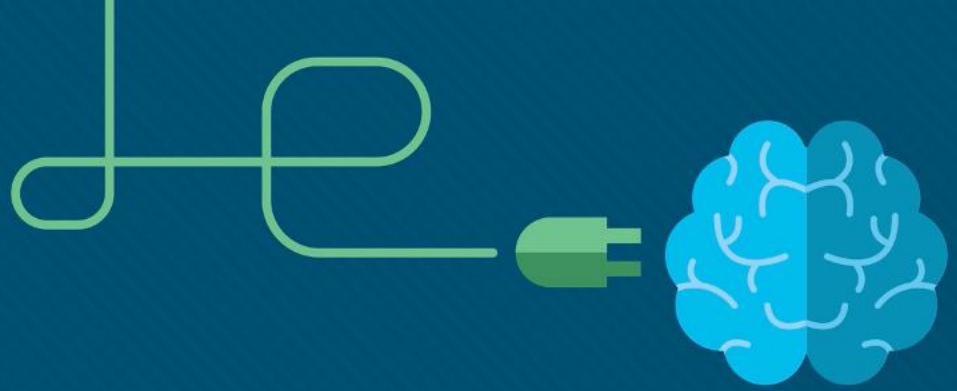


Module 1 : Introduction à la Cybersécurité

Introduction à la Cybersécurité

Objectifs du module

Titre du module : Introduction à la cybersécurité

Objectifs du module: Expliquer les bases de la sécurité en ligne, y compris la définition de la cybersécurité et son impact potentiel.

Titre du Rubrique	Objectif du Rubrique
Le monde de la cybersécurité	Expliquer le concept de cybersécurité et son impact potentiel
Données de l'entreprise	Identifier les types d'informations sensibles que les hackers peuvent utiliser pour violer votre vie privée et/ou nuire à votre réputation, identifier les failles qui leur permettent d'accéder à ces informations et comprendre pourquoi elles intéressent les cybercriminels
Données volées	Expliquer ce que sont les données d'entreprise et les raisons pour lesquelles elles doivent être protégées
Cybercriminels	Décrire le profil des cybercriminels et ce qu'ils recherchent
Guerre cybernétique	Expliquer ce qu'est la guerre cybernétique et les raisons qui incitent les pays et gouvernements à recourir aux professionnels de la cybersécurité pour les aider à protéger leurs citoyens et leurs infrastructures

1.1 Le monde de la Cybersécurité

Qu’est-ce que la Cybersécurité ?

- La cybersécurité est l'effort continu visant à protéger les individus, les organisations et les gouvernements contre les attaques numériques en protégeant les systèmes et les données en réseau des utilisations non autorisées ou d'un quelconque dommage.

- **Personnel :** À titre personnel, vous devez protéger votre identité, vos données et vos appareils informatiques.

- **Professionnel :** Au niveau professionnel, il est de la responsabilité de chacun de protéger la réputation, les données et les clients de l'organisation.

- **Gouvernement** : À mesure que de plus en plus d'informations numériques sont collectées et partagées, leur protection devient encore plus vitale au niveau du gouvernement, où la sécurité nationale, la stabilité économique et la sécurité et le bien-être des citoyens sont en jeu.

1.1.2 Protection de vos Données Personnelles

- Les données personnelles sont toutes les informations qui peuvent être utilisées pour vous identifier, et elles peuvent exister à la fois hors ligne et en ligne.

- **Identité hors ligne**
  - Il s'agit de la personne que vous présentez tous les jours à la maison, à l'école ou au travail.
  - Ainsi, votre famille et vos amis connaissent des informations sur votre vie personnelle, notamment votre nom complet, votre âge et votre adresse.
  - Il est important de ne pas négliger l'importance de la sécurisation de votre identité hors ligne.
  - Les usurpateurs d'identité peuvent facilement voler vos données sous votre nez lorsque vous ne regardez pas !

- **Identité en ligne**
  - Ce n'est pas qu'un nom, c'est qui vous êtes et comment vous vous présentez aux autres en ligne.
  - Il inclut le nom d'utilisateur ou l'alias que vous utilisez pour vos comptes en ligne, ainsi que l'identité sociale que vous établissez et présentez sur les communautés en ligne et les sites web.
  - Vous devez veiller à limiter la quantité d'informations personnelles que vous divulguez via votre identité en ligne.

