Veille technologique

La cybersécurité dans les infrastructures réseau pour un administrateur système et réseau

Table des matières :

Veille technologique sur la cybersécurité dans les infrastructures réseau pour un administrateur système et réseau

INTRODUCTION :

Alors que les bases de données produites et utilisées par les entreprises se démultiplient, les domaines de la cybersécurité et de l'infrastructure informatique et réseaux représentent des enjeux importants et un point d'attention particulier se centre autour de ces secteurs en pleine croissance.

1-Cybersécurité infrastructure informatique, systèmes et réseaux… Que veulent dire tous ces termes ?

Chaque année, **les cyberattaques concerneraient plus de 978 millions de personnes dans le monde** selon le **Ministère de l'Intérieur**. Pour cette raison, les domaines de la cybersécurité, et notamment de sa mise en place au sein de de l'infrastructure informatique, sont devenus primordiaux au sein des stratégies des entreprises. Il est important de noter ici que les enjeux de sécurité ont la plupart du temps des conséquences économiques.

A-En quoi consiste la cybersécurité ? Qu'est-ce que c'est ?

Par définition, si l'on voulait résumer la cybersécurité en quelques mots, on dirait qu'elle consiste en…

- **La détection, l'analyse et la résolution d'incidents** de sécurité au sein d'un système d'information
- **La compréhension de la source de l'infection**
- **La prévention** par limitation des failles de sécurité et le combat contre les cyberattaques et les menaces informatiques
- **La protection de la confidentialité des données** au sein d'une infrastructure informatique

Vous l'aurez compris, la cybersécurité protège non seulement les bases de données, mais également les personnes et les idées qui y sont liées.

Autre aspect de la cybersécurité : s'assurer que les processus qui font tourner une structure se déroulent correctement et qu'il n'y ait pas de problème lié à…

- **La disponibilité** : par exemple, si son système ne fonctionne pas, une structure est "paralysée".
- **Des fonctionnements anormaux** : par exemple, si le système d'une structure fait autre chose que ce qu'il devrait faire, soit il produira des résultats qui mettent la structure en danger, soit il sera détourné pour le compte d'un tiers.

B-Infrastructure informatique et réseaux : qu'est-ce que l'on entend par ces termes ?

Une infrastructure informatique rassemble tous les **composants**…

- **Matériels** : serveurs, postes de travail (ordinateurs de bureau ou portables), smartphones et équipements téléphoniques...
- **Logiciels** : système d'exploitation, comme GNU/Linux par exemple, mais également des serveurs web (apache, ngnix), des logiciels de travail collaboratif, etc. ;
- **Réseaux** : connexion Internet, réseau physique (câbles et équipements d'interconnexion), routeurs, pare-feu…

Ces derniers sont connectés entre eux et forment ce que l'on appelle l'infrastructure informatique (ou réseau informatique). Il existe d'ailleurs différents types d'infrastructures informatiques :

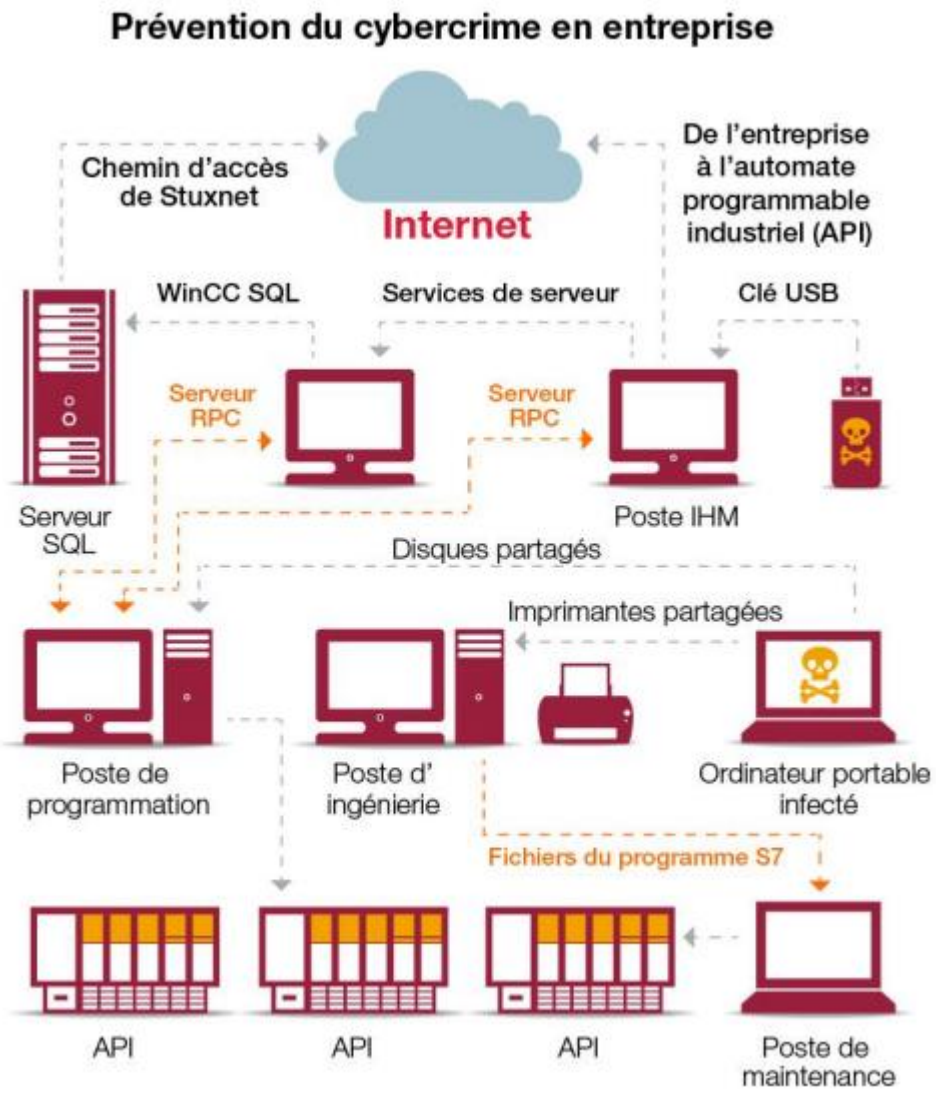
- Infrastructure classique
- Infrastructure cloud
- Infrastructure hybride (quand on mixe classique et cloud)

