POLITIQUE DE SECURITE

1. Sécurité informatique vs sécurité des systèmes d'information :

Un système d'information est un ensemble de systèmes informatiques (matériel et logiciel) ainsi que l'ensemble des moyens non informatiques : êtres humains, matériel, règles de gestion, etc. Donc la sécurité des systèmes d'information SSI est loin d'être réduite à la sécurité informatique SI.

La plus grande vulnérabilité d'un SI est l'être humain, ainsi la sécurité d'un tel système est loin d'être limitée à des solutions techniques. En revanche il faut se doter par d'autres mesures de formation, de sensibilisation et de sanctions envers les différents types de comportements humains.

Donc la sécurité d'un système d'information doit être une stratégie mise en place comportant :

- Un staff humain piloté par un responsable appelé RSSI (responsable de la sécurité du système d'information), veillant à garder le niveau de sécurité du système le plus haut possible.
- Des solutions techniques combinant entre solutions matérielle et logicielle.
- Des règles de sécurité à appliquer strictement par l'ensemble du personnel et partenaires.
- Des schémas et des plans de sécurité servant à connaitre l'état du système à n'importe quel moment, et à préciser les actions nécessaires pour stabiliser le système.
- Des directives de formations et de sensibilisation pour l'ensemble du personnel envers la sécurité du système.
- De règlement servant à déterminer les responsabilités des différentes entités.

2. Politique de sécurité :

La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI). Elle est traduite par un ensemble de documents cadres (référentiel) qui répond à la question 'Qui fait Quoi ?' en matière de la sécurité théoriquement à tout moment, au sein du périmètre dans lequel il s'applique.
C'est un ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.

3. Objectif de la politique de sécurité :

La politique de sécurité constitue le document de référence en matière de sécurité. Elle permet en outre :

- D'institutionnaliser et de reconnaître la légitimité de la sécurisation de la structure : le RSSI voit ainsi son rôle officialisé et ses différentes actions n'ont plus uniquement une étiquette informatique;
- D'assurer une cohérence dans les décisions, projets et investissement : les différents acteurs de la sécurité ayant une vision globale et transverse de la sécurité, le niveau de sécurité sera plus homogène et les phénomènes de factorisation et de mutualisation engendrés permettront globalement de réaliser des économies;
- De sensibiliser et de responsabiliser les différents acteurs : certains éléments de la politique (une charte par exemple) seront largement communiqués à l'ensemble des acteurs du SI, qu'ils soient utilisateurs internes, sous-traitant ou prestataires ou

stagiaires. Cette prise de conscience des règles et des contraintes notamment juridiques participe à l'amélioration de la culture de la sécurité.

4. *Les différents aspects de la PSSI :*

La solution proposée par la PSSI doit prendre en considération les trois aspects suivants :

a) Aspect organisationnel (procédural) :

- Règles de travail : il faut définir des règles de travail et de gestion à respecter strictement par l'ensemble de personnel.
- Sensibilisation : sensibiliser le personnel sur l'importance de la sécurité et la gravité des dangers provenant de l'internet.
- Formation : organiser périodiquement des séances de formation au profit du personnel sur les nouvelles technologies, les nouvelles techniques d'intrusion et les nouvelles contre-mesures.
- Faire périodiquement des **audits** de sécurité pour tester les nouvelles techniques, méthodes de travail, le nouveau matériel et dispositif, et la conscience du personnel. Ces tests peuvent même arriver à faire provoquer des situations d'insécurité réduites (sous contrôle) afin d'étudier et évaluer la réaction du personnel, et faire accroitre leur conscience envers l'importance de la sécurité. Au-delà de ces tests il faut prévenir des plans d'action à exécuter des situations critiques à savoir le plan de continuité, et le plan de reprise, des procédures d'archivage et de gestion de traces.
- Sauvegarde et gestion des traces des utilisateurs internes et externe.
- Archivage périodique des données sensibles.
- Etablir des plans d'action à appliquer en cas d'insécurité à savoir le Plan de Continuité, le Plan de Reprise...etc.
- Révision et réévaluation des processus métiers et des procédures de travail, afin de découvrir s'il y en a de failles qui peuvent être source d'exploitation par des personnes malveillantes.
- Etc.

b) Aspect juridique (législatif) :

