www.reparateurweb.fr

TOUT SAVOIR SUR LA

CYBER SÉCURITÉ

Apprenez à vous protéger
contre le piratage informatique

Table de matières

INTRODUCTION 4

CHAPTITRE 1 5

Aperçu global de la cybersécurité 5

CHAPTITRE 2 14

Dernières tendances en matière de cybersécurité 14

CHAPTITRE 3 20

Guide sur le piratage et comment l'éviter ? 20

CHAPTITRE 4 28

Comment protéger votre smartphone du piratage ? 28

CHAPTITRE 5 33

Un registre sur les types de malwares et comment les gérer 33

CHAPTITRE 6 45

Comment vous prémunir contre la visite de sites Web dangereux 45

CHAPTITRE 7 54

Comprendre le phishing et le ransomware et savoir comment les prévenir 54

CHAPRITRE 8 66

Conseils pour concevoir un budget cyber sécurité post covid-19 66

CHAPITRE 9 71

Comment les entreprises adapteront-elles leurs nouvelles stratégies de cyber sécurité post pandémie ? 71

CHAPITRE 10 75

Étude de cas 75

CONCLUSION 85

INTRODUCTION

Les années 2020 et 2021 ont été une épreuve pour la plupart des organisations, entreprises et sociétés notamment dans le domaine de la cybersécurité.

Malgré un ralentissement, les entreprises réalisent l'importance continue de la protection des données et des systèmes, et les dirigeants sont parfaitement conscients du rôle qu'elle jouera à l'avenir.

Les chefs d'entreprise accordent de plus en plus d'importance à la cybersécurité pour leur entreprise.

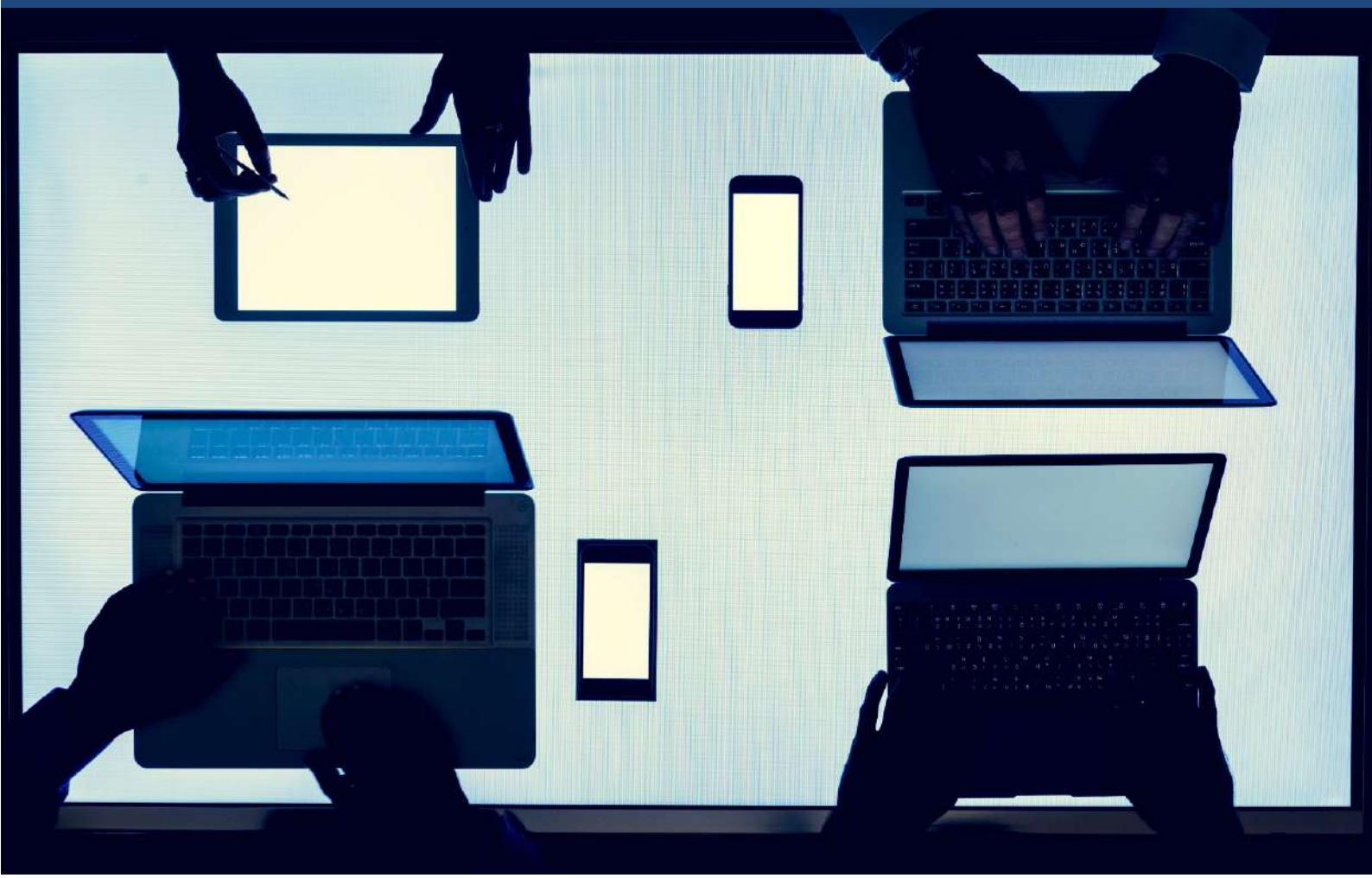
Pour l'année à venir, il est essentiel de continuer à faire de la cybersécurité un enjeu commercial stratégique et de développer davantage de partenariats entre les industries, les chefs d'entreprise, les régulateurs et les décideurs.

