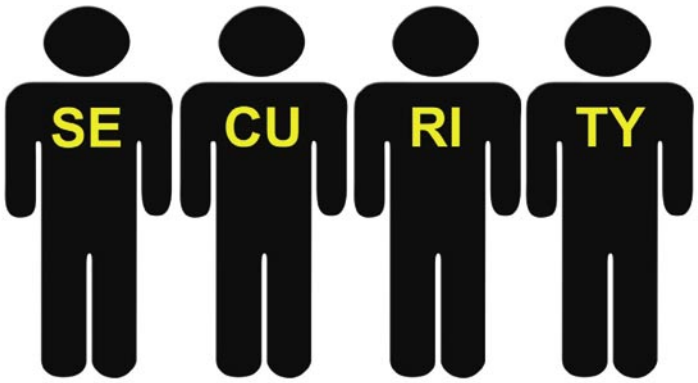
La sécurisation de l'information
et du système d'information

Régis SENET

La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir et garantir la sécurité de l'information et du système d'information.



D'une manière générale le système d'information concerne l'ensemble des moyens (organisation, acteurs, procédures et systèmes informatiques) nécessaires à l'élaboration, au traitement, au stockage, à l'acheminement et à l'exploitation des informations.

De nos jours, l'essentiel du système d'information est porté par le système informatique et la notion de sécurité informatique recouvre pour l'essentiel la notion de sécurité des systèmes d'information (SSI).

Les évolutions récentes et rapides de l'informatique ont contribué à l'accélération des échanges d'informations. Les entreprises se trouvent désormais confrontées au contrôle efficace de la confidentialité, de l'intégrité et de la disponibilité de ces informations. Véritable point vital, le système d'information est donc naturellement devenu la proie de multiples attaques qui menacent l'activité économique des entreprises et requièrent la mise en place d'une politique de sécurité.

Certaines menaces peuvent causer directement ou indirectement d'importants dommages d'ordre financier. En effet de nombreuses entreprises déclarent avoir souffert de lourdes pertes financières suite à une attaque ou un problème technique lié à leur système d'information. Des sommes de l'ordre de plusieurs milliards de dollars US ont été avancées suite à des dommages causés par des programmes malveillants comme le ver Code Red. D'autres dommages substantiels, comme ceux liés au vol de numéros de cartes de crédit, ont été déterminés plus précisément. Outre les aspects financiers, des bris de sécurité informatique peuvent causer du tort à la vie privée de l'entreprise en divulguant des informations confidentielles qui entre de mauvaises mains pourraient s'avérer être très dangereuses pour l'entreprise.

Certaines menaces peuvent nuire à l'image même du propriétaire du système d'information. Des techniques répandues de *defacing* permettent à une personne mal intentionnée de mettre en évidence des failles de sécurité sur un serveur web. Ces personnes peuvent aussi profiter de ces vulnérabilités pour diffuser de fausses informations sur son propriétaire.

La sécurité du système d'information fait donc appel à différentes techniques dont :

- le chiffrement de l'information (cryptologie),
- la protection contre les signaux parasites compromettants (sécurité électronique),

- la protection contre les intrusions dans les logiciels, mémoires ou banques de données(sécurité informatique),
- la protection contre les accidents naturels et les actes malveillants (sécurité physique).

Évaluation des risques

Pour assurer la sécurité informatique ou plus généralement la sécurité des systèmes d'information, l'entreprise doit identifier et évaluer les risques informatiques, risques des systèmes d'information, et installer des mesures de sécurité organisationnelles, physiques et logiques contre ces risques.

Les informations

L'évaluation des risques est une étape importante dans la sécurisation des données d'une entreprise (également vrai pour ce qui est des données individuelles). Avant de penser à protéger les informations que nous possédons, il est d'abord nécessaire de déterminer quelles sont les informations sensibles, quelles sont les informations *personnelles*. En effet, il est rare qu'une entreprise veuille sécuriser au même point l'ensemble de ces données. Cela serait couteux tant en énergie, qu'en temps. Il est donc primordial de bien déterminer les informations sensibles. Suivant les entreprises, les critères de sécurité vont bien évidement être différents. Néanmoins, dans la majorité des cas, nous retrouvons les critères suivants :

- Confidentialité,
- Disponibilité,
- Traçabilité,
- Intégrité.

Méthodes d'analyse et d'évaluation des risques

Actuellement, il existe de nombreuses méthodes d'analyse des risques, certaines d'entre elles sont simples d'utilisation avec parfois des logiciels permettant de simplifier leur l'utilisation. D'autres méthodes quant à elles sont réservées à des grands comptes du fait de leur complexité ou des ressources humaines qu'elles impliquent.

