Évolution des Menaces en Cybersécurité et Meilleures Pratiques pour la Protection de Vos Données

Introduction

La cybersécurité est l'ensemble des pratiques, technologies et procédures conçues pour protéger les systèmes informatiques, les données et les réseaux contre les menaces en ligne.

La protection des données est cruciale car les informations sensibles sont de plus en plus stockées et échangées électroniquement

Évolution des Menaces en Cybersécurité

1. Les Menaces Traditionnelles

Les **malwares**, tels que les virus et les chevaux de Troie, ont évolué pour devenir plus sophistiqués.

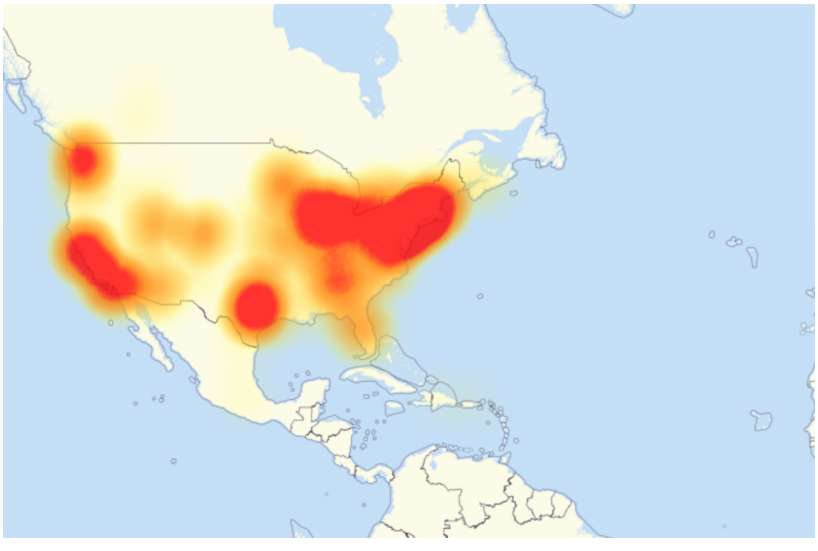
Un exemple notoire de malware est le ver WannaCry, qui a fait la une des actualités en 2017. WannaCry était un ransomware, un type de malware qui chiffre les fichiers d'un utilisateur et exige une rançon pour les déchiffrer. Ce ransomware a exploité une vulnérabilité connue dans le système d'exploitation Windows, que Microsoft avait déjà publié un correctif pour.

Le **phishing** est devenu plus ciblé et élaboré. C'est une technique de cyberattaque où les attaquants tentent de tromper les utilisateurs en se faisant passer pour des entités légitimes afin de leur voler des informations personnelles ou financières.

Un exemple notable de phishing élaboré est l'attaque contre le Comité national du parti démocrate des États-Unis en 2016. Cette attaque, largement médiatisée, a utilisé des tactiques d'ingénierie sociale pour tromper les utilisateurs et a eu un impact significatif sur la scène politique.

Les **attaques par déni de service distribué (DDoS)** sont devenues un problème majeur en matière de cybersécurité, car elles peuvent paralyser les services en ligne en saturant leurs infrastructures avec un trafic excessif. Une tendance inquiétante est l'augmentation de la puissance des attaques DDoS, principalement due à la sophistication croissante des botnets.

L'attaque DDoS contre Dyn en 2016 a perturbé l'accès à de nombreux sites Web populaires.