Dans l'absence de sanction la solution organisationnelle reste une solution bidon, généralement l'être humain ne se sent responsable que s'il connait qu'il peut être sanctionné en cas de viol du comportement normal (légal). Ainsi cet aspect de solution se base sur deux parties

- **Loi (code pénal) :** cette partie ne dépend pas de l'entreprise elle-même mais de l'état dans lequel se situe l'entreprise, et dans l'absence d'articles législatifs définissant les sanctions qui correspondent à un tel fait, ce dernier reste considéré comme légal et la sanction ne peut prendre son amplitude espérée.
- **Règlement intérieur :** le règlement intérieur peut être utilisé pour combler l'absence de la loi, ou accomplir son insuffisance. Il est utilisé aussi pour sanctionner les faits moins graves que ceux sanctionnés par la loi.

c) Aspect technique :

Méthodes et techniques :

- Gestion du contrôle d'accès.
- Chiffrement de données.
- Stéganographie.
- Audits de sécurité.

- Archivage de données et sauvegarde de traces.
- Plans de reprise d'activité PRA et plan de continuité d'activité PCA.

Dispositifs de sécurité (matériels et/ou logiciels) :

- Système de détection d'intrusion (IDS, NIDS, IPS)
- Pare-feu (firewall)
- Logiciel anti-virus (mis à jour régulièrement).
- Interface pour le réseau à protéger (réseau interne) ;
- Interface pour le réseau externe.
- Détecteur de sniffer.
- Les réseaux virtuels.
- Installation des correctifs logiciels (patchs).
- Etc.

5. Contenu d'une politique de sécurité :

Le contenu de la politique de sécurité varie d'une entreprise à l'autre, selon le domaine d'activité de chaque entreprise et selon la vue propre de leurs dirigeants. Classiquement une politique de sécurité comporte au minimum deux niveaux :

a) Une politique de sécurité cadre :

Ce document décrit généralement l'organisation de la sécurité au sein de la structure, en définissant en particulier les rôles et responsabilités de chaque partie prenante, en fonction des enjeux, exigences et contraintes de l'entreprise.

b) Des déclinaisons opérationnelles :

Prennent différentes formes, adaptées à un public et un usage particulier :

- **Chartes :** la plus connue est celle concernant les utilisateurs, décrivant les droits et les devoirs des utilisateurs du SI. Elle est générale **signée** par l'ensemble des employés ou **annexée** au **règlement intérieur**. Dans tous les cas, elle est validée par les instances représentatives du personnel. Il existe d'autre types de charte, notamment à destination des personnels de la DSI ou d'entités juridiques différentes (fournisseurs, clients..) ou dédiée à un besoin métier particulier (accès distant à une application sensible). L'objectif des chartes est double : d'abord sensibiliser et puis servir de recours juridique en cas de nécessité.
- **Bonnes pratiques :** souvent confondues avec la charte quand elles sont destinées aux utilisateurs, il s'agit généralement d'une liste de conseils en sécurité explicitant par exemple les modalités de choix d'un bon mot de passe, ou de comportement à adopter face à un émail suspect.
- **Procédures :** destinées aux administrateurs informatiques, ces recettes permettent notamment de suivre un comportement préétabli face à une situation donnée (par exemple dans le cas de gestion des incidents de sécurité). Elles peuvent également décrire les modalités de mise à jour de règles techniques.
- **Règles techniques :** alors que les procédures décrivent le "**Comment**", les règles techniques décrivent le "**Quoi**". En l'occurrence on pensera immédiatement aux règles de paramétrages des équipements de sécurité (Firewall, antivirus.)
- **Sensibilisation :** complémentaire aux autres déclinaisons qui prennent généralement une forme écrite, la sensibilisation permet d'aborder la cible d'une manière différente.

Généralement réalisée à travers des sessions de groupes sur une base orale, dans l'esprit d'une formation aux bonnes pratiques, elle peut également utiliser des formes de médias différents : intranet, affiches, vidéo conférence.

6. *Démarche de développement d'une politique de sécurité :*

Pour développer une politique de sécurité il faut :

- D'une part, définir un ensemble de propriétés de sécurité qui doivent être satisfaites par le système. Par exemple "une information classifiée ne doit pas être transmise à un utilisateur non habilité à la connaître";
- D'autre part, établir un schéma d'autorisation, qui présente les règles permettant de modifier l'état de protection du système. Par exemple "le propriétaire d'une information peut accorder un droit d'accès pour cette information à n'importe quel utilisateur".

