CYBER AND INTERNET SECURITY

ICT313

M. MOYOU Léonel, Doctorant, UY1.

Table des matières

Ce chapitre introduit :

- les notions de base de la sécurité informatique : menace, risque, vulnérabilité;
- il effectue un premier parcours de l'ensemble du domaine, de ses aspects humains, techniques et organisationnels, sans en donner de description technique.

INTRODUCTION

La **sécurité informatique** est une branche de l'informatique qui vise à protéger les informations stockées dans un système informatique. Il n'existe aucune technique capable d'assurer l'inviolabilité d'un système. Les menaces peuvent dériver de programmes malveillants qui s'installent sur l'ordinateur de l'utilisateur (comme un virus) ou venir à distance à travers internet.

I. LA NOTION DE SECURITE INFORMATIQUE

1) Terminologie de la securite informatique

Le **système d'information** définit l'ensemble des données et des ressources matérielles et logicielles de l'entreprise. Ce système permet de stocker et de faire circuler les ressources qu'il contient. Ce système représente la valeur de l'entreprise) il est essentiel de le protéger. Le compromettre revient à compromettre l'entreprise.

La **menace** qui plane sur un système englobe les types d'actions menées dans le but de nuire à ce système (attaque) espionnage, vol d'informations...).

La **vulnérabilité** représente les failles, les brèches dans le système, tout ce qui expose le système à la menace : manque de sauvegardes, de robustesse, une architecture défaillante.

Les **attaques** (exploits): elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.

Les **contre-mesures** sont les actions mises en oeuvre pour prévenir la menace) une fois qu'elle est mesurée, ce qui passe d'abord par une prise de conscience.

Le **risque** encouru par un système est lié de manière étroite à la menace et à la vulnérabilité qui le touchent, mais également aux contre-mesures mises en oeuvre.

Puisque le SI est vital, tout ce qui le menace est potentiellement mortel : cela semble couler de source, et pourtant les auteurs de ce livre peuvent témoigner des difficultés qu'ils ont pu éprouver en essayant de convaincre leurs employeurs de consacrer quelques efforts à la sécurité de leur SI. Conjurer les menaces contre le SI est devenu impératif, et les lignes qui suivent sont une brève description de ce qu'il faut faire pour cela.

Les menaces contre le système d'information entrent dans l'une des catégories suivantes : **atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles**.

Les menaces engendrent des risques et des coûts humains et financiers : **perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, dommages** pour le patrimoine intellectuel et la notoriété. **Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.**

Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence : **risque = préjudice x probabilités d'occurrence**

Cette formule exprime qu'un événement dont la probabilité à survenir est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible. Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces.

2) Services principaux de la securite informatique

Pour mettre en place une politique de sécurité, il faut d'abord commencer par identifier la menace, le risque potentiel. Il faut connaître son ennemi, ses motivations et prévoir la façon dont il procède pour s'en protéger et limiter les risques d'intrusion. La sécurité d'un système repose sur cinq grands principes:

- **L'intégrité des données**: il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.

- **La confidentialité** : seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possédant la clé de compréhension.

- **La disponibilité**: il faut s'assurer du bon fonctionnement du système} de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- **La non-répudiation** des données : une transaction ne peut être niée par aucun des correspondants. La non-répudiation de l'origine et de la réception des données prouve que les données ont bien été reçues. Cela se fait par le biais de certificats numériques grâce à une clé privée.

- **L'authentification** : elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

3) Les champs d'application de la securite informatique

Dans un contexte global la sécurité doit être assurée:
- **au niveau utilisateur** : les acteurs doivent comprendre l'importance de leur position.
- **au niveau des technologies utilisées** : elles doivent être sûres et ne pas présenter de failles.
- **au niveau des données en elles-mêmes** : avec une bonne gestion des droits d'accès (authentification et contrôle) l'utilisateur doit posséder uniquement les droits qui lui sont nécessaires).
- **au niveau physique** (accès à l'infrastructure) au matériel) : rien ne sert de sécuriser un système logiquement si matériellement l'accès à la salle des machines n'est pas sécurisé.

