Dossier de veille technologique

L’Avenir de la cybersécurité

Sommaire

Table des matières

Quelques définitions

- Veille Technologique

La veille technologique constituée par l'ensemble des techniques visant à organiser de façon systématique la collecte, l'analyse, la diffusion de l'exploitation des informations techniques utiles à la sauvegarde et à la croissance des entreprises. « La veille technologique se doit de prévenir et alerter tout responsable d'un changement, d'une nouveauté ou d'une innovation qu'elle soit technique ou scientifique. Dès lors qu'elle peut modifier le paysage ou faire perdre / gagner un avantage économique, la veille devient critique et doit intervenir le plus tôt possible ».

Pour ma veille technologique j'ai choisi de vous parler du futur de la cybersécurité.

- Environnement numérique

Un espace qui permet d'accéder à des ressources matérielles et logicielles et à des services numériques en ligne (WAN Public) ou locales (LAN Privé).

Le préfixe « cyber » va regrouper plusieurs termes liés à l'informatique/le numériques tel que : Cybersécurité, Cybercafé, Cyberdéfense, Cybercriminalité, Cyberguerre, etc.

-Cybersécurité : Représente la protection des ressources, des données, des outils connectées ou installés. La cybersécurité regroupe l'ensemble des moyens utilisés (lois, dispositifs, gestion des risques, actions, etc..) pour assurer la défense d'un particulier (utilisateur lambda) ou d'une entreprise.

- Cyberattaque : Attaques/actions qui vise le cyberspace ou des infrastructure, systèmes, etc., ayant un but malveillant. Ces actions sont volontaires et offensives. Elles peuvent être faites par des personnes seules ou des groupes de pirate ou biens d'organisation (état). L'objectif de ces attaques est des créer des dommages ou des perturbations sur les informations et les systèmes afin de voler des données ou nuire leurs utilisations.

- Cyberguerre : La cyberguerre est en quelques sorte un regroupement de cyberattaques (attaque dans le cyberspace) mais sur un niveau géopolitique (confrontations entre états, entre grande ou petites entreprises, etc..). Ces attaques ont principalement des buts politiques à différentes échelles (entreprises, état, continentale, mondiale).

Introduction

Aujourd'hui, la technologie est présente partout : à l'école, au travail, à la maison et même dans les objets du quotidien. Cette transformation numérique offre de nombreuses opportunités, mais elle comporte aussi des inconvénients. Comme on dit, toutes commodités engendrent des risques. En effet, les cyberattaques sont de plus en plus nombreuses et dangereuses. La cybersécurité est donc devenue un enjeu mondial essentiel. Protéger les données, les systèmes informatiques et les utilisateurs est devenu une priorité pour les entreprises, les États et les citoyens.

Mais à quoi ressemblera la cybersécurité de demain ?

Que pourront nous nous attendre de la cybersécurité dans le futur ?

Quelles seront les nouvelles menaces et les solutions mises en place pour y faire face ?

Nous essayerons de répondre à toutes ces questions dans notre développement.

Ce sujet a été choisi par passion à la cybersécurité. Actuellement en BTS SIO option SISR (Solutions d'infrastructure, systèmes et réseaux), j'ai le souhait qu'a la fin de mon parcours me spécialiser dans le cyber. Car selon moi c'est l'avenir. Et en ayant des notions de bases en systèmes et réseaux, ça pourrait être un plus pour la spécialisation.

Vu le nombre d'attaques chaque semaine, surtout pour les grandes firmes ou entreprises, nous pensons que le domaine de la cybersécurité aurait un besoin particulier sur le marché de l'emploi.

Développement

Afin de mieux contextualiser le sujet, nous allons en première partie définir la cybersécurité en donnant les types de cyberattaques.

Qu'est-ce que la cybersécurité ?