2-Quels sont les trois principes fondamentaux du monde de la cybersécurité ?

A) La prévention : comment se prémunir contre les cybermenaces ?

Les menaces que représentent la cybercriminalité sont réelles, et peuvent toucher n'importe quelle entreprise qui ne serait pas assez protégée et dont la vigilance est limitée.
Pour se prémunir contre les cybermenaces, il est important de…

- **Sensibiliser les différents services d'une entreprise** à la sécurité et aux risques éventuels (ransomwares, phishing…)
- **Effectuer toutes les mises à jour logiciels**
- **Utiliser des mots de passe fiables**
- **Renforcer la sécurité du réseau Wi-Fi**



B) La détection : comment détecter les cybermenaces ?

Certains signes inhabituels peuvent vous mettre la puce à l'oreille :

- **Vous n'arrivez pas à vous connecter à un compte** ou à accéder à certaines données
- **Des fichiers ont disparu**, ou ont été modifiés ou endommagés
- **Votre poste de travail est plus lent** que d'habitude
- **Le taux d'activité de votre site web est inhabituel**
- **Votre ordinateur ne démarre pas correctement**
- **Des messages ont été envoyés de votre adresse mail** mais ne viennent pas de vous
- Et bien d'autres…

Pour cette raison, un monitoring* doit être effectué régulièrement afin de détecter les attaques le plus rapidement possible.

**Un monitoring est un système qui permet de superviser et contrôler différents éléments de l'infrastructure informatique d'une entreprise. La mesure des activités de cette dernière va permettre de détecter les anomalies*

C) La réaction

Une fois l'anomalie identifiée, il est primordial de **réagir de façon rapide et efficace** afin de favoriser le déploiement des actions de défense et les configurations nécessaires. En effet, plus la prise en charge est rapide, plus les dégâts pourront être limités.

3-La multiplication des cyberattaques

A- Les tendances en matière d'attaques informatiques :

