Partie 1 :
Notions de la cybersécurité

Formateur : Azer Zairi
(azer.zairi@gnet.tn)

Partie 1 – Sections et objectifs

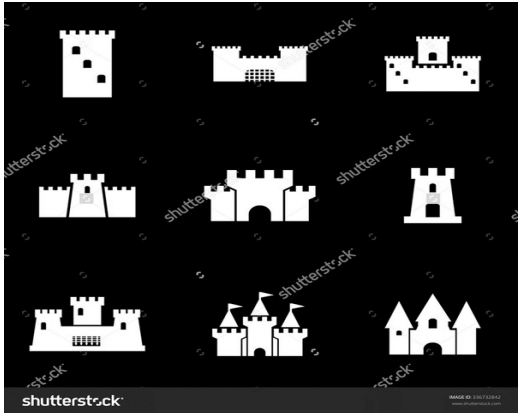
- 1.1 Caractéristiques du monde de la cybersécurité
  - Décrire les caractéristiques communes de l'univers de la cybersécurité
- 1.2 Criminels et professionnels de la cybersécurité
  - Faire la différence entre les cybercriminels et les héros
- 1.3 Comparaison des menaces de cybersécurité
  - Comparer la manière dont les menaces de cybersécurité affectent les individus et les entreprises
- 1.4 Facteurs de croissance de la cybercriminalité
  - Analyser le comportement des entreprises et les efforts consentis pour augmenter les effectifs dédiés à la cybersécurité

1.1 Le monde de la cybersécurité

Les royaumes

Présentation du monde de l'internet

- **Sites web et puissance des données**
  - La **collecte** et **l'exploitation** de la puissance des **données** et de leur **analyse** ont contribué à la **création de grandes entreprises**.
  - Il incombe à ces **entreprises de protéger ces données** contre les utilisations frauduleuses et les accès non autorisés.
  - La **croissance des données** crée des **opportunités** exceptionnelles pour les **spécialistes** de la **cybersécurité**.
- **Royaumes**
  - Les entreprises de toutes tailles reconnaissent la puissance du **Big Data et de l'analyse de données**.
  - ***Par exemple :*** Google, LinkedIn, Meta, Microsoft et Amazon, proposent des services et des opportunités essentiels à leurs clients.
  - La collecte et l'analyse des données évoluant de façon exponentielle,
    - ⇒ les **risques** pour les personnes et la vie quotidienne sont **de plus en plus nombreux**.
  - Il faut donc **prendre** des **précautions** pour protéger les données sensibles contre les criminels ou toute personne mal intentionnée.



Les royaumes

Présentation du monde de l'internet (suite)

- Les **experts en cybersécurité** disposent désormais d'une **technologie** capable :
  - d'assurer le **suivi** des tendances météorologiques dans le monde entier,
  - de **surveiller** le trafic internet et **d'analyser** les activités et le comportement
    - des **personnes** et des **objets** en temps réel.
- De nouvelles technologies, comme **GIS** (Geospatial Information Systems) et l'**Internet of Everything** (IoE), ont fait leur apparition.
- Toutes **dépendent** de la **collecte** et de **l'analyse** d'un très grand volume de **données**.
- Cette collecte croissante des données aide à **économiser** de **l'énergie**, à **améliorer l'efficacité** et à **réduire** les **risques** de sécurité.

1.2 Cybercriminels contre professionnels de la cybersécurité

Cybercriminels contre héros de la cybersécurité

Les cybercriminels

- **Hackers** : Ce groupe de criminels accèdent aux ordinateurs et aux réseaux afin d'accéder aux données qu'ils contiennent.
- Leurs **motifs** sont **variés**.
  - Les hackers au ***chapeau blanc*** s'introduisent dans les systèmes réseau et informatique afin d'en détecter les faiblesses et d'améliorer la sécurité.
  - Les hackers au ***chapeau noir*** sont des criminels qui compromettent la sécurité des systèmes informatiques et des réseaux à des fins de profit personnel ou avec des intentions malveillantes, comme le vol, la modification ou la suppression des données.
  - Les hackers au ***chapeau gris*** se situent entre les chapeaux noirs et les chapeaux blancs.
    - Parfois, les hackers au chapeau gris détectent une vulnérabilité et en font part aux propriétaires du système si cela s'intègre à leurs objectifs.

Cybercriminels contre héros de la cybersécurité

Les cybercriminels (suite)

Les criminels sont aussi divers que variés.

