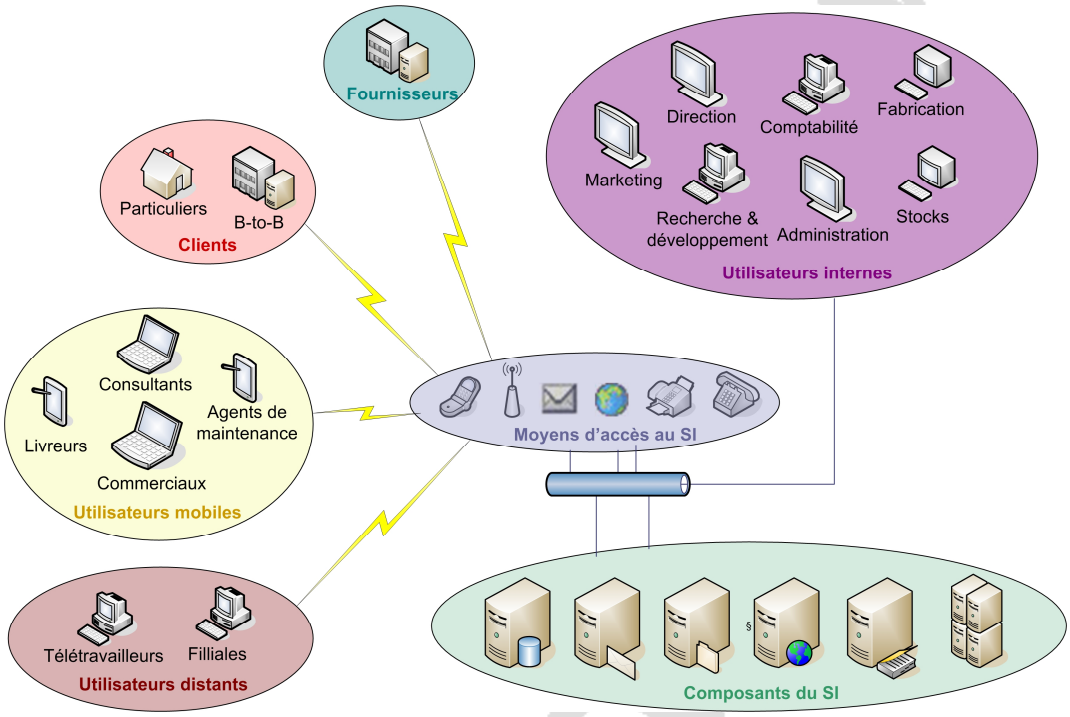

Figure 3 : le système d'information type des années post-2000

De même que « le tout vaut plus que la somme des parties », la valeur d'un système informatique ne peut pas être estimée en additionnant le prix, fût-il élevé, de chacune de ses composantes. Car le tout formé par les câbles, disques durs, processeurs, logiciels et fichiers constitue un outil dont la valeur est bien supérieure à leur coût d'achat et d'entretien. Cet outil permet de stocker, traiter et diffuser toutes les informations nécessaires à une organisation. C'est la raison pour laquelle on parle de **système d'information**.

Pourtant, l'importance stratégique du système d'information (SI) est encore souvent sous estimée, peut être parce que les éléments physiques du système ne représentent en rien sa valeur réelle. La valeur du SI est virtuelle avant tout, ce qui ne l'empêche pas d'être essentielle : par exemple, croyez-vous que le montant de votre compte en banque ou de votre deuxième pilier corresponde vraiment à des billets de banque enfermés dans un coffre ? Cet argent est lui aussi virtuel, il ne s'agit que d'un enregistrement dans un système informatique… une simple donnée.

1.1 Risques et conséquences

Analogie

A quoi bon poser des verrous sur toutes les portes et des barreaux à toutes les fenêtres… sauf une ? C'est évidemment par celle-là que les cambrioleurs entreront.

Les risques existent dans des domaines très différents : matériel, logiciel, réseaux, personnes, procédures… Elaborer une politique de sécurité implique donc de nombreux intervenants qui doivent se comprendre et s'accorder, malgré des spécialités et des objectifs différents. De plus, une stratégie de sécurité doit impérativement être exhaustive sans quoi elle devient inefficace : il n'est donc pas suffisant d'agir sur les risques les plus évidents, il faut n'en oublier aucun.

1.1.1 Domaines de risques

Assurer la protection des données nécessite d'intervenir sur tous les domaines auxquels elles sont liées, c'est-à-dire sur l'infrastructure matérielle et logicielle qui permet leur stockage et leur accès mais aussi sur les personnes qui les gèrent et les utilisent. Le découpage suivant peut être utilisé afin de distinguer les familles de risques et de mesures :

Personnes : les utilisateurs finaux et le personnel IT[1] représentent une partie des risques et sont également essentiels à la mise en œuvre de mesures de protection.

Organisation : au-delà des individus, c'est l'organisation qui définit l'utilisation du SI, ce qui peut introduire des vulnérabilités ou, au contraire, contribuer à la sécurité, selon la manière dont les procédures et les mandats de travail sont définis.

Réseaux : par leur capacité à permettre l'accès aux données à partir d'emplacements distants (donc difficiles voire impossibles à contrôler), les réseaux constituent une vulnérabilité importante contre laquelle de nombreuses mesures spécifiques existent.

Matériel et locaux : éléments physiques indispensables au stockage et à l'accès aux données, les composants matériels des systèmes informatiques et les locaux qui les hébergent doivent être protégés contre les menaces physiques pouvant les mettre temporairement hors service ou les détruire.

[1] Information Technology : technologies de l'information, plus souvent appelées en français informatique.

Applications : les applications constituent l'interface entre les utilisateurs et les données, il leur revient donc de limiter les erreurs que ces derniers pourraient commettre, ainsi que de fonctionner de manière non nuisible pour les données et le SI de façon générale.

Systèmes d'exploitation : les systèmes d'exploitation contrôlent les communications réseaux, les applications ainsi que l'accès aux données stockées sur les systèmes de fichiers. Constituant le point de convergence entre plusieurs domaines de risques, ils sont une brique essentielle de la sécurité… ou de l'insécurité !

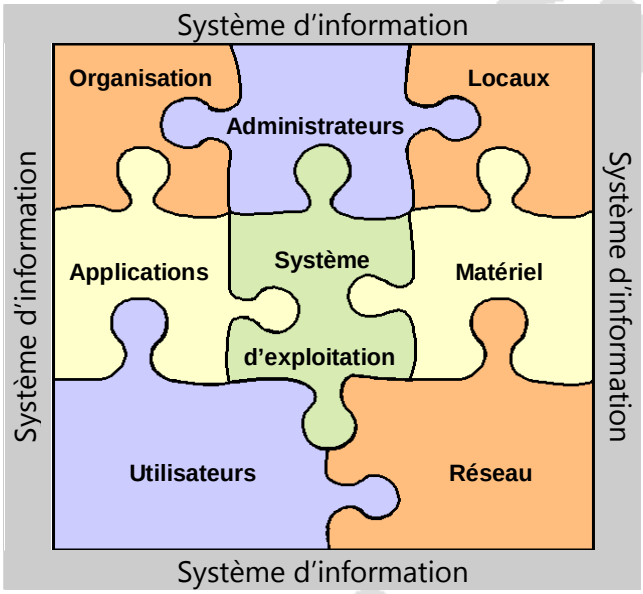

Figure 4 : la SSI, un puzzle aux pièces étroitement imbriquées