La cybersécurité représente tous les moyens utilisés afin d'assurer la protection et l'intégrité des données. Cette notion devient de plus en plus récurrente grâce la transformation numérique des entreprises (utilisation d'outils informatiques, etc ...). Dans une entreprise, les dirigeants sont responsables de l'intégrité et de la confidentialité des données qui circulent pour son activité. En tant qu'employeur, il s'agit également de protéger les salariés en ce qui concerne leurs informations personnelles. Les entreprises peuvent internaliser les compétences dans le domaine de la cybersécurité grâce à une DSI (Direction des Systèmes d'Information). L'intervention d'un expert extérieur est également une bonne pratique (externalisation).

Différents types d'attaques TYPE D'ATTAQUE

Nous évoquerons les types d'attaques les plus fréquents en 2025

Attaques malveillantes

Les programmes malveillants font référence à un large éventail de programmes nuisibles destinés à perturber, endommager ou obtenir un accès non autorisé aux systèmes informatiques. Cela inclut les virus, les vers, les chevaux de Troie, les ransomware, les spyware et les adware. Les logiciels malveillants peuvent infecter les appareils par différents moyens, notamment les pièces jointes aux emails, les sites Web compromis et les téléchargements de logiciels. Une fois installé, il exécute des actions malveillantes telles que le vol de données, le détournement de système et l'incapacité des appareils. Il peut fonctionner de manière furtive pour échapper à la détection, en exploitant les vulnérabilités des logiciels ou en utilisant des tactiques d'ingénierie sociale pour inciter les utilisateurs à l'installer par inadvertance, ce qui présente des risques importants pour la cybersécurité et la confidentialité des données. La suppression des programmes malveillants implique généralement l'utilisation d'un logiciel antivirus spécialisé pour analyser, détecter et mettre en quarantaine ou supprimer des fichiers ou programmes malveillants, restaurant ainsi l'appareil infecté à un état sécurisé.

Phishing et spear phishing

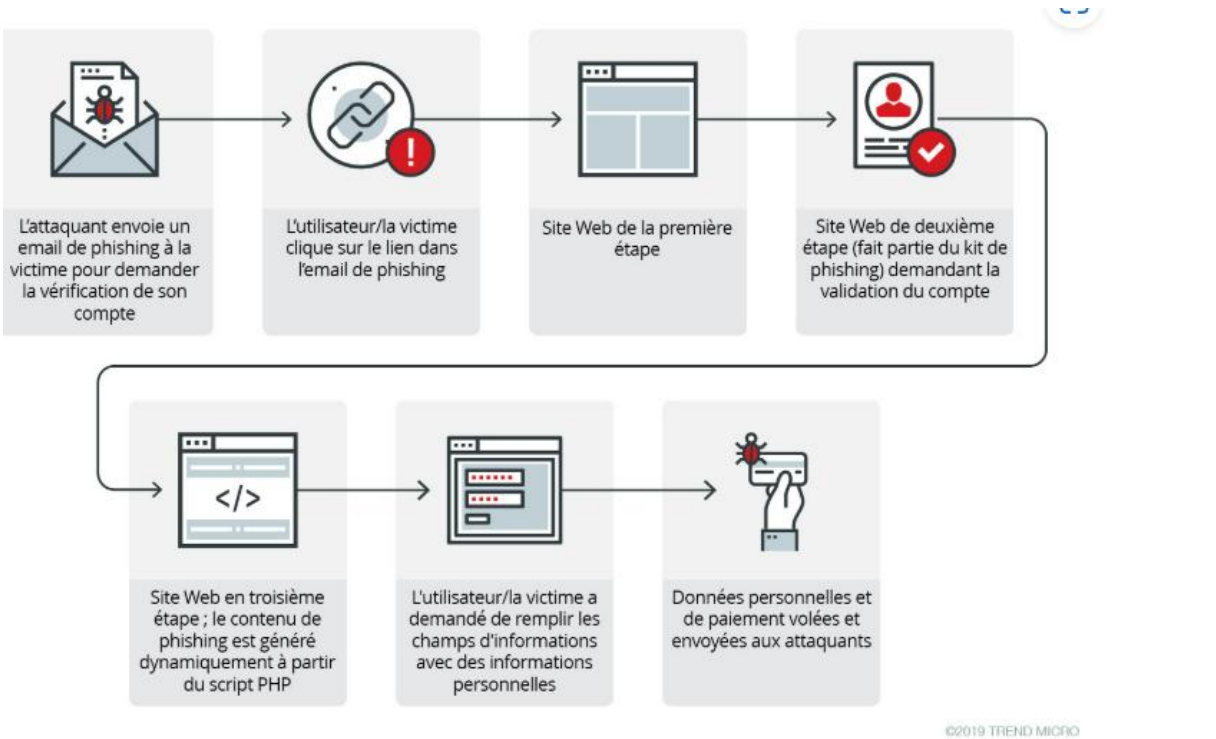
Le phishing est un type de cyber-attaque consistant en l'envoi de courriels génériques par des cybercriminels se faisant passer pour des personnes légitimes. Ces courriels contiennent des liens frauduleux qui permettent de voler les informations privées des