1. Etape de définition :

a) Définition des enjeux :

C'est la définition des grands objectifs à réaliser souvent à long terme, ou de défis à surmonter. Ces enjeux prennent l'aspect généralement économique, juridique ou technique.

b) Analyse des risques :

C'est la définition des menaces susceptibles de survenir, et l'analyse de leurs impacts et leurs coûts sur l'entreprise. Cette analyse est souvent faite en utilisant une des méthodes reconnues dans ce domaine :

- MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux),
- MEHARI (*MEthode Harmonisée d'Analyse de RIsques*).
- EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité).*
- La norme ISO 17799.
- OCTAVE.

c) Définition des besoins :

C'est la définition des besoins en ressource humaine (nombre, qualité, qualification), matériel (logistique), et logiciel)

d) Définition des propriétés de sécurité du système :

C'est la définition des différents états du système dans lesquels ce dernier est considéré comme étant sécurisé (par exemple si le système peut gérer la demande de 1000 demande de connexion par seconde, ainsi il est considéré comme sécurisé). Il faut noter que ces propriétés changent souvent selon la progression du système dans le temps, ainsi un état considéré comme sécurisé maintenant peut être considéré après quelques mois comme étant insécurisé.

2. Elaboration de politique de sécurité :

L'élaboration de la politique doit être faite sous forme de règles écrites à respecter, et des mécanismes mis en place. Elle doit prendre en charge les deux aspects de sécurité :

Physique : c'est la protection physique des biens contre tout type d'accès, de vol ou de détérioration que ce soit contre des menaces internes ou externes.

Logique : c'est la protection des biens informatiques logiques (données et logiciels), contre tout type de risques informatiques (attaques malveillantes ou par erreurs). Elle consiste dans ce cas à élaborer un ensemble de règles d'utilisation, et de mécanismes logiques pour

permettre la protection et la bonne utilisation du système (authentification, chiffrement, sauvegarde, droit d'accès, ..)

D'une manière générale, les règles de la politique de sécurité sont spécifiées en terme de permissions (par exemple tout médecin a le droit d'accéder aux dossiers médicaux de ses patients) et d'interdictions (par exemple, les médecins n'ont pas le droit d'effacer des diagnostiques déjà établis), mais aussi en terme d'obligations (les médecins sont obligés de conserver les dossiers médicaux pendant la durée fixée par la loi).

3. Mise en place et Validation :

C'est la validation des différentes règles et mécanismes élaborés par la direction générale ou bien le comité de sécurité crée à cet effet.

Pour être efficace, la politique de sécurité doit être connue, pour cela elle doit donc être diffusée via différents média : papier, intranet, conférence…

Après la mise en marche de la PSSI des audits de conformité doivent être emmenés afin de vérifier la conformité entre ce qui est écrit, et la politique de sécurité appliquée sur terrain (rien de pire dans la sécurité qu'un faux sentiment de sécurité).

4. Suivi de la PSSI Révision et mise à jour :

Une fois la politique de sécurité est mise en place et testée, celle-ci doit être continuellement révisée afin de corriger les écarts et adapter les différents composants.

7. Condition de succès de la PSSI :

- Une volonté directoriale.
- Une politique de sécurité simple, précise, compréhensible et applicable.
- La publication de cette politique.
- Un niveau de confiance déterminé des personnes du système.
- Personnel sensibilisé et formé à la sécurité avec une haute valeur morale.
- Des procédures d'enregistrement, de surveillance, d'audit et d'organisation.
- Une certaine éthique et un respect des contraintes légales.

