INTITULÉ : HACKING ET SECURITE - NIVEAU 2

PRÉNOM : ARTHUR

NOM : MENDJANA

1 - LA SENSIBILISATION A LA SÉCURITÉ INFORMATIQUE

1- 1 L’apparition des cyberattaques

Une **cyberattaque** ou attaque informatique est une action volontaire et malveillante menée au moyen d'un réseau informatique visant à causer un dommage aux informations et aux personnes qui les traitent (particuliers, entreprises, hôpitaux , institutions...).
Une cyberattaque peut être le fait d'une personne seule (hacker), d'un groupe de pirates, d'un État ou d'une organisation criminelle.
Les cyberattaques sont facilitées par la quantité croissante d'informations mises en ligne (cloud) et par des failles de sécurité dans les systèmes. Elles peuvent être prévenues par une vigilance humaine, des mots de passe forts, une mise à jour régulière des logiciels et la sécurisation des données (cybersécurité).

Les différents types de cyberattaque :

- ❑ installation de programmes espion ou de malwares
- ❑ phishing (hameçonnage)
- ❑ attaque par déni de service (DDoS - perturbation ou inondation du réseau afin de le rendre indisponible)
- ❑ intrusion
- ❑ vol l'information
- ❑ ransomware (demande de rançon en échange d'une clé de chiffrement des données cryptées)
- ❑ renvoi vers un faux site
- ❑ attaque par brute force (trouver un mot de passe en testant successivement toutes les combinaisons possibles)

1- 1 L’apparition des cyberattaques

Quelques Cyberattaques

- 1999 : **Melissa**. Ce **virus** infectant des pièces jointes **Microsoft** et se disséminant via le carnet d'adresses aurait causé 385 millions de dollars de dommages. Il est le fait d'un hacker nommé David Smith qui a écopé de 20 mois de prison.

- 2010 : **Stuxnet**. Ce virus touchant les systèmes Windows a neutralisé les centrifugeuses du site d'enrichissement **d'uranium** de Natanz en Iran. Stuxnet a été le premier malware à utiliser l'arme informatique contre un État. Les services secrets israéliens seraient derrière cette cyberattaque.

- 2013 : **Yahoo**. Victime d'un gigantesque piratage en août 2013, Yahoo voit ses **3 milliards de comptes affectés**, soit le plus important vol de données de l'histoire. Bien qu'aucun mot de passe ni données bancaires n'aient été dérobés, Yahoo a été vivement critiqué pour avoir révélé le piratage seulement trois ans après.

- 2012 : **Shamoon**. Ce logiciel malveillant a paralysé la société pétrolière Saudi Aramco pendant 15 jours en août 2012. Le virus a à nouveau ciblé plusieurs sociétés pétrolières et agences gouvernementales saoudiennes en 2017. L'Iran est suspecté.

1- 1 L’apparition des cyberattaques

Quelques Cyberattaques

•2014 : **Sony Pictures**. Les pirates, sous le nom de Guardian of Peace, ont menacé la compagnie de dévoiler des informations sensibles si l'entreprise n'accédait pas à leurs requêtes. Cinq films ont ensuite été divulgués sur Internet. L'attaque a été attribuée à la Corée du Nord, qui aurait voulu se venger d'un film caricaturant le dictateur Kim Jong-un.

•2016 : **Mirai.** Cette attaque transforme des ordinateurs Linux en bots contrôlés à distance, formant alors un immense botnet utilisé notamment pour réaliser des attaques par déni de service (DDoS). L'attaque a notamment visé la société Dyn, paralysant de nombreux sites et services (Twitter, PayPal, AirBnB ou Netflix).

•2017 : **WannaCry**. Ce logiciel malveillant de type ransomware a touché plus de 300.000 ordinateurs dans 150 pays en 2017. Il exploite une faille de sécurité Windows à travers des pièces jointes contaminées. Il serait le fait d'un groupe de hackers nord-coréens ou chinois.