Pour commencer, notre guide de formation sur la cybersécurité vous aidera à chaque étape de la création de votre système de protection de vos données sensibles.

Ce guide sur la cybersécurité vous d'obtenir de précieuses informations sur la sécurité à l'ère du COVID.

Ce sont :

- L'élaboration de plans et de budgets de sécurité Les types de menaces
- L'augmentation de leur portée et les solutions correspondantes.
- Il est temps de commencer !



CHAPTITRE 1

Aperçu global de la cybersécurité

Aperçu global de la cyber sécurité

Cybersécurité – Signification

La cybersécurité est le processus de protection des systèmes, des appareils, des réseaux et des données contre tout type d'accès non autorisé ou d'attaque.

Les cyberattaques tentent généralement d'accéder à des informations sensibles et de modifier, perturber, détruire ou contrôler ces informations à des fins malveillantes ou criminelles.

Ces attaques inquiètent de plus en plus les entreprises et les particuliers.

Alors que de plus en plus d'informations et de données continuent de circuler en ligne, tout, des courriels aux cartes de crédit en passant par les systèmes de navigation et les dossiers médicaux, est vulnérable aux attaques numériques.

Types courants de menaces

Les cyberattaques peuvent varier en taille et en portée, mais certains des types de menaces les plus courants incluent :

Hameçonnage

Cela prend généralement la forme d'e-mails qui semblent provenir d'une source fiable et légitime.

Ces communications frauduleuses visent à voler des informations sensibles, telles que des informations de connexion ou des numéros de carte de crédit.

Logiciels malveillants

Un malware est un logiciel malveillant conçu pour obtenir un accès non autorisé ou perturber un ordinateur.

Il viole généralement un réseau si un utilisateur clique sur un lien dangereux, une pièce jointe à un e-mail ou un téléchargement.

Les logiciels malveillants peuvent prendre de nombreuses formes, notamment les virus, les chevaux de Troie, les logiciels espions et les logiciels de rançonnement.

Attaque par interception

Ce type d'attaque implique un cybercriminel interceptant une communication entre deux parties. Le criminel écoute la conversation et se fait passer pour l'une ou les deux parties pour contrôler des informations ou voler des données.

Attaque par déni de service

Dans cette attaque, les cybercriminels submergent et épuisent le réseau et les serveurs avec du trafic pour arrêter ou perturber la disponibilité des services.

Les ressources sont alors indisponibles ou inaccessibles pour les utilisateurs légitimes.

Injection SQL

Une injection SQL, ou requête en langage structuré, se produit lorsqu'un code SQL malveillant est inséré dans la base de données d'une application via une instruction SQL, permettant aux attaquants d'afficher des données sensibles.

Le but de la cybersécurité est de se défendre contre ces menaces courantes en créant des systèmes et en développant des tactiques pour protéger les données.

