Master – Memento Gestion des risques

Critères de sécurité

Afin de mener une étude la plus pertinente possible il est nécessaire de cadrer le plus possible cette étude et les méthodes d'analyses de risque sont là pour nous y aider. À ce stade afin d'éviter toute ambiguïté il faut définir finement des attendus.

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

Créer des tableaux de métriques

Les critères de sécurité retenus dans le cadre des analyses de risque seront toujours les critères de **Disponibilité**, **Intégrité**, **Confidentialité** et au besoin de **Trace**/**Preuve** bien que l'on puisse imbriquer ces critères au sein du critère d'intégrité de par une manipulation réfléchie lors de l'expression des besoins de sécurité.

Afin d'exprimer ces besoins de sécurité, on retiendra toujours les critères de sécurité définis dans la PSSI de l'entreprise ou de l'organisme qui s'applique à la situation. Dans le cas ou plusieurs PSSI sont applicables à un même projet on retiendra alors la PSSI qui a été déclinée le plus finement vis-à-vis du périmètre de l'analyse, cette dernière ne doit en

toute logique pas contredire la politique mère à partir de laquelle elle a été déclinée et est normalement plus détaillée que cette dernière.

Échelle de disponibilité

Niveaux de l'échelle	Description détaillée de l'échelle
Aucun ou Faible (D1)	Le bien essentiel a un délai maximal d'interruption autorisée entre une semaine et un mois.
Moyen (D2)	Le bien essentiel a un délai maximal d'interruption autorisée de 3 à 5 jours consécutifs ouvrés.
Critique (D3)	Le bien essentiel a un délai maximal d'interruption autorisée de 1 à 2 jours consécutifs ouvrés.
Majeur (D4)	Le bien essentiel a un délai maximal d'interruption autorisée d'une journée ź8 heures).

Échelle d'intégrité

Niveau de l'échelle	Description détaillée de l'échelle
Aucun ou faible (L1)	Une perte ou modification non prévue, volontaire ou non volontaire, n'affecte en rien les activités d'un service, d'une direction ou d'un organisme utilisateur.
Moyen (L2)	Aucune modification non autorisée n'est acceptée. L'exactitude des informations est avérée mais sans contrôle particulier. La modification illicite des informations traitées ne provoque pas de gêne significative. Un contrôle à posteriori est suffisant pour détecter toute modification illicite.
Critique (L3)	Aucune modification non autorisée n'est acceptée et toute modification autorisée doit être tracée.
Majeure (L4)	Aucune modification non autorisée n'est acceptée et toute modification autorisée doit être tracée de façon sécurisée. L'exactitude des informations et l'authenticité des transactions sont garanties par un procédé technique difficilement contournable. La modification illicite n'est pas tolérée et doit être détectée automatiquement, le plus rapidement possible.

Échelle de confidentialité

Niveau de l'echelle	Description détaillée de l'échelle
Aucun (C1)	La diffusion d'une information dans le domaine public n'affecte en rien les activités d'un service, d'une direction ou d'un organisme utilisateur.
Non publique (C2)	Ce niveau traduit que la diffusion est seulement possible en interne et au sein des organismes utilisateurs, ainsi qu'à l'ensemble de l'Administration et de ses prestataires.
Confidentiel (C3)	Ce niveau restreint la diffusion d'information au niveau d'une direction, d'un service, d'un projet métier ou transverse.
Très confidentiel (C4)	Ce niveau restreint la diffusion d'information à quelques agents, ou externes, nommément identifiés pour un sujet donné.

Échelle de gravité

Il s'agit de faire exprimer aux responsables métier sur un ensemble de thèmes retenus quel serait l'impact pressenti (faible, modéré, significatif et grave) du point de vue financier, juridique, maintien de l'activité et image du client

Échelle de vraisemblance générale

L'échelle de vraisemblance générale est à destination de la réflexion générale autour des scénarios de menaces (peu probable, moyennement probable, probable, très probable), du niveau de compétence des attaquants et de l'intérêt de réaliser un scénario. (voir EDC)

Les critères de gestion des risques

Ces critères de gestion explicitent la démarche proposée au client. Ainsi la méthode mise en œuvre afin de réaliser l'analyse de risque est totalement traçable, étapes par étapes, via la colonne de droite.

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Expression des besoins de sécurité (module 2)	Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié.
Estimation des événements redoutés (module 2)	Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet.
Évaluation des événements redoutés (module 2)	Les événements redoutés sont classés par ordre décroissant de gravité.
Estimation des scénarios de menaces (module 3)	Les scénarios de menaces sont estimés en termes de vraisemblance à l'aide de l'échelle définie à cet effet.
Évaluation des scénarios de menaces (module 3)	Les scénarios de menaces sont classés par ordre décroissant de vraisemblance.
Estimation des risques (module 4)	La gravité d'un risque est égale à celle de l'événement redouté considéré. ¢ La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques (module 4)	cf. planche matrice de criticité
Choix de traitement des risques (module 4)	cf. planche matrice de criticité

Homologation de sécurité (module 5)	Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables.

Matrice de criticité des risques

Lorsque l'on fait se rejoindre vraisemblance et impact cela nous donne la criticité du risque qui a été analysé.

Les biens essentiels

Les fonctions sont regroupées en processus dans un souci de clarté. La méthode veut qu'après une revue documentaire du projet, les besoins en termes de DICP soient recueillis directement auprès des représentants fonctionnels du métier lors d'entretiens, où les échelles et la méthode utilisée pour l'analyse leur sont donc expliquées dans le détail.

Les biens supports

Les biens supports quant à eux sont classés selon la typologie suivante, proposée par EBIOS:2010 :

- **SYS : Systèmes informatiques et de téléphonie**
- **SYS-MAT : Matériels**
- **SYS-LOG : Logiciels**

- **SYS-RSX : Réseaux**
- **ORG : Organisations**
- **ORG-PER : Personnes**
- **ORG-PAP : Supports papier**
- **ORG-CAN : Canaux interpersonnels**
- **LOC : Locaux**

Présenter les mesures de sécurité déjà en place

Les mesures identifiées comme étant déjà en place :

- acteurs
- antivirus
- firewall
- IDS
- formation
- …

Apprécier les événements redoutés

Un événement redouté est un scénario générique représentant une situation crainte par l'organisme. Il s'exprime par la combinaison des sources de menaces susceptibles d'en être à l'origine, d'un bien essentiel, d'un critère de sécurité, du besoin de sécurité concerné et des impacts potentiels auxquels est associé un niveau de gravité pour l'organisme.

La gravité d'un événement redouté est obtenue en retenant le niveau de gravité associé à la conséquence maximale en termes d'impacts survenant lorsque le besoin de sécurité n'est plus respecté.