2. Les Menaces Avancées

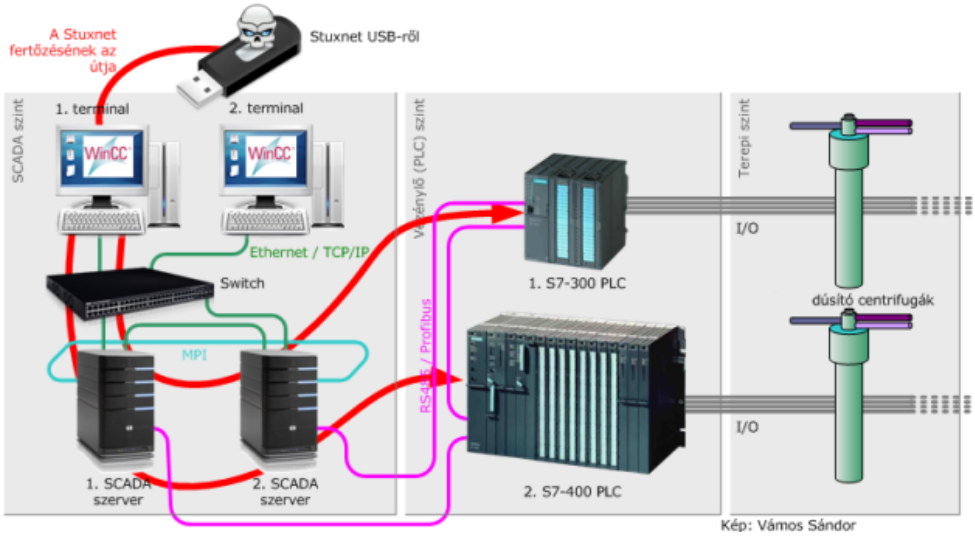
Les menaces avancées, telles que les **APT (Advanced Persistent Threats)**, sont des attaques soutenues et ciblées à long terme.

Un exemple est l'attaque contre Sony Pictures en 2014 qui a été l'une des attaques cybercriminelles les plus médiatisées de l'histoire. Cette attaque a été attribuée à la Corée du Nord et a eu un impact significatif sur les opérations de Sony Pictures.

Les **zero-days**, également appelées "0-day," sont des vulnérabilités de sécurité dans les logiciels, les systèmes d'exploitation, les applications ou les matériels informatiques qui sont inconnues de l'éditeur du logiciel ou du fournisseur de la technologie, d'où le terme "zero-day."

Ces vulnérabilités sont appelées ainsi parce qu'elles sont exploitées par des attaquants dès le premier jour où elles sont découvertes, avant que l'éditeur ou le fournisseur n'ait eu la possibilité de développer un correctif (patch) pour les résoudre.

L'attaque Stuxnet a utilisé des zero-days pour attaquer les centrifugeuses nucléaires en Iran.