SOLUTION TECHNIQUE

Les mécanismes faisant partie de la solution technique peuvent être répartis en deux volets :

Méthodes et techniques :

- Contrôle d'accès.
- Chiffrement (symétrique ou asymétrique).
- Stéganographie.
- Audits de sécurité.
- Archivage de données et sauvegarde de traces.
- *Plans*
- *Tableaux de bord.*

Dispositifs de sécurité (matériel et/ou logiciel) :

Installation des différents dispositifs de protection :

- Système de détection d'intrusion (IDS, NIDS, IPS).
- Pare-feu (firewall).
- Logiciel anti-virus (mis à jour régulièrement).
- Utiliser un détecteur de sniffer.
- Interface pour le réseau à protéger (réseau interne) ;
- Interface pour le réseau externe (proxy).
- Utiliser des réseaux virtuels (VPN).
- Pour les réseaux sans fils il est conseillé de réduire la puissance des matériels de telle façon à ne couvrir que la surface nécessaire. Cela n'empêche pas les éventuels pirates d'écouter le réseau mais réduit le périmètre géographique dans lequel ils ont la possibilité de le faire.
- Installer régulièrement les correctifs logiciels (patchs).
- Balayage de ports par différents outils disponibles afin de réaliser un audit de sécurité (déterminer les ports ouverts, structure des paquets TCP/IP, conseiller les mises à jour nécessaires).

I. METHODES ET TECHNIQUES :

a) Contrôle d'accès :

Sujet : l'entité qui initie la demande d'accès à un objet : il peut être un utilisateur, un programme, un processus, un fichier, un ordinateur, une base de données, etc.

Objets : ou ressources sont les éléments auxquels le sujet veut accéder. Une ressource peut être une imprimante, un programme, un processus, un fichier, un ordinateur, un matériel, une base de données, un site, un lieu, une fonction, etc.

Accéder : entrer, lire, voir, écouter, exploiter, afficher, exécuter, utiliser, travailler, assister...

Le contrôle d'accès désigne les différentes solutions et techniques qui permettent de sécuriser et gérer les accès physiques et/ou logiques à une ressource (objet).

Les étapes de gestion du contrôle d'accès :

Le contrôle d'accès peut être décomposé en quatre étapes:

- **L'identification :** Le sujet désirant un accès à une ressource doit avant tout s'identifier, c'est-à-dire qu'il doit annoncer qui il est.
- **Authentification :** Après l'identification, le sujet doit prouver son identité.
- **Droits d'accès :** Le sujet se voit attribuer les permissions qui lui ont été accordées vis-à-vis de la ressource sollicitée.
- **Traçabilité :** Après l'authentification, les actions du sujet seront tracées et conservées au sein d'une base de données ou d'un fichier de log.

On distingue trois types de contrôles d'accès :

Contrôle d'accès administratif : intervient principalement sur les employés, et consiste à vérifier le passé de l'employé (si l'employé à un casier judiciaire avant de l'embaucher par exemple), ou à surveiller son comportement en permanence.

- **Outils :** questions, discussion, observation, suivi, enquête de police ou judiciaire, détective privée.

Contrôle d'accès physique : intervient notamment sur le matériel et les lieux de l'entreprise. Il consiste à empêcher l'accès aux zones sensibles au personnel ou aux étrangers non autorisés, ou encore éviter que l'employé ne modifie ses outils de travail.

- **Outils :** garde, porte, serrure, barrière, antivol, cadenas, fil de fer barbelé, interphone, vidéophone, contrôle de l'unicité de passage, lecteur de proximité, lecteur d'application, clavier à codes, lecteur biométrique, caméra, ...

Contrôle d'accès logique : intervient principalement aux ressources informatiques (fichiers, bases de données, machines, équipement informatique, et réseaux). Ce contrôle utilise des techniques purement informatiques. Il vise à limiter l'action d'un compte sur un système/réseau logique en lui attribuant les permissions appropriées. Cela peut être le droit de lire certains fichiers, d'installer de nouveaux programmes (compte utilisateur restreint) ou encore d'accéder à certains éléments du réseau (imprimante, serveur…) par le biais d'ACL (Access Control List).

- **Outils :** login, mot de passe, code, questions, captcha, empreinte digitale, iris, biométrie, puce,.etc

b) Stéganographie :

La stéganographie est l'art de la dissimulation : son objectif est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche à rendre un message inintelligible à autre que qui-de-droit.

Moyens modernes: dissimuler de l'information dans des fichiers graphiques, sons, vidéos. Cas particulier du Watermarking.

c) Cryptographie :

Le mot Cryptographie : est formé initialement des deux mots grecques Kruptos = secret, Graphein = écriture. Ainsi la cryptographie est l'art de dissimuler (transformer) une information écrite pour qu'elle soit incompréhensible (ce processus est appelé "Chiffrement"). Ceci permet ainsi de stocker et de transmettre les données dans des réseaux mêmes non sécurisés, sans qu'il soit possible de comprendre leurs sens.

