La cybersécurité



1. Définition
2. Les différents métiers de la cybersécurité
3. Les types de cybermenaces
4. Protection des utilisateurs
5. Les sources

**Définition :**

La cybersécurité est la convergence des personnes, des processus et des technologies qui servent à protéger les entreprises, les individus ou les réseaux contre les attaques numériques.

**Qu’est-ce que la cybersécurité ?**

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. On l’appelle également sécurité informatique ou sécurité des systèmes d'information. Vous pouvez la rencontrer dans de nombreux contextes, de l'informatique d'entreprise aux terminaux mobiles. Elle peut être divisée en plusieurs catégories.

* **La sécurité réseaux** consiste à protéger le réseau informatique contre les intrus, qu’il s’agisse d’attaques ciblées ou de malwares opportuniste.
* **La *sécurité des applications*** vise à protéger les logiciels et les appareils contre les menaces. Une application corrompue pourrait ouvrir l’accès aux données qu’elle est censée protéger. Un système de sécurité fiable se reconnaît dès l’étape de conception, bien avant le déploiement d’un programme d’un appareil.
* **La sécurité des informations** veille à garantir l’intégrité et la confidentialité des données, qu’elles soient stockées ou en transit.
* **La sécurité opérationnelle** comprend les processus et les décisions liés au traitement et à la protection des données. Les autorisations des utilisateurs pour l’accès au réseau et les procédures qui définissent le stockage et l’emplacement des données relèvent de ce type de sécurité.
* **La reprise après sinistre et la continuité des opérations** spécifient la manière dont une entreprise répond à un incident de cybersécurité ou tout autre événement causant une perte des opérations ou de données. Les politiques de reprise après sinistre régissent la manière dont une entreprise recouvre ses opérations et ses informations pour retrouver la même capacité de fonctionnement qu'avant l'événement. La continuité des opérations se réfère au plan sur lequel s'appuie une entreprise tout en essayant de fonctionner sans certaines ressources.
* **La formation des utilisateurs finaux** porte sur le facteur le plus imprévisible : les personnes. Tout le monde peut accidentellement introduire un virus dans un système habituellement sécurisé en ne respectant pas les bonnes pratiques de sécurité. Apprendre aux utilisateurs à supprimer les pièces jointes suspectes et à ne pas brancher de clés USB non identifiées est essentiel pour la sécurité d'une entreprise.

**Les différents métiers de la cybersécurité :**



* **Gestion et pilotage de projets sécurité**

-Responsable de la sécurité des systèmes d’information (RSSI) ] Niveau Bac+5 (et 5 à

-Coordinateur sécurité ] 10 ans d’expérience)

-Directeur cybersécurité ] Salaire : 100000€/an

* **Conception et maintien d’un système d’information sécurisé**

-Développeur sécurité ]

-Cryptologue ] Niveau Bac+3/Bac+5

-Auditeur sécurité(pentester) ] Salaire : 65000/an

-Spécialistes cybersécurité ]

* **Gestion des incidents et des crises**

-Analyste de la menace ] Niveau Bac+3/Bac+5

-Opérateur / Responsable SOC ]

-Opérateur CERT (Computer Emergency Response Team) ] Salaire : 40000/an

* **Conseil, services et recherche**

-Consultant cybersécurité ] Niveau Bac - 3

-Formateur cybersécurité ] à

-Chercheur cybersécurité ] Bac+8

Une image contenant texte, aquarium, capture d’écran, art

Description générée automatiquement**Les types de cybermenaces :**

**Les menaces contrées par la cybersécurité sont au nombre de trois :**

* **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 saper les systèmes électroniques pour entraîner panique ou peur.

**Programmes malveillants :**

Les malwares désignent des logiciels malveillants. Le malware, l'une des cybermenaces les plus courantes, est un logiciel créé par un cybercriminel ou un hacker pour perturber ou endommager l'ordinateur d'un utilisateur. Souvent propagé via la pièce jointe d'un e-mail indésirable ou un téléchargement d'apparence sûr, le malware peut être utilisé par les cybercriminels pour gagner de l'argent ou lors de cyberattaques sur fond de politique.

Il existe de nombreux types de malwares différents, notamment :

* **Le 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.
* **Le 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
* **Les spywares :** des programmes espions qui enregistrent secrètement les actions d'un utilisateur au profit des cybercriminels. Par exemple, un spyware peut enregistrer des coordonnées bancaires.
* **Les ransomwares :** des malwares qui verrouillent les fichiers et les données de l’utilisateur sous menace de les effacer si une rançon n’est pas payée.
* **Adware :** un logiciel publicitaire qui peut être utiliser pour propager un malware
* **Les 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 via une déclaration SQL malveillante. Ils gagnent ainsi l'accès à des informations sensibles contenues dans ladite 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 dite de l’homme du milieu :**

Une attaque dite de l'homme du milieu 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.



**Protection des utilisateurs :**

La protection des utilisateurs, ou la sécurité des terminaux, est un aspect essentiel de la cybersécurité. Après tout, la faute revient souvent à une personne (l'utilisateur final) qui télécharge accidentellement un malware ou une autre forme de cybermenace sur son ordinateur de bureau, ordinateur portable ou appareil mobile.

Comment les mesures de cybersécurité protègent-elles donc les utilisateurs et les systèmes ? Premièrement, la cybersécurité s’appuie sur des protocoles cryptographiques utilisés pour chiffrer les emails, les fichiers et les autres données sensibles. Cela permet non seulement de protéger les informations qui sont transmises, mais également de se prémunir contre la perte ou le vol.

Deuxièmement, les logiciels de sécurité des utilisateurs analysent les ordinateurs à la recherche de codes malveillants, les mettent en quarantaine, puis les suppriment de la machine. Les programmes de sécurité peuvent même détecter et supprimer les codes malveillants cachés dans le primairie Boot Record conçus pour chiffrer ou effacer les données du disque dur de l'ordinateur.

Les protocoles de sécurité électronique se concentrent également sur la détection en temps réel des malwares. Bon nombre de personnes utilisent l’analyse heuristique et comportementale pour évaluer le comportement d’un programme en plus de son code, permettant ainsi de se protéger contre les virus ou les chevaux de Troie capables de changer de forme à chaque exécution (malwares métamorphiques ou polymorphes). Les programmes de sécurité peuvent confiner les programmes potentiellement malveillants dans une bulle virtuelle séparée du réseau d'un utilisateur pour analyser leur comportement et apprendre à mieux détecter les nouvelles infections.

Ces programmes continuent d'élaborer de nouvelles défenses à mesure que les professionnels de la cybersécurité identifient de nouvelles menaces et de nouveaux moyens de les combattre. Pour profiter au mieux des logiciels de sécurité des utilisateurs finaux, les collaborateurs doivent être formés à leur utilisation. Il est essentiel de les garder activés et de les mettre à jour fréquemment afin qu'ils puissent protéger les utilisateurs contre les dernières cybermenaces.

**Les sources :**

<https://www.cisco.com/c/fr_fr/products/security/what-is-cybersecurity.html>

<https://www.kaspersky.fr/resource-center/definitions/what-is-cyber-security>

<https://www.youtube.com/watch?v=W8GNMNQn2Fo>