La cybersécurité est aussi parfois appelée sécurité des technologies de l'information.

Quels sont les types de cybersécurité ?

Il existe cinq principaux types de cybersécurité :

Ce sont :

1. La sécurité des infrastructures critiques
2. La sécurité des mobiles et des applications
3. La sécurité des réseaux
4. La sécurité du cloud
5. La sécurité de l'Internet des objets.

Sécurité des infrastructures critiques

Les infrastructures critiques comprennent les systèmes et les réseaux sur lesquels la société compte, tels que les réseaux électriques, les feux de circulation, la purification de l'eau et les hôpitaux.

Bien qu'il s'agisse d'infrastructures physiques, elles reposent sur des cyber systèmes.

Les gouvernements travaillent avec les propriétaires et les opérateurs d'infrastructures critiques pour les protéger des cyberattaques potentielles.

Sécurité Internet

Ce type de cybersécurité est conçu pour protéger les réseaux internes contre les accès non autorisés. Différents outils, politiques et procédures peuvent être utilisés pour garantir que les réseaux ne seront pas exploités.

Les outils courants incluent les pares-feux, les programmes antivirus et antimalware et les réseaux privés virtuels.

Sécurité des mobiles et des applications

Alors que les utilisateurs stockent davantage de données personnelles sur leurs smartphones, tablettes, ordinateurs portables et autres appareils, la sécurité mobile est un domaine de plus en plus important.

Si un appareil est perdu ou volé, il existe des outils qui peuvent verrouiller l'utilisation d'un appareil mobile ou exiger des mots de passe multi-facteurs avant de pouvoir y accéder.

Au sein de la sécurité mobile se trouve la sécurité des applications, qui consiste à rechercher, prévenir et corriger les vulnérabilités des applications.

Les métiers de la cybersécurité s'efforcent de rendre les applications plus sécurisées afin qu'il n'y ait aucun risque d'accès non autorisé aux données et aux appareils.

La sécurité des applications commence pendant les étapes de conception et de développement et se poursuit après le déploiement des applications.

Sécurité cloud

Ce type de cybersécurité protège les données et les applications stockées sur des systèmes basés sur le cloud.

Les principales menaces pour la sécurité du cloud incluent les données exposées, les utilisateurs non autorisés accédant aux données et les attaques malveillantes pour infecter ou détruire l'infrastructure du cloud.

Les défenses courantes dans la sécurité du cloud incluent le cryptage, les pares-feux et les réseaux privés virtuels.

Sécurité de l'Internet des objets

L'Internet des objets (IoT) fait référence à une variété de systèmes connectés à Internet, tels que les appareils électroménagers, les téléviseurs, les routeurs Wi-Fi et les caméras de sécurité.

De nombreux appareils IoT ont un cryptage faible et des vulnérabilités non corrigées, ce qui signifie qu'ils peuvent être facilement exploités.

Le nombre croissant d'appareils IoT en fait un domaine hautement prioritaire en matière de cybersécurité.

Pourquoi la cybersécurité est-elle importante ?

La cybersécurité est importante car une grande partie de nos informations sensibles, y compris les données personnelles et de santé, la propriété intellectuelle et les systèmes d'information gouvernementaux, sont vulnérables aux attaques et doivent être correctement protégées.

Les cyberattaques peuvent se produire à n'importe quel niveau, grand ou petit. On a enregistré des cas d’intrusions dans les réseaux d'organisations gouvernementales et de citoyens perdant l'accès aux services essentiels.

Au niveau individuel, les victimes de la cybercriminalité ont été confrontées à l'usurpation d'identité, au chantage et à l'extorsion.

Les cyberattaques sont l'un des crimes qui connaissent la croissance la plus rapide au monde. On s'attend à ce que les dommages causés par la cybercriminalité puissent coûter au monde 6 000 milliards de dollars par an.

Les cybercriminels sont de plus en plus innovants dans leurs tactiques, ce qui rend la cybersécurité d'une importance cruciale.

Quels sont les avantages de la cybersécurité ?

Il existe de nombreux avantages en matière de cybersécurité.

Certains des principaux avantages sont qu'il protège les données contre les accès non autorisés, améliore les performances de l'entreprise et contribue à renforcer la confiance des clients.

