Introduction à la sécurité des systèmes d'information

François Pouit

September 7, 2021

Généralités

Définition, Objectifs

Notion de riques.

Intrusions et attaques

Mécanismes de défense

Plan

Généralités

Définition, Objectifs

Notion de riques.

Intrusions et attaques

Mécanismes de défense

Généralités

- Définition, Objectifs
- Notion de riques.
- Intrusions et attaques
- Mécanismes de défense

Plan

Généralités

Définition, Objectifs

Notion de riques.

Intrusions et attaques

Mécanismes de défense

Généralités

- Définition, Objectifs
- Notion de riques.
- Intrusions et attaques
- Mécanismes de défense

Définition

source : wikipédia

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.

Objectifs

L'objectif est de garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre qui a été prévu.
La SSI vise les objectifs suivants :

- **La 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.
- **L'intégrité** les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. Cet objectif utilise généralement des méthodes de calculs de checksum ou de hachage.
- **La disponibilité** l'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues.

Objectifs

- **L'authentification** 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, tandis que dans le deuxième cas, il doit fournir un mot de passe ou un élément que lui-seul connaît. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.
- **La tracabilité** Chaque action sur le SI doit pouvoir être tracée afon de pouvoir détecter à postériori une faille ou une attaque : elle permet disposer de preuves lors d'une intrusion ou pour prouver la modification de données.

Risques

Les risques sont nombreux et sont en constante évolution.
Il y a trois types de risques :

- Le risque humain
- Le risque technique
- le risque juridique

Le risque humain

C'est et de loin le plus important !

Il est trop souvent minimisé ou même ignoré.
Il concerne les utilisateurs, et les informaticiens eux-mêmes.
Ce risque est causé par différents facteurs.

On peut citer par exemple : la maladresse, l'inconscience et l'ignorance, la malveillance et enfin l'espionnage.

Le risque humain

Le risque humain se matérialise de nombreuses façons.

À titre d'exemples :

- l'usurpation d'identité (Spoofing) par détournement de mot de passe par exemple
- vols de matériels
- abus de droits par des personnes ayant des privilèges systèmes
- la sustitution c'est à dire l'interception des messages de connexion-déconnexion permettant de continuer une session régulièrement ouverte sans que le système ne remarque le changement d'utilisateur.

etc...

Le risque technique

C'est celui qui est lié aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels.
En effet la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts et finissent un jour ou l'autre par tomber en panne.
Certaines de ces pannes sont assez difficiles à déceler car intermittentes ou rares.
Les incidents liés aus logiciels sont de loin les plus fréquents : les développeurs font inévitablement des erreurs que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité, d'autant plus, que de plus en plus, la réalisation de logiciels nécessite de très nombreux intervenants.