Vos Données

- Les données personnelles correspondent à toutes les informations vous concernant, notamment votre nom, votre numéro de sécurité sociale, votre numéro de permis de conduire, votre date et votre lieu de naissance, le nom de jeune fille de votre mère et même les photos ou les messages que vous échangez avec votre famille et vos amis ;
- Les cybercriminels peuvent utiliser ces informations sensibles pour vous identifier et se faire passer pour vous, portant atteinte à votre vie privée et pouvant potentiellement nuire gravement à votre réputation ;
- Les hackers peuvent accéder à vos données personnelles en les enregistrant :

Dossiers médicaux	Chaque fois que vous consultez un médecin, des informations personnelles concernant votre santé physique et mentale et votre bien-être sont ajoutées à vos dossiers médicaux électroniques. Étant donné que la majorité de ces dossiers sont enregistrés en ligne, vous devez être conscients des informations médicales que vous partagez. Et ces dossiers vont au-delà des limites du cabinet du médecin.
Dossiers scolaires	Les dossiers scolaires contiennent des informations sur vos diplômes et vos résultats. Cependant, ces dossiers peuvent également inclure vos coordonnées, vos registres de présence, les rapports disciplinaires, les dossiers de santé et de vaccination ainsi que tout dossier d'éducation spéciale, y compris les programmes d'éducation individualisés (PEI).
Dossier d'emploi et dossier financier	Les données sur l'emploi peuvent être précieuses pour les hackers s'ils peuvent collecter des informations sur vos anciens emplois ou même sur le compte-rendu de vos performances actuelles. Vos dossiers financiers peuvent contenir des informations sur vos revenus et vos dépenses. Vos dossiers fiscaux peuvent inclure des chèques, des relevés de carte de crédit, votre cote de crédit et vos coordonnées bancaires.

Où sont mes Données ?

Imaginez qu'hier, vous avez partagé quelques photos de votre premier jour de travail avec quelques-uns de vos amis proches, mais cela ne devrait pas poser de problème, n'est-ce pas ? Voyons…

- Vous avez pris des photos au travail sur votre téléphone portable.
- Des copies de ces photos sont désormais disponibles sur votre appareil mobile.
- Vous les avez partagées avec cinq amis proches, qui vivent dans divers endroits à travers le monde.
- Tous vos amis ont téléchargé les photos et ont maintenant des copies de vos photos sur leurs appareils.
- L'un de vos amis était si fier qu'il a décidé de publier et de partager vos photos en ligne.
- Les photos ne sont plus uniquement sur votre appareil.
- En fait, elles se sont retrouvées sur des serveurs situés dans différentes parties du monde et des personnes que vous ne connaissez même pas ont maintenant accès à vos photos.

Quoi de plus ?

- Ce n'est qu'un exemple qui nous rappelle que chaque fois que nous collectons ou partageons des données personnelles, nous devons tenir compte de notre sécurité.
- Il existe différentes législations qui protègent votre confidentialité et vos données dans votre pays.
- Mais est-ce que vous savez où sont vos données ?
  - Après un rendez-vous, le médecin met à jour votre dossier médical.
    - À des fins de facturation, ces informations peuvent être partagées avec la compagnie d'assurance.
    - Dans ce cas, votre dossier médical, ou une partie de celui-ci, est désormais accessible par la compagnie d'assurance.
  - Les cartes de fidélité en magasin peuvent être un moyen pratique d'économiser de l'argent sur vos achats.
    - Cependant, le magasin utilise cette carte pour créer un profil de votre comportement d'achat, qu'il peut ensuite utiliser pour vous proposer des offres spéciales de ses partenaires marketing.

Périphériques Intelligents

- Réfléchissez à la fréquence à laquelle vous utilisez vos équipements informatiques pour accéder à vos données personnelles.
- À moins que vous n'ayez choisi de recevoir des relevés sur papier, vous accédez probablement aux copies numériques des relevés de compte bancaire via le site web de votre banque.
- Et lorsque vous payez une facture, il est fort probable que vous ayez transféré les fonds requis via une application bancaire mobile.
- Mais en plus de vous permettre d'accéder à vos informations, les appareils informatiques peuvent désormais également générer des informations vous concernant.
- Les technologies connectées telles que les montres connectées et les moniteurs d'activité collectent vos données pour la recherche clinique, la surveillance de l'état de santé des patients et le suivi de leur condition physique et de leur bien-être.
- À mesure que le marché mondial des bracelets d'activité se développe, le risque pour vos données personnelles augmente également.