utilisateurs. Les attaques par hameçonnage sont plus efficaces lorsque les utilisateurs n'en ont pas conscience.

Le terme de phishing désigné principalement les attaques génériques par email. Il se produit lorsqu'un attaquant envoie des emails à un maximum d'adresses, à l'aide de services courants tels que PayPal ou Bank of America.

Le phishing a évolué au fil des ans pour inclure des attaques visant différents types de données. En plus de l'argent, les attaques peuvent cibler des données sensibles ou des photos.

Le spear phishing est l'une des formes de cyberattaques les plus dangereuses et ciblées. Contrairement aux attaques de phishing classiques, qui visent un large public dans l'espoir d'attraper des victimes peu méfiantes, le spear phishing est une forme d'attaque par phishing hautement personnalisée et ciblée, qui cible un utilisateur plutôt qu'un réseau.



Exemple d'attaque de phishing

Déni de service (DoS) et Déni de service distribué (DDoS)

Une attaque DDoS est conçue pour interrompre ou arrêter un réseau, un service ou un site Web. Une attaque DDoS se produit lorsque les attaquants utilisent un vaste réseau de PC distants appelés botnets pour submerger la connexion ou le processeur d'un

autre système, ce qui entraîne un refus de service au trafic légitime qu'il reçoit. L'objectif et le résultat final d'une attaque DDoS réussie est de rendre le site Web du serveur cible indisponible aux demandes de trafic légitimes.

Les attaques DDoS ont différentes finalités, des blagues et des vendettas personnels contre les entreprises et les organisations aux criminels qui utilisent les attaques DDoS comme forme de chantage pour un gain financier et les protestations pour attirer l'attention sociale (par ex., les hacktivistes). À ces fins, par exemple, les agences gouvernementales et les entreprises ont été fréquemment ciblées par des attaques DDoS ces dernières années, ce qui en fait un type de cyberattaque dont il faut se méfier. Il existe également des criminels sur le marché souterrain qui vendent des outils pour les attaques DDoS et des services pour mener des attaques DDoS. Ainsi, les obstacles à la réalisation des attaques DDoS ont été réduits, et la menace des attaques DDoS devrait continuer à croître.

Attaques de l'homme au milieu (MitM)

Une attaque de l'homme au milieu (MitM) est un type d'attaque qui implique un élément malveillant « d'écoute » sur les communications entre les parties et constitue une menace importante pour les organisations. Ces attaques compromettent les données envoyées et reçues, car les intercepteurs ont non seulement accès aux informations, mais ils peuvent également saisir leurs propres données. Compte tenu de l'importance des informations qui vont et viennent au sein d'une organisation, les attaques MiTM représentent une menace très réelle et puissante que les professionnels IT doivent pouvoir traiter.