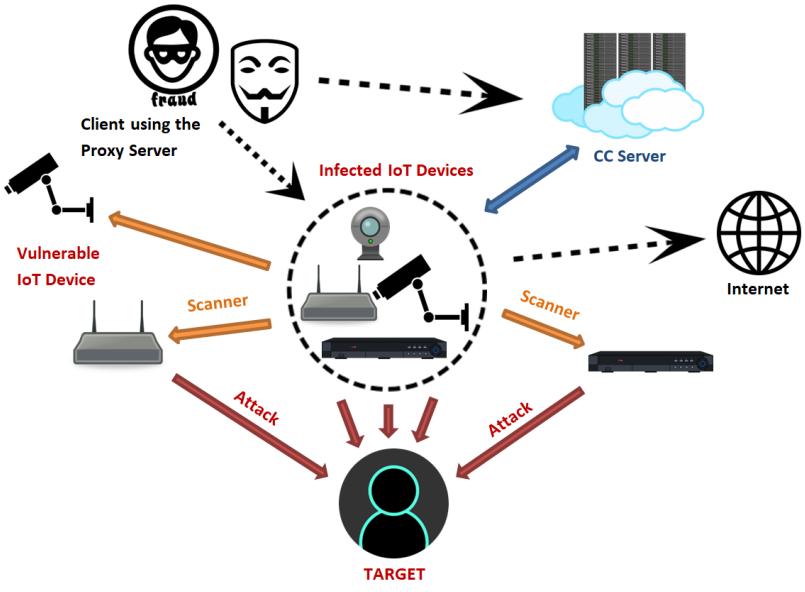


Kép: Vámos Sándor

3. Les Menaces Émergentes

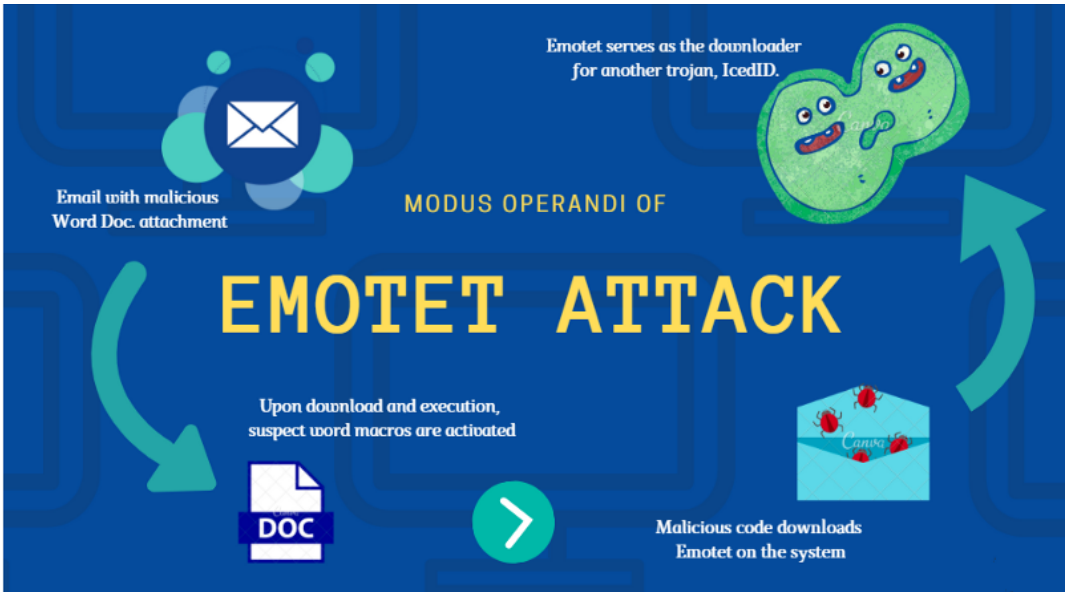
L'**Internet des objets (IoT)** a apporté de nombreuses opportunités et avantages, mais en même temps, il a ouvert de nouvelles portes aux attaquants et aux menaces en matière de cybersécurité.

En 2016, le botnet Mirai a utilisé des dispositifs IoT infectés pour lancer des attaques DDoS massives.



L'**intelligence artificielle** est utilisée par les attaquants pour automatiser les attaques et améliorer la précision du phishing

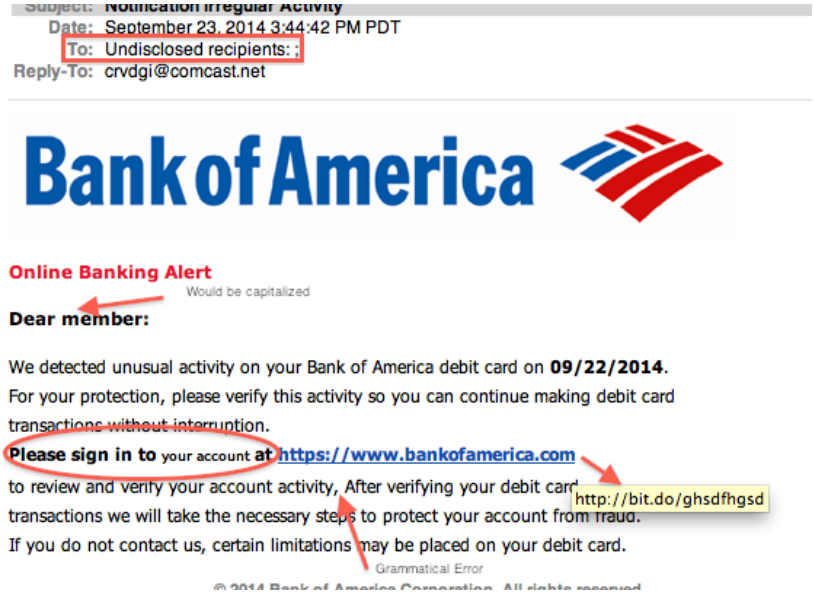
L'attaque menée en 2020 par le groupe de pirates informatiques derrière le cheval de Troie Emotet en est un exemple. Emotet est un malware notoire qui a été utilisé pour diffuser d'autres malwares, tels que des ransomwares et des chevaux de Troie bancaires.