La Cryptanalyse : est l'art d'analyser des données cryptées afin de découvrir leur secret (les reconstruire dans leur forme originale) sans avoir connaître les clés utilisées dans le chiffrement.

Le Processus cryptographique : est constitué de deux processus :

- **Chiffrement :** la transformation d'un texte écrit en clair en un texte crypté (chiffré) par le biais d'une clé appelée "clé de chiffrement".
- **Déchiffrement :** c'est le processus inverse, qui permet la restitution du texte crypté dans sa forme originale, par le biais d'une clé appelée "clé de déchiffrement".

Le schéma suivant illustre ces deux processus :

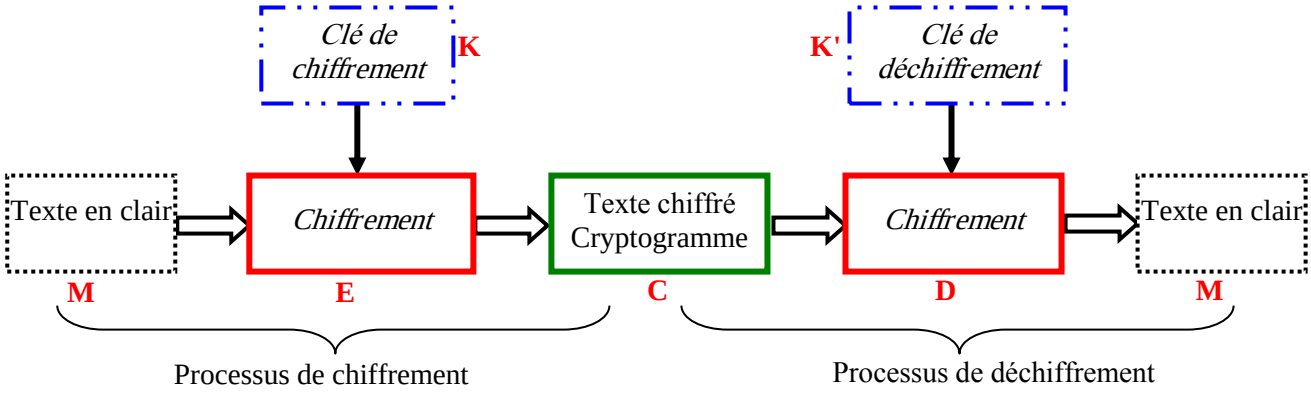

Schéma représentant le processus cryptographique

En notation mathématique : $C = E_k(M)$, $M = D_{k'}(C) = D_{k'}(E_k(M))$.

Principe de Kerckhoffs : En 1883, Kerckhoffs énonce plusieurs principes concernant la cryptographie :

- La sécurité d'un système ne doit pas être fondée sur son caractère secret.
- Seule une donnée de petite taille (clé) doit assurer la sécurité.

1) Cryptographie symétrique (à clé privée) :

- Les clés K et K' sont les mêmes, ou bien chacune peut être calculée facilement de l'autre.
- Ces clés sont partagées entre l'émetteur et le récepteur.
- Les deux chiffres E et D sont réversibles ($E_k = D_{k'}^{-1}$, et $D_{k'} = E_k^{-1}$).

On distingue deux procédés de chiffrement symétrique :

a) **La substitution :** qui consiste à substituer une lettre par une autre ou un groupe de lettres par un autre groupe de lettres. Le secret dans ce cas (la clé) peut être une table qui donne pour chaque lettre de l'alphabet la lettre par laquelle sera remplacée dans le message chiffré, ou bien une fonction ou un décalage des lettres dans l'alphabet. La clé de déchiffrement est l'inverse de la table précédente ou le décalage inverse (fonction inverse).

Plusieurs catégories de substitution existent à savoir :

+ **La substitution mono-alphabétique :** chaque lettre est substituée par la même lettre tout au long du message.
+ **La substitution poly-alphabétique :** chaque occurrence d'une lettre sera substituée périodiquement par une lettre différente.
+ **La substitution homophonique :** les lettres ou groupe de lettres qui sont phonétiquement identiques seront substitués de la même manière.
+ **La substitution par poly-gramme :** chaque groupe de lettre est substitué par un autre groupe de lettres.

