Sécurité des systèmes d'information

(Extrait d’une formation officielle en cybersécurité)

La **sécurité des systèmes d’information** (**SSI**) ou plus simplement **sécurité informatique**, est l’ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information.

Aujourd’hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l’ensemble des acteurs qui l’entourent. Elle n'est plus confinée uniquement au rôle de l’informaticien. Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients. La finalité sur le moyen terme est la cohérence de l’ensemble du système d’information. Sur le court terme, l’objectif est que chacun ait accès aux informations dont il a besoin. La norme traitant des systèmes de management de la sécurité de l'information (SMSI) est l’ISO/CEI 27001 qui insiste sur Confidentiality – Integrity – Availability, c'est-à-dire en français disponibilité, intégrité et confidentialité.

Sommaire

Historique

Les responsables de systèmes d'information se préoccupent depuis longtemps de sécuriser les données. Le cas le plus répandu, et sans aucun doute précurseur en matière de sécurité de l'information, reste la sécurisation de l'information stratégique et militaire. De même, le principe de sécurité multi-niveau trouve ses origines dans les recherches de résolution des problèmes de sécurité de l'information militaire. La défense en profondeur, tout droit sorti d'une pratique militaire ancienne, et toujours d'actualité aujourd'hui. Cette pratique consiste à sécuriser chaque sous-ensemble d'un système.

Les conséquences d'une mauvaise sécurisation peuvent concerner les organisations, mais aussi la vie privée d'une ou plusieurs personnes, notamment par la diffusion d'informations confidentielles comme leurs coordonnées bancaires, leurs situations patrimoniales, leurs codes confidentiels, etc. De manière générale, la préservation des données relatives aux personnes fait l'objet d'obligations légales régies par la Loi Informatique et Libertés.

Aujourd'hui, il est généralement admis que la sécurité ne peut être garantie à 100 % et requiert donc le plus souvent la mobilisation d'une panoplie de mesures pour réduire les chances de pénétration des systèmes d'information.

Objectifs

« Le système d'information représente un patrimoine essentiel d'une entreprise, qu'il convient de protéger. La sécurité informatique consiste à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu »[1].

La sécurité des systèmes d'information vise les objectifs suivants (C.A.I.D.) :

1. **Confidentialité** : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (notions de droits ou permissions). Tout accès indésirable doit être empêché.
2. **Authenticité** : les utilisateurs doivent prouver leur identité par l'usage de code d'accès. *Il ne faut pas mélanger identification et authentification : dans le premier cas, l'utilisateur n'est reconnu que par son identifiant public, tandis que dans le deuxième cas, il doit fournir un mot de passe ou un élément que lui-seul connaît (secret)*. Mettre en correspondance un identifiant public avec un secret est le mécanisme permettant de garantir l'**authenticité** de l'identifiant. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.
3. **Intégrité** : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets. Cet objectif utilise généralement des méthodes de calcul de checksum ou de hachage.
4. **Disponibilité** : l'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

1. **La traçabilité** (ou « **preuve** ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
2. **La non-répudiation** et **l'imputation** : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Une fois les objectifs de la sécurisation déterminés, les risques pesant sur chacun de ces éléments peuvent être estimés en fonction des **menaces**. Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les

précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Il faut pour cela estimer :

- **La gravité** des conséquences au cas où les risques se réaliseraient ;
- **La vraisemblance** des risques (ou leur *potentialité*, ou encore leur *probabilité d'occurrence*).

Démarche générale

Pour sécuriser les systèmes d'information, la démarche adopte une spirale évolutive régulière : la fin d'un cycle entraîne le début d'un nouveau, comme dans la roue de Deming. En sécurité cela consiste à :

évaluer les risques et leur criticité
: quels risques et quelles menaces, sur quelles données et quelles activités, avec quelles conséquences ?
On parle de « cartographie des risques ». De la qualité de cette cartographie dépend la qualité de la sécurité qui va être mise en œuvre.

rechercher et sélectionner les parades
: que va-t-on sécuriser, quand et comment ?
Étape difficile des choix de sécurité : dans un contexte de ressources limitées (en temps, en compétences et en argent), seules certaines solutions pourront être mises en œuvre.

mettre en œuvre les protections et vérifier leur efficacité
: C'est l'aboutissement de la phase d'analyse et là que commence la protection du système d'information. Une faiblesse fréquente de cette phase est d'omettre de vérifier que les protections sont bien efficaces (tests de fonctionnement en mode dégradé, tests de reprise de données, tests d'attaque malveillante, etc.).

Approche par phases.