4) LES ATTAQUES

1. Types d'attaques

Les attaques peuvent à première vue être classées en 2 grandes catégories :

- **les attaques passives** : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- **les attaques actives** : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

2. Profils et capacites des attaquants

Les attaquants peuvent être classés non-seulement par leurs connaissances (newbies, experts, etc...) mais également suivant leurs capacités d'attaques dans une situation bien définie. Ainsi, on dénombrera les capacités suivantes :

- transmission de messages sans capacité d'écoute (IP spoofing...)
- écoute et transmission de messages
- écoute et perturbation des communications (blocage de paquets, DoS et DDoS...)
- écoute, perturbation et transmissions de messages
- écoute et relai de messages (attaques type man-in-the-middle)

II. TYPES DE TESTS DE PENETRATION

Les deux types principaux de tests d'intrusion :

1) Test de pénétration de type boîte blanche

visibles (boîte blanche) : Un test de type boîte blanche (ou test white hat) est réalisé en accord avec l'organisation qui a été préalablement avertie.

Lors d'un test de pénétration de type boîte blanche, vous travaillez avec l'organisation pour identifier les menaces potentielles. L'avantage principal de ce type de test est que vous avez accès aux connaissances de quelqu'un de l'intérieur et que vous pouvez lancer vos attaques sans craindre d'être bloqué. L'inconvénient est que vous pourriez ne pas avoir de résultats exacts en ce qui concerne le programme de sécurité et sa capacité à détecter certaines attaques.

2) Test de pénétration de type boîte noire

invisibles (boîte noire). un test de type boîte noire est conçu pour simuler les actions d'un attaquant inconnu survenu à l'improviste.

Contrairement aux tests boîte blanche, les tests de pénétration de type boîte noire permettent de simuler les actions d'un attaquant et sont effectués à l'insu de l'organisation. Les tests boîte noire sont réalisés afin de tester la capacité de l'équipe de sécurité interne à détecter une attaque et à y répondre.

3) SCANNERS DE VULNERABILITE

Les scanners de vulnérabilité sont des outils automatisés qui servent à identifier les failles de sécurité affectant un système ou une application. En comparant les empreintes, ils identifient le système d'exploitation de la cible (la version et le type) ainsi que les services en cours d'exécution.

Les scanners jouent un rôle très important dans les tests d'intrusion, en particulier dans le cas d'un test overt, qui permet de lancer des attaques multiples sans avoir à se soucier d'éviter la détection. La richesse des informations qu'ils proposent est inestimable, mais prenez garde à trop compter sur eux.
EXEMPLE : NMAP, NESSUS, METASPLOIT, etc.

III. L'ETHIQUE DE TRAVAIL

Les hackers sont également capables de détourner un objet ou un logiciel de son fonctionnement originel. Ils utilisent leur savoir pour découvrir les choses auxquelles ils ne sont pas censés avoir accès. Les différents types de cette grande famille sont :

1) Les hackers « black hats » les chapeaux noirs

Généralement, ces hackers ne respectent pas la loi, ils pénètrent par effraction dans les systèmes dans un intérêt qui n'est pas celui des propriétaires du réseau. L'intérêt y est personnel, généralement financier, en tout cas le but est nuisible à la personne (physique ou morale) visée. Ces hackers sont d'ailleurs plus généralement appelés des **crackers**. Les crackers ayant une nette attirance pour ce côté obscur sont par exemple les créateurs de virus, de chevaux de Troie ou de logiciels espions.

2) Les hackers « white hats », les chapeaux blancs

Techniquement, l'action menée par les white hats est très proche de celle des black hats. Cependant, elle se différencie par le **but ou la finalité**. En effet, les « white hackers » ont plutôt comme ambition d'aider à la sécurisation du système, sans en tirer profit de manière illicite. Les white hats bricolent et testent les systèmes d'information pour découvrir les vulnérabilités pas encore connues ou non publiques, les « 0 day » (**zéro day**, zéro jour). La technique employée est la même que pour un hacker à chapeau noir. Les white hats rendent alors publiques les vulnérabilités, et parfois même les exploits, qui sont les bouts de code permettant de tester la vulnérabilité d'un système à cette faille.