Injections SQL

L'injection SQL est une attaque qui manipule illégalement une base de données en injectant des instructions SQL (Structured Query Language) involontaires dans une application qui possède une base de données relationnelle (RDBMS). Il existe plusieurs types d'injection SQL en fonction de la méthode et de l'objectif, et du point de vue des cyberattaques, elles vont du vol d'informations à la falsification de données et à l'investigation des vulnérabilités. Bien qu'il s'agisse d'une ancienne attaque, elle cause encore beaucoup de dommages aujourd'hui, c'est donc l'une des attaques dont les organisations d'entreprise doivent particulièrement se méfier.

Bien que l'injection SQL soit une ancienne attaque, il existe encore de nombreux cas confirmés de dommages importants au cours des dernières années. Par conséquent, il s'agit toujours d'une attaque dont les organisations doivent se méfier. Si une technique telle que l'injection UNION est utilisée et que l'attaque est réussie, elle peut entraîner une fuite d'informations à grande échelle. Cependant, en prenant les mesures appropriées, il est possible d'éviter ces dommages avant qu'ils ne se produisent. En tant que mesure de sécurité pour les organisations d'entreprise, en plus des mesures du point de vue de la défense en profondeur mentionnées ci-dessus, nous recommandons que des évaluations de sécurité soient régulièrement effectuées, telles que des tests de pénétration externes et un diagnostic de vulnérabilité.

Exploits zero-day

Une vulnérabilité zero-day est un défaut, une faiblesse ou un bug dans un logiciel, un firmware ou un matériel qui peut avoir déjà été divulgué publiquement, mais qui n'a pas été corrigé. Les chercheurs ont peut-être déjà divulgué la vulnérabilité, et le fournisseur ou le développeur peut déjà avoir connaissance du problème de sécurité, mais un correctif ou une mise à jour officielle qui traite de cette vulnérabilité n'a pas été publié.

Le défaut est appelé vulnérabilité « zero-day », car le fournisseur ou le développeur, et en conséquence, les utilisateurs et les organisations dont les systèmes sont affectés par la vulnérabilité, viennent d'apprendre la vulnérabilité. Une fois que la vulnérabilité devient publique et que le fournisseur ou le développeur a déjà déployé un correctif pour elle, elle devient une vulnérabilité connue, ou « n-day ».

Lorsque les pirates ou les acteurs malveillants développent et déploient avec succès des preuves de concept (PoC) ou un malware réel qui exploite la vulnérabilité alors que le fournisseur travaille toujours sur le déploiement d'un correctif (ou parfois, sans connaître l'existence de la vulnérabilité), cela devient un exploit ou une attaque zero-day. Alors que les développeurs et les fournisseurs, ainsi que les chercheurs et les experts en sécurité, investissent continuellement du temps et des efforts pour trouver et corriger les failles de sécurité, il en va de même pour les acteurs malveillants. Le résultat est une course d'armes entre les acteurs malveillants qui trouvent et essaient d'exploiter une vulnérabilité et les fournisseurs qui s'efforcent de publier un correctif pour la corriger.