•2017 : **NotPetya**. Ce programme de type ransomware à l'origine d'une cyberattaque mondiale vise la même faille que WannaCry. Il a paralysé plusieurs grandes entreprises comme Saint-Gobain ou Auchan ainsi que la SNCF ou le métro de Kiev. NotPetya serait l'attaque informatique la plus couteuse de tous les temps (10 milliards de dollars).

1- 2 Les caractéristiques juridiques

Contrairement à ce que l'on pourrait penser, le cyberespace n'est pas totalement libre et désordonné.
Cependant, la nature décentralisée d'Internet fait de lui un espace « contrôlé » par plusieurs organismes, états ou entreprises.
À tous les échelons, de nombreux organismes exercent ou peuvent exercer un contrôle ou une censure sur les informations qui y circulent.

LEGISLATION ET DROIT DU MONDE CYBER EN FRANCE

- **La loi n°78-17**

du 6 janvier 1978 relative à l'informatique,aux fichiers et aux libertés, plus connue sous le nom de << **loi informatique et libertés** >> qui règlemente la liberté de traitement des données personnelles, c'est-à-dire la liberté de ficher les personnes.

- **LOI GODFRAIN**

La **Loi Godfrain** du 5 janvier 1988 , relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage.
Nommée ainsi d'après le député Jacques Godfrain, c'est l'une des lois pionnières concernant le droit des NTIC, après la loi Informatique et libertés de 1978, qui introduit la notion de système de traitement automatisé de données (STAD)
Elle concerne notamment les obligations du responsable du traitement quant à la garantie de la sécurité des données.

1- 2 Les caractéristiques juridiques

LEGISLATION ET DROIT DU MONDE CYBER EN FRANCE

- **LCEN**

La loi pour la confiance dans l'économie numérique, **n°2004-575** du 21 juin 2004, abrégée sous le sigle **LCEN**. est une loi française sur le droit de l'Internet, transposant la directive européenne 2000 / 31 / CE
du 8 juin 2000 sur le commerce électronique et certaines dispositions de la directive du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques. Elle vise à promouvoir le commerce électronique au sein de l'Union européenne

- **LE SECRET DES CORESPONDANCES**

Le secret des correspondances est un droit au maintien du caractère privé et secret. Il s'applique aux correspondances dont l'expéditeur pouvait attendre qu'elles bénéficient d'un minimum de confidentialité.
En général, il s'applique aux courriers postaux et aux courriers électroniques
Une correspondance est en général définie comme toute relation par écrit entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis ouverts ou fermés.
En France, la violation du secret des correspondances,qu'elles circulent par voie postale ou par télécommunication,est actuellement punie **d'un an d'emprisonnement et de 45 000 euros d'amende** pour les personnes facilitant cette violation dans l'exercice
Cette peine peut s'alourdir à **3 ans d'emprisonnement** de leurs fonctions (hors cas prévus par la loi).

1- 2 Les caractéristiques juridiques

LEGISLATION ET DROIT DU MONDE CYBER EN FRANCE

- **RÉFERENTIEL GÉNÉRAL DE SÉCURITÉ (RGS)**

Le Référentiel Général de Sécurité (**RGS**) a pour objectif de sécuriser les échanges et les transactions entre les usagers et les autorités administratives.
Il s'agit d'un cadre règlementaire permettant d'instaurer la confiance dans les échanges au sein de l'administration (**télé-services**) et avec les citoyens.
Indirectement, le Référentiel Général de Sécurité s'adresse à l'ensemble des prestataires de services qui assistent les autorités administratives dans la sécurisation des échanges électroniques qu'elles mettent en œuvre,ainsi qu'aux industriels dont l'activité est de proposer des produits de sécurité.
De façon générale, pour tout autre organisme souhaitant organiser la gestion de la sécurisation de ses systèmes d'information et de ses échanges électroniques, **le Référentiel Général de Sécurité. se présente comme un guide de bonnes pratiques conformes à l'état de l'art.**