3) Les hackers « grey hats », les chapeaux gris

Le hacker au chapeau gris est un peu un hybride du chapeau blanc et du chapeau noir. Il s'agit d'un hacker compétent, qui agit parfois avec l'esprit d'un white hat, parfois avec celui d'un black hat. Son intention n'est pas forcément mauvalse mais il commet cependant occasionnellement un délit.

4) Les « scripts kiddies »

Dans le problème lié à la publication sur Internet des vulnérabilités découvertes, on trouve l'un des éléments clés de la discorde, les scripts kiddies, autrement dit des jeunes pirates néophytes. Ces individus récupèrent les exploits laissés par les white hats sur les outils publics et les exécutent sur des machines, sans aucune connaissance, dans le but de provoquer des pannes volontaires, des mass-root.

Le terme **cybercriminalité** est utilisé pour décrire une activité illégale dans laquelle des ordinateurs ou des appareils informatiques tels que des smartphones, des tablettes, des assistants numériques personnels (PDA), etc., autonomes ou faisant partie d'un réseau, sont utilisés comme un outil ou / et cible de l'activité criminelle. Il est commis par des gens à l'état d'esprit destructeur et criminel, que ce soit pour la vengeance, la cupidité ou l'aventure.

I. CLASSIFICATION DES CYBERCRIMES

Le cybercriminel peut être interne ou externe à l'organisation confrontée à la cyberattaque. Sur la base de ce fait, la cybercriminalité pourrait être classée en deux types:

- **Attaque interne**: une attaque contre le réseau ou le système informatique par une personne disposant d'un accès autorisé au système est appelée attaque d'initié. Il est généralement effectué par des employés ou des entrepreneurs insatisfaits ou mécontents. Le motif de l'attaque interne pourrait être la vengeance ou la cupidité. Il est relativement facile pour un initié d'effectuer une cyberattaque, car il connaît bien les **politiques, les processus, l'architecture informatique et le bien-être du système de sécurité**. De plus, l'attaquant a un accès au réseau. Par conséquent, il est relativement facile pour un attaquant interne d'acquérir des informations sensibles, de planter le réseau, etc. dans les politiques informatiques. L'attaque interne pourrait être évitée en planifiant et en installant un système de détection d'intrusion interne (IDS) dans l'organisation.
- **Attaque externe**: lorsque l'attaquant est embauché par un initié ou une entité externe à l'organisation, on parle d'attaque externe. L'organisation victime d'une cyberattaque fait non seulement face à des pertes financières mais également à une perte de réputation. Étant donné que l'attaquant est externe à l'organisation, ces **attaquants analysent et collectent généralement des informations**. Un administrateur réseau / sécurité expérimenté surveille régulièrement le journal généré par les pare-feu, car les attaques externes peuvent être détectées en analysant soigneusement ces journaux de pare-feu. De plus, des systèmes de détection d'intrusion sont installés pour garder un œil sur les attaques externes.

Il existe des offres et des services à la demande pour les cybercriminels. La personne, l'organisation ou un pays peut contacter ces cybercriminels pour pouvoir pirater une organisation afin d'accéder à certaines données sensibles, ou créer une attaque massive par déni de service contre leurs concurrents. Sur la base de la demande du client, les pirates créent des logiciels malveillants, des virus, etc. en fonction de leurs besoins. Une organisation effectuée par une cyberattaque, non seulement fait face à une perte financière, mais sa reputation est également affectée négativement, et l'organisation concédante en bénéficiera définitivement.

II. RAISONS D'ETRE DES CYBERCRIMES

Il existe de nombreuses raisons qui agissent comme un catalyseur dans la croissance de la cybercriminalité. Certaines des principales raisons sont:

a. **Argent**: les gens sont motivés à commettre des cybercrimes, c'est de gagner de l'argent rapidement et facilement.