Leur motivation peut aussi varier :

- **Scripts-kiddie** : adolescents ou **amateurs** qui se limitent généralement à des canulars et du vandalisme.
  - Ils ont peu ou **pas de compétences**,
  - Utilisent souvent les outils ou instructions disponibles sur Internet pour lancer des attaques.
- **Testeurs de vulnérabilité** : hackers au **chapeau gris** qui tentent de découvrir des exploits et les signalent aux fournisseurs,
  - parfois en contrepartie d'un prix ou d'une récompense.
- **Hacktivistes** : hackers au **chapeau gris** qui **manifestent** et **contestent** les idées politiques et sociales différentes des leurs.
  - Les hacktivistes **protestent publiquement** contre les entreprises ou les gouvernements en publiant des articles et des vidéos, en divulguant des informations sensibles et en lançant des **attaques** par déni de service distribué (**DDoS**).

Cybercriminels contre héros de la cybersécurité

Les cybercriminels (suite)

- **Cybercriminels** : hackers au **chapeau noir** qui travaillent à **leur compte** ou pour de grandes **organisations** de **piratage** informatique.
  - Chaque année, les cybercriminels volent des milliards de dollars auprès des clients et d'entreprises.
- **Hackers financés par des gouvernements** : selon les points de vue, il peut s'agir de hackers au **chapeau blanc** ou au chapeau **noir** qui **volent** des **secrets** aux **gouvernements**, collectent des informations et sabotent les réseaux.
  - Ils ciblent généralement les gouvernements étrangers, les groupes terroristes et les grandes entreprises.
  - Plusieurs pays du monde financent, dans une certaine mesure, des activités de piratage.

Cybercriminels contre héros de la cybersécurité

Spécialistes de la cybersécurité

Contrecarrer les plans des cybercriminels est une tâche difficile.

Les entreprises, les gouvernements et les organisations internationales commencent à mener des actions coordonnées pour limiter ou contrer les attaques des cybercriminels : coordonnées :

- **Base de données de vulnérabilités :** la base de données **Common Vulnerabilities and Exposures (CVE**) est un exemple de base de données développée au niveau national.
  - La base de données CVE a été développée afin de divulguer toutes les vulnérabilités connues. http://www.cvedetails.com/
- **Systèmes d'alerte :** le projet **Honeynet** est un exemple de système d'alerte (Early Warning System).
  - Le projet propose un HoneyMap qui affiche les attaques en temps réel. https://www.honeynet.org/node/960
- **Partage d'informations sur la sécurité informatique : InfraGard** est un exemple de partage à grande échelle d'informations sur la sécurité informatique.
  - Le programme InfraGard est un partenariat entre le FBI et le secteur privé.
  - Les participants partagent des informations et des renseignements pour éviter les attaques informatiques hostiles. https://www.infragard.org/

Cybercriminels contre héros de la cybersécurité

Spécialistes de la cybersécurité (suite)

- **Normes ISM :** les normes ISO 27000 constituent un exemple en matière de gestion de la sécurité de l'information.
  - Les normes fournissent un cadre qui permet d'implémenter des mesures de cybersécurité dans une entreprise. http://www.27000.org/
- **Nouvelles lois :** le groupe **ISACA** suit les lois adoptées liées à la cybersécurité.
  - Ces lois peuvent traiter de la **protection** de la **vie privée** à la protection de la **propriété intellectuelle**.
  - Par exemple on trouve les lois suivantes :
    - Cybersecurity Act, Federal Exchange Data Breach Notification Act
    - et Data Accountability and Trust Act.

http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Les outils pour contrer la cybercriminalité

1.3 Menaces sur internet

Les menaces envers le royaume

Les domaines des menaces

- Sur internet circulent **beaucoup** de **données** personnelles et professionnelles
- Et les informaticiens savent que c'est à partir de ces données qu'ils pourront
  - créer de grandes entreprises,
  - fournir des services
  - et protéger les utilisateurs contre les cyberattaques.
- Toutefois, ils sont **conscients** de la **dangerosité** des données lorsqu'elles sont utilisées contre des individus.
- **Une menace de cybersécurité est la possibilité qu'un événement nuisible, tel qu'une attaque, survienne.**
- **Une vulnérabilité informatique est une faiblesse qui rend une cible susceptible aux attaques.**
- Les menaces de cybersécurité sont particulièrement dangereuses pour certains secteurs d'activité et le type de données qu'ils collectent et protègent.