Les Méthodes d'Attaque

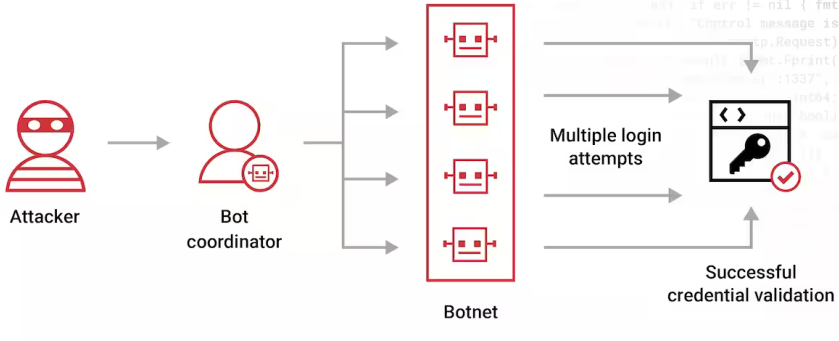
L'**ingénierie sociale** implique la manipulation psychologique des individus pour obtenir des informations confidentielles.

Par exemple, l'envoi de courriels de phishing se faisant passer pour une banque pour obtenir les informations de connexion.

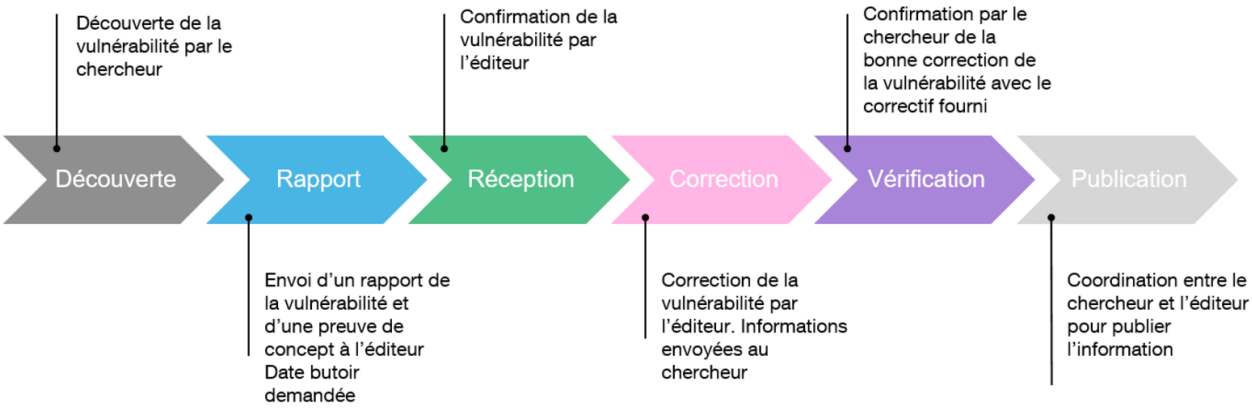


Les **attaques de force brute** consistent à essayer toutes les combinaisons possibles de mots de passe jusqu'à ce que le bon soit trouvé.

Par exemple, une attaque de force brute contre un compte utilisateur.



L'**exploitation de vulnérabilités** consiste à rechercher des failles dans les logiciels et ces attaquants peuvent utiliser des outils automatisés pour trouver et exploiter ces vulnérabilités.

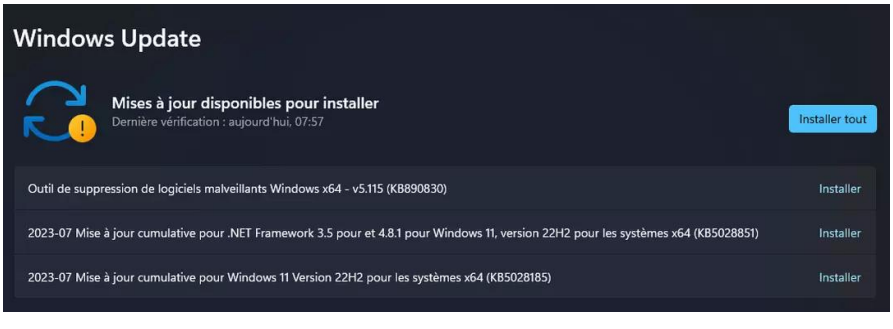


Les Meilleures Pratiques pour la Protection de Vos Données

Mise à Jour et Patch Management

Les mises à jour régulières des logiciels et des systèmes d'exploitation sont essentielles pour corriger les vulnérabilités connues.