Parmi ces nombreuses méthodes, certaines sont plus connues que d'autres. Nous pouvons entre autre parler d'EBIOS, Mehari, Marion, Cobra etc. Pour exemple, EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*) permet d'identifier les risques d'un système informatique (SI) et de proposer une politique de sécurité adaptée aux besoins de l'entreprise.

Voici les 5 grandes étapes de la méthode EBIOS :

- Etude du contexte,
- Expression des besoins de sécurité,
- Etude des menaces,
- Identification des objectifs de sécurité,
- Détermination des exigences de sécurité.

Les menaces

Parallèlement à l'évaluation des risques et la recherche des informations sensibles que nous voulons protéger, il est important de déterminer l'ensemble des menaces sans pousser au scénario catastrophe. Objectivement et sans rentrer dans les détails, il existe trois grandes catégories de menaces :

- Les menaces humaines,
- Les menaces techniques,
- Les menaces informatiques.

Les menaces humaines

Le facteur humain est une constante dans tout système informatique mis en place. On a tendance à l'oublier mais les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent l'ensemble des personnes gravitant autour du système d'information. Dans le facteur humain, nous pouvons parler de la maladresse (erreur), l'ignorance ou l'incompétence des personnes en charge du système informatique pour ce qui est des menaces humaines *involontaires*.

Il existe également des menaces de type *volontaire* telles que le social engineering, l'espionnage industriel ou encore la malveillance dans de très nombreux cas.

Ainsi, certains utilisateurs, pour des raisons très diverses, peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus ou en introduisant volontairement de mauvaises informations dans une base de données. Les principaux buts de ces malveillances sont bien sûr le préjudice encouru par l'entreprise mais aussi, il est possible que la personne malveillante cherche des profits (financier par exemple).

Les menaces techniques

Les menaces techniques regroupent de nombreuses menaces de natures très différentes qui ne peuvent ni se classifier dans la partie humaine, ni dans la partie informatique que nous allons découvrir dans le paragraphe suivant.

Dans ces menaces, nous retrouvons tout d'abord les menaces liées au matériel. En effet, nous ne sommes jamais à l'abri d'une défaillance technique du matériel fréquemment employé.

Il existe également des menaces liées à l'environnement que de nombreuses entreprises ne prennent pas en compte du fait qu'elles pensent que cela ne peut jamais leur arriver. Dans ces menaces, nous pouvons parler des menaces liées aux inondations, aux incendies, aux coupures d'électricité et autres.

Ces types de menaces bien qu'un peu moins fréquents peuvent s'avérer ravageurs au cas où ils n'auraient pas été pris en compte dans le politique de sécurité de l'entreprise.

Les menaces informatiques

La menace informatique est bien évidemment à l'heure actuelle la menace à prendre le plus au sérieux. Virus, vers informatique, cheval de Troie, Backdoor, exploit et bien d'autres termes sont de plus en plus présents dans les conversations de tous les jours. En effet, le marché de l'Internet n'intéresse pas uniquement des âmes charitables mais également des pirates informatiques intéressés par l'argent, le pouvoir, la renommée etc.

Avec le temps et les années aidant, les attaques se font de plus en plus fréquentes et de plus en plus dévastatrices du fait que la cybercriminalité est réellement devenue un commerce intéressant pour certaines personnes.

La combinaison de l'ensemble de ces menaces laisse clairement paraitre qu'un système informatique n'est, à l'heure actuelle, vraiment pas un système en sécurité par défaut. Afin d'améliorer cela, il est nécessaire de mettre en place des moyens de protection permettant d'éviter que de tels troubles puissent arriver à notre entreprise ainsi qu'aux données que le système d'informatique renferme.

Moyens de sécurisation d'un système

La sécurité d'un système informatique peut être comparée à un chaine de maillons plus ou moins résistants que les personnes malintentionnées vont tenter de briser. La sécurité du système d'in-

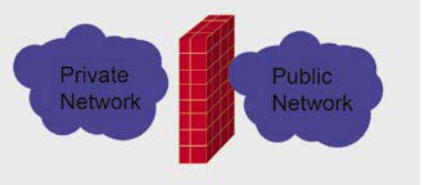


Figure1. La représentation d'un pare feu

À propos de l'auteur

Régis SENET est actuellement étudiant en quatrième année à l'école Supérieur d'informatique Supinfo. Passionné par les tests d'intrusion et les vulnérabilités Web, il tente de découvrir la sécurité informatique d'un point de vue entreprise. Il est actuellement en train de s'orienter vers le cursus CEH et Offensive Security.

Contact : *regis.senet@supinfo.com*

formation se doit d'être la plus uniforme possible du fait que la sécurité de l'ensemble du système d'information sera toujours inférieure à la sécurité du maillon le plus faible.