b. **Vengeance**: Certaines personnes essaient de se venger d'une autre personne / organisation / société / caste ou religion en diffamant sa réputation ou en apportant une perte économique ou physique. Cela relève de la catégorie du cyber-terrorisme.
c. **Amusement**: l'amateur fait de la cybercriminalité pour le plaisir. Ils veulent juste tester le dernier outil qu'ils ont rencontré.
d. **Reconnaissance**: il est considéré comme une fierté si quelqu'un pirate les réseaux hautement sécurisés comme les sites ou les réseaux de défense.
e. **Anonymat** - Souvent, l'anonymat fourni par un cyberespace motive la personne à commettre une cybercriminalité, car il est beaucoup plus facile de commettre une cybercriminalité sur le cyberespace et de rester anonyme par rapport au monde réel. Il est beaucoup plus facile de s'en sortir avec une activité criminelle dans un cyber-monde que dans le monde réel. Il existe un fort sentiment d'anonymat qui peut amener des citoyens par ailleurs respectables à abandonner leur éthique à la recherche d'un gain personnel.
f. **Cyberespionnage**: Parfois, le gouvernement lui-même est impliqué dans la cyber-intrusion pour surveiller d'autres personnes / réseaux / pays. La raison pourrait être politiquement, économiquement et socialement motivée.

III. TYPES DE CYBER CRIME

Différents types de cybercrimes sont :

1) Le cyber-harcèlement

Il s'agit d'un acte de traque, de harcèlement ou de menace d'une personne utilisant Internet / un ordinateur comme moyen de communication. Ceci est souvent fait pour diffamer une personne et utiliser le courrier électronique, le réseau social, la messagerie instantanée, la publication sur le Web, etc. Le comportement comprend de fausses accusations, des menaces, l'exploitation sexuelle des mineurs, la surveillance, etc.

2) Pornographie juvénile

Il s'agit d'un acte de possession d'image ou de vidéo d'un mineur (moins de 18 ans), engagé dans un comportement sexuel.

3) Falsification et contrefaçon

C'est une utilisation de l'ordinateur pour la contrefaçon et la falsification d'un document. Avec l'avancement du matériel et du logiciel, il est possible de produire des contrefaçons qui correspondent au document original à un point tel qu'il n'est pas possible de juger de l'authenticité du document sans jugement d'expert.

4) Piratage de logiciels et délits liés aux DPI

Le piratage de logiciels est une reproduction et une distribution illégales pour un usage personnel ou professionnel. Il relève de la criminalité liée à la violation des DPI (droit public individuel). Certains des autres crimes en vertu de la violation des DPI sont: le téléchargement de chansons, le téléchargement de films, etc.

5) Cyber Terrorisme

Il est défini comme l'utilisation de ressources informatiques pour intimider ou contraindre le gouvernement, la population civile ou tout segment de ceux-ci à des fins politiques ou des objectifs sociaux.

6) Phishing

Il s'agit d'un processus d'acquisition d'informations personnelles et sensibles d'un individu par e-mail en se déguisant en entité de confiance dans une communication électronique. Le but du phishing est le vol d'identité et les informations personnelles telles que le nom d'utilisateur, le mot de passe et le numéro de carte de crédit, etc. peuvent être utilisées pour voler de l'argent sur le compte de l'utilisateur. Si un téléphone est utilisé comme moyen de vol d'identité, il est connu sous le nom de Vishing (phishing vocal). Une autre forme de phishing est le smishing, dans lequel les sms sont utilisés pour attirer les clients.

7) Vandalisme informatique

Il s'agit d'un acte de destruction physique des ressources informatiques en utilisant la force physique ou un code malveillant.

8) Piratage informatique

Il s'agit d'une pratique consistant à modifier le matériel informatique et les logiciels pour atteindre un objectif en dehors de l'objectif initial du créateur. Le but du piratage d'un système informatique peut aller de la simple démonstration de la capacité technique au scellement, à la modification ou à la destruction d'informations pour des raisons sociales, économiques ou politiques. Maintenant, l'entreprise embauche des pirates informatiques, une personne engagée dans le piratage d'ordinateurs, pour pirater intentionnellement l'ordinateur d'une organisation afin de trouver et de corriger les failles de sécurité.

9) Création et distribution de virus sur Internet

La propagation d'un virus peut entraîner des pertes commerciales et financières pour une organisation. La perte comprend le coût de réparation du système, le coût associé à la perte d'activité pendant les temps d'arrêt et le coût de la perte d'opportunité. L'organisation peut poursuivre le pirate informatique, s'il est trouvé, pour la somme supérieure ou équivalente à la perte supportée par l'organisation.