Attaque de Ransomware

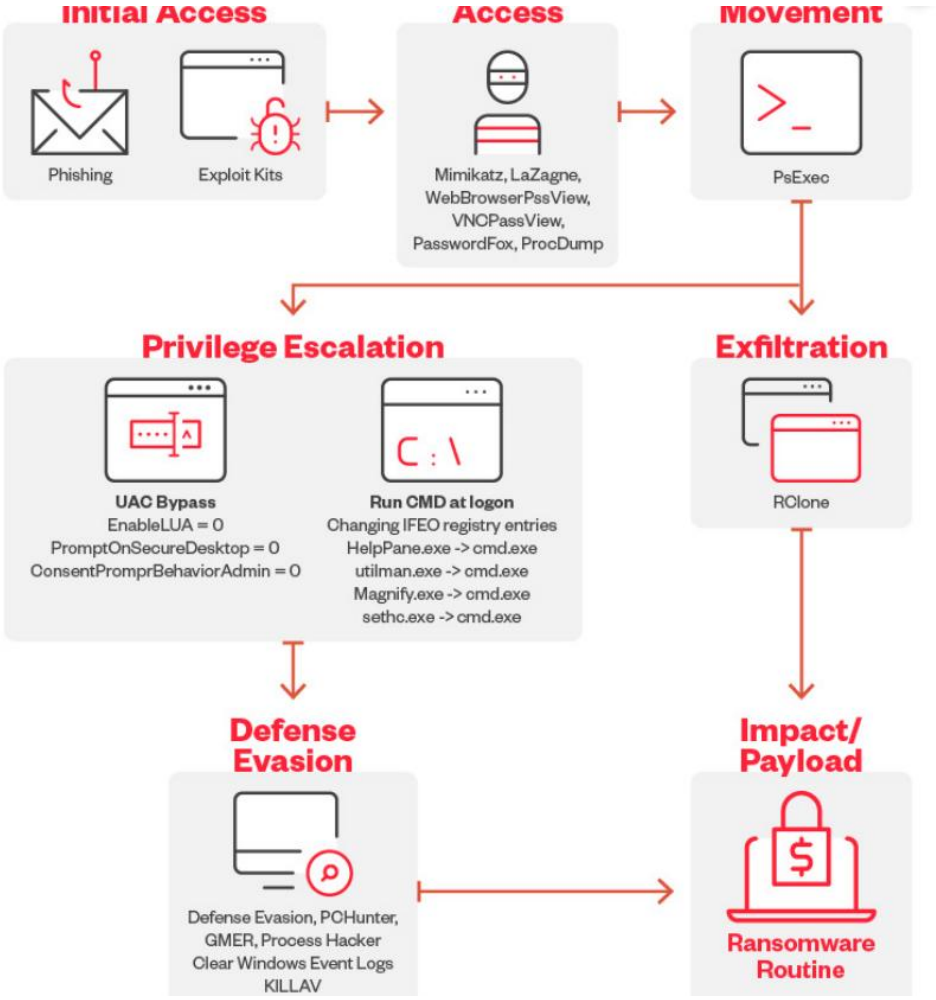
Le ransomware est un malware qui chiffre les fichiers importants sur le stockage local et sur le réseau, et demande une rançon pour déchiffrer les fichiers. Les pirates développent ce malware pour gagner de l'argent par extorsion numérique. Le ransomware est chiffré, de sorte qu'il est impossible de trouver la clé. Le seul moyen de récupérer les informations consiste à accéder à une sauvegarde.

Le fonctionnement du ransomware cause particulièrement de dégâts. Les autres types de malwares détruisent ou volent les données, mais permettent de recourir à d'autres options de récupération. Avec le ransomware, en l'absence de sauvegardes, vous devez payer la rançon pour récupérer les données. Il arrive même qu'une entreprise paie la rançon et que l'attaquant n'envoie pas la clé de déchiffrement.

Lorsque le ransomware se lance, il parcourt le stockage local et sur le réseau, à la recherche de fichiers à chiffrer. Il cible les fichiers qu'il considère comme importants pour votre entreprise ou pour les individus. Cela inclut les fichiers de sauvegarde qui pourraient aider à récupérer les informations.

Les différents types de ransomware ciblent différents ensembles de fichiers, mais il existe également des cibles courantes. La plupart des ransomware ciblent les fichiers Microsoft Office, car ils contiennent souvent des informations stratégiques. Le fait de

cibler des fichiers importants augmente les chances que vous acceptiez de payer la rançon.



Supply Chain Attack

Supply Chain Attack est un type de cyberattaque qui cible des éléments moins sécurisés dans la chaîne d'approvisionnement d'une organisation plutôt que d'attaquer directement l'organisation. L'objectif est d'infiltrer le réseau ou les systèmes d'une organisation en compromettant un fournisseur tiers ou un partenaire qui a accès à ses données, logiciels ou infrastructures réseau.