Apprécier les scénarios de menaces

La vraisemblance d'un scénario de menace est la probabilité que celui-ci se réalise. Pour un scénario précis, elle est obtenue en rapprochant les vulnérabilités du bien support concerné, les mesures de sécurité dont bénéficient les bien supports, la capacité et la motivation d'une source de menace à vouloir exploiter les vulnérabilités.

Apprécier les risques

Pour identifier les risques sur un bien essentiel, pour chaque événement redouté du bien essentiel, la méthode appliquée consiste à :

Pour identifier les risques sur un bien essentiel, pour chaque événement redouté du bien essentiel, la méthode appliquée consiste à :

- retenir la gravité associée à l'événement redouté considéré ;
- identifier l'ensemble des scénarios de menaces pouvant affecter les biens supports dont dépend le bien essentiel ;
- retenir les scénarios de menaces de nature à affecter le critère de sécurité correspondant à l'événement redouté ;
- retenir le maximum de la vraisemblance de ces scénarios de menace.

Identifier les objectifs de sécurité

L'objectif est de proposer des nouvelles mesures de sécurité, afin de permettre de ramener tous les risques qui ont été identifiés comme intolérables.

Les solutions

Que les risques identifiés soient accidentels ou volontaires, les risques informatiques sont nombreux et menacent les systèmes informatiques, pouvant avoir des conséquences dramatiques. Il est donc nécessaire de mettre en place des systèmes de sécurité, tant au niveau de la prévention, pour limiter les facteurs de risque, qu'au niveau de la protection, pour diminuer l'ampleur des dégâts lorsqu'un sinistre se produit. Ainsi il existe des principes fondamentaux qu'il est obligatoire d'étudier avant de proposer des solutions sous la forme de mesures de sécurité dans une analyse de risque.

Politique de sécurité

Il faut toujours garder à l'esprit que la sécurité à 100% n'existe pas et qu'il y a nécessairement un compromis entre la valeur qui est protégée et son coût de protection. Une entreprise ou un organisme possédant des ressources informatiques doit donc déterminer les biens à protéger et les moyens raisonnables de protection à mettre en place il s'agit de la première mesure de prévention à prendre. Il n'existe pas de solution générale adaptable pour tous les cas de figure. Chaque entreprise comporte un scénario de risques particuliers et ne peut pas se voir attribuer une solution typique. C'est pour cette raison

qu'une importante étude doit être réalisée afin de définir les besoins en matière de sécurité.

La politique de sécurité de l'information est alors l'aboutissement de ces réflexions et le client dispose d'une politique de sécurité. La méthode utilisée actuellement en France par les entreprises et les organismes d'États afin d'y parvenir est la méthode EBIOS ou plutôt ses dérivés de la version 2010 comme celle que nous avons adaptée pour la mission. En effet, la méthode en elle-même est très axée sur la forme et ne s'engage pas sur le fond et les mesures concrètes à mettre en œuvre, pour cela on doit se reporter à des préconisations il a donc fallu élargir l'étude. Du côté de l'élaboration d'une PSSI c'est la norme **ISO 27001 < https://www.iso.org/fr/isoiec-27001-information-security.html>** et son annexe A constituée de 133 mesures de sécurité qui est la plus employée à la création de PSSI c'est donc un référentiel à prendre en compte. L'annexe A de l'ISO 27001 à sa propre norme, c'est l'ISO **27002 < https://www.iso.org/fr/standard/54533.html>** . L'ISO 27002 est nouvelle version de l'ISO **17999 < https://www.iso.org/fr/standard/39612.html>** qui avait déjà eu beaucoup de succès dans le passé, certains l'utilisent d'ailleurs encore aujourd'hui car la 17999 avait le mérite d'aller plus loin que la 27002 en termes de conseil d'implémentation de mesure de sécurité, un peu comme ITILv2 qui traitait de l'implémentation concrète de bonnes pratiques alors que **ITILV3 < http://www.itilfrance.com/>** ne traite plus de manière détaillée l'implémentation des bonnes pratiques.

Le facteur humain

La sécurité informatique d'une entreprise est tout d'abord une affaire de direction, qui seule a les pouvoirs d'ordonner la mise en œuvre effective des recommandations. Mais son élaboration et sa mise en pratique ne doivent en aucun cas reposer sur une seule personne. Tout le monde est concerné et doit coopérer à sa mise en place : les administrateurs qui ont la responsabilité du système, mais également les utilisateurs, qui considèrent souvent à tort que les problèmes de sécurité ne les concernent pas. À cette fin, la politique de sécurité ne doit pas être perçue comme une contrainte, mais plutôt comme un ensemble de règles librement consenties. On peut multiplier les mesures de sécurité, mais si elles ne sont pas comprises, leur utilité se réduit très vite. Les utilisateurs doivent donc être largement informés et sensibilisés sur les risques encourus et leurs conséquences.

La détermination des risques

L'évaluation des conséquences financières d'un sinistre avec les équipes du client a été difficile. Lors du vol d'un ordinateur par exemple, le coût immédiat est le remplacement de la machine. Mais il faut également prendre en compte la perte des informations contenues sur le support et l'indisponibilité des ressources dérobées. De même il faut compter les éventuelles pertes que l'utilisation de ces informations par des entités externes peut entraîner. C'est pour cela qu'il est très important de bien identifier les ressources, c'est à dire savoir ce qu'il faut protéger et à quel niveau. De même, les différentes structures n'ont pas le même profil, des ressources critiques pour l'une pouvant être secondaires pour l'autre. Il est ensuite nécessaire de déterminer les risques encourus pour les ressources définies précédemment. L'analyse des risques peut être effectuée par audit et à l'aide d'outils spécifiques. Des sociétés externes sont également spécialisées dans ce domaine et peuvent procurer des conseils ou établir un diagnostic.

Une fois les risques encourus déterminés, il est intéressant de se pencher sur leur probabilité d'apparition au moment où il faut proposer des mesures.

Pour chacune des ressources déterminées et des menaces qui la concernent, il convient de déterminer le coût de l'éventualité d'une destruction totale, afin de pouvoir classifier l'importance du niveau de protection à mettre en place. À ce niveau, il est possible également de se focaliser sur les ressources les plus sensibles, tant en termes de coût de reconstitution que de probabilité de perte.

Moyens de sécurisation

Moyens de défense :

- catégorisation des utilisateurs (administrateur, utilisateurs) ;
- habilitation ;
- identification et authentification ;
- révocation stricte et immédiate ;
- contrôles.