Les menaces envers le royaume

Les domaines des menaces (suite)

Dans les entreprises bien établies, on peut par exemple trouver les sources de données suivantes :

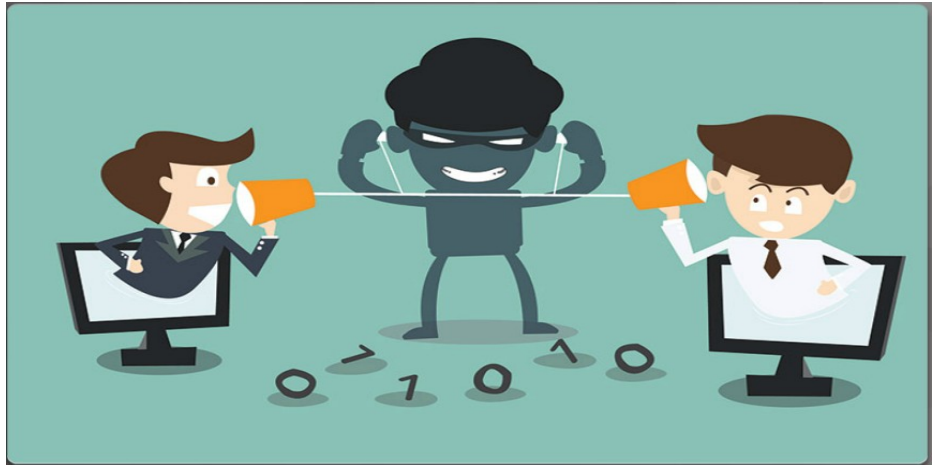
- **Informations personnelles**
- **Dossiers médicaux**
- **Dossiers scolaires**
- **Dossiers professionnels et financiers**

Les menaces envers le royaume

Les domaines des menaces (suite)

Les **services réseau** comme DNS, HTTP et les bases de données en ligne sont des **cibles privilégiées** pour les **cybercriminels**.

- Les criminels utilisent des **outils d'interception** des paquets pour capturer les flux de données sur un réseau.
- Ces outils surveillent et enregistrent toutes les informations qui transitent sur un réseau.
- Les criminels peuvent aussi utiliser des **appareils non autorisés**, comme des points d'accès Wi-Fi non protégés.
- La **falsification de paquets** interfère avec une communication réseau établie en créant des paquets qui semblent faire partie d'une communication.

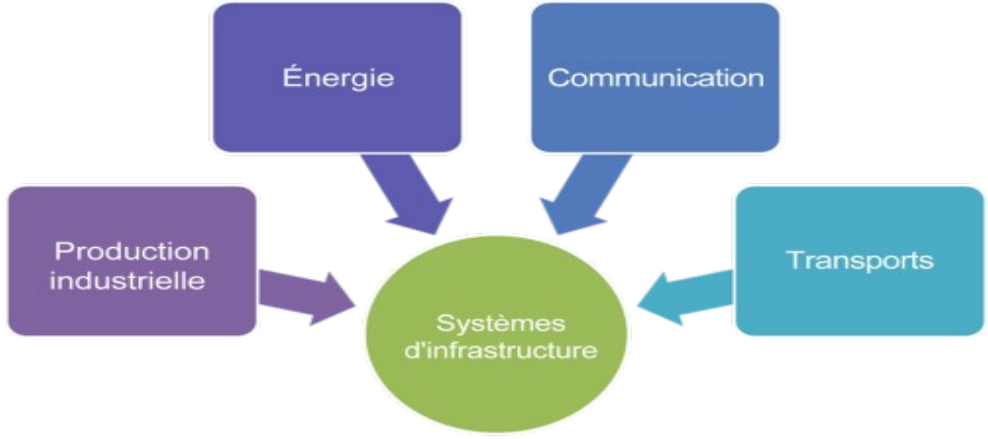


Les menaces envers le royaume

Les domaines des menaces (suite)

Le monde de l'internet est divisé en **plusieurs secteurs** :

- **Production**
  - Machines électriques
  - Automatisation et machines programmables
  - SCADA : Supervisory Control And Data Acquisition,...
- **Production et distribution d'énergie**
  - Distribution électrique et réseaux intelligents
  - Pétrole et gaz,...
- **Communication**
  - Téléphone
  - E-mail
  - Messagerie,...
- **Systèmes de transport**
  - Transport aérien
  - Transport ferroviaire
  - Transport routier,...



Les menaces envers le royaume

Les domaines des menaces (suite)

- Au **niveau personnel**, tout le monde doit protéger son identité, ses données et ses appareils informatiques.
- Au **niveau professionnel**, chaque collaborateur est responsable de la protection de la réputation, des données et des clients de l'entreprise.
- Au **niveau national**, la sécurité nationale ainsi que la sécurité et le bien-être des citoyens sont en jeu.

Remarque

- Les efforts consacrés à la protection du mode de vie des citoyens entrent souvent en conflit avec le respect de leur vie privée.