Phase *plan* : Planification de la démarche de sécurisation des systèmes d'information

Étape 1 : Périmètre et Politique

Il est important de prendre en compte les actifs ayant de la valeur en définissant un périmètre du système de management du système d'information. Il peut être orienté sur l'ensemble de l'entreprise, sur un site précis, sur un service en fonction de la stratégie de l'entreprise. Le capital intellectuel des entreprises intègre des informations sensibles, ce patrimoine informationnel doit être protégé. L'entreprise doit donc mettre en place une politique de sécurité des systèmes d'information, de sécurité des données, et des mécanismes d'identification. De plus, il faut définir une politique du SMSI, qui est l'engagement de l'entreprise sur un certain nombre de points en matière de sécurité. Ces deux points forment la pierre angulaire du SMSI, dans le but d'établir la norme ISO/CEI 27001 et ainsi d'apporter la confiance aux parties prenantes.

Étape 2 : Évaluation des risques

Tenter de sécuriser un système d'information revient à essayer de se protéger contre les menaces intentionnelles[2] et d'une manière plus générale contre tous les risques pouvant avoir une influence sur la sécurité de celui-ci ou des informations qu'il traite.

Méthode d'analyse des risques

Différentes méthodes d'analyse des risques sur le système d'information existent. Voici les méthodes d'appréciation des risques les plus courantes :

En France, la première méthode développée a été Marion. Aujourd'hui, elle a été remplacée, même si certaines entreprises ont conservé ce modèle initial, par la méthode Méhari (Méthode harmonisée d'analyse des risques) développée par le CLUSIF, et par la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) développée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

En Angleterre, Cramm est une méthode d'analyse des risques développée par l'organisation du gouvernement britannique ACTC (Agence centrale de communication et des télécommunications). C'est la méthode d'analyse des risques préférée par le gouvernement britannique, mais elle est également utilisée par beaucoup d'autre pays.

Les États-Unis utilisent OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), développée par l'Université de Carnegie Mellon.

À l'international, on utilise ISO/CEI 27005, qui est une norme internationale répondant point par point aux exigences de la certification ISO/CEI 27001. C'est la norme la plus récente, de plus elle est facilement applicable car pragmatique.

Même si le but de ces méthodes est identique, les termes et les expressions utilisés peuvent varier. Celles utilisées ci-dessus sont globalement inspirés de la méthode Feros.

Paradoxalement, dans les entreprises, la définition d'indicateurs « sécurité du SI » mesurables, pertinents et permettant de définir ensuite des objectifs dans le temps raisonnables à atteindre, s'avère délicate. Pour mesurer la performance on peut désigner comme indicateurs les états d'installation d'outils ou de procédures, mais les indicateurs de résultats sont plus complexes à définir et à apprécier, par exemple ceux concernant les « alertes virales »[évasif].

Identifier les actifs . Mais aussi tous les risques et conséquences.

Exemple : Plan de continuité d'activité (informatique) et Plan de reprise d'activité.

Cela consiste à faire une liste de tous les éléments importants en matière d'information au sein du périmètre SMSI. Il existe différent types d'actifs :

1. matériel
2. physique
3. logiciel
4. humain
5. documents
6. immatériels

Pour l'identification des actifs, trois problèmes se posent :

1. Le niveau de granularité : plus la notion de granularité est élevée plus la notion d'actif est large.
2. Lister le plus important : le but n'est pas de faire une liste exhaustive d'actifs mais de recenser les plus importants d'entre eux.
3. Ne pas confondre les actifs avec les actifs d'information : un actif est un élément qui possède de la valeur pour l'entreprise, alors qu'un actif d'information est ce qui possède de l'importance en matière d'information.

Il est aujourd'hui indispensable de disposer de plans de sécurisation de l'activité pour en assurer la continuité et la reprise si un sinistre survient (Plan de reprise d'activité). Ces plans tentent de minimiser les pertes de données et d'accroître la réactivité en cas de sinistre majeur. Un plan de continuité d'activité efficace est quasi-transparent pour les utilisateurs, et garantit l'intégrité des données sans aucune perte d'information.

Identifier les personnes responsables

C'est la personne responsable d'un bien qui en répond. Il s'agit en général de celle qui connaît le mieux la valeur et les conséquences de disponibilité, d'intégrité et de confidentialité de l'actif. Dans une entreprise c'est généralement le responsable de la sécurité des systèmes d'information qui connaît le mieux les actifs de l'information.

Identifier les vulnérabilités

Chaque actif recensé présente des vulnérabilités, c'est une propriété intrinsèque du bien qui l'expose à des menaces.

Identifier et modéliser les menaces

Article détaillé : Insécurité du système d'information.