La confidentialité

De la même manière que les serveurs ne doivent être accessibles que par les administrateurs systèmes, les postes de travail ne doivent pas être accessibles par tous les

utilisateurs. Les bureaux doivent pouvoir être fermés à clé et les postes de travail doivent comporter des mots de passe valides

Audits et conformité

Les audits, inspections, diagnostics flash et autres appellations participent dans un cycle itératif d'amélioration continu à l'amélioration générale de la sécurité de nos environnements. Les normes de sécurité tel que **l'ISO 27001 https://www.iso.org/fr/isoiec-27001-information-security.html** ont prises une grande place dans le domaine de la sécurité et les certifications associés sont un bienfait pour toute la communauté. Les audits et la conformité dans son ensemble sont des outils puissants et essentiels.

Supervision sécurité

Des sources d'événements claires permettent une stratégie de lutte informatique défensive claire, on parlera également de stratégie de surveillance.

La visibilité du système

Il faut être en mesure de pouvoir à tout moment identifier l'état de sécurisation du système VIA un tableau de bord de la sécurité (**TDBSSI https://www.ssi.gouv.fr/guide/tdbssi-guide-delaboration-de-tableaux-de-bord-de-securite-des-systemes-dinformation/**) veille technologique et audit régulier (**ISO 19001 https://www.iso.org/fr/standard/70017.html**).

La protection physique

La protection de l'accès aux ressources informatiques est une des priorités des politiques de sécurité

les locaux

les contrôles d'accès

La redondance

La redondance consiste à introduire dans le système des éléments capables de prendre le relais, dans le cas où des organes vitaux viendraient à être défaillants.

La gestion des sauvegardes

Une politique de sauvegarde rigoureuse est plus que nécessaire dans tout système d'information. Le stockage des sauvegardes doit être sécurisé et des tests de restauration sont indispensables afin d'en vérifier la pertinence.

La défense des installations

Premier pas, il faut sécuriser l'environnement physique des installations.

- zonage ;
- accès réglementé ;
- rapport d'alarme (feu, inondation) ;
- cage de faraday, brouillage GSM ;
- caméra de surveillance ;
- drone de surveillance ;
- poste de sécurité.

La défense des réseaux

Second pas, sécuriser le réseau lui-même, mais aussi les interactions entre différents réseaux

- sécuriser tous les éléments du réseau, même les plus secondaires et ceux d'une tierce partie ;
- séparer les réseaux de sensibilité différente ;
- penser au secours électrique ;
- penser à l'accessibilité des armoires électriques et des éléments isolés (commutateur…) ;
- avoir une documentation et un schéma global à jour ;
- appliquer le principe des flux directionnel de confiance : les flux réseaux d'un domaine de confiance A, dit sure, vers un domaine de confiance B de confiance moindre et limiter au maximum l'inverse ;
- contrôler les flux qui entrent ainsi que ceux qui sortent ;
- recourir à des ruptures de protocoles ;
- identifier et contrôler strictement les voies de communication (modem pirate) ;
- sécuriser le réseau à tous les niveaux (couche physique, réseau, transport) ;

- respecter la RFC 1918 pour les plans d'adressage ;
- avoir recours à la translation d'adresses.

Les solutions

Que les risques identifiés soient accidentels ou volontaires, les risques informatiques sont nombreux et menacent les systèmes informatiques, pouvant avoir des conséquences dramatiques. Il est donc nécessaire de mettre en place des systèmes de sécurité, tant au niveau de la prévention, pour limiter les facteurs de risque, qu'au niveau de la protection, pour diminuer l'ampleur des dégâts lorsqu'un sinistre se produit. Ainsi il existe des principes fondamentaux qu'il est obligatoire d'étudier avant de proposer des solutions sous la forme de mesures de sécurité dans une analyse de risque.

Solution possible

- celui du moindre privilège : tout ce qui n'est pas explicitement autorisé doit être interdit, on aura remarqué que dans le cadre de notre étude ce principe fait partis des mesures de sécurité en place comme plusieurs des mesures suivantes ;
- la défense par couche ou défense en profondeur, qui est une protection successive à tous les niveaux ou il est possibles d'agir. Si une couche est corrompue, d'autres protections de nature différentes se présenteront à l'attaquant ;
- la mise en place de tableau de bord et journalisation : contrôles de l'état du SI ;
- la mise en place de moyen de détection (Alerte) et de réaction.
- La sécurité absolue n'existe pas, les règles de sécurité doivent donc évoluer en permanence ;
- la sécurité d'une application doit être prise en compte au plus tôt dans son cycle de vie, dès la rédaction du cahier des charges et des besoins non fonctionnels puis durant la conception, le développement et doit se concrétiser par une surveillance régulière quand l'application est en production ;
- la sécurité dès la conception c'est du bon sens, faire simple, éviter de faire de la sécurité par l'obscurité et privilégier une stratégie de défense en profondeur.
- la sécurité durant le développement, c'est filtrer les données entrantes, faire attention aux possibilités d'injection, les pièges des jeux de caractères, suivre les données, protéger les sorties et auditer son code ;
- la sécurité d'une application au quotidien, c'est modérer son contenu, analyser régulièrement les fichiers de « logs ». Se tenir continuellement informé. Tenir le socle

physique et logique de ses SI à jour. Un navigateur sur un poste client qui n'est pas à jour n'est pas sans risque ;

- prendre en compte les aspects légaux, même si ceux-ci demandent de plus en plus d'investissement aux entreprises et même si l'entreprise n'arrive déjà pas à gouverner son système d'information car elle n'arrivera pas à faire respecter les exigences légales qui lui incombent.

Pendant longtemps, on a pensé que la fiabilité d'une chaîne reposait sur celle de son maillon le plus faible. Ainsi, si R était la fonction de fiabilité (ou de survie), alors en fonction du temps, on pensait pouvoir écrire :
Rchaîne (t) = Min1 ≤ i ≤ nRi(t)
où les items indexent les n maillons de la chaîne. Or, il s'est avéré que, dans une chaîne, ce n'était pas systématiquement le maillon le plus faible qui se rompait en premier. La fiabilité de la chaîne est alors devenue une certaine fonction de la fiabilité de ses maillons, les plus faibles participant d'avantage que les plus solides à l'éventualité d'une rupture.

C'est Eric Pieruschka qui va finalement donner la formule de calcul de la fiabilité d'une chaîne :

Rchaîne (t) = P1 ≤ i ≤ nRi(t).
La probabilité de survie d'une chaîne à une date t arbitraire est le produit des probabilités de survie de chacun de ses composants à cette date, dans l'hypothèse où lesdits composants sont indépendants les uns des autres.

Il faut donc « penser sécurité » globalement, pour chaque composant d'un système d'information : poste client, pare-feu, routeur, sonde, serveur, applications…

Politique de sécurité

Il convient au préalable d'identifier les ressources et les causes de vulnérabilité en fonctionnement normal, c'est à dire de définir les points faibles du système. Une fois l'état des lieux réalisé, il faut effectuer un choix des mesures à mettre en place, en tenant compte du coût de la menace si celle-ci se produit et de l'évaluation du coût du système de protection.