Usurpation d'identité

- Non content de voler votre argent pour un gain financier à court terme, les cybercriminels s'investissent dans l'usurpation d'identité à long terme.

Le vol médical

- L'augmentation des coûts médicaux a entraîné une augmentation des vols d'identité médicale, les cybercriminels volant les assurances médicales pour en profiter eux-mêmes.
- Dans ce cas, tous les actes médicaux effectués en votre nom sont enregistrés dans votre dossier médical.

Bancaire

- Le vol de données privées peut aider les cybercriminels à accéder aux comptes bancaires, aux cartes de crédit, aux profils sociaux et à d'autres comptes en ligne.
- Armé de ces informations, un voleur d'identité pourrait produire une fausse déclaration de revenus et percevoir le remboursement.
- Ils peuvent même contracter des prêts en votre nom et ruiner votre cote de crédit (et votre vie au passage).

Qui d'autre veut mes Données ?

- Il n'y a pas que les criminels qui recherchent vos données personnelles.
- Le tableau décrit les autres entités intéressées par votre identité en ligne et explique pourquoi.

Votre fournisseur d'accès Internet (FAI)	Votre FAI suit votre activité en ligne et, dans certains pays, il peut vendre ces données à des annonceurs pour faire un profit.Dans certaines circonstances, Ils peuvent être légalement tenus de partager vos informations avec des agences de surveillance ou des autorités gouvernementales.
Annonceurs	La publicité ciblée fait partie de l'expérience Internet. Les annonceurs surveillent et suivent vos activités en ligne, telles que vos habitudes d'achat et vos préférences personnelles, et vous envoient des publicités ciblées.
Moteurs de recherche et plateformes de réseaux sociaux	Ces plateformes collectent des informations sur votre sexe, votre géolocalisation, votre numéro de téléphone et vos idéaux politiques et religieux en fonction de vos recherches et de votre identité en ligne. Ces informations sont ensuite vendues à des annonceurs pour générer un profit.
Les sites web que vous visitez	Les sites web utilisent des cookies pour suivre vos activités afin de fournir une expérience plus personnalisée.Mais cela laisse une trace de données liée à votre identité en ligne qui peut souvent se retrouver entre les mains des annonceurs !

1.2 Données d'entreprise

Les Différents types de Données d’entreprise

Les données traditionnelles sont généralement générées et gérées par toutes les organisations, grandes et petites.

- Il comprend les éléments suivants:
  - **Les données transactionnelles** telles que les informations relatives à l'achat et à la vente, aux activités de production et aux opérations organisationnelles de base telles que les informations utilisées pour prendre des décisions en matière d'emploi.

  - **La propriété intellectuelle**, comme les brevets, les marques déposées et les plans produit, permet à une entreprise d’avoir un avantage économique sur ses concurrents. Ces informations sont souvent considérées comme un secret commercial et leur perte peut s'avérer désastreuse pour l'avenir de l'entreprise.

  - **Les données financières** tels que les comptes de résultat, les bilans comptables et les tableaux de trésorerie d'une entreprise, qui donnent un aperçu de la santé de l'entreprise.

Différents types de Données d'entreprise (Suite)

Internet des objets et Big Data

- **L'IoT** est un vaste réseau d'objets physiques, tels que des capteurs, des logiciels et d'autres équipements.
- Toutes ces « objets » sont connectés à Internet, avec la possibilité de collecter et de partager des données.
- Les options de stockage des données se multiplient grâce au cloud et à la virtualisation.
- L'émergence de l'IOT a entraîné une croissance exponentielle des données, créant un nouveau domaine d'intérêt dans la technologie et les affaires appelé "Big Data".

Le Cube

Ce modèle de sécurité comporte trois dimensions :

1. **Les principes fondamentaux de la protection des systèmes d'information.**

- **La confidentialité** est un ensemble de règles qui empêche la divulgation d'informations sensibles à des personnes, des ressources et des processus non autorisés. Les méthodes visant à garantir la confidentialité comprennent le chiffrement **des données**, **la vérification de l'identité** et **l'authentification à deux facteurs**.

