Cybersécurité - Cours 2: Les risques et menaces

SIO - Bloc 1 - SMDSI

M. SPINA

Sommaire

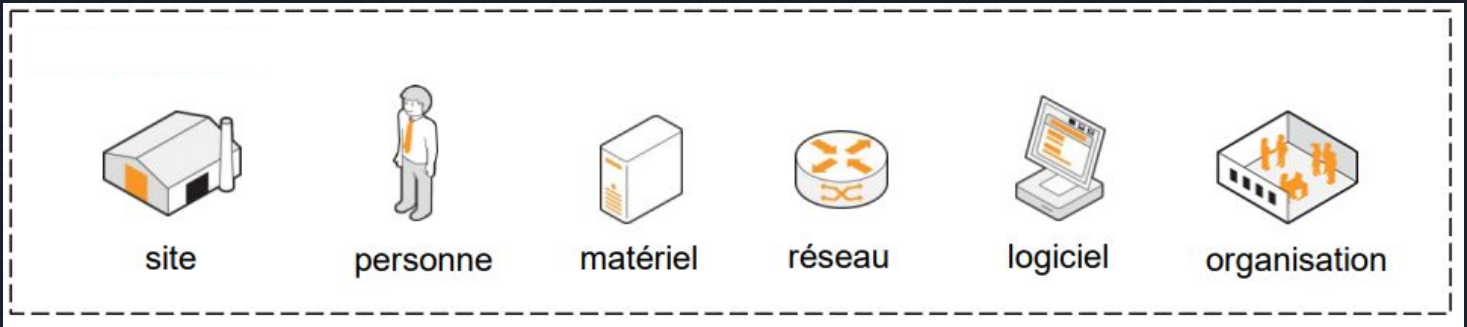
1. Introduction
2. Quels sont les risques ?
3. Classification du risque
4. Les différents types de menaces
5. Les différents types d’attaques

Introduction

Système d'Information (S.I.)

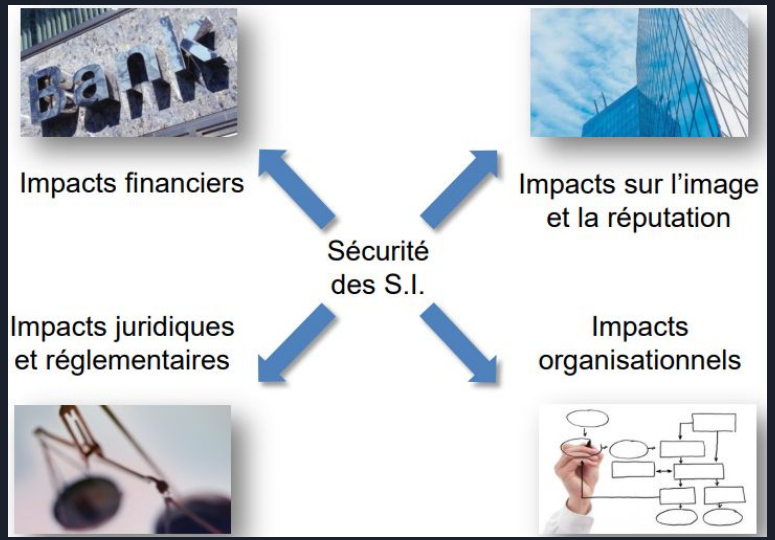
→ Ensemble des ressources destinées à collecter, classifier, stocker, gérer, diffuser les informations au sein d'une organisation

Le S.I. doit permettre et faciliter la mission de l'organisation



Introduction

La **sécurité** a pour objectif de réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des organisations…



La sécurité du S.I. consiste à assurer la sécurité de l'ensemble des biens

Quels sont les risques ?

Classification par le CLUSIF [*http://www.clusif.fr/*] basées sur les déclarations de sinistres des entreprises :

- **accidents naturels:** incendie, dégâts des eaux, etc.
- **perte des services essentiels:** coupure courant, réseau, rupture de stocks
- **erreurs:** tous les secteurs d'activité : analyse, conception, réalisation, mise en œuvre, utilisation
- **malveillance:** vol, vandalisme, fuite d'informations

Classification du risque

1. **Nul:** risque jugé non significatif
2. **Faible:** événement générant une nuisance organisationnelle, des pertes financières faibles, peu gênant pour l'utilisateur
3. **Sensible:** événement occasionnant des pertes financières significatives, nuisible à l'image, gênante pour l'utilisateur
4. **Critique:** événement occasionnant des pertes financières inacceptables, une perte de clientèle
5. **Stratégique:** événement susceptible d'entraîner un arrêt immédiat d'une activité de l'entreprise

Les différents types de menaces

Les menaces contrées par la cybersécurité sont au nombre de 3 :

- La **cybercriminalité** comprend des acteurs isolés ou des groupes qui ciblent des systèmes pour des gains financiers ou pour causer des perturbations.
- Les **cyberattaques** impliquent souvent la collecte d'informations pour des raisons politiques.
- Le **cyberterrorisme** vise à affaiblir les systèmes électroniques pour entraîner la panique ou la peur.