Ainsi, l'analyse plus générale et pas seulement orientée « analyse de risque » peut se résumer comme suit :

- identification des ressources ;
- établissement des scénarios des risques encourus ;

- calcul des pertes face à ces événements ;
- détermination des moyens de sécurité nécessaires ;
- évaluation des contraintes techniques et financières
- choix final des solutions.

Moyens (non exhaustifs) de sécurisation

Dressons une liste de risques potentiels et ainsi de spécifier le « **quoi** » de la réflexion.
Apport de quelques éléments de réponse concernant le
« **comment** » en proposant différentes mesures et des moyens de défense.

Un principe, est aujourd'hui systématiquement évoqué, celui de la Défense en profondeur.

Dans une architecture interconnectée, quels sont les besoins courants ?

- connexion de l'entreprise à l'internet ;
- connexion de deux sites distants d'une même entreprise ;
- connexion d'un portable distant au réseau d'entreprise ;
- connexion d'un partenaire à l'entreprise ;
- mise à jour du public d'un moyen de paiement en ligne.

La politique et la stratégie de défense

Il faut s'assurer des accès licites aux diverses ressources.

Moyens de défense :

- catégorisation des utilisateurs (administrateur, utilisateurs) ;
- habilitation ;
- identification et authentification ;
- révocation stricte et immédiate ;
- contrôles.

La confidentialité

De la même manière que les serveurs ne doivent être accessibles que par les administrateurs systèmes, les postes de travail ne doivent pas être accessibles par tous les

utilisateurs. Les bureaux doivent pouvoir être fermés à clé et les postes de travail doivent comporter des mots de passe valides. Pour être efficaces, ceux-ci doivent être choisis avec soin et respecter quelques règles de base :

- Ne jamais choisir un mot de passe du langage courant. Comme nous l'avons vu dans la partie précédente, les pirates utilisent des dictionnaires pour venir à bout des mots de passe. S'il est choisi parmi des termes usuels, ce type de protection à toutes les chances de ne pas résister longtemps.
- Ne jamais choisir un mot proche de soi, tel que son nom, le prénom de ses enfants, sa date de naissance, le nom du chien, le numéro de sa plaque d'immatriculation, son passe-temps favori… N'importe qui connaissant suffisamment la personne aura tôt fait de trouver le mot de passe choisi.
- Choisir un mot de passe long. Les logiciels de force brute arrivent aisément à décrypter les mots comportant moins de 6 caractères dans un laps de temps raisonnable.
- Les bureaux en libre-service avec le mot de passe de la machine inscrit sur un papier collé à l'écran sont évidemment à proscrire. N'importe quel pirate se faisant passer pour un technicien ou un client extérieur à la société pourrait ainsi se procurer facilement des informations confidentielles.
- Le mieux est de prendre un mot de passe constitué de chiffres et de lettres, de majuscules et de minuscules. Il est prudent d'y ajouter des caractères de ponctuation ou des caractères peu souvent utilisés, ceci afin de compliquer le travail de décryptage.
- De nombreux procédés mnémotechniques permettent de se rappeler comment générer et surtout retrouver ce type de mots de passe. Une fois un de ces procédés choisi, il est aisé de posséder un mot de passe différent pour chaque application et d'en changer régulièrement.

Malgré ces quelques règles, les mots de passe utilisateur sont généralement simples et possèdent une longue durée de vie. Pour éviter qu'un pirate s'empare du mot de passe et le réutilise pour se connecter, le plus simple est d'en changer à chaque connexion. Les mots de passe à usage unique (OTP, One Time Password) permettent à un client de se connecter avec un mot de passe différent grâce à un dialogue avec la machine cible. Alors que la plupart des authentifications se font de manière simple (login / mot de passe), les OTP se basent sur le couple challenge / réponse.

Voici le déroulement d'une authentification utilisant les OTP :

- le client fait une demande de connexion au serveur à distance (ftp, ssh, telnet, …) ;
- le serveur envoie un challenge au client, composé d'un compteur (un nombre plus grand que 1) et d'une graine (2 caractères suivis de 5 chiffres : aa11111) ;

- le client calcule alors le mot de passe jetable localement grâce à un programme, en entrant le challenge et une phrase secrète qu'il a choisi auparavant. Une fois le mot de passe calculé, il est envoyé au serveur ;
- le serveur vérifie que le mot de passe correspond bien au challenge envoyé crypté, et permet ou non l'accès.
- Le mot de passe jetable est généré en concaténant la graine et la phrase secrète, puis en appliquant une fonction de hachage (exemple : MD5 ou SHA) autant de fois qu'indiqué par le compteur. Le résultat est ensuite converti en six courts mots anglais qui constituent le mot de passe non réutilisable.
- Le compteur est décrémenté à chaque connexion de l'utilisateur, et lorsque celui-ci arrive à 0, l'utilisateur se voit demander la création d'une nouvelle phrase secrète et d'une nouvelle graine.

Comme tout système, les OTP possèdent des failles, cependant elles restent plus difficiles à exploiter qu'avec l'utilisation de mots de passe classiques. Ces failles tournent essentiellement autour de l'attaque brut ou par dictionnaire en récupérant le challenge puis la réponse, et en essayant de retrouver la phrase secrète par exemple. L'utilisation d'un keylogger peut également servir à récupérer la phrase secrète de l'utilisateur lorsqu'il utilise un outil pour générer le mot de passe jetable.

Audits et conformité

Les audits, inspections, diagnostics flash et autres appellations participent dans un cycle itératif d'amélioration continu à l'amélioration générale de la sécurité de nos environnements. Les normes de sécurité tel que **l'ISO 27001 <https://www.iso.org/fr/isoiec-27001-information-security.html>** ont prises une grande place dans le domaine de la sécurité et les certifications associés sont un bienfait pour toute la communauté. Les audits et la conformité dans son ensemble sont des outils puissants et essentiels.

Supervision sécurité

Comment évoquer les moyens de supervision de sécurité sans parler de la gestion et de la corrélation des logs. Très à la mode, le SIEM (Security Information and Event Management) a pour objectif de répondre au besoin des entreprises d'analyser les événements de sécurité en temps réel, au regard de la gestion interne et externe des menaces. Cette solution permet de surveiller des applications, des comportements utilisateurs et des accès aux données. A travers les fonctionnalités fournis par la solution, il est donc possible de collecter, normaliser, agréger, corréler et analyser les données des

événements issus des machines, systèmes et applications (pare-feu, IDS/ISP, Machines réseau, Machines de sécurité, Applications, bases de données, serveurs, annuaires, IAM).

Des sources d'événements claires permettent une stratégie de lutte informatique défensive claire, on parlera également de stratégie de surveillance.