Au lieu d'attaquer directement l'organisation cible, les attaquants compromettent un tiers de confiance, tel qu'un fournisseur de logiciels, un fournisseur de matériel ou un prestataire de services. Ce tiers devient ensuite un canal pour fournir la charge utile malveillante à la cible finale.

L'impact d'une attaque de la chaîne d'approvisionnement peut être important, affectant non seulement la cible principale, mais potentiellement des milliers d'autres organisations qui comptent sur le tiers compromis.

Cross-Site Scripting (XSS)

Le cross-site Scripting (XSS) est une vulnérabilité de sécurité généralement trouvée sur les sites Web et/ou les applications Web qui acceptent les entrées des utilisateurs. Les moteurs de recherche, les formulaires de connexion, les forums et les zones de commentaires en sont des exemples.

Les cybercriminels exploitent cette vulnérabilité en entrant des chaînes de code malveillant exécutable dans ces fonctions. Cela injecte le code malveillant dans le contenu du site Web ciblé, en faisant ainsi partie du site Web et lui permettant ainsi d'affecter les victimes qui peuvent visiter ou consulter ce site Web. Le code peut également se présenter comme un contenu transitoire qui ne fait pas réellement partie du site Web, mais semble uniquement être destiné au visiteur. Cela donne l'impression que le site Web est effectivement compromis par des cybercriminels.

Les cybercriminels peuvent également utiliser cette vulnérabilité pour prendre le contrôle ou compromettre directement un site Web, ainsi que pour exploiter d'autres vulnérabilités existantes sur le serveur ou le logiciel du site Web.

Social Engineering

L'ingénierie sociale est un type d'attaque qui utilise l'interaction humaine et la manipulation pour atteindre les objectifs de l'attaquant. Cela implique souvent de persuader les victimes de compromettre leur sécurité ou de violer les meilleures pratiques de sécurité pour le gain financier ou informationnel de l'attaquant. Les acteurs malveillants utilisent l'ingénierie sociale pour se déguiser et se déguiser en leurs motivations, souvent en agissant comme des personnes de confiance.

En fin de compte, l'objectif principal est d'influencer, de pirater l'esprit, plutôt qu'un système. De nombreux exploits de ce type s'appuient sur la bonne nature ou la peur des situations négatives. L'ingénierie sociale est populaire parmi les attaquants, car il est plus facile d'exploiter les personnes plutôt que les vulnérabilités du réseau et des logiciels.

Whaling

Le whaling est un genre spécialisé d'attaque de phishing qui cible les cadres ou les personnes haut placées dans des organisations, comme les dirigeants, les responsables et d'autres leaders. Le terme de « whaling » (pêche à la baleine) se rapporte au fait que l'attaque cible les « gros poissons », qui détiennent généralement une autorité importante et un accès à des informations sensibles. Contrairement aux attaques de phishing traditionnelles qui peuvent cibler un grand volume de personnes lambda, le whaling est une attaque hautement ciblée qui utilise des informations détallées sur la victime pour créer des emails convaincants et personnalisés.

Les personnes influentes sont des cibles intéressantes pour les cybercriminels, car elles ont souvent accès à des informations précieuses, à des ressources financières et à des capacités de prise de décision. En compromettant le compte de messagerie d'un dirigeant, les attaquants peuvent autoriser des transactions frauduleuses, accéder à des données confidentielles et modifier les processus organisationnels.

Phishing vs. whaling

Cheval de Troie

En cybersécurité, le terme « cheval de Troie » ou « cheval de Troie » fait référence à un type de malware qui trompe les utilisateurs en se déguisant en logiciel légitime. Cette menace numérique porte le nom de l'ancienne légende grecque du cheval de Troie, où les soldats grecs se sont cachés à l'intérieur d'un cheval en bois pour s'infiltrer et capturer la ville de Troie. De même, un cheval de Troie en cybersécurité cache son intention malveillante sous couvert d'une application inoffensive, incitant les utilisateurs à exécuter un code nuisible sur leurs appareils. Les chevaux de Troie sont devenus l'une des formes de malware les plus courantes et polyvalentes, posant des risques majeurs pour les personnes et les organisations. Contrairement aux virus ou vers, les chevaux de Troie ne peuvent pas se répliquer ou s'exécuter eux-mêmes et s'appuient plutôt sur des techniques d'ingénierie sociale à installer.