Ce fait aidant, il est important de comprendre que la sécurité du système d'information doit être abordée avec une conception très globale tant les points à prendre en compte sont différents mais en même temps complémentaires :

- La sécurité des systèmes d'exploitation,
- La sécurité des télécommunications,
- La sécurité de l'information,
- La sécurité des données,
- La sécurité des réseaux,
- La sécurité physique.

Il est donc important de garder à l'idée que l'ensemble des sécurités citées précédemment doivent être prises en compte d'une manière globale pour l'entreprise afin de ne pas provoquer la présence d'un maillon faible qui fragiliserait l'ensemble du système d'information.

Les moyens techniques

À l'heure actuelle, les restrictions au niveau des moyens techniques sont de plus en plus faibles tant l'avancée technologique actuelle est grande. Ces nombreux moyens permettent d'assurer une sécurité du système d'information. Il convient, pour chaque entreprise, de choisir les moyens nécessaires, suffisants et justes quant à leurs activités, leurs données à protéger etc. Dans les moyens techniques, nous retrouvons.

Les contrôles d'accès au système/réseau local

Le contrôle d'accès permet de ne laisser entrer seulement les personnes spécifiquement autorisées à le faire afin d'éviter par exemple, qu'une personne externe à l'entreprise puisse avoir accès au Datacenter. Le contrôle d'accès va combiner une action logique à une action physique afin de permettre à une personne identifiée ou non d'avoir accès à telle ou telle ressource.

En effet, le contrôle logique va s'effectuer par exemple grâce à un lecteur de carte, un lecteur biométrique ou tout simplement un clavier nécessitant un mot de passe. Quant à l'action physique que cela va impliquer, il peut s'agir de l'ouverture d'une porte, d'un tourniquet tripode ou encore plus simplement du déverrouillage d'un poste informatique.

Les authentifications fortes sont très en vogue en ce moment. Une authentification forte est une procédure d'identification qui requiert la concaténation d'au moins deux éléments ou facteurs d'authentification différents (biométrie plus mot de passe par exemple).

Les systèmes de protection contre les menaces physiques et environnementales

Comme nous avons pu en parler précédemment, les menaces environnementales ne sont absolument pas à prendre à la légère. Même si ces dernières sont relativement rares, il est impératif de garder à l'esprit que cela peut être dévastateur.

Il est donc nécessaire de mettre en place une politique de sécurité regroupant l'ensemble des risques possibles : incendie, inondation, foudre, électricité (surtension ou panne d'électricité) etc.

Les systèmes de protection contre ces menaces sont connus, pour plus de renseignement n'hésitez pas à regarder le dossier sur la sécurisation des Datacenters présent dans la partie *Liens*.

Surveillance du réseau et des systèmes

Il est absolument indispensable pour un administrateur réseau de savoir ce qui se passe dans son réseau ainsi que ce qui y transite afin de révéler toute tentative d'intrusion sur le réseau. Pour cela, il est possible de mettre en place des systèmes de détection d'intrusion, plus connus sous le nom d'IDS (*Intrusion Detection System*). Par définition, un IDS est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée que ce soit un réseau d'entreprise ou simplement une machine hôte.

Les IDS sont divisés en trois grandes catégories :

- Les NIDS (*Network Based Intrusion Detection System*) surveillant l'état de la sécurité du réseau.
- Les HIDS (*HostBased Intrusion Detection System*) surveillant l'état de la sécurité des hôtes.
- Les IDS hybrides, qui utilisent les NIDS et HIDS afin d'avoir des alertes plus pertinentes.

Il est fortement conseillé de posséder au moins un NIDS afin d'avoir une vue d'ensemble du réseau. L'IDS Snort est un excellent IDS réseau étant capable d'effectuer en temps réel des analyses de trafic ainsi que de logger les paquets sur un réseau IP.

Ajouté à cela un ou plusieurs HIDS par hôte permettant d'accroitre la sécurité de chacun d'entre eux. En effet, chaque HIDS ne recherchant pas les mêmes types d'attaque, il est possible d'en avoir plusieurs en sa possession afin de couvrir le plus grand nombre de menaces possibles sur la machine. *Chkrootkit aura pour but de vérifier et d'éradiquer la présence de rootkit sur un hôte GNU/Linux alors que Tripwire aura pour but de vérifier si l'ensemble des fichiers n'ont pas été modifiés sur le système.*

Emploi de technologies ad-hoc

Pour en finir avec les moyens de protection, nous allons parler des technologies ad-hoc. Dans ces technologies, nous allons parler en premier lieu du pare-feu. Un *pare-feu* est l'une des pièces maitresses d'un réseau informatique. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés ou interdits.

De manière très simplifiée,, la représentation qu'il est possible de donner d'un pare feu sur Figure 1. Il a donc pour tâche de contrôler le trafic entre différentes zones de confiance, en filtrant les flux de données qui y transitent. Généralement, les zones de confiance incluent Internet et au moins un réseau interne (une zone dont la confiance est plus importante).