Les vulnérabilités précédemment identifiées exposent les biens à des menaces. La norme ISO/CEI 27001 impose l'identification des menaces pour tous les biens recensés.

Les principales menaces auxquelles un système d'information peut être confronté sont :

1. un utilisateur du système : l'énorme majorité des problèmes liés à la sécurité d'un système d'information a pour origine un utilisateur, généralement insouciant. Il n'a pas le désir de porter atteinte à l'intégrité du système sur lequel il travaille, mais son comportement favorise le danger ;
2. une personne malveillante : une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes

auxquels elle n'est pas censée avoir accès. Le cas fréquent est de passer par des logiciels utilisés au sein du système, mais mal sécurisés. Le Shoulder surfing est également une faille.
3. un programme malveillant : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données ; des données confidentielles peuvent être collectées à l'insu de l'utilisateur et être réutilisées à des fins malveillantes ;
4. un sinistre (vol, incendie, dégât des eaux) : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.

Identifier les conséquences

La norme ISO 27001 oblige l'évaluation de conséquences ; tel que : la perte de confidentialité, de disponibilité ou d'intégrité. Cela revient à donner une note en trois dimensions (confidentialité ; disponibilité et intégrité), selon des critères définis, pour chaque actif.

Identifier les dommages

Quatre types de dommages peuvent affecter le système d'information d'une organisation:

1. Les dommages **financiers :**
    1. Sous forme de dommages directs, c'est l'action de reconstituer des bases de données qui ont disparu, de reconfigurer un parc de postes informatiques ou de réécrire une application,
    2. Sous la forme de dommages indirects, c'est le dédommagement des victimes d'un piratage, le vol d'un secret de fabrication ou la perte de marchés commerciaux ;
2. La perte de **l'image de marque :**
    1. Perte directe par la publicité négative faite autour d'une sécurité insuffisante tel que l'hameçonnage,
    2. Perte indirecte par la baisse de confiance du public dans une société, par exemple, les techniques répandues de *défacement* ;
3. Les dommages **réglementaires** :
    1. L'indisponibilité d'un systèmes d'informations peut mettre en défaut l'entité devant ses obligations légales et juridiques ;
4. Les dommages **écologiques** et/ou Sanitaires :
    1. La défaillance d'un système peut provoquer des catastrophes écologiques (ex. : AZF, marées noires, etc.),
    2. La défaillance d'un système peut provoquer des dégâts sanitaires (ex. : les centrales nucléaires, etc.).

Évaluer la vraisemblance

Il s'agit de remettre le bien d'information dans son contexte environnemental et donc de prendre en compte les mesures qui sont déjà mises en place (ex. : si un fichier client est déjà chiffré, alors la vraisemblance de voir sa confidentialité compromise est limitée). Il est possible d'évaluer la notion de vraisemblance par une note sur une échelle de 1 à 5.

Estimer les niveaux de risque

L'attribution d'une note finale reflétera le niveau de risque réel tout en tenant compte des éléments ci-dessus. La norme ISO 27001 n'impose aucune formule c'est donc à l'implémenteur de la choisir. Il peut s'agir d'une note allant de 0 à 100 ou d'un code couleur.

Étape 3 : Traiter le risque et identifier le risque résiduel

L'entreprise peut traiter les risques identifiés de 4 façons :

Accepter le risque
: solution ponctuelle lorsque la survenance du risque entraîne des répercussions acceptables pour l'entreprise.

Éviter le risque
: solution lorsque les conséquences d'une attaque sont jugées trop périlleuses pour l'entreprise.

Transférer le risque
: solution quand l'entreprise ne peut pas faire face au risque par ses propres moyens (souscription d'une assurance ou contrat de sous-traitance).

Réduire le risque
: solution pour rendre le risque acceptable.

Enfin, il ne faut pas oublier de prendre en compte les *« Risques résiduels »* qui persistent après la mise en place de l'ensemble des mesures de sécurité. Il faut prendre des mesures complémentaires de protection pour rendre ces risques acceptables.

Étape 4 : Sélectionner les mesures à mettre en place .

L'implémentation de la norme ISO2/CEI 27001 se déroule généralement en cinq phases complémentaires:

- Phase 1 Réunion de lancement : cette réunion sert à cadrer la prestation et à présenter la démarche des consultants.
- Phase 2 Entretiens : rencontres avec les différents responsables des services clé de l'entreprise dans le but de faire le point sur leur niveau de conformité avec la norme ISO/CEI 27001.
- Phase 3 Prise de connaissance de la documentation : documents de la politique générale (politique de sécurité, charte utilisateurs, etc.), documents de politique spécifiques (mots de passe, accès distant et procédure).
- Phase 4 Rédaction du rapport : rapport tenant compte de tous les éléments obtenus lors des phases précédentes.
- Phase 5 Présentation des résultats : réunion au cours de laquelle les points suivants sont traités ; rappel synthétique des points clé, présentation du plan de mise en conformité ISO/CEI 27001 et discussion.