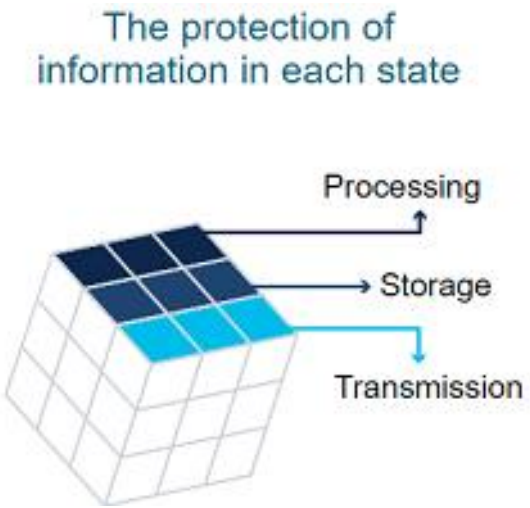
- **L'intégrité** garantit que les informations ou les processus du système sont protégés contre toute modification intentionnelle ou accidentelle . Une façon de garantir l'intégrité consiste à utiliser une fonction de hachage ou une **somme de contrôle**.

- **La disponibilité** signifie que les utilisateurs autorisés peuvent accéder aux systèmes et aux données quand et où ils en ont besoin, tandis que ceux qui ne répondent pas aux conditions établies ne le sont pas. La maintenance des équipements , la réparation du matériel , **la mise à jour des systèmes d'exploitation et des logiciels** , **et la création de sauvegardes permettent de garantir la disponibilité du réseau** et **des données pour les utilisateurs autorisés** .

Le Cube (suite)

2. **La protection des informations dans chacun de ses états possibles.**

- **Le traitement** fait référence aux données qui sont utilisées pour effectuer une opération telle que la mise à jour d'un enregistrement de base de données (données en cours).
- **Le stockage** fait référence aux données stockées dans la mémoire ou sur un périphérique de stockage permanent tel qu'un disque dur, un disque SSD (solid-state drive) ou une clé USB (données au repos).
- **La transmission** fait référence aux données qui voyagent entre les systèmes d'information (données en transit).



Le Cube (suite)

3. **Les mesures de sécurité utilisées pour protéger les données.**

- **La sensibilisation, la formation et** l'éducation sont les mesures mises en place par une entreprise pour s'assurer que les utilisateurs connaissent les menaces potentielles pour la sécurité et les mesures qu'ils peuvent prendre pour protéger les systèmes d'information.

- **La technologie** fait référence aux solutions logicielles et matérielles conçues pour protéger les systèmes d'information tels que les pare-feux, qui surveillent en permanence votre réseau à la recherche d'éventuels incidents malveillants.

- **Les politiques et procédures** font référence aux contrôles administratifs qui servent de base à la mise en œuvre du contrôle des informations par une entreprise, tels que les plans de réponse aux incidents et les directives de bonnes pratiques.

Est-ce réel ?

- Oui, le phishing est très courant et fonctionne souvent.
- Par exemple, en août 2020, la marque d'élite de jeux Razer a subi une violation de données qui a révélé les informations personnelles d'environ 100 000 clients.
- Un consultant en sécurité a découvert qu'un cluster cloud (un groupe de serveurs liés fournissant le stockage de données, les bases de données, le réseau et les logiciels via Internet) était mal configuré et exposait un segment de l'infrastructure Razer à l'Internet public, entraînant une fuite de données.
- Il a fallu plus de trois semaines à Razer pour protéger l'instance cloud contre l'accès public, période pendant laquelle les cybercriminels ont eu accès à des informations sur les clients qui auraient pu être utilisées dans des attaques par ingénierie sociale et des fraudes, comme celle que vous venez de découvrir.
- Les entreprises doivent donc adopter une approche proactive de la sécurité du cloud pour s'assurer que les données sensibles sont sécurisées.