1.4 Les forces obscures de la cybersécurité

Les forces obscures de la cybersécurité

La propagation des forces obscures

Les attaques peuvent provenir de l'intérieur d'une entreprise ou de l'extérieur :

Menaces internes pour la sécurité

- Un utilisateur interne, par exemple un employé ou un partenaire contractuel, peut **accidentellement ou intentionnellement altérer ou supprimer des données** ; ou même endommager un équipement.
- **Les menaces internes sont susceptibles d'entraîner des dégâts plus importants que les menaces externes,**
  - car les utilisateurs internes disposent d'un accès direct au bâtiment et à l'équipement de l'infrastructure.
- Les hackers internes connaissent généralement le réseau de l'entreprise, ses ressources et ses données confidentielles.
- Ils connaissent aussi parfois les mesures de sécurité, les politiques et les privilèges administratifs de niveau supérieur.

Menaces externes pour la sécurité

- Les menaces externes **provenant de hackers amateurs ou expérimentés** tirent parti des vulnérabilités des appareils réseau ou font appel à des techniques d'ingénierie sociale pour accéder aux données.
- Les attaques externes exploitent les faiblesses ou les vulnérabilités pour accéder aux ressources internes.

Les forces obscures de la cybersécurité

La propagation des forces obscures (suite)

Vulnérabilités des terminaux mobiles :

- De nos jours, les terminaux mobiles comme les smartphones, les tablettes et les milliers d'autres appareils, remplacent parfaitement les ordinateurs classiques ou viennent les compléter.
- De plus en plus de personnes utilisent ces terminaux pour accéder aux informations de l'entreprise.
- La tendance du **BYOD** (Bring Your Own Device) **gagne du terrain**.
- Or, comme il est impossible de gérer et de mettre à jour de façon centralisée ces terminaux mobiles, **les entreprises** qui autorisent leur utilisation sur leur réseau **s'exposent** à de grands **risques**.

Les forces obscures de la cybersécurité

La propagation des forces obscures (suite)

- **L'émergence de l'Internet des objets :** l'Internet des objets (IoT) est l'ensemble de technologies qui permettent de connecter différents appareils à Internet.
- **Les technologies IoT permettent de connecter des milliards d'appareils à Internet**,
- notamment des appliances, des verrous, des moteurs et des appareils de divertissement, ...
- Cette technologie accroît le volume de données à protéger.
- Les utilisateurs accèdent à ces appareils à distance, ce qui augmente le nombre de réseaux à protéger.
- Avec l'émergence de l'IoT, on doit protéger et gérer encore plus de données.
- Toutes ces **connexions**, associées à **l'augmentation** de la capacité de **stockage** et aux services de stockage via le **cloud** et la **virtualisation**, ont engendré une croissance exponentielle des données.

Les forces obscures de la cybersécurité

La propagation des forces obscures (suite)

Impact du Big Data : le Big Data est la conséquence de grands ensembles de données complexes qui rendent les applications classiques de traitement des données inadéquates.

Le Big Data présente des challenges et offre des opportunités s'articulant autour de trois dimensions :

- Le **volume** ou la **quantité** de données
- La **vélocité** ou la **vitesse** des données
- La **variété** ou la plage de **types** et de **sources** de données

Par conséquent, les **systèmes** d'entreprise doivent être **profondément remaniés** :

- les solutions de sécurité doivent être repensées et des mises à niveau substantielles des technologies et des pratiques s'imposent.

En outre, les gouvernements et les différents secteurs d'activités mettent en œuvre davantage de réglementations et de règles qui exigent une meilleure protection des données et l'application de contrôles de sécurité afin de protéger le Big Data.

La propagation des forces obscures

La sophistication des forces obscures

Armes avancées : APT (Advanced Persistent Threat)

- Une menace persistante avancée est un **piratage informatique continu et non détecté** ciblant un objet spécifique.
- Les criminels choisissent habituellement une attaque persistante avancée pour des **raisons économiques** ou **politiques**.
- Les attaques basées sur des algorithmes assurent le suivi des données autodéclarées du système, comme la quantité d'énergie utilisée par un ordinateur, et les utilisent pour choisir une cible ou lancer de fausses alertes.
- Les attaques basées sur des algorithmes sont plus sournoises, car elles exploitent des conceptions utilisées pour multiplier les économies d'énergie, diminuer les pannes du système et améliorer l'efficacité.
- Sélection intelligente des victimes : les attaques sélectionnaient des cibles faciles ou les victimes les plus vulnérables.
- La plupart des attaques les plus sophistiquées sont lancées uniquement si le hacker parvient à reproduire les signatures de la victime ciblée.