Phase 1** Mise en place des objectifs

Plan de traitement des risques

L'étape de planification identifie les mesures à prendre dans l'organisation, mais ne permet pas de les mettre en place concrètement. Il faut les organiser, sélectionner les moyens nécessaires et définir les responsabilités en établissant un plan de traitement des risques. Cette étape relève de la gestion de projet.

Déployer les mesures de sécurité

De nombreux moyens techniques peuvent être mis en œuvre pour assurer une sécurité du système d'information. Il convient de choisir les moyens nécessaires, suffisants, et justes. Voici une liste non exhaustive de moyens techniques pouvant répondre à certains besoins en matière de sécurité du système d'information :

1. Contrôle des accès au système d'information ;
2. Surveillance du réseau : sniffer, système de détection d'intrusion ;
3. Sécurité applicative : séparation des privilèges, audit de code, rétro-ingénierie ;
4. Emploi de technologies *ad hoc* : pare-feu, UTM, anti-logiciels malveillants (antivirus, anti-spam, anti-logiciel espion) ;
5. Cryptographie : authentification forte, infrastructure à clés publiques, chiffrement.
6. Plan de continuité d'activité : sauvegarde et restauration de données, Plan de Reprise d'activité.

Générer des indicateurs

Une des nouveautés de la norme ISO/CEI 27001 est d'exiger une vérification régulière de la sécurité. Le responsable doit choisir des indicateurs qui permettent de mesurer sa fiabilité. Ils peuvent être de deux sortes :

1. indicateurs de performance : ils mesurent l'efficacité des mesures ;
2. indicateurs de conformité : ils mesurent l'adéquation des mesures aux normes.

Former et sensibiliser le personnel

L'information du personnel est primordiale dans la réussite d'un projet de sécurisation du SI, pour qu'il en comprenne l'utilité et sache l'appliquer. Une bonne pratique est donc de sensibiliser l'ensemble du personnel aux enjeux de la sécurité informatique pour leur organisation, de manière généraliste. Cette explication doit rappeler les engagements de l'organisation, et donner des exemples très pratiques et des procédures internes pour éviter les incidents les plus habituels. Les employés directement concernés par la sécurité informatique doivent être formés pour qu'ils sachent utiliser correctement les outils.

Une formation incluant l'inoculation psychologique contre les techniques d'ingénierie sociale, permet aux gens de résister aux tentations de s'écarter des procédures et des principes de sécurité.

Gérer le SMSI au quotidien

La norme ISO/CEI 27001 n'impose pas seulement de mettre en place un système de sécurité, mais aussi de prouver son efficacité. Les entreprises doivent donc gérer correctement leurs ressources et développer la traçabilité.

Détection et réaction rapide des incidents

Cette phase repose sur la théorie de *time-based security*. Le principe est de prendre en compte le délai nécessaire pour qu'une attaque contre la sécurité réussisse. Pendant ce laps de temps, l'entreprise doit être capable de détecter la menace et de la contrer, avec une marge de sécurité supplémentaire.

Phase 2 : Mise en place de moyens de contrôle

Il doit y avoir des moyens de contrôle pour surveiller l'efficacité du SMSI ainsi que sa conformité.

Il existe des outils pour vérifier cela comme :

Les audits internes : Audit planifié longtemps en avance et faisant appel à des auditeurs.

Le contrôle interne : Contrôle en permanence au sein de l'organisation, pour vérifier que chacun applique les procédures au quotidien.

Les réexamens : Prendre du recul pour mettre en adéquation le SMSI et son environnement.

On peut s'aider de :

- COBIT : permet l'analyse des risques et le contrôle des investissements
- ITIL : l'objectif est de favoriser l'efficacité des affaires dans l'utilisation du SI dans le but de satisfaire les demandes d'organisation pour réduire les coûts tout en maintenant ou améliorant les services informatiques
- ISO/CEI 27007 : lignes directrices pour aider les auditeurs internes ou externes à contrôler si le SMSI est correctement développé.

Phase 3 : Mise en place d'actions

Après la mise en lumière de dysfonctionnements grâce à la phase Check, il est important de les analyser et de mettre en place des :

- Actions correctives : Il faut agir sur le dysfonctionnement et en supprimer les effets.
- Actions préventives : On agit avant que le dysfonctionnement ne se produise.
- Actions d'amélioration : On améliore les performances d'un processus.