Violations de Sécurité des Données

- Les conséquences d'une faille de sécurité des données sont graves, mais elles sont de plus en plus courantes.
- L'IoT connecte de plus en plus d'équipements, créant de plus en plus d'opportunités d'attaques pour les cybercriminels.
- Deux failles bien connues de la sécurité des données sont les suivantes :

  - **Le botnet Persirai**
    - En 2017, un botnet de l'Internet des objets (IoT), Persirai, a ciblé plus de 1000 modèles différents de caméras IP (Internet Protocol), accédant aux ports ouverts pour injecter une commande qui force les caméras à se connecter à un site qui leur faisait installer un malware.
    - Une fois que le malware était téléchargé et exécuté, il se supprimait et pouvait donc s'exécuter dans la mémoire pour éviter d'être détecté.
    - Plus de 122 000 de ces caméras de différents fabricants ont été piratées et utilisées pour mener des attaques par déni de service distribué (DDoS), à l'insu de leurs propriétaires.
    - Une attaque DDoS se produit lorsque plusieurs périphériques infectés par des malwares inondent les ressources d'un système ciblé.

Les Failles de la Sécurité des Données (suite)

- **Equifax Inc.**
  - En septembre 2017, Equifax, une agence d'évaluation du crédit à la consommation aux États-Unis, a annoncé publiquement une violation de données : des hackers ont pu exploiter une vulnérabilité de son application web pour accéder aux données personnelles sensibles de millions de clients.
  - En réponse à cette faille, Equifax a créé un site web dédié qui a permis aux clients d'Equifax de déterminer si leurs informations ont été compromises.
  - Cependant, en utilisant un nouveau nom de domaine à la place d'un sous-domaine d'equifax.com, les cybercriminels ont pu créer des sites web non autorisés avec des noms similaires.
  - Ces sites web étaient utilisés pour inciter les clients à fournir des informations personnelles.
  - Les hackers pouvaient utiliser ces informations pour usurper l'identité d'un client.
  - Dans de tels cas, il serait très difficile pour le client de prouver le contraire, étant donné que le hacker a également accès à ses informations personnelles.

Conséquences d’une Brèche dans la Sécurité

Ces exemples montrent que les conséquences potentielles d'une faille de sécurité peuvent être

Dommages sur la réputation	Une faille de sécurité peut avoir un impact négatif à long terme sur la réputation d'une entreprise qui a mis des années à se construire. Les clients, en particulier ceux qui ont été affectés par la faille, doivent en être informés et peuvent demander une indemnisation et/ou se tourner vers un concurrent fiable et sécurisé. Les employés peuvent également choisir de partir en raison d'un scandale. Selon la gravité d'une faille, la restauration de la réputation d'une entreprise peut prendre beaucoup de temps.
Vandalisme	Un hacker ou un groupe de hackers peut vandaliser le site web d'une entreprise en publiant de fausses informations. Ils peuvent même apporter quelques modifications mineures au numéro de téléphone ou à l'adresse de votre entreprise, ce qui peut être plus difficile à détecter.Dans les deux cas, le vandalisme en ligne peut dépeindre un manque de professionnalisme et avoir un impact négatif sur la réputation et la crédibilité de votre entreprise.
Vol	Une violation de données implique souvent un incident au cours duquel des données personnelles sensibles ont été volées. Les cybercriminels peuvent rendre ces informations publiques ou les exploiter pour voler l'argent et/ou l'identité d'une personne.
Perte de revenus	L'impact financier d'une faille de sécurité peut être dévastateur. Par exemple, les hackers peuvent fermer le site web d'une entreprise, empêchant les actions commerciales en ligne. La perte de toutes ces informations peut entraver la croissance et l’expansion de l’entreprise. Elle peut nécessiter des investissements supplémentaires dans l'infrastructure de sécurité de l'entreprise. Et n'oublions pas que les entreprises s'exposent à de lourdes amendes ou sanctions si elles ne protègent pas les données en ligne.
Propriété intellectuelle endommagée	Une faille de sécurité peut également avoir un impact dévastateur sur la compétitivité d'une entreprise, en particulier si les hackers parviennent à mettre la main sur des documents confidentiels, des secrets commerciaux et la propriété intellectuelle.

1.3 Quelles Données Ciblées?

Scénario 1

- Aujourd'hui, les failles de sécurité sont trop courantes, les hackers trouvant constamment de nouvelles façons innovantes d'infiltrer les entreprises à la recherche d'informations précieuses.
- Ces derniers suivent les scénarios suivants:

Scenario 1:

- Selon nos sources, une chaîne d'hôtels bien connue qui opère à travers le monde a signalé une violation de données massive, avec les informations personnelles de plus de trois millions de clients exposées aux hackers.
- L'hôtel a découvert que des hackers avaient eu accès à sa base de données clients en utilisant les informations de connexion d'un de ses collaborateurs.
- À ce stade, l'hôtel ne pense pas que les hackers aient pu accéder aux mots de passe d'un quelconque compte ou aux informations financières.
- Les clients récents sont encouragés à consulter le site web de la chaîne hôtelière pour voir s'ils ont été affectés par cette faille.