La substitution est très sensible à l'attaque statistique.

b) **La transposition :** consiste à permuter l'ordre des lettres du message original suivant des règles bien définies, afin de le rendre inintelligible. On obtient ainsi une anagramme du message original. Cette méthode ne peut être efficace que pour les messages assez longs. Parmi les techniques de transposition qui existent on cite :

+ **La transposition simple (à base matricielle) :** consiste à écrire les lettres du message dans une matrice ligne par ligne puis à construire le message chiffré en prenant les lettres colonne par colonne par ordre.
+ **La transposition rectangulaire (avec substitution) :** le même procédé que celui de la transposition simple sauf que les colonnes sont prises dans un ordre donné par une clé (généralement un mot clé).

Avantages et inconvénients du chiffrement symétrique :

+ Les processus de chiffrement et de déchiffrement sont généralement rapides, et simples à implémenter.
+ Les clés sont généralement très courtes
+ Les processus sont peu gourmand en ressources machine.
– Problème de management de clés (nombre élevé de clé, leur stockage et leur échange).
– Ne peut garantir la non-répudiation.

2) Cryptographie asymétrique (à clé publique) :

- Chaque utilisateur possède deux clés K (clé publique connue par tout le monde) et K' (clé privée secrète).
- Il est quasiment difficile (voir impossible) de connaître une clé à partir de l'autre.
- En chiffrant un message par la clé publique, le résultat ne peut être déchiffré que par la clé privée correspondante.
- Si les deux clés peuvent être utilisée réciproquement pour chiffrer et déchiffrer le processus de chiffrement permet ainsi d'utiliser la signature numérique.

Exemple : soit deux utilisateurs A et B possédant respectivement les paires de clés (K_a, K'_a) et (K_b, K'_b).

Si A veut envoyer un message chiffré à B, il calcule ainsi : $C = E_{Kb}(M)$. Ainsi B déchiffre en calculant $M = E_{K'b}(C)$.

Si B veut envoyer un message chiffré à A, il calcule ainsi : $C = E_{Ka}(M)$. Ainsi A déchiffre en calculant $M = E_{K'a}(C)$.

Si l'algorithme E garantie la non-répudiation, et A calcule $C = E_{K'a}(M)$ et l'envoie à B, ce message ne puisse être déchiffré que par la clé K_a et B sera certain que ce dernier a été envoyé par A.

Signature numérique :

A calcule le condensat du message M par une fonction de hachage H, et obtient H(M) qui est souvent de taille très courte par rapport à celle du message M. Ce condensat peut être utilisé pour vérifier l'intégrité du message. En chiffrant ce condensat par la clé privé de l'émetteur K'a on obtient ainsi $C_H = E_{K'a}(H)$. Ce dernier est appelé ainsi signature numérique du message M, et est utilisé ainsi pour s'assurer de l'intégrité du message et l'authenticité de l'émetteur.

Avantage et inconvénient :

+ Pas de gestion de clés.
+ On peut garantir la non-répudiation.
– Les processus de chiffrement et déchiffrement sont souvent lents, ce qui implique une charge très importante sur les machines.
– Le choix des clés n'est pas facile.

Problème de la cryptographie :

Quel que soit le cryptosystème utilisé pour le chiffrement, ceci reste toujours cassable un jour ou l'autre. La sécurité d'un cryptosystème repose en fait sur la complexité des algorithmes définis et sur les puissances de calcul disponibles pour une attaque.

Exemples :

- L'algorithme du sac à dos. Proposé comme une solution à clé publique => Rejeté en quelques années
- Le DES 56 bits => Déclassifié en 1988

Evidence : Ainsi la solution adoptée actuellement est de faire « ***retarder le travail des cryptanalystes*** », c'est-à-dire faire en sorte que la durée nécessaire pour casser un code soit supérieure à la durée de validité des données.

d) Audit de sécurité :

L'audit de sécurité d'un système d'information (SI) est une vue à un instant T de tout ou partie du SI, permettant de comparer l'état du SI à un référentiel.

L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'auditeur dresse également une série de recommandations pour supprimer les vulnérabilités découvertes. L'audit est généralement réalisé conjointement à une analyse de risques, et par rapport au référentiel. Le référentiel est généralement constitué de :

- La politique de sécurité du système d'information (PSSI)
- La base documentaire du SI
- Réglementations propre à l'entreprise
- Textes de loi
- Documents de référence dans le domaine de la sécurité informatique

Pourquoi un audit de sécurité ?