Il protège des cyberattaques

Les mesures et outils de cybersécurité évaluent les vulnérabilités et empêchent les menaces d'infiltrer les systèmes.

Cela permet de sécuriser les données sensibles et de garantir que seuls les utilisateurs autorisés peuvent accéder aux informations.

Aide à économiser du temps et de l'argent

Les virus peuvent ralentir les ordinateurs et interrompre les opérations commerciales.

Si une violation importante se produit, il peut être coûteux de faire appel à des services externes et à des experts pour en gérer les conséquences.

À long terme, les mesures de cybersécurité finissent par faire gagner du temps et de l'argent aux entreprises.

Améliore la confiance des clients

Une stratégie de cybersécurité robuste inspirera confiance aux clients. De nombreuses entreprises recueillent des informations auprès de leurs clients, de sorte que les clients ont besoin de sentir que leurs données sont entre de bonnes mains.

Récupération rapide d'une violation de données

En cas de cyberattaque, la mise en place des bonnes politiques et des bons plans de récupération permettra à l'entreprise de récupérer et de reprendre rapidement ses activités.

Utilisation de l'automatisation en cybersécurité

L'automatisation est devenue un élément essentiel pour protéger les entreprises contre le nombre croissant et la sophistication des cybermenaces.

L'utilisation de l'intelligence artificielle (IA) et de l'apprentissage automatique dans les domaines où les flux de données sont volumineux peut aider à améliorer la cybersécurité dans trois catégories principales :

Détection des menaces

Les plateformes d'IA peuvent analyser les données et reconnaître les menaces connues, ainsi que prédire de nouvelles menaces.

Réponse aux menaces

Les plateformes d'IA créent et appliquent également automatiquement des paramètres de sécurité.

Réduction de l'intervention humaine

Les professionnels de la sécurité sont souvent surchargés d'alertes et de tâches répétitives.

L'IA peut aider à éliminer la fatigue des alertes en triant automatiquement les alarmes à faible risque et en automatisant l'analyse des mégadonnées et d'autres tâches répétitives, libérant les humains pour des tâches plus sophistiquées.

Les autres avantages de l'automatisation en matière de cybersécurité incluent :

- La classification des attaques
- La classification des logiciels malveillants L'analyse du trafic
- L'analyse de la conformité, etc.

Principaux défis en matière de cybersécurité

La cybersécurité est continuellement mise à l'épreuve par les pirates, la perte de données, la confidentialité, la gestion des risques et l'évolution des stratégies de cybersécurité.

Le nombre de cyberattaques ne devrait pas diminuer de sitôt. De plus, l'augmentation des points d'entrée pour les attaques, comme avec l'arrivée de l'Internet des objets (IoT), augmente le besoin de sécuriser les réseaux et les appareils.

L'un des éléments les plus problématiques de la cybersécurité est la nature évolutive des risques de sécurité.

À mesure que de nouvelles technologies émergent et que la technologie est utilisée de manières nouvelles ou différentes, de nouvelles voies d'attaque sont développées.

Il peut être difficile de suivre ces changements et progrès fréquents en matière d'attaques, ainsi que de mettre à jour les pratiques pour s'en protéger.

Les problèmes consistent notamment à s'assurer que tous les éléments de la cybersécurité sont continuellement mis à jour pour se protéger contre les vulnérabilités potentielles.

Cela peut être particulièrement difficile pour les petites organisations sans personnel ou ressources internes.

De plus, les organisations peuvent collecter de nombreuses données potentielles sur les personnes qui utilisent un ou plusieurs de leurs services.

Avec plus de données collectées, la probabilité qu'un cybercriminel veuille voler des informations personnellement identifiables (PII) est une autre préoccupation.

Par exemple, une organisation qui stocke des informations personnelles dans le cloud peut être soumise à une attaque de ransomware. Les organisations doivent faire face à d’énormes défis pour empêcher une violation du cloud.

Les programmes de cybersécurité doivent également aborder la formation des utilisateurs finaux, car les employés peuvent accidentellement introduire des virus sur leur lieu de travail sur leurs ordinateurs portables ou leurs appareils mobiles.

Une formation régulière de sensibilisation à la sécurité aidera les employés à faire leur part pour protéger leur entreprise des cybermenaces.

Un autre défi à la cybersécurité comprend une pénurie de personnel qualifié en matière de cybersécurité.