La propagation des forces obscures

La sophistication des forces obscures (Suite)

Une portée plus large et un effet domino

- La gestion des identités fédérées se définit de la manière suivante : les utilisateurs de plusieurs entreprises peuvent utiliser les mêmes informations d'identification pour accéder aux réseaux de toutes les entreprises du groupe.
- La gestion des identités fédérées a pour objectif de partager automatiquement les informations d'identification à plus grande échelle.
- Pour protéger les identités fédérées, il convient généralement de relier les autorisations de connexion à un appareil autorisé.

La propagation des forces obscures

La sophistication des forces obscures (suite)

Les implications en matière de sécurité

- L'action des forces obscures de la cybersécurité peut avoir de nombreuses conséquences en matière de sécurité.
- **Par exemple**, les centres d'appel aux États-Unis sont vulnérables aux cyberattaques qui interrompent les réseaux de communication de secours (911), compromettant ainsi la sécurité publique.
- Une attaque téléphonique par déni de service (TDoS) consiste à saturer un réseau téléphonique cible d'appels téléphoniques afin d'empêcher les appels légitimes d'aboutir.
- Les centres d'appels d'urgence de nouvelle génération sont vulnérables car ils utilisent des systèmes VoIP au lieu des lignes terrestres classiques.

Une meilleure reconnaissance des menaces de cybersécurité

- Au début, les systèmes de défense contre les cyberattaques n'étaient pas nombreux. Un lycéen intelligent ou un script kiddie étaient capables accéder à des systèmes.
- Désormais, les pays du monde entier sont conscients de la menace des cyberattaques.
- Les cyberattaques arrivent désormais en tête de la liste des principales menaces pour la sécurité nationale et économique de la plupart des pays.

1.5 Augmenter le nombre d’experts en cybersécurité

Augmenter le nombre de héros

Un cadre pour l'embauche de collaborateurs experts en cybersécurité

Gérer le manque de spécialistes en cybersécurité

- Plusieurs pays ont créé un cadre pour les entreprises et les organisations qui recherchent des professionnels de la cybersécurité.
- Ce cadre leur permet d'identifier les principaux types de responsabilités, de postes et de compétences recherchés.

Les sept catégories de experts de la cybersécurité

Le cadre pour l'embauche de collaborateurs classe les postes du domaine de la cybersécurité en sept catégories.

- **Exploiter et maintenir en conditions opérationnelles** : assurer l'assistance, l'administration et la maintenance requises pour garantir la performance et la sécurité du système informatique.
- **Protéger et défendre** : identifier, analyser et réduire les menaces pour les systèmes et les réseaux internes.
- **Enquêter** : enquêter sur les événements informatiques et/ou les cyberattaques impliquant des ressources informatiques.
- **Collecter et exploiter** : collecter des informations sur les opérations frauduleuses, les dénis de service et la cybersécurité.

Augmenter le nombre de héros

Un cadre pour l'embauche de collaborateurs experts en cybersécurité (suite)

- **Analyser** : examen et évaluation ultra spécialisés des informations de cybersécurité entrantes afin de déterminer si elles sont utiles.
- **Surveiller et développer** : leadership, encadrement et direction nécessaires pour assurer l'efficacité des experts en cybersécurité.
- **Provisionner en toute sécurité** : conceptualisation, conception et création de systèmes informatiques sécurisés.

Chaque catégorie compte plusieurs domaines de spécialité.

Ces domaines de spécialité définissent ensuite les divers types de postes les plus courants en cybersécurité.

Augmenter le nombre de héros

Les communautés de cybersécurité en ligne

Organisations professionnelles

- Il arrive souvent que les spécialistes de la cybersécurité travaillent en collaboration. Les entreprises technologiques internationales parrainent souvent des ateliers et des conférences.

1.6 Résumé de la première partie

Résumé de la première partie

Résumé

- Au cours de ce chapitre, nous avons expliqué la structure de l'univers de la cybersécurité et pourquoi il continue à gagner du terrain avec l'augmentation du nombre de données et d'informations à protéger.
- Nous avons présenté les motivations des cybercriminels.
- Nous avons montré l'étendue des forces obscures liée aux transformations techniques toujours plus nombreuses qui se déroulent partout dans le monde.
- Nous avons expliqué comment devenir un expert en cybersécurité et lutter contre les cybercriminels qui nourrissent les forces obscures.
- Nous avons détaillé quelles étaient les ressources disponibles pour augmenter le nombre de héros.
- Nous avons démontré que les professionnels de la cybersécurité doivent avoir les mêmes compétences que les cybercriminels.