L'audit peut être effectué dans différents buts :

- Réagir à une attaque ;
- Se faire une bonne idée du niveau de sécurité du si ;
- Tester la mise en place effective de la PSSI ;
- Tester un nouvel équipement ;
- Evaluer l'évolution de la sécurité (implique un audit périodique).

Dans tous les cas, il a pour but de vérifier la sécurité. Dans le cycle de sécurisation, la vérification intervient après la réalisation d'une action. Par exemple, lors de la mise en place d'un nouveau composant dans le SI, il est bon de tester sa sécurité après avoir intégré le composant dans un environnement de test, et avant sa mise en œuvre effective. La roue de Deming illustre ce principe.

Le résultat est le rapport d'audit. Celui-ci contient la liste exhaustive des vulnérabilités recensées par l'auditeur sur le système analysé. Il contient également une liste de recommandations permettant de supprimer les vulnérabilités trouvées.

L'audit ne doit pas être confondu avec l'analyse de risques. Il ne permet que de trouver les vulnérabilités, mais pas de déterminer si celles-ci sont tolérables. Au contraire, l'analyse de risque permet de dire quels risques sont pris en compte, ou acceptés pour le SI. L'auditeur (le prestataire) dresse donc des recommandations, que l'audité (le client) suivra, ou ne suivra pas. Le client déterminera s'il suivra les recommandations ou non, en se référant à la politique de sécurité.

Pratique de l'audit :

Pour arriver à dresser une liste la plus exhaustive possible des vulnérabilités d'un système, différentes pratiques existent et sont traditionnellement mises en œuvre.

a) Interviews :

Les interviews sont généralement essentiels à tout audit. Dans le cas où l'organisation du SI est analysée, ils sont même indispensables. Toutes les personnes ayant un rôle à jouer dans la sécurité du SI sont à interroger :

- Le directeur des systèmes d'information (DSI)
- Le ou les responsable(s) de la sécurité des systèmes d'information (RSSI)
- Les administrateurs

- Les utilisateurs du système d'information, qu'ils aient un rôle dans la production de l'entreprise, dans la gestion, ou la simple utilisation des moyens informatiques
- Tout autre rôle ayant un lien avec la sécurité

Il est important de formuler les questions avec tact. En effet, interroger des personnes à propos de leur travail peut faire qu'elles se sentent jugées et les résultats peuvent être faussés. La diplomatie est donc une compétence essentielle pour la pratique des audits.

b) Les tests d'intrusion :

Les tests d'intrusion sont une pratique d'audit technique. On peut diviser les tests d'intrusion en trois catégories principales : les tests boîte blanche, les tests boîte grise et les tests dits boîte noire.

Un **Test Boîte Noire** signifie que la personne effectuant le test se situe dans des conditions réelles d'une intrusion : le test est effectué de l'extérieur, et l'auditeur dispose d'un minimum d'informations sur le système d'information. Ce genre de tests débute donc par l'identification de la cible :

- Collecte d'informations publiques : pages web, informations sur les employés, entreprise ayant un lien de confiance avec la cible ;
- Identification des points de présence sur internet ;
- Écoute du réseau.

Lors de la réalisation de **Tests Boîte Grise**, l'auditeur dispose de quelques informations concernant le système audité. En général, on lui fournit un compte utilisateur. Ceci lui permet de se placer dans la peau d'un « utilisateur normal ».

Les **Tests Boîte Blanche** débutent avec toutes ces informations (et beaucoup plus) à disposition. Ensuite commence la recherche des vulnérabilités, à l'aide de différents tests techniques, comme la recherche des ports ouverts, la version des applications, etc.

La dernière phase est **l'exploitation des vulnérabilités**. Des effets indésirables pouvant survenir (déni de service par exemple), le côté pratique de cette phase n'est pas systématique. Elle consiste à déterminer les moyens à mettre en œuvre pour compromettre le système à l'aide des vulnérabilités découvertes. Selon les moyens à mettre en œuvre, le client pourra décider que le risque associé à la vulnérabilité décelée est négligeable (probabilité d'exploitation faible) ou au contraire à prendre en compte. Pour prouver la faisabilité de l'exploitation, les auditeurs créent des programmes qui exploitent la vulnérabilité, appelés exploits.