À mesure que la quantité de données collectées et utilisées par les entreprises augmente, le besoin en personnel de cybersécurité d'analyser, de gérer et de répondre aux incidents augmente également.

Des centres de recherches ont estimé l'écart sur le lieu de travail entre les emplois nécessaires en cybersécurité et les professionnels de la sécurité à 3,1 millions d'unités.

Maintenir la cybersécurité dans un paysage de menaces en constante évolution est un défi pour toutes les organisations.

Les approches réactives traditionnelles, dans lesquelles des ressources étaient consacrées à la protection des systèmes contre les plus grandes menaces connues, alors que les menaces moins connues n'étaient pas défendues, ne sont plus une tactique suffisante.

Pour suivre l'évolution des risques de sécurité, une approche plus proactive et adaptative est nécessaire.

Plusieurs organisations clés de conseil en cybersécurité offrent des conseils.

Par exemple, le National Institute of Standards and Technology (NIST) recommande d'adopter une surveillance continue et des évaluations en temps réel dans le cadre d'une évaluation des risques pour se défendre contre les menaces connues et inconnues.

CHAPTITRE 2

Dernières tendances en matière de cybersécurité

Dernières tendances en matière de cybersécurité

Au cours de la dernière année, le COVID-19 a eu un impact plus important sur les habitudes de travail et les environnements de sécurité que toute autre urgence sanitaire connue à ce jour.

Cela, combiné à des avancées technologiques telles que la 5G, a conduit à plusieurs tendances que nous prévoyons voir cette année et l'année à venir également.

Voici donc notre top dix :

Une augmentation des attaques sur les infrastructures distantes

En raison de la pandémie, nous avons vu une énorme augmentation du nombre de travailleurs quittant des emplacements centralisés vers des bureaux à domicile.

Ceci, à son tour, a conduit à une augmentation de l'utilisation de technologies facilitant le travail à distance, telles que le courrier électronique, le VPN et le bureau à distance (RDP).

Dans de nombreux cas, les travailleurs ont commencé à travailler à distance si rapidement que les organisations n'ont pas eu suffisamment de temps pour examiner pleinement les implications en matière de sécurité.

Cela a créé un potentiel d'attaque accru, dans lequel les criminels comprennent les points faibles et comment en tirer parti, en particulier avec le VPN.

Malheureusement, nous avons déjà pu enregistrer plusieurs compromissions et nous nous attendons à ce que cela continue. Autant dire que les entreprises doivent se concentrer sur la sécurisation de leurs infrastructures VPN et RDP.

Les appareils intelligents évolueront de connectés à autonomes

Les villes intelligentes, la fabrication intelligente, le transport intelligent et la logistique investiront pour devenir plus autonomes.

Les appareils intelligents utilisés pour l'automatisation dans les usines de fabrication, le transport et la logistique deviendront plus autonomes, avec plus d'intelligence intégrée et moins de connexions à temps plein.

Cela aura un impact sur la latence, la disponibilité de la connexion et les problèmes de sécurité.

Le problème de latence est dû au fait de devoir communiquer avec des services cloud centralisés, ce qui peut prendre plus de temps qu'il n'est idéal pour que les systèmes en temps réel réagissent aux événements qui se produisent dans le monde physique.

De même, une perte de connectivité pour un certain nombre de raisons (panne de courant, panne de cloud, cyberattaque) peut avoir un impact sur les appareils intelligents qui ne sont pas autonomes.

Et plus vous êtes connecté et interagissez avec des services externes, plus la sécurité est exposée aux attaques.

En tant que tel, nous verrons plus de systèmes intelligents qui peuvent fonctionner par eux- mêmes, en utilisant des connexions principalement pour la surveillance à distance.

L'intelligence sera fournie par MEC et les services cloud de périphérie, et la vitesse fulgurante de la 5G sera un moteur essentiel pour une collaboration intelligente entre les systèmes.

Internet deviendra une grande usine de services interconnectée

Nous nous dirigeons vers des API pour les applications Web, les organisations prenant certains services et les plaçant dans différents clouds interconnectés.

C'est le début d'un maillage complet de services interconnectés de la périphérie aux clouds centraux, créant efficacement une hiérarchie entièrement maillée.