La visibilité du système

Il faut être en mesure de pouvoir à tout moment identifier l'état de sécurisation du système.

Moyens de défense :

- tableau de bord de la sécurité (**TDBSSI https://www.ssi.gouv.fr/guide/tdbssi-guide-delaboration-de-tableaux-de-bord-de-securite-des-systemes-dinformation/**) ;
- veille technologique ;
- audit régulier (**ISO 19001 https://www.iso.org/fr/standard/70017.html**).

La protection physique

La protection de l'accès aux ressources informatiques est une des priorités des politiques de sécurité. Il convient alors à nouveau de se poser plusieurs questions :

- les machines sont-elles en lieu sûr et inaccessibles par des personnes non autorisées ;
- certaines machines restent-elles connectées inutilement sans surveillance ;
- des sauvegardes de données sont-elles effectuées régulièrement ;
- les utilisateurs sont-ils des gens de confiance.

Les locaux

Il est indispensable de protéger physiquement les éléments critiques du système contre les risques naturels, tels que la foudre, les coupures de courant, ou même les dégâts des eaux et les incendies.

Pour cela, il faut respecter quelques règles :

- protéger le matériel vital, comme les serveurs, par des onduleurs qui prennent le relais en cas de défaillance du secteur, et qui offrent une protection vis à vis des surtensions ;

- placer ces systèmes dans des locaux protégés. Il faut leur réserver une pièce à l'abri des inondations (éviter les sous-sols), exempte de poussière et climatisée. Le local doit être fermé à clé, et pourra être couplé à des systèmes d'alarme ;
- les administrateurs systèmes devront au moins être deux, l'absence de la seule personne capable de remettre le système en état (maladie, congé…) pouvant être aussi dramatique qu'un système mal protégé ;
- les composants des ordinateurs et les supports de stockages sont sensibles aux effets magnétiques. Il faut donc les tenir écartés des appareils source de magnétisme.

Quelles que soient les précautions prises pour garantir son bon fonctionnement, le matériel informatique n'est pas à l'abri d'une panne. Tout matériel doit donc disposer d'une garantie solide, nécessitant le moins d'immobilisation possible de la ressource, tant pour son remplacement que pour sa réparation.

La redondance

Certaines données conservées sur le système d'information d'une entreprise sont nécessaires à son fonctionnement, elles ne doivent donc en aucun cas être perdues ou indisponibles. La redondance consiste à introduire dans le système des éléments capables de prendre le relais, dans le cas où des organes vitaux viendraient à être défaillants.

Les disques durs peuvent être protégés physiquement à l'aide de la technologie **RAID (Redundant Array of Inexpensive Disks) https://www.shooga.ovh/bts-abonne/proteger-ses-donnees**. Ce système offre une double utilité : accélérer les accès disques et éviter les pertes de données.

La gestion des sauvegardes

Une politique de sauvegarde rigoureuse est plus que nécessaire dans tout système d'information. Le stockage des sauvegardes doit être sécurisé et des tests de restauration sont indispensables afin d'en vérifier la pertinence.

Que la cause de la perte de données soit due à une panne matérielle ou à un acte malveillant, dans la mesure ou la protection système n'a pas pu l'empêcher, il est nécessaire de pouvoir restaurer au plus vite l'information. Seules les sauvegardes peuvent remédier à cette perte, c'est pour cela que ces solutions doivent être mises en place au plus tôt.

Les sauvegardes sont des copies de fichiers permettant leur restauration lorsqu'un incident se produit. Leur but est d'éviter une perte de temps et d'argent, et de se prémunir contre une situation catastrophe.

Plusieurs stratégies de **sauvegarde https://www.shooga.ovh/bts-abonne/proteger-ses-donnees** sont possibles, il faut choisir la plus adaptée en termes de méthodes et de support.

L'utilisation de plusieurs supports est importante, pour éviter l'usure de ceux-ci, et ne pas courir le risque de perdre toute la sauvegarde en cas de détérioration.

Il est également prudent de placer ces sauvegardes dans un endroit différent du système à sécuriser, ceci afin d'éviter leur destruction simultanée dans le cas d'un incendie par exemple.

De plus, le lieu de stockage doit répondre à des critères de sécurité stricts : problèmes de confidentialité, conditions de température et d'hygrométrie…

La sécurité physique fait appel à la notion de zonage d'un système d'information et une salle serveur devra posséder ainsi à minima :

- un mécanisme d'authentification protégeant son accès ;
- des détecteurs d'incendie et d'humidité ;
- une journalisation des accès ;
- des procédures d'intervention (dépannage, personnel, extérieurs) ;
- un système de climatisation adapté ;
- des moyens de secours d'alimentation électrique ;
- Une protection des éléments actifs du réseau et des zones de sauvegarde.

La défense des installations

Premier pas, il faut sécuriser l'environnement physique des installations.

Moyens de défense :

- zonage ;
- accès réglementé ;
- rapport d'alarme (feu, inondation) ;

- cage de faraday, brouillage GSM ;
- caméra de surveillance ;
- drone de surveillance ;
- poste de sécurité.

La défense des réseaux

Second pas, sécuriser le réseau lui-même, mais aussi les interactions entre différents réseaux

Moyens de défense :

- sécuriser tous les éléments du réseau, même les plus secondaires et ceux d'une tierce partie ;
- séparer les réseaux de sensibilité différente ;
- penser au secours électrique ;
- penser à l'accessibilité des armoires électriques et des éléments isolés (commutateur…) ;
- avoir une documentation et un schéma global à jour ;
- appliquer le principe des flux directionnel de confiance : les flux réseaux d'un domaine de confiance A, dit sure, vers un domaine de confiance B de confiance moindre et limiter au maximum l'inverse ;
- contrôler les flux qui entrent ainsi que ceux qui sortent ;
- recourir à des ruptures de protocoles ;
- identifier et contrôler strictement les voies de communication (modem pirate) ;
- sécuriser le réseau à tous les niveaux (couche physique, réseau, transport) ;
- respecter la RFC 1918 pour les plans d'adressage ;
- avoir recours à la translation d'adresses.

Protocoles TLS, SSL et HTTPS

Transport Layer Security (TLS), et son prédécesseur Secure Sockets Layer (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le protocole SSL était développé à l'origine par Netscape. L'IETF en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire aux objectifs de sécurité suivants :

- l'authentification du serveur ;
- la confidentialité des données échangées (ou session chiffrée) ;
- l'intégrité des données échangées ;
- de manière optionnelle, l'authentification du client (mais dans la réalité celle-ci est souvent assurée par le serveur).

Le protocole est très largement utilisé, sa mise en œuvre est facilitée du fait que les protocoles de la couche application, comme HTTP, n'ont pas à être profondément modifiés pour utiliser une connexion sécurisée, mais seulement implémentés au-dessus de SSL/TLS, ce qui pour HTTP a donné le protocole HTTPS.