Les différents types d’attaques

Ces acteurs malveillants utilisent des **méthodes courantes** pour prendre le contrôle des systèmes, voici une liste non exhaustive:

- Programme malveillants
- Injection SQL
- Attaque par phishing
- Attaque de l’homme du milieu
- Attaque par déni de service
- Attaque par mot de passe

Programme malveillants

Il existe de nombreux types de malwares différents, notamment :

- **Virus:** un programme pouvant se dupliquer qui s'attache à un fichier sain et se propage dans tout le système en infectant les fichiers à l'aide d'un code malveillant.

- **Cheval de Troie:** type de programmes malveillants se faisant passer pour des logiciels authentiques. Les cybercriminels piègent les utilisateurs en téléchargeant des chevaux de Troie dans leur ordinateur pour endommager ou collecter des données.

Programme malveillants

- **Spyware:** un programme espion qui enregistre secrètement les actions d'un utilisateur au profit des cybercriminels. Par exemple, un spyware peut enregistrer des coordonnées bancaires.

- **Ransomware:** un malware qui verrouille les fichiers et les données de l'utilisateur sous menace de les effacer si une rançon n'est pas payée.

Programme malveillants

- **Adware:** un logiciel publicitaire qui peut être utilisé pour propager un malware.

- **Botnets:** des réseaux d'ordinateurs infectés par des malwares que les cybercriminels peuvent utiliser pour effectuer des tâches en ligne sans l'autorisation de l'utilisateur.

Injection SQL

Une **injection SQL** (Structured Query Language, ou langage de requête structurée) est un type de cyberattaque utilisé pour **contrôler et voler les données d'une base de données.** Les cybercriminels exploitent les vulnérabilités dans les applications orientées données pour insérer du code malveillant dans une base de données. Ils gagnent ainsi l'accès à des informations sensibles contenues dans la base.

Attaque par phishing

Le **phishing** désigne le fait, pour des cybercriminels, d'**envoyer des emails** qui semblent provenir d'une entreprise légitime pour demander des informations sensibles à leurs victimes. Les attaques de phishing servent souvent à tromper les utilisateurs pour récupérer leurs coordonnées bancaires et d'autres informations personnelles.

Attaque de l’homme du milieu

Une attaque dite de **l'homme du milieu** (“*man-in-the-middle*”) désigne un type de cybermenace consistant à intercepter la communication entre deux individus pour leur voler des données. Par exemple, sur un réseau wifi non sécurisé, un cybercriminel pourrait intercepter les données transitant entre l'appareil de la victime et le réseau.

Attaque par déni de service

Une **attaque par déni de service** désigne le fait, pour les cybercriminels, **d'empêcher un système informatique de répondre** à des requêtes légitimes **en surchargeant les réseaux et les serveurs** avec du trafic. Le système devient ainsi inutilisable, empêchant une entreprise de mener à bien l'essentiel de ses tâches.

Attaque par mot de passe

L’attaque par mot de passe permet, aux cybercriminels, d’essayer de se connecter à un compte utilisateur en entrant un mot de passe soigneusement construit pour tous les identifiants d’utilisateur qu’il a collectés.

S'il a de la chance, le pirate informatique peut accéder à un compte à partir duquel il peut pénétrer davantage dans le réseau informatique.

Attaque par mot de passe

Attaque par force brute: Le mot de passe est cassé en testant tous les mots de passe possibles. Technique demandant une forte puissance de calcul, mais il existe des outils permettant d'utiliser les puces des cartes graphiques ou de distribuer des calculs sur de milliers d'ordinateurs dans le monde entier.

Attaque par dictionnaire: Le mot de passe est craqué en testant des mots se trouvant dans des dictionnaires (la majorité des utilisateurs choisissent des mots de passe avec une signification réelle). Technique plus rapide et moins gourmande que l'attaque par force brute.

Attaque hybride: force brute + dictionnaire

Questions