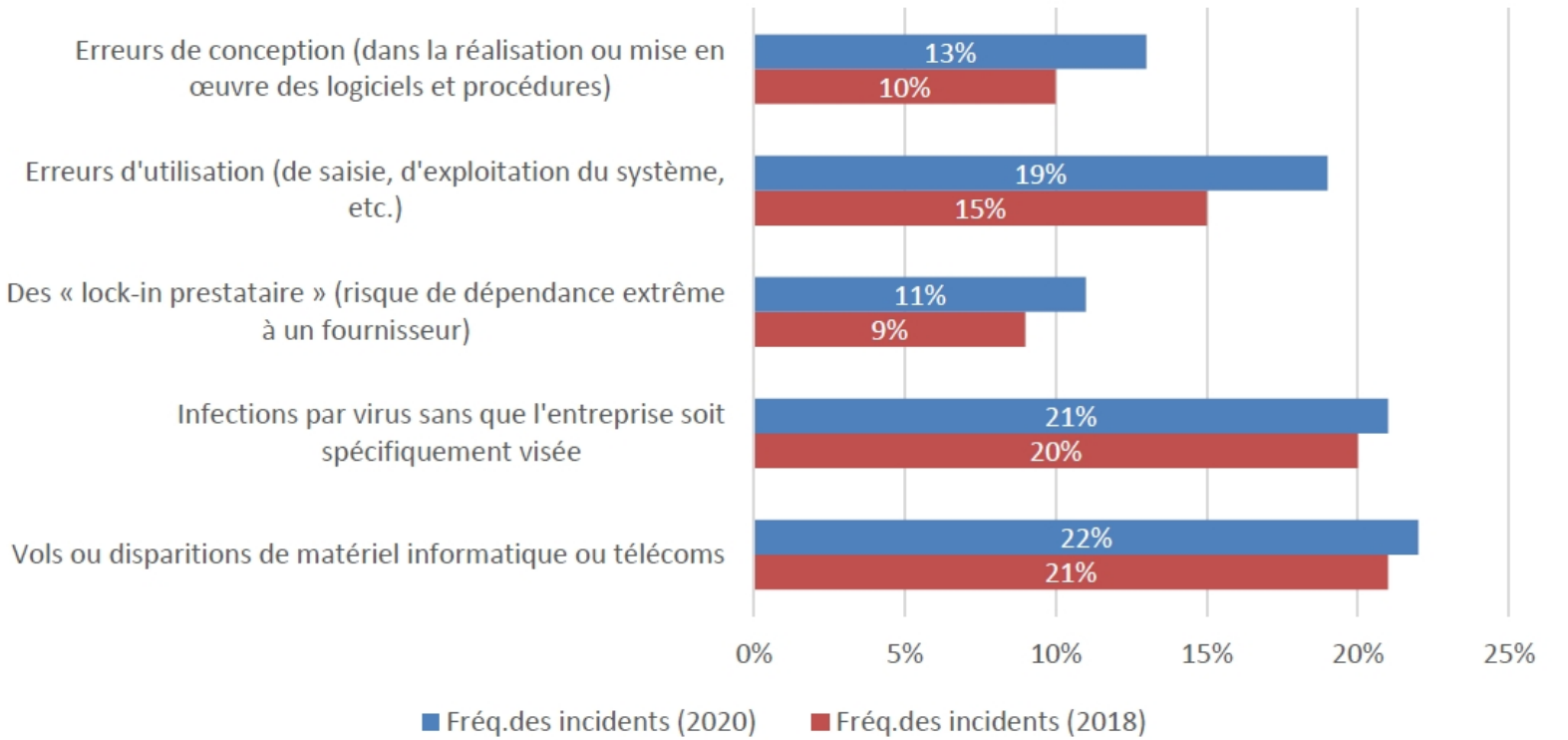
Le risque juridique

Ce sont les applications web et la multiplication des messages électroniques qui augmentent les risques juridiques liés à l'usage des technologies de l'information. On peut citer notamment :

- Le non-respect de la législation relative à la signature numérique;
- Les risques concernant la protection du patrimoine informationnel (droits d'auteurs par exemple)
- Le non-respect de la législation relative à la vie privée (notamment sur les réseaux sociaux)

Origine des incidents SI

source : étude du Club de la Sécurité de l'Information Français (CLUSIF)
rapport 2020, Menaces Informatiques et pratiques de la sécurité en France



Programmes malveillants

Un logiciel malveillant (malware) est un logiciel développé dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :

- Le virus : programme se dupliquant sur d'autres ordinateurs ;
- Le ver (worm) : exploite les ressources d'un ordinateur afin d'assurer sa reproduction ;
- Le cheval de Troie (trojan) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;
- La porte dérobée (backdoor en anglais) : ouvreur d'un accès frauduleux sur un système informatique, à distance.
- Le logiciel espion (spyware) : collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers.

Programmes malveillants

- L'enregistreur de frappe (keylogger) : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier .
- L'exploit : programme permettant d'exploiter une faille de sécurité d'un logiciel.
- Le rootkit : ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.
- La bombe : programme dormant dont l'exécution est conditionné par l'occurrence d'un événement ou d'une date.
- déni de service en surchargeant un ou des serveurs

Attaques par messageries

On liste ici les attaques spécifiques aux messageries :

- Le pourriel (spam) : un courrier électronique non sollicité notamment la publicité. Ils encombrent le réseau, et font perdre du temps à leurs destinataires.
- L'hameçonnage (phishing) : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme officiel (comme une banque, opérateur, ou autre) et demandant au destinataire de fournir des informations confidentielles ou de l'argent.
- Le canular informatique (hoax) : un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes. Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

Attaques sur le réseau

- L'écoute réseau (Sniffing) : utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications, et pour identifier les machines qui communiquent sur le réseau.
- L'usurpation d'IP (Spoofing) : prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles.
- La perturbation : fausser le comportement du SI ou l'empêcher de fonctionner comme prévu (saturation, dégradation du temps de réponse, génération d'erreurs ...).

Attaques sur le réseau

- Le réseau de robots logiciels (Botnet) : réseau de robots logiciels installés sur de nombreuses machines. Les robots se connectent sur des serveurs IRC (Internet Relay chat) au travers desquels ils peuvent recevoir des instructions de mise en oeuvre de fonctions non désirées. (envoi de spams, vol d'information, participation à des attaques de saturation ...).
- Le déni de service (denial of service) : générer des arrêts de service, et ainsi empêcher le bon fonctionnement du système.
  etc...

Attaques passives

L'objectif de ces attaques est d'obtenir des informations pendant une transmission d'informations.
Elles n'altère pas les messages et la communication.
Deux types d'attaques :

1. L'écoute clandestine (eavesdropping) : Sniffing, Spoofing etc ...
2. Capture et analyse de traffic afin de connaître le réseau cible.