Scénario 2

Scenario 2:

- L'équipe d'@Apollo est inquiète. Les plateformes d'e-learning deviennent des cibles de choix pour les hackers alors que de plus en plus d'entreprises adoptent l'apprentissage numérique.
- Une plate-forme de formation en ligne populaire a admis avoir exposé les données personnelles de millions de ses étudiants (dont beaucoup de mineurs) dans une base de données cloud accessible au public.
- Les hackers ont pu accéder directement aux noms, aux adresses e-mail, aux numéros de téléphone et aux détails d'inscription des étudiants sur Internet !
- Bien qu'on ne sache pas exactement ce que les hackers ont fait avec ces informations, on peut affirmer sans se tromper qu'ils disposent de tout ce dont ils ont besoin pour mener des attaques de phishing ou de malwares à grande échelle.

Les Principaux Enseignements

- Une faille de sécurité est un incident qui entraîne un accès non autorisé aux données, aux applications, aux services ou aux équipements, exposant des informations privées que les hackers peuvent utiliser à des fins financières ou autres.
- Mais il existe de nombreuses façons de vous protéger, vous et votre entreprise.
- Il est important d'être conscient des cybermenaces courantes et de rester vigilant afin de ne pas devenir la prochaine victime.

Plus d'infos

Recherchez d'autres exemples de failles de sécurité récentes.

- Dans chaque cas, pouvez-vous identifier :
  - qu'est-ce qui a été pris ?
  - quels exploits les hackers ont-ils utilisés ?
  - quelles mesures pourraient être prises pour empêcher la faille de se reproduire à l’avenir ?

1.4 Cybercriminels

Les Différents types d’agresseurs

- Qu'ils soient amateurs ou professionnels, les hackers sont prêts à tout pour mettre la main sur vos informations personnelles.
- Ils sont souvent classés comme attaquants au chapeau blanc, au chapeau gris ou au chapeau noir.

Hackers amateurs

- Le terme « script kiddies » est apparu dans les années 1990 et désigne les hackers amateurs ou inexpérimentés qui utilisent des outils ou des instructions disponibles sur Internet pour lancer des attaques.
- Certains script kiddies sont simplement curieux, d'autres essaient de démontrer leurs compétences et de causer du tort.
- Bien que ces hackers « chapeau blanc » utilisent des outils de base, leurs attaques peuvent avoir des conséquences dévastatrices.

Types d'attaquants (suite)

Pirates informatiques

- Ce groupe d'attaquants s'introduit dans les systèmes informatiques ou les réseaux pour y accéder.

- En fonction de l'intention de leur intrusion, ils peuvent être classés comme suit :
  - **Les attaquants au chapeau blanc** s'introduisent dans les réseaux ou les systèmes informatiques pour identifier les faiblesses afin d'améliorer la sécurité d'un système ou d'un réseau.Ils effectuent ces intrusions sur autorisation et tous les résultats sont signalés au propriétaire.

  - **Les hackers au chapeau gris** peuvent chercher des vulnérabilités dans un système, mais ils ne signaleront leurs découvertes aux propriétaires d'un système que si cela coïncide avec leur objectif. Ils peuvent même publier des détails sur la vulnérabilité sur Internet afin que d'autres attaquants puissent l'exploiter.

  - **Les attaquants au chapeau noir** ils profitent de toute vulnérabilité à des fins illégales, financières ou politiques.

Types d'attaquants (suite)

Les hackers organisés

- Ces pirates incluent des organisations de cybercriminels, des hacktivistes, des terroristes et des pirates financés par des gouvernements.
- Ils sont très sophistiqués et organisés et ils peuvent même offrir des services de cybercrime à d'autres criminels.
- Les hacktivistes effectuent des déclarations politiques pour sensibiliser sur les questions qui leur sont importantes.
- Les attaquants parrainés par un État rassemblent des renseignements ou commettent des sabotages au nom de leur gouvernement.
- Ces agresseurs sont généralement très bien formés et bien financés et leurs attaques sont axées sur des objectifs spécifiques qui profitent à leur gouvernement.