Dernièrement, afin d'assurer un niveau de sécurité suffisamment élevé dans le réseau de l'entreprise, il est indispensable que l'ensemble des ordinateurs, connectés à Internet ou non, dispose de plusieurs moyens de protection contre les menaces les plus fréquentes. Pour cela, il est donc nécessaire de s'équiper :

- Un antivirus,
- Un anti spam,
- Un anti spyware,
- Un anti malware.

De nombreuses offres commerciales ou même gratuites combinent l'ensemble des fonctions précédemment citées en un seul et même produit.

Méthode de chiffrement

Par définition, le chiffrement est le procédé grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Le chiffrement des données se retrouve actuellement à deux niveaux :

- Chiffrement des données transitant sur le réseau,
- Chiffrement des données personnelles.

En effet, la majeure partie des protocoles que nous utilisons envoient les données en clair sur Internet permettant à une personne malveillante de récupérer l'ensemble de ces informations qu'il s'agisse de mot de passe, de compte utilisateur ou de mail. Les protocoles ainsi cités sont par exemple HTTP, FTP, IMAP qui par défaut n'ont aucune méthode de chiffrement des données. Pour éviter tout ennui, il est préférable de revoir les politiques de sécurité permettant de remplacer au maximum les protocoles potentiellement dangereux par des protocoles sécurisés. Il est donc nécessaire de remplacer HTTP par HTTPS, FTP par FTPS ainsi

qu'IMAP par IMAPS. La majeure partie de ces chiffrements se réalise grâce à *Transport Layer Security* (TLS), anciennement nommé *Secure Socket Layer* (SSL) étant un protocole ayant pour but la sécurisation des échanges sur internet.

Le chiffrement peut également s'appliquer aux données personnelles d'un utilisateur par exemple. En effet, depuis la popularisation des ordinateurs portables s'est vu apparaitre de très nombreux vols de disque dur ou même d'ordinateur portable afin de récupérer l'ensemble des données qu'il contient. Actuellement, il existe de nombreux logiciels propriétaires ou non permettant de chiffrer l'ensemble des données sur un disque dur grâce à différents algorithmes.

Les tests

Une fois l'ensemble des configurations effectué, à court comme à long terme, il est nécessaire de continuellement *tester* la sécurité. Pour cela, il est nécessaire de mettre en place des audits de sécurité. Ces audits, qu'ils soient de configuration ou de vulnérabilités sont principalement effectués par des acteurs externes à l'entreprise afin d'avoir un point de vue impartial et externe quand à la sécurité du système d'information.

Audit de configuration

Un audit de configuration représente une liste de points à vérifier afin de voir si la sécurité d'une nouvelle machine peut être acceptable. L'auditeur va suivre pas à pas une liste de points définie en fonction du niveau de sécurité voulu par l'entreprise et vérifier que l'ensemble de ces points sont respectés. (Communication chiffrées en SSLV3, présence d'une clé WPA etc.). Dans le cas où l'un d'entre eux n'est pas respecté, il est nécessaire de mettre en place des correctifs adaptés avant de repasser un audit quelques semaines plus tard. Au cours de ce prochain audit, l'auditeur va principalement s'attarder sur les points ayant posé problème lors de son dernier passage tout en analysant à nouveau les autres.

L'auditeur se doit d'éditer un rapport synthétisant l'ensemble des tests effectués sur les machines ainsi que de donner un résumé de l'audit.

Audit de vulnérabilités

Ce type d'audit est impérativement à mettre en place et arrive en règle générale juste après l'audit de configuration. Cet audit à pour but de tester l'ensemble des services et des applications de manière interne et externe afin de simuler la tentative d'intrusion d'un Hacker. Ce processus est à mettre en place principalement lors de l'arrivée d'un nouveau serveur par exemple mais doit également se faire de manière régulière sur les autres équipements. En effet, Internet et ses failles évoluent constamment, il est donc nécessaire d'être à jour en tout temps. Le magazine *Hakin9 N°7-2007 - Tests des vulnérabilités* – détaille en profondeur les audits de vulnérabilité qu'il est possible de mettre en place pour la sécurisation des machines présentes dans le Datacenter.

Tous comme pour les audits de configuration, il est nécessaire d'éditer un rapport synthétisant l'ensemble des vulnérabilités détectées lors de l'audit. Les vulnérabilités vont être classées en fonction de leur importance (critique, élevé, moyen et informations) afin d'attirer l'attention sur les vulnérabilités importantes ainsi qu'en fonction de leur zone (DMZ, VPN, local, VoIP etc.).

Sur Internet

- Méthode EBIOS : *http://www.ysosecure.com/methode-securite/methode-ebios.asp*,
- Méthode Mehari : *http://www.ysosecure.com/methode-mehari/principes-mehari.asp*,