Si un cheval de Troie est installé avec succès sur l'appareil d'un utilisateur, il peut effectuer plusieurs actions malveillantes en fonction de son type et de son objectif. Par exemple, fournir une entrée de porte dérobée pour les pirates, accéder aux données, mots de passe et autres informations sensibles.

Watering Hole Attack

Watering Hole Attack est une cybermenace furtive dans laquelle les pirates informatiques compromettent un site Web de confiance fréquemment visité par un groupe spécifique, comme les employés d'une organisation ciblée. En injectant des logiciels malveillants sur le site, les attaquants infectent les appareils des visiteurs, en accédant aux réseaux et aux données sensibles. Souvent liées aux menaces persistantes avancées (APT), ces attaques sont difficiles à détecter et peuvent entraîner des violations à grande échelle.

Menaces persistantes avancées (APT)

Les menaces persistantes avancées sont des attaques ciblées visant à obtenir un accès à long terme à un réseau pour voler des données sensibles au fil du temps. Les acteurs parrainés par l'État ou les cybercriminels bien financés mènent souvent des menaces persistantes avancées, ciblant des secteurs critiques tels que le gouvernement et la finance. La subtilité des menaces persistantes avancées les rend particulièrement difficiles à détecter, ce qui permet aux attaquants d'exfiltrer en silence des informations précieuses tout en échappant aux défenses de sécurité.

Attaques basées sur l'IoT

L'essor des appareils de l'Internet des objets (IoT) a introduit de nouveaux défis en matière de sécurité, car de nombreux gadgets IoT manquent d'une protection robuste. Les attaquants chercheront à exploiter ces vulnérabilités, en utilisant souvent des appareils compromis dans des botnets à grande échelle, tels que le tristement célèbre botnet Mirai, pour lancer des attaques DDoS ou infiltrer des réseaux plus larges. La sécurisation des appareils IoT est devenue essentielle pour minimiser les risques associés à ces connexions numériques en expansion rapide.

Dans notre deuxième partie, nous évoquerons l'évolution de la cybersécurité.

Evolution de la cybersécurité

1. Des menaces en constante évolution

L'avenir de la cybersécurité sera marqué par l'apparition de nouvelles menaces de plus en plus sophistiquées. Les pirates informatiques utilisent déjà des techniques avancées comme l'intelligence artificielle, les ransomwares (logiciels de rançon) ou encore les attaques ciblées sur les objets connectés (IoT). À l'avenir, les cyberattaques pourraient même viser les infrastructures critiques comme les hôpitaux, les réseaux électriques ou les transports publics.

2. L'intelligence artificielle au service de la protection

Face à ces nouvelles menaces, les spécialistes de la cybersécurité développent des technologies innovantes. L'intelligence artificielle jouera un rôle essentiel pour détecter rapidement les attaques et réagir en temps réel. Les systèmes de sécurité du futur seront capables d'apprendre automatiquement des comportements suspects et de renforcer les défenses sans intervention humaine.

3. Une sensibilisation indispensable

La technologie seule ne suffira pas. L'avenir de la cybersécurité passe aussi par l'éducation des utilisateurs. Les écoles, les entreprises et les administrations devront former les citoyens aux bons réflexes à adopter en ligne : protéger ses mots de passe, reconnaître les tentatives de phishing, sécuriser ses appareils... La cybersécurité deviendra l'affaire de tous.

Avant de finir nous dédierons une partie pour les solutions.

Solutions

Nous savons bien que la technologie règne dans ce monde aujourd'hui. Il ne peut y avoir de marche en arrière pour son évolution. Cependant, il serait judicieux de pouvoir trouver des mesures afin de se protéger.