Des tests d'intrusion « *Red Team* » peuvent également être mis en place. Il s'agit de faire une simulation grandeur nature d'une attaque qui pourrait être menée par un groupe ou des individus malveillants. Le périmètre d'attaque n'est pas défini, et plusieurs techniques aussi bien informatiques que d'ingénierie sociale, voire d'intrusion physique peuvent être utilisées dans ce type de test.

c) Les relevés de configuration :

Il s'agit ici d'analyser, profondément, les composants du système d'information. Les configurations sont inspectées dans les moindres détails. À la suite de cette observation, la liste des vulnérabilités est dégagée en comparant le relevé à des configurations réputées sécurisées, et à des ensembles de failles connues.

Tout peut être inspecté, allant de l'architecture réseau du SI aux systèmes et aux applications. Par exemple sur un serveur, les points suivants sont analysés :

- Le chargeur de démarrage ;

- Les mécanismes d'authentification (robustesse des mots de passe, utilisation d'authentification forte, etc.) ;
- Le système de fichiers (permissions, utilisation de chiffrement etc.) ;
- Les services ;
- La journalisation ;
- La configuration réseau ;
- Les comptes présents ;
- Etc.

d) L'audit de code :

Il existe des bases de vulnérabilités très fiables pour les applications répandues. Néanmoins, pour des applications moins utilisées, ou codées par l'entreprise elle-même, il peut être nécessaire d'analyser leur sécurité. Si les sources de l'application sont disponibles, il faut lire et comprendre le code source, pour déceler les problèmes qui peuvent exister. Notamment, les dépassements de tampon (*buffer overflow*), les bugs de format, ou pour une application web, les vulnérabilités menant à des injections SQL...

L'audit de code est une pratique très fastidieuse et longue. De plus, elle ne permet généralement pas, en raison de la complexité, de dresser une liste exhaustive des vulnérabilités du code. Des méthodes automatiques existent, et permettent de dégrossir le travail, avec des outils comme RATS5. Mais se reposer uniquement sur ce genre de méthodes peut faire passer à côté de problèmes flagrants pour un humain.

e) Fuzzing :

Pour les applications boite noire, où le code n'est pas disponible, il existe un pendant à l'analyse de code, qui est le fuzzing. Cette technique consiste à analyser le comportement d'une application en injectant en entrée des données plus ou moins aléatoires, avec des valeurs limites. Contrairement à l'audit de code qui est une analyse structurelle, le fuzzing est une analyse comportementale d'une application.

e) Archivage et sauvegarde :

Sauvegarde (Backup) :

Une sauvegarde correspond à une copie de données qui peut être utilisée pour **restaurer** les données originales dans le cas où ces dernières seraient endommagées ou perdues (suppressions accidentelles, corruptions de fichiers, problèmes techniques, etc.). Cela concerne généralement les données qui sont encore en usage au sein de l'entreprise.

Archivage :

Un archivage correspond à un ou plusieurs enregistrements de données, spécialement sélectionnées pour une conservation plus ou moins longue dans l'éventualité d'un accès ultérieur pour des raisons légales le plus souvent. Cela concerne généralement des données qui ne sont plus utilisées au sein de l'entreprise.

L'une des différences fondamentales à relever est que la sauvegarde est toujours une copie, alors que l'archive doit être le document original, supprimé de son emplacement initial et transféré ailleurs.

Références bibliographiques :

- J-F. Carpentier "La sécurité informatique dans la petite entreprise. Etat de l'art et Bonnes Pratiques" ENI 3ème édition 2016.
- L. Bloch & C. Wolfhugel "Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs" Eyrolles 2ème édition 2013.
- M. Lafitte "Sécurité des systèmes d'information et maîtrise des risques- Les essentiels de la banque" Edition Revue Banque 2003.
- C. Llorens, L. Levier & D. Valois "Tableaux de bord de la sécurité réseau" Eyrolles 2ème édition 2003.
- COMPUTER SECURITY RESOURCE CENTER https://csrc.nist.gov/
- S. Ghernaouti « Cybersécurité Analyser les risques Mettre en œuvre les solutions » DUNOD 6ème édition 2019.
- Sécurité des systèmes d'information https://fr.wikipedia.org/