1- 2 Les caractéristiques juridiques

LÉGISLATION ET DROIT EN EUROPE

La directive NIS (Directive Network and Information Security)

s'inscrit dans la lignée de la « **stratégie sur la cybersécurité** » dans l'Union européenne,publiée en 2013 par la Commission. Cette stratégie a pour but de promouvoir un cyberespace « libre et sécurisé » dans l'Union européenne afin de prévenir et de réagir aux cyberattaques et d'assurer ainsi la croissance de l'économie numérique.
Le but de cette directive est d'assurer un niveau commun élevé de cybersécurité dans l'Union européenne :

- ❑ En améliorant les capacités de cybersécurité des états membres
- ❑ En améliorant la coopération entre les états et entre les secteurs publics et privés
- ❑ En exigeant que les entreprises de secteurs critiques - par exemple l'énergie, le transport, les finances et la santé - ainsi que des services internet clés adoptent des pratiques de gestion des risques et communiquent les accidents majeurs aux autorités nationales.

1- 2 Les caractéristiques juridiques

LÉGISLATION ET DROIT EN EUROPE

RGPD
Règlement Général sur la Protection des Données

Le nouveau règlement européen sur la protection des données personnelles est paru au journal officiel de l'Union européenne le 4 mai 2016 et entre en application en 2018.
Le règlement général de protection des données (**RGPD**) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. Il est entré en application le 25 mai 2018.

Le RGPD s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de 3 objectifs :

- ❑ renforcer les droits des personnes
- ❑ responsabiliser les acteurs traitant des données
- ❑ crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

1- 3 La veille technologique, dans le domaine de la sécurité

La veille en sécurité informatique est une activité indispensable, pour tous les professionnels. Elle vous permet de rester au fait des évolutions et tendances.
Mais, plus important, la veille vous donne la capacité d'anticiper les attaques informatiques et mieux vous préparer et donc de limiter le risque d'un incident.
Les technologies sont en évolutions permanentes, les attaques et les vulnérabilités également. C'est un vrai jeux du chat et de la souris que se livrent pirates et défenseurs.
Chaque semaine, des vulnérabilités sont découvertes, des entreprises sont victimes de piratages, entraînant des dommages importants, voire irrémédiables.
Pourtant malgré le buzz autour des **failles Zero Day** ou autres APT, c'est bien souvent les failles connues mais non corrigées qui sont exploités par les pirates… Les pirates profitent, entre autre, du temps entre la publication d'un correctif et le moment où vous appliquerez le patch pour agir.
Autant dire qu'il est indispensable :

- ❑ de se tenir au courant des vulnérabilités et des patchs,
- ❑ des tendances d'attaques des pirates.

1- 3 La veille technologique, dans le domaine de la sécurité

Faire sa veille en sécurité informatique

Les ressources communes sont assez connues et l'inventaire serait assez peu intéressant. De plus, au-delà de la veille globale, le reste dépend surtout de vos centres d'intérêts.

Le moyen déjà : privilégiez le RSS, qui vous évitera des heures de navigation, de pub et gardera uniquement l'important.

Les ressources incontournables :

Les alertes de sécurité

- ❑ **le CERT-FR**, Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques
- ❑ **CVE**, la référence en matière d'alertes de sécurité, souvent reprise par le CERT-FR
- ❑ **CVE Details**, un autre site de référence en termes de vulnérabilités recensées
- ❑ **Exploit Database**, indiquant les exploits les plus courants

1- 3 La veille technologique, dans le domaine de la sécurité

Faire sa veille en sécurité informatique

Les sites de référence

- ❑ **les publications du CLUSIF**
- ❑ **L'ANSSI**, Agence nationale de la sécurité des systèmes d'information
- ❑ **Orange Business Services** (pas de RSS)
- ❑ **Cyberdéfense Orange**
- ❑ **SecureList**, un site édité par Kaspersky
- ❑ **SecLists.org**
- ❑ **Google Security Blog**
- ❑ **Zythom**