Notons que les entreprises sont les plus grandes cibles des attaques informatiques. Il est donc important d'avoir un service de cybersécurité en externalisant ou de façon interne en nommant un responsable qui préviendra, analysera les risques et proposera des plans d'actions. Les employés doivent également être formé sur les bons gestes à avoir pour limiter les risques. Il est également important d'avoir d'une habitude de sauvegarde régulière des données (sur support physique et cloud) pour minimiser les dégâts causés par une cyberattaque. L'utilisation de logiciel d'antivirus efficace et de confiance. L'utilisation de mots de passe sécurisés (12 caractères minimum avec lettre majuscules, chiffres, caractères spéciaux) permet de bien protéger ces données. Il est impératif de changer les mots de passe au bout de quelque mois ou en cas de doutes de fuites.

De plus, quelques points essentiels seront fournis ci- après afin de se protéger contre les malveillants

Mettre à jour votre logiciel

La mise à jour de tous vos logiciels et systèmes ajoute une résilience supplémentaire à vos mesures de sécurité. Les mises à jour contiennent généralement des correctifs pour toutes les vulnérabilités connues qui ont été trouvées.

Utiliser des mots de passe forts et une authentification à deux facteurs (2FA)

Vous devez utiliser des mots de passe forts qui contiennent au moins 12 caractères, avec une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux. Essayez de ne pas réutiliser le même mot de passe pour différents comptes, car cela augmente le risque qu'un pirate accède à vos informations. Vous devez également activer la 2FA pour ajouter des couches de sécurité supplémentaires à vos comptes en ligne.

Formation et sensibilisation des employés

L'ingénierie sociale restant un point d'entrée commun pour les attaquants, une formation régulière fournit aux employés les connaissances nécessaires pour reconnaître les emails de phishing, éviter les pièges d'ingénierie sociale et suivre les meilleures pratiques pour protéger les données sensibles. La formation du personnel sur ces tactiques réduit la probabilité d'attaques réussies

Installer un pare-feu

Les pares-feux sont utiles pour empêcher une variété d'attaques de bloquer les accès non autorisés, tels que les ddos ou les attaques de backdoor. Les pares-feux contrôlent le trafic réseau qui circule dans votre système et bloquent le trafic non autorisé entrant ou sortant.

Renforcement de la sécurité avec XDR

La détection et la réponse étendues (XDR) améliorent la cybersécurité en intégrant les données des endpoints, des courriels, des réseaux et des environnements cloud. Il détecte les menaces et y répond en temps réel, empêchant ainsi les attaques telles que les ransomware de se propager sur les réseaux d'entreprise. Grâce à l'analytique et à l'automatisation basées sur l'IA, XDR améliore la détection des menaces, réduit le temps de réponse et renforce la sécurité globale.

Conclusion

En résumé, l’avenir de la cybersécurité repose sur un équilibre entre innovations technologiques et prévention humaine. Les menaces informatiques continueront d’évoluer, mais les moyens de protection s’amélioreront également grâce à l’intelligence artificielle, au développement de systèmes toujours plus performants et à une meilleure sensibilisation des utilisateurs. Dans un monde numérique en constante évolution, rester vigilant et s’adapter aux nouvelles formes de cybercriminalité sera plus que jamais indispensable pour garantir un avenir numérique sûr et sécurisé.

Annexes

Les 15 Types de Cyberattaques les Plus Courantes en 2025 | Trend Micro (FR)

Que faire en cas de cyberattaque ? (Guide pour les dirigeants) - Assistance aux victimes de cybermalveillance

Cybersécurité : les enjeux de 2025 et l'évolution des menaces

Cyberattaques : qui, quoi et pourquoi ?

Comment se protéger contre les cyberattaques ? | UnderNews

Produits et solutions de sécurité Cisco - Cisco

Se protéger des cyberattaques : les 7 piliers de la sagesse | Entrepreneurs