Menaces Internes et Externes

- Les cyberattaques peuvent provenir de l'intérieur ou de l'extérieur de l'entreprise.

- **Interne**
  - Les collaborateurs, les contractuels ou les partenaires de confiance peuvent accidentellement ou intentionnellement :
    - mal gérer des données confidentielles
    - faciliter les attaques externes en connectant un support USB infecté au système informatique de l'organisation
    - inviter des malwares sur le réseau de l'entreprise en cliquant sur des e-mails ou des sites web malveillants.
    - menacer le fonctionnement des serveurs internes ou des appareils de l'infrastructure réseau

- **Externe**
  - Les hackers amateurs ou expérimentés en dehors de l'entreprise peuvent :
    - exploiter les vulnérabilités du réseau
    - utiliser des accès non autorisés à vos données ou à vos appareils informatiques
    - utiliser l'ingénierie sociale pour obtenir un accès non autorisé aux données de l'entreprise.

1.5 Guerre Cybernétique

Un signe des temps (Stuxnet)

- Un exemple d'attaque parrainée par un État est le logiciel malveillant Stuxnet, conçu non seulement pour détourner des ordinateurs ciblés, mais aussi pour endommager physiquement des équipements contrôlés par des ordinateurs !

- Regardez une courte vidéo sur le cas de Stuxnet et découvrez l'impact que ce logiciel malveillant a eu sur l'usine d'enrichissement nucléaire de l'Iran.

L’objectif de la guerre Cybernétique

- L’objectif principal de la guerre cybernétique est d’obtenir un avantage sur les adversaires, qu’ils soient des nations ou des concurrents.
- La cyberguerre est utilisée de plusieurs manières :

- **Pour collecter des informations compromises et/ou des secrets défense**

  - Un pays ou une organisation internationale peut s'engager dans une cyberguerre afin de voler des secrets défense et de collecter des informations sur les technologies qui aideront à combler les lacunes de ses industries et de ses capacités militaires.

  - En outre, des données sensibles compromises peuvent permettre aux agresseurs de faire chanter le personnel d'un gouvernement étranger.

L'objectif de la Cyberguerre (suite)

- **Pour avoir un impact sur l'infrastructure d'un autre pays**
  - Outre l'espionnage industriel et militaire, un pays peut envahir en permanence l'infrastructure d'un autre pays afin de provoquer des perturbations et le chaos.
  - Par exemple, une attaque peut interrompre l’infrastructure électrique d’une grande ville.
  - Réfléchissez aux conséquences si cela devait se produire. les routes seraient encombrées, l'échange de biens et de services serait interrompu, les patients ne pourraient pas recevoir les soins dont ils auraient besoin en cas d'urgence, l'accès à Internet serait interrompu.
  - En coupant un réseau électrique, une cyberattaque peut avoir un impact considérable sur la vie quotidienne de citoyens ordinaires.

1.6 Module Questionnaire

Qu'est-ce que j'ai appris dans ce module?

- La cybersécurité est l'effort continu visant à protéger les individus, les organisations et les gouvernements contre les attaques numériques en protégeant les systèmes et les données en réseau des utilisations non autorisées ou d'un quelconque dommage.
- Les données personnelles sont toutes les informations qui peuvent être utilisées pour vous identifier, et elles peuvent exister à la fois hors ligne et en ligne.
- Les données traditionnelles sont généralement générées et gérées par toutes les organisations, grandes et petites.
- Le Cube McCumber est un modèle créé par John McCumber en 1991 pour aider les entreprises à mettre en place et à évaluer des initiatives de sécurité de l'information en tenant compte de tous les facteurs connexes qui les affectent.
- Une faille de sécurité peut avoir un impact négatif à long terme sur la réputation d'une entreprise qui a mis des années à se construire.
- Une violation de données implique souvent un incident au cours duquel des données personnelles sensibles ont été volées.
- Les cybercriminels peuvent rendre ces informations publiques ou les exploiter pour voler l'identité d'une personne.
- Les cyberattaques peuvent provenir aussi bien de l'intérieur d'une organisation que de l'extérieur.