Par exemple, Microsoft publie des correctifs de sécurité chaque mois pour ses produits.

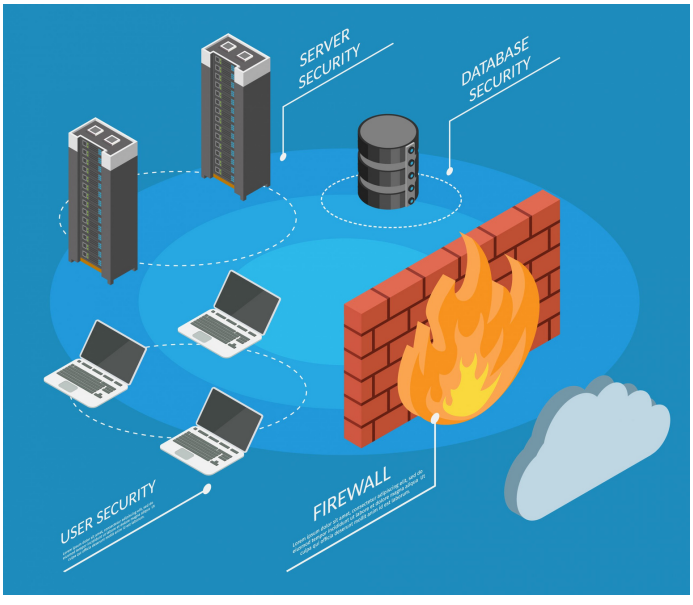


La gestion des correctifs garantit que les mises à jour sont appliquées de manière cohérente à tous les systèmes.

Utilisation de Pare-feu et d'Antivirus

Les pare-feu filtrent le trafic réseau pour bloquer les menaces. Ils surveillent le trafic entrant et sortant de votre ordinateur pour s'assurer que rien de malveillant ne pénètre.

Par exemple, un pare-feu peut empêcher les attaques par DDoS.

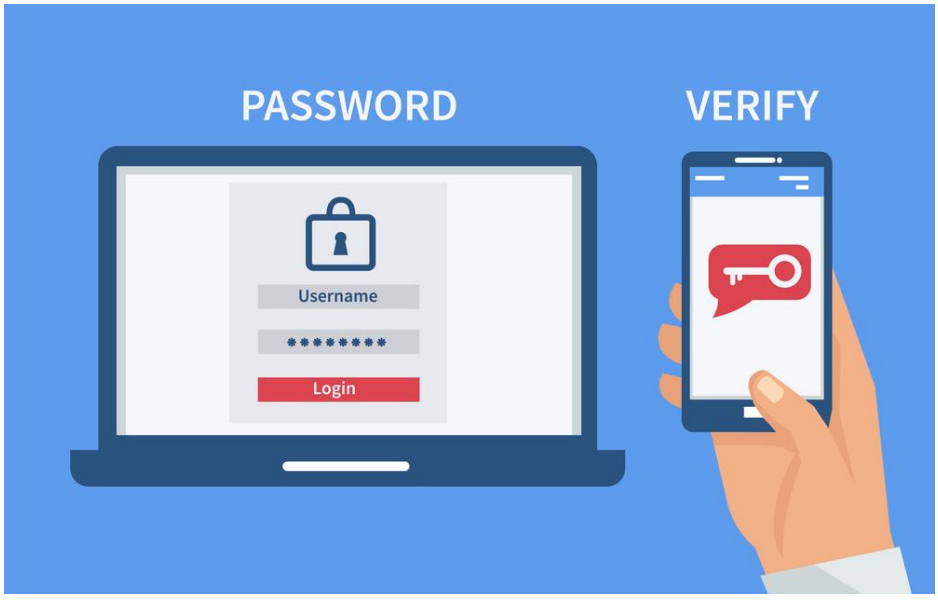


Les antivirus et antimalware détectent et suppriment les logiciels malveillants. Ils doivent être mis à jour régulièrement pour être efficaces.