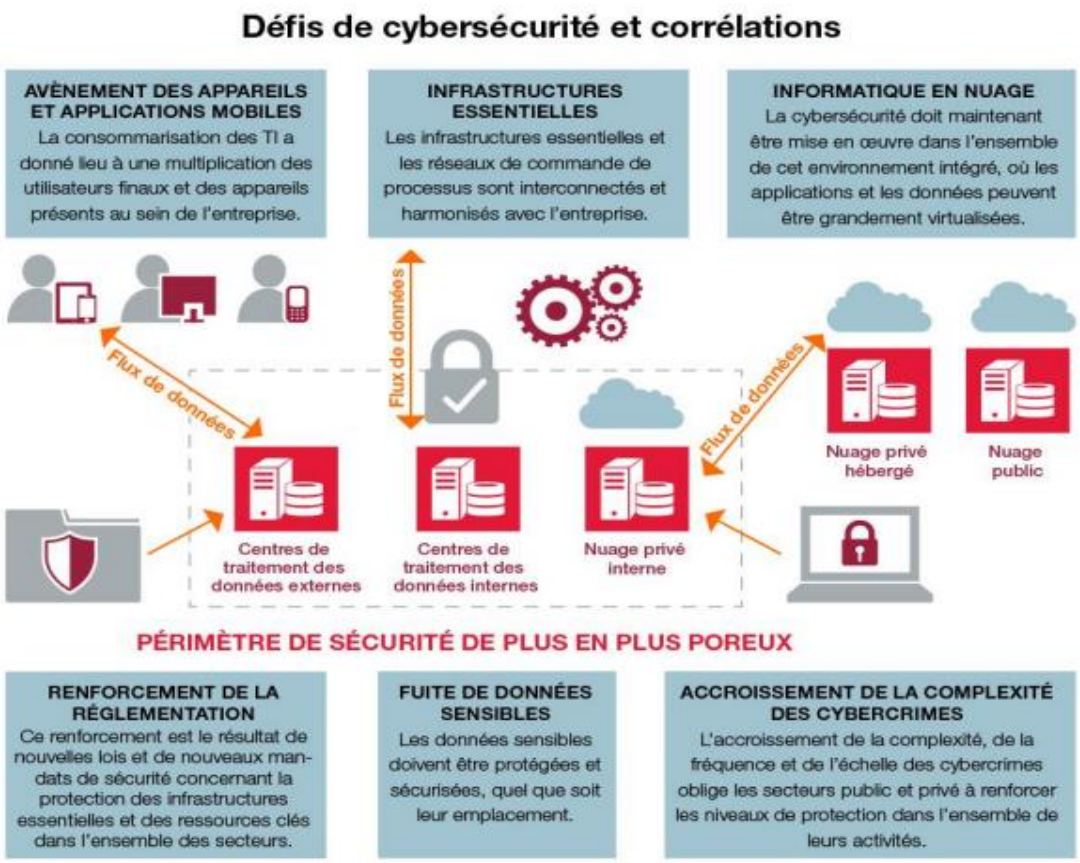
1)Une nouvelle technique d'attaque par ransomware appelée "double extorsion" est de plus en plus utilisée par les cybercriminels. Cette technique consiste à chiffrer les données de l'entreprise et à menacer de les rendre publiques si la rançon n'est pas payée. (Source : Kaspersky)

2)Les attaques de type "man-in-the-middle" sont de plus en plus courantes. Il s'agit d'une technique qui permet à un attaquant de s'interposer entre deux parties qui communiquent pour intercepter les données échangées. (Source : TrendMicro)

B-FACTEURS ET DÉFIS OPÉRATIONNELS

Voici les principaux facteurs opérationnels en matière de cybersécurité dont les entreprises d'aujourd'hui doivent tenir compte

- Accroissement de la complexité, de la fréquence et de l'échelle des cybercrimes
- Fuite de données sensibles, par malveillance ou par inadvertance
- Perte de propriété intellectuelle
- Renforcement de la réglementation
- Interconnexion des réseaux d'entreprise et des réseaux de commande de processus
- Vulnérabilités créées par l'avènement de l'informatique en nuage, des appareils mobiles et des applications Web 2.0 au sein de l'entreprise (voir le graphique ci-dessous)



C- Les normes et les réglementations de cybersécurité :

1_Le NIST a publié une mise à jour de son Framework de cybersécurité qui inclut maintenant une catégorie de gestion de la confidentialité des données. (Source : NIST)

2_L'Union Européenne a publié une nouvelle directive sur la cybersécurité appelée "NIS 2" qui renforce les exigences de sécurité pour les entreprises opérant dans des secteurs critiques tels que l'énergie, les transports et la santé. (Source : Commission Européenne)

CONCLUSION :

La cybersécurité est un enjeu crucial pour les entreprises, et les administrateurs système et réseau jouent un rôle clé dans la protection des infrastructures informatiques. Pour se prémunir contre les cyberattaques, ils doivent suivre une veille technologique régulière pour rester à jour sur les dernières tendances, technologies, normes et réglementations en matière de sécurité. En agissant de manière proactive, ils peuvent garantir la continuité de l'activité de leur entreprise et protéger leurs systèmes contre les menaces croissantes.

Références

Kaspersky: https://www.kaspersky.com/blog/double-extortion-ransomware/37265/

TrendMicro: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/whats-a-man-in-the-middle-attack-and-how-can-it-be-prevented

Gartner: https://www.gartner.com/en/information-technology/glossary/extended-detection-and-response-edr-xdr

PaloAlto: https://www.paloaltonetworks.com/cyberpedia/what-is-network-segmentation

NIST: https://www.nist.gov/news-events/news/2020/04/nist-releases-version-11-cybersecurity-framework

Commission Européenne: https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_320

ANSSI: https://www.ssi.gouv.fr/guide/le-guide-dhygiene-informatique/

ZDNet: https://www.zdnet.com/article/ransomware-attacks-on-healthcare-organisations-are-rising-fast-and-the-problem-is-about-to-get-a-lot-worse/

wildcodeschool : HTTPS://WWW.WILDCODESCHOOL.COM/FR-FR/BLOG/CYBERSECURITE-INFRASTRUCTURE-INFORMATIQUE-ET-RESEAUX-LA-BONNE-ALTERNANCE