Les réseaux privés virtuels IPSEC

Un RVP (réseau virtuel privé) est un réseau dont l'accès est réservé à une certaine communauté. On utilise un réseau WAN « public » : une infrastructure partagée mais qui garantit la confidentialité des données échangées.

Le protocol IPSEC permet de sécuriser le trafic :

- entre deux stations ;
- entre une station et un routeur ;
- entre deux routeurs ;

Les réseaux privés virtuels (VPN, Virtual Private Network) permettent de réaliser une liaison sécurisée entre deux réseaux distants à travers un réseau public. Ils sont généralement utilisés pour le télétravail, permettant à des employés de se connecter à leur entreprise par l'intermédiaire d'internet via un chemin virtuel sécurisé. Ils peuvent aussi permettre de relier deux sites d'une entreprise sans recourir à des lignes spécialisées. Il existe donc deux utilisations principales de VPN :

- un réseau privé virtuel client-serveur, où un utilisateur distant se connecte au réseau local de son entreprise ;
- un réseau privé virtuel de serveur à serveur, lorsque deux réseaux locaux sont connectés entre eux.

Bien que les VPN nécessitent l'acquisition de produits matériels et logiciels supplémentaires, le coût des communications est moindre, l'entreprise ne s'acquittant que d'un accès internet.

Un VPN nécessite :

- un serveur VPN pour accepter les connexions des clients VPN
- un client VPN
- un tunnel par lequel les données transitent
- une connexion VPN dans laquelle les données sont chiffrées et encapsulées

Cette technique fonctionne grâce à un principe de tunnel dont chaque extrémité est identifiée. Ensuite la source chiffre les données, les encapsule et les achemine vers la destination. Cette technique met donc en œuvre le chiffrement et l'authentification des données.

Relais SMTP

Un relai SMTP (Simple Mail Transfer Protocol) permet de recevoir les flux de messagerie venant d'Internet sens qu'il va rentrer dans le système d'information ;

- il permet de dicter des règles d'anti Replay et d'anti spam ;
- il permet l'envoi de courriels du serveur de messagerie interne d'Internet ;
- il peut, en outre, vérifier l'identité des émetteurs autorisé.

Les AP (Access point)

Ils permettent la connexion de nomades sur un système d'information ou sur internet. Les nombreuses vulnérabilités du protocole 802.11 nécessitent la mise en place des éléments de filtrage et de détection d'intrusion. Un bon AP doit répondre à minima aux critères suivants :

- Filtrage des adresses MAC ;
- Activation du WPA ;
- Paramétrage de la puissance d'émission ;
- Filtrage des flux à la ligne ;
- Filtrage des flux nappe ;
- Implémentation VPN IPSec.

Les pares-feux

Un pare-feu est un matériel ou un logiciel qui permet de protéger un réseau des attaques extérieures, effectuant un filtrage sur les communications entrantes et sortantes. Il empêche ainsi toute personne d'accéder, de détruire ou de dérober des données du système informatique.

Le pare-feu :

- crée un fichier journal du trafic sur le réseau ;
- filtre les paquets entrants et sortants du réseau. C'est à dire qu'il les accepte ou les rejette suivant une stratégie d'accès prédéfinie. (Adresse IP, protocole…) ;
- ferme l'accès aux ports ouverts par les ordinateurs du réseau ou les cache (ports furtifs)
- traduit les adresses IP utilisées sur internet en adresses différentes dans le réseau interne. La machine sur laquelle le pare-feu est installé sera alors la seule machine du réseau accessible depuis l'extérieur. (technologie NAT, Network Address Translation, soit traduction des adresses sur le réseau) ;
- prend en charge un ensemble d'applications et détecte les requêtes d'ouverture de session pour déterminer celles qui n'ont pas lieu d'être.

On distingue différents parefeux

- le logiciel pare-feu personnel s'exécute sur l'ordinateur qu'il protège. Il offre en général le filtrage de la couche TCP/IP et des applications, c'est à dire qu'il arrête les intrus et fournit un bon niveau de protection contre les attaques ;
- le pare-feu matériel se branche entre le réseau et la connexion extérieure. Appelés généralement routeurs à large bande ou passerelles internet, ils proposent le blocage des ports et la traduction des adresses du réseau (NAT). Lors d'une attaque, le réseau n'est pas affecté puisque le pare-feu encaisse le choc en premier ;
- le pare-feu autonome est un ordinateur possédant deux cartes réseau, un système d'exploitation de base et un logiciel pare-feu. C'est une solution bon marché qui nécessite une grande compréhension dans la configuration des fonctionnalités du logiciel et du système d'exploitation.

Principes de la Zone démilitarisée (DMZ)

En informatique une zone démilitarisée, (ou DMZ, de l'anglais demilitarized zone) est

un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

Le pare-feu bloquera donc les accès au réseau local pour garantir sa sécurité. Et les services susceptibles d'être accédés depuis Internet seront situés en DMZ.

En cas de compromission d'un des services dans la DMZ, le pirate n'aura accès qu'aux machines de la DMZ et non au réseau local.

La défense des interconnexions

Troisième pas, il faut sécuriser les moyens qui permettent des interactions entre deux réseaux différents Moyens de défense :

- identifier et contrôler strictement les interconnexions (routeurs) ;
- identifier clairement les flux nécessaires (diagramme des flux) ;
- limiter les flux à ceux strictement nécessaires ;
- contrôler les flux par des éléments dédiés (sondes d'intrusion) ;
- veille technologique.

Les systèmes de détection/prévention d'intrusions

Un système de détection d'intrusions IDS (intrusion détection système) peut être assimilé à un renifleur utilisé dans le sens de la protection réseau. Un IDS ne filtre pas les paquets à la manière d'un pare-feu, mais il les capture et les inscrit dans un fichier. Il est aussi doté de fonctions spéciales, permettant entre autres de détecter des activités anormales, de rechercher d'éventuelles faiblesses et de détecter des changements dans le système de fichiers. Mais le système de détection d'intrusions sert avant tout à relever les tentatives de sondage ou de connexion au système. Une utilité des IDS est de savoir ce que filtre réellement le pare-feu. Pour cela il suffit d'en installer un avant et un autre après le dispositif et de comparer les résultats de sortie.

En fait, Le système de détection d'intrusion complète efficacement une protection préventive comme celle du pare-feu. Mais il n'existe pas de système infaillible, un comportement anormal étant difficile à définir. Une configuration trop restrictive entraîne une succession de fausses alertes, alors qu'à l'inverse une configuration trop lâche ne sert à rien. Il est alors plus intéressant de se concentrer sur des groupes d'activités. Une heure tardive combinée à une commande inhabituelle attirera donc plus l'attention que des

commandes isolées. Les IPS (Systèmes de prévention d'intrusion) tentent quant à eux de bloquer l'attaque en cours mais ils sont difficiles à paramétrer.