Très difficile à détecter ...

Attaques actives

Elles ont pour objectif d'altérer la communication :

- altération des messages
- déni de services (DDoS pour Distributed Denial of Service): envoi d'un très grand nombre d'informations (requêtes ou données) pour rendre le service inopérant. Assez simple à mettre en oeuvre.

Démarche générale

Ce sont les responsables des systèmes d'information qui se préoccupent depuis longtemps de sécuriser les données. Les objectifs mentionnés plus sont d'assurer notamment la confidentialité, l'authentification l'intégrité et la disponibilité des données.
Pour cela ils :

- Évaluent les risques et leur criticité.
- Participent à l'élaboration d'une politique de sécurité.
- recherchent et sélectionnent les parades.(Les utilisateurs sont mis à contribution).
- mettent en oeuvre les protections et vérifient leur efficacité.

Cette démarche est régulièrement répétée (notamment lors des audits), en effet les solutions adoptées ont souvent une efficacité temporaire.

prévention des attaques

Les attaques passives sont difficiles à détecter mais simples à prévenir :
Cryptage de l'information et/ou du médium de communication
détection des écoutes.

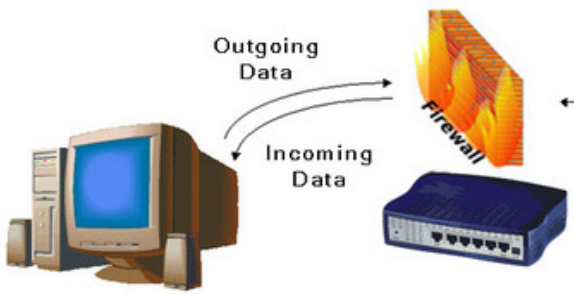
Les attaques actives sont simples à détecter mais difficiles à arrêter.
Il faut mettre l'accent sur la détection et sur la récupération des données.
On fait de la prévention :
Ex: Firewall, Systèmes de détection d'intrusion, signatures, antivirus, sauvegardes ...

mécanismes de sécurité

Il s'agit de détecter, prévenir les attaques et de récupérer les données/fonctionalités éventuellement perdues.

Exemples de mécanismes :

- L'authentification
- Le chiffrement des données
- La signature des données
- Le contrôle d'accès
- Le contrôle du routage



- Le bourrage de trafic (des données sont ajoutées pour assurer la confidentialité en particulier au niveau du volume de trafic)
- La notarisation (utilisation de tiers de confiance pour assurer certains services de sécurité : certification, distribution de clés par ex)

principe du moindre privilège

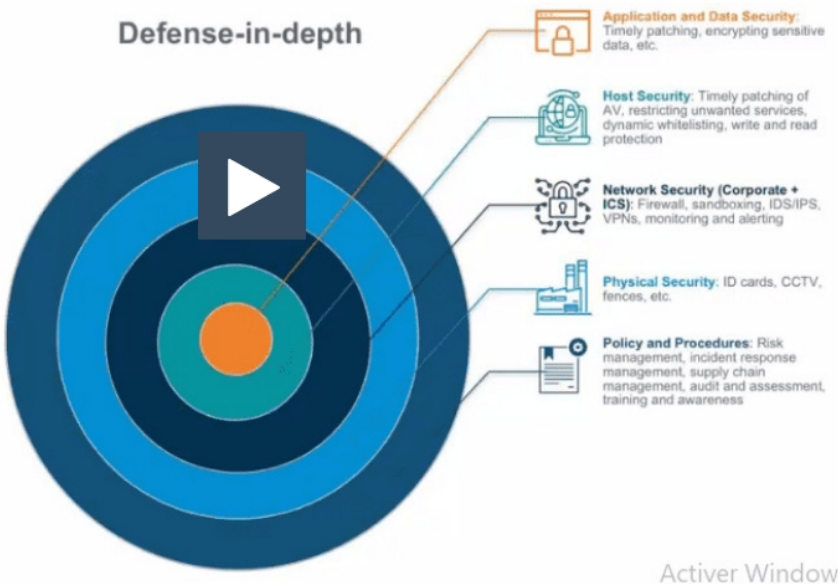
On autorise que ce qui est indispensable à l'utilisateur.

Tout ce qui n'est pas autorisé est interdit.

Par exemple :
Les droits donnés par l'administrateur aux utilisateur d'une BDD.
Blocage des ports de communication non indispensables par un responsable réseau.

Défense en profondeur

Il s'agit d'utiliser plusieures techniques de sécurité parfois redondantes pour ralentir ou arrêter l'attaquant.
par exemple :
antivirus sur les terminaux et les serveurs.
parefeu sur chaque serveur et à l'entrée du reseau.



Activer Windows