Authentification Forte

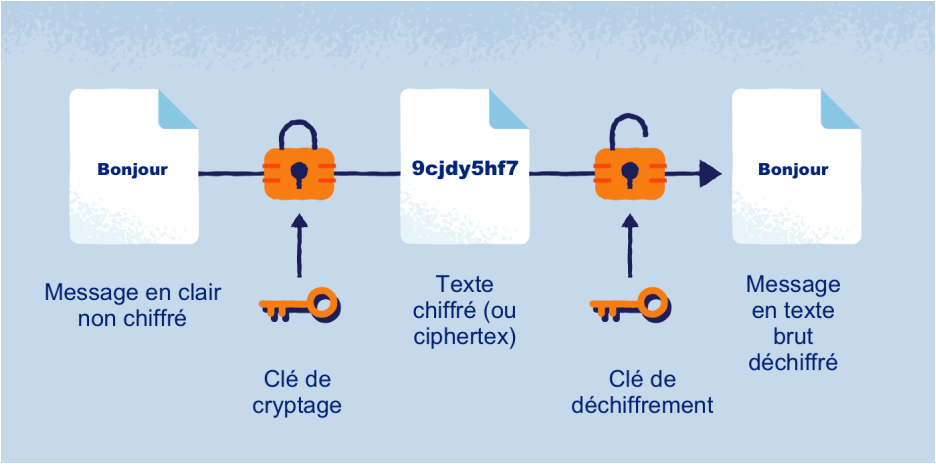
L'authentification à deux facteurs (2FA) et à plusieurs facteurs (MFA) renforce la sécurité en exigeant des informations supplémentaires pour se connecter.

Par exemple, après avoir saisi un mot de passe, l'utilisateur peut recevoir un code sur son téléphone pour se connecter



Chiffrement des Données

Le chiffrement de bout en bout garantit que seules les parties autorisées peuvent accéder aux données.



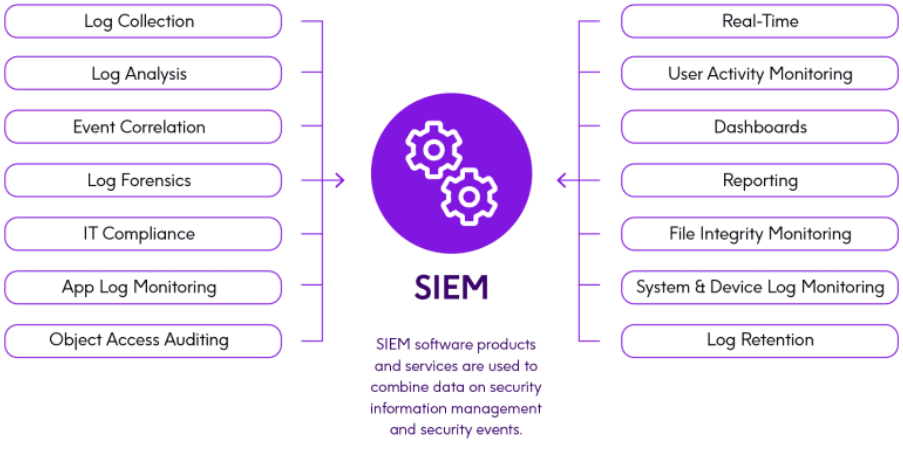
Lorsque vous envoyez des informations en ligne, elles sont transformées en une forme illisible pour quiconque ne possède pas la "clé" pour les déchiffrer. Cela signifie que même si quelqu'un intercepte vos données, il ne pourra pas les comprendre.

Par exemple, WhatsApp utilise le chiffrement de bout en bout pour sécuriser les messages.

Surveillance et Détection

Les systèmes SIEM (Security Information and Event Management) analysent les journaux et les événements pour détecter des comportements anormaux.

Par exemple, un SIEM peut alerter en cas de tentative d'accès non autorisé.



Conclusion

La cybersécurité est devenue un enjeu majeur dans le monde numérique, car les menaces qui pèsent sur les systèmes informatiques et les données continuent d'évoluer de manière exponentielle.

> «Oublier la cybersécurité, c'est "rouler à 200 km/h à moto sans casque" »
>
> **Guillaume Poupard, patron de l'agence française de cyberdéfense (Anssi)**

Les raisons de cette préoccupation sont nombreuses, et il est crucial de comprendre pourquoi une vigilance constante et la mise en place de meilleures pratiques sont essentielles pour protéger les données dans cet environnement en constante évolution.