10) Spamming

L'envoi de messages en masse non sollicités et commerciaux sur Internet est connu sous le nom de spamming. Un e-mail peut être classé comme spam s'il répond aux critères suivants: a. Mailing de masse: - l'e-mail n'est pas destiné à une personne en particulier mais à un grand nombre de personnes. b. Anonymat: - L'identité réelle de la personne n'est pas connue c. Non sollicité: - l'e-mail n'est ni attendu ni demandé pour le destinataire. Ces spams non seulement irritent les destinataires et surchargent le réseau, mais font également perdre du temps et occupent le précieux espace mémoire de la boîte aux lettres.

11) Scripts intersites

Il s'agit d'une activité qui consiste à injecter un script malveillant côté client dans un site Web de confiance. Dès que le navigateur exécute le script malveillant, le script malveillant accède aux cookies et autres informations sensibles et est envoyé à des serveurs distants. Désormais, ces informations peuvent être utilisées pour obtenir un avantage financier ou un accès physique à un système pour un intérêt personnel.

12) Fraude aux enchères en ligne

Il existe de nombreux sites Web authentiques qui proposent des enchères en ligne sur Internet. Profitant de la réputation de ces sites Web, certains des cybercriminels attirent les clients vers des systèmes de fraude aux enchères en ligne qui conduisent souvent à un trop-payé du produit ou que l'article n'est jamais livré une fois le paiement effectué.

13) Cyber Squatting

C'est un acte de réservation des noms de domaine de la marque de quelqu'un d'autre avec l'intention de la vendre par la suite à l'organisation qui est le propriétaire de la marque à un prix plus élevé.

14) Bombes logiques

Il s'agit de codes malveillants insérés dans des logiciels légitimes. L'action malveillante est déclenchée par une condition spécifique. Si les conditions sont remplies à l'avenir, l'action malveillante commence et en fonction de l'action définie dans le code malveillant, elles détruisent les informations stockées dans le système ou rendent le système inutilisable.

15) Web Jacking

Le pirate informatique accède au site Web d'une organisation et le bloque ou le modifie pour servir des intérêts politiques, économiques ou sociaux. Les exemples récents de web jacking sont certains des sites Web des instituts d'enseignement ont été piratés par des pirates pakistanais et une animation contenant des drapeaux pakistanais a été affichée sur la page d'accueil de ces sites. Un autre exemple est le piratage du site Web des chemins de fer pakistanais par des pirates indiens et le drapeau indien sur la page d'accueil pendant plusieurs heures à l'occasion du jour de l'indépendance de l'Inde en 2014.

16) Vol de temps sur Internet

Piratage du nom d'utilisateur et du mot de passe du FAI d'un individu et surfant sur le Internet à ses frais est le vol de temps Internet.

17) Attaque par déni de service

Il s'agit d'une cyberattaque dans laquelle le réseau est étouffé et souvent effondré en l'inondant de trafic inutile et empêchant ainsi le trafic réseau légitime.

18) Salami Attack

C'est une attaque qui se déroule avec de petits incréments et une somme finale pour conduire à une attaque majeure. Les incréments sont si petits qu'ils restent inaperçus. Un exemple d'attaque de salami est l'accès à la banque en ligne d'un individu et le retrait d'un montant si petit qu'il reste inaperçu par le propriétaire. Souvent, le déclencheur par défaut est défini sur le site Web bancaire et les transactions ci-dessous, par exemple, Rs. 1000 retraits ne sont pas signalés au propriétaire du compte. Montant de retrait de Rs. 1000 sur une période de temps entraînera le retrait total d'une somme importante.

19) Data Diddling

Il s'agit d'une pratique consistant à modifier les données avant leur entrée dans le système informatique. Souvent, les données d'origine sont conservées après l'exécution des données. Par exemple, DA ou le salaire de base de la personne est modifié dans les données de paie d'un individu pour le calcul de la paie. Une fois le salaire calculé et transféré sur son compte, le salaire total est remplacé par son salaire réel dans le rapport.

20) Usurpation d'e-mail

Il s'agit d'un processus consistant à modifier les informations d'en-tête d'un e-mail afin que sa source d'origine ne soit pas identifiée et qu'il apparaisse à une personne à l'extrémité de réception que l'e-mail provient d'une source autre que la source d'origine.