Routeur

Ils permettent de séparer deux réseaux sur un même site de relier deux sites distants. Il possède un acces qu'il convient de paramétrer correctement pour sécuriser le système d'information et économiser de la bande passante.

Les serveurs proxy

Un proxy est un serveur, il va se substituer au client et effectuer les requêtes en son nom propre. Il permet donc d'accéder à internet et va pouvoir contrôler le protocole au niveau applicatif. Il en existe différentes sortes, http, ftp, smtp. Les proxys d'accès internet permettent d'identifier les clients et ils possèdent un cache qui améliore les performances.

Un serveur proxy, permettant aux machines d'un réseau d'accéder à internet, peut combiner tout un ensemble de solutions citées précédemment.

Un serveur proxy est un ordinateur comportant deux cartes réseau, un routeur de réseau, un pare-feu et des logiciels de sécurisation :

- Cartes réseau : L'une des cartes réseau permet la connexion à internet, tandis que l'autre permet de se connecter au réseau privé.
- Routeur: Le composant logiciel routeur de réseau permet à l'ordinateur de partager une connexion entre les différents ordinateurs du réseau.
- Pare-feu : Dans la plupart des cas, il combine un pare-feu de niveau réseau et application pour offrir une sécurité maximale.
- Antivirus: Il permet d'empêcher virus, vers et chevaux de Troie d'infecter le réseau et réduit la nécessité d'installer un antivirus par poste.
- Filtrage: Le filtrage permet d'empêcher l'accès à Certains sites.

Le niveau de configuration offert par un proxy est donc très élevé. Il représente une bonne mesure de protection de par la complémentarité de ses fonctions.

Quant à ce que l'on qualifie de « reverse proxy », il permet à une communauté internet d'accéder à un serveur web d'une entreprise. Il effectue une coupure des flux entre internet et le serveur web. Il permet un contrôle approfondi des requêtes émises d'internet vers le serveur web et ainsi de contrôler les attaques.

Pot de miel ou Honeypots

Le concept est de mettre en place des systèmes volontairement vulnérables conçus pour être scannés, attaqués et compromis. Le but est d'observer les comportements et de connaître les outils et les méthodes d'attaques de pirates.

Principes des « Pots de miels » (Honeypots)

Dans le jargon de la sécurité informatique, un pot de miel, ou honeypot, est une méthode de défense active qui consiste à attirer, sur des ressources (serveur, programme, service) , des adversaires déclarés ou potentiels afin de les identifier et éventuellement de les neutraliser.

Le terme désigne à l'origine des dispositifs informatiques spécialement conçus pour susciter des attaques informatiques.

Dans le cadre de la supervision en sécurité, le honeypot pourra être utilisé en tant que « sonde » faisant partie intégrante du dispositif de surveillance. Le honeypot alors considéré doit alors faire l'objet d'une étude d'intégration à la stratégie de surveillance globale du système d'information. L'objectif est de dégager à partir de la sonde des événements unitaires ou corrélés pouvant donner lieu à des alertes de sécurité.

Ce système est censé ne jamais être contacté. Tout contact avec la sonde est en soit une piste qui peut amener à détecter une attaque ou un problème.

La défense des données

Identifier les moyens de stockages (disque dur, clé USB) et les transits (internet, intranet, extranet, domiciles) .

Moyens de défense : contrôler les accès aux informations (ACP) . Chiffrement. Identification. Authentification. Éducation des utilisateurs. Politique de sauvegarde. Différenciation du niveau de sensibilité des données.

La défense des applications

Pensez dès le début du projet et en abstraction de la sécurité du système d'exploitation sur lequel elle reposera.

Moyen de défense : développement selon l'état de l'art (**OWASP https://fr.wikipedia.org/wiki/Open_Web_Application_Security_Project**), gestion des droits des applications dans le contexte de la politique de gestion des mots de passe. Maintenance à jour de la version de l'application. Audit du code. Documentation complète et explicite.

Cryptographie : elle permet essentiellement de protéger des données. Elle permet également avec la signature électronique d'assurer l'authentification d'une source. Elle est utilisée dans des protocoles tels qu'IPSEC, HTTPS, SSH, par exemple pour sécuriser les échanges.

- Cryptographie symétrique et asymétrique
- Signatures et normes X509
- Le chiffrement

La défense des hôtes

Installation des services à minima. Politique de mot de passe, identification/authentification. Mise à jour régulière des correctifs du système d'exploitation. Niveau et mesures de sécurisation adaptés à chaque hôte. Chiffrement maintenance. Sauvegarde régulière et automatisé. Partitionnement système d'exploitation + applications + journaux. Secours électrique. Accessibilité. Antivirus mis à jour et automatisé. Détection d'intrusion. Analyse et corrélation des fichiers de logs

L'antivirus

Une conscience d'utilisation de la part des utilisateurs est également nécessaire. Ils doivent avoir connaissance des menaces potentielles lorsqu'ils utilisent l'outil informatique. Les quelques mesures de précaution suivantes permettent d'assurer une bonne sécurité vis à vis du code malveillant :

- utilisation d'un antivirus mis à jour régulièrement ;
- information des utilisateurs sur les risques encourus ;
- suppression du courrier électronique dont on ne connaît pas la provenance ;

- réglage des paramètres de courrier électronique pour désactiver l'ouverture automatique des scripts joints au courrier ;
- désactivation des contrôles ActiveX et JavaScript dans le navigateur Web ;
- désactivation de l'exécution automatique des macros dans les applications bureautiques et définition d'un niveau de sécurité ;
- ajout de sa propre adresse dans son carnet d'adresse pour détecter l'envoi automatique de courrier électronique en cas de contamination

L'authentification

Il existe plusieurs façons d'identifier : login, mot de passe, biométrie, certificats, carte à puce. Utilisateurs connus et associés à une matrice des droits d'accès aux ressources de l'entreprise. Tous les accès au réseau (intranet) son authentifiés. Tous les accès distants au réseau sont fortement authentifiés. Aucune connexion directe au réseau Internet n'est autorisée.

Protocole d'authentification

Il en existe plusieurs :

- OTP (One Time Password), un mot de passe différent est exigé à chaque nouvelle connexion ;
- Kerberos ;
- SRP (Secure Remote Passwords) ;
- Radius (Remote Authentication Dial-In User Service) ;
- LDAP (Lightweight Directory Access Protocol SSO) ;
- EAP (Extensible Authentification Protocol).

L'authentification est donc un aspect à ne pas négliger lors de la réalisation d'échanges et l'authentification des correspondants, c'est à dire la vérification de l'identité des parties.

Dans un environnement à clé publique, il est essentiel de s'assurer que la clé utilisée appartient bien à la personne à laquelle on destine les données. Cette fonction est assurée par les certificats numériques.

Un certificat est un document électronique qui atteste de l'identité de son détenteur, pour prévenir la contrefaçon. Il contient des informations sur la clé publique d'une personne,

afin de garantir son authenticité.

Le certificat doit être généré par un tiers de confiance, c'est à dire un organisme indépendant qui contrôle la véracité de ces informations. La mise en place d'une PKI nécessite une étude préalable. Elle permet une sécurisation lors d'échanges de type e-commerce, notamment pour :

- les banques en ligne ;
- les impôts, TVA, les services du ministère des finances… en ligne;
- les extranets sensibles.

La PKI (Public Key Infrastructure) regroupe tous les éléments requis par une autorité de certification (Certifying Authority) pour l'émission et l'administration des certificats. Les certificats peuvent être déposés et récupérés par l'intermédiaire d'une base de données appelée serveur de certificats.

La cryptographie à clé publique permet également l'utilisation des signatures numériques dont l'objectif est de garantir l'authentification et l'intégrité des données. La signature s'effectue à l'aide de la clé privée pour sa création et de la clé publique pour sa vérification. Une empreinte générée par hachage est codée à l'aide de la clé privée, puis envoyée avec le certificat contenant la clé publique. Le destinataire vérifie la validité du certificat en décodant la signature avec la clé publique et en le comparant à l'empreinte du message reçu. A ce stade, le destinataire s'assure de l'identité de l'expéditeur et la non-modification du message.

Les évolutions du commerce électronique entraînent l'apparition de moyens de paiement sécurisé. C'est notamment le cas de SSL (Secure Socket Layer) développé par Netscape. SSL est la plus répandue des solutions de sécurisation de transaction. Intégrée dans tous les navigateurs du marché, son succès est dû avant tout à simplicité d'utilisation. SSL assure l'authentification des parties et le cryptage des données. Une session SSL démarre lorsqu'une adresse de type « https:// » est demandée. Le fondement de ce protocole est l'algorithme de cryptage à clé publique RSA décrit précédemment. Toutes les données transmises sont chiffrées, l'ensemble du processus étant totalement transparent pour l'utilisateur. Il existe typiquement deux types de certificats : serveur et client. Les certificats serveur sont principalement utilisés par SSL. Les certificats clients servent à identifier les utilisateurs individuels, et sont généralement utilisés pour les logiciels de messagerie avec des systèmes comme PGP (Pretty Good Privacy). PGP est un logiciel de protection des données, souvent utilisé pour le courrier électronique et très facile d'utilisation.

Suivie des patchs

La première protection d'un système d'information est la mise à jour des patchs publiés par l'éditeur. Afin d'y arriver, une centralisation de mises à jour est indispensable pour une entreprise.

Configuration des ordinateurs

Les serveurs devront toujours être installés avec les seuls services nécessaires.

- Il est préférable de ne pas multiplier les services sur un même serveur, un service devrait être égal à un serveur ou à une machine virtuelle ;
- le BIOS devra être protégé par mot de passe et ne jamais permettre de booter sur un support extérieur ;
- les postes de travail doivent être inventoriés ;
- le strict nécessaire des logiciels doit être installé ;
- l'uniformité des logiciels est un atout dans la gestion des failles et de l'obsolescence.

Anti spyware

Les spywares sont devenus courant sur les ordinateurs naviguant sur internet. Il est recommandé de posséder des logiciels antispyware afin de nettoyer les ordinateurs.

- *Filtrer, avec les expressions rationnelles, pour se protéger*

Une expression rationnelle (ou expression régulière par traduction de l'anglais regular expression) est en informatique une chaîne de caractères que l'on appelle parfois un motif et qui décrit un ensemble de chaînes de caractères possibles selon une syntaxe précise.

Les expressions rationnelles sont issues des théories mathématiques des langages formels des années 1940. Leur puissance à décrire des ensembles réguliers explique qu'elles se retrouvent dans plusieurs domaines scientifiques dans les années d'après-guerre et justifie leur adoption en informatique. Les expressions rationnelles sont aujourd'hui utilisées par les informaticiens dans l'édition et le contrôle de texte ainsi que dans la manipulation des langues formelles que sont les langages de l'informatique.

Sécurisation des serveurs

Une architecture Web est une architecture 3-tiers, elle est composée d'un client, d'un serveur d'application et d'un serveur de données. Chacun de ces composants est vulnérable et donc attaquable. La force d'une chaine n'est égale qu'à celle de son plus faible maillon.

- attaque coté client sur le navigateur (virus, trojan, cookies, cross site scripting,..) ;
- attaque coté serveur d'application (Apache, Tomcat) ;
- attaque coté serveur de données (MySQL) ;
- injection SQL, dénis de service, prise de main.

La veille technologique

Elle permet l'adaptation de la sécurité du système d'information en fonction de l'actualité.

Moyen de défense : Pour les administrations et les entreprises il s'agit de mettre en place des services.

- CERT-FR https://www.cert.ssi.gouv.fr/ ;
- revues spécialisées, HSC, MISC, etc… ;
- listes de diffusion spécialisées ;
- offres de service CERT.

Formaliser les mesures de sécurité à mettre en œuvre

1. **Déterminer les moyens nécessaires** pour la réductions des risques et la prise en charge des incidents, qu'il s'agisse de moyens matériels ou humains
2. **Définir les procédures adaptées**, notamment en matière de gestion des incidents, ou de gestion de la continuité d'activité
3. **Rédiger une charte informatique**, à l'attention des collaborateurs
4. **Communiquer sur la politique de sécurité informatique** auprès de l'ensemble de l'entreprise

Mesures de sécurité complémentaires

Une mesure de sécurité peut avoir plusieurs états totalement indépendants du traitement du risque :

- **Non retenue** : exemple, la proposition est interdite par la PSSI de l'entreprise, ou l'entreprise à un mauvais RETEX vis-à-vis de cette solution ;
- **En étude** : exemple, les équipes doivent vérifier que la solution est compatible avec l'application et ne va pas empêcher son fonctionnement ;
- **Proposée** : cette mesure est officiellement proposée à l'arbitrage du commanditaire qui choisira en fonction des risques qui lui sont liés, ainsi que de sa facilité de mise en œuvre, de la sélectionner définitivement ou non.
- **En place** : exemple, l'équipe a été sensibilisée à la sécurité et utilise des méthodes de développement sécurisé.

Calcul des risques résiduels

On doit évaluer les risques résiduels dans un tableau dans l'hypothèse où l'ensemble des mesures de sécurité seraient retenues et correctement appliquées.