Le risque est qu'en cas de défaillance d'un composant, l'ensemble du système soit impacté.

La centralisation dans les principaux fournisseurs de cloud tels qu'Amazon Web Services (AWS) et DNS augmente la probabilité de pannes à grande échelle.

Attendez-vous à en voir de plus en plus dans les années à venir.

Nous verrons des impacts plus importants dus à la centralisation, notamment des pannes généralisées et des dommages collatéraux.

La plupart des utilisateurs d'appareils intelligents courants ne comprennent pas à quoi ils sont connectés.

Ainsi, lorsque AWS tombe en panne et que les appareils domestiques IoT cessent de fonctionner, cela peut être problématique.

Nous en sommes venus à compter sur les systèmes de sonnette intelligente et d'aspirateur robotique sans tenir compte de l'importance de connexions sécurisées et fiables.

Les utilisateurs en ligne plus avancés et non étatiques tenteront d'influencer et de perturber

Les utilisateurs ordinaires apprennent maintenant les compétences TTPS utilisées par les groupes APT et d'autres organisations cybercriminelles.

Nous prévoyons des opérations plus localisées par les citoyens locaux pour influencer et perturber les processus à l'intérieur de leurs pays. Et en raison de leur accès aux médias sociaux, ils peuvent avoir un impact significatif.

Les fournisseurs de connectivité Internet devront fournir plus de bande passante excédentaire pour faire face au « bruit gris » d'Internet

Les méthodes de “white, grey and black” hacking, ainsi que les attaques DDoS, consomment de la bande passante Internet.

En tant que tel, chaque échange Internet, fournisseur de transit et FAI devra prendre en compte ce trafic lors du dimensionnement du réseau.

L'augmentation du bruit gris rend plus chronophage et coûteux la détermination du bon trafic du mauvais. En fin de compte, les coûts pour cela seront répercutés sur les entreprises et les consommateurs.

Attendez-vous à plus de problèmes de robots malveillants

En 2020, nous avons vu des campagnes de scalping PS5/XBOX Series X|S impacter les consommateurs. Maintenant, des individus utilisent des robots de sniping pour contrer les scalpers sur les marchés. Et ce ne sont pas seulement les acteurs malveillants ou les pirates informatiques qui créent des scripts pour acheter quelque chose plus rapidement.

Les gens ordinaires achètent du matériel ou créent des objets, recettes... appris via des vidéos YouTube. Si vous n'avez pas de bot, vous êtes désormais désavantagé pour acheter des produits convoités.

Les entreprises auront besoin d'une atténuation avancée des bots pour mieux se protéger et protéger leurs marques contre les individus utilisant des bots qui limitent la disponibilité pour les clients potentiels.

Les ransomwares continueront de régner sur le pays

Attendez-vous à voir encore plus d'e-mails qui vous incitent à cliquer sur des liens frauduleux.

Ces schémas de phishing peuvent utiliser des problèmes d'actualité tels que l'accès précoce aux vaccinations contre le COVID-19 ou d'autres sujets qui ont une forte attraction émotionnelle.

En conséquence, nous verrons encore plus de charges utiles de ransomware livrées via le phishing.

Les fausses nouvelles "fake news" deviendront une seconde nature

Habituez-vous, il n'y a pas de solution miracle. Des entreprises telles que Facebook et Twitter ont essayé de le combattre avec l'IA (intelligence artificielle), mais ces technologies ne sont pas encore assez sophistiquées pour une détection et une classification de haute qualité.

Le problème majeur est que l'IA a besoin de données historiques pour comprendre si quelque chose est vrai ou faux, quelque chose qui n'est pas toujours disponible.

En conséquence, nous voyons beaucoup de faux positifs. Malheureusement, les attaquants ne se soucient pas des faux positifs, contrairement aux défenseurs.

Lorsqu'une fausse campagne est identifiée, les attaquants en développent simplement une meilleure.

Pour aller de l'avant avec l'intelligence artificielle, nous aurons besoin d'un apprentissage en profondeur amélioré pour une meilleure détection.

Attendez-vous à voir une augmentation de la propagande Covid-19

Cette désinformation peut être liée au nombre d'infections et de décès ainsi qu'à l'efficacité des masques et autres équipements de protection individuelle.

Nous verrons également des mythes se répandre autour des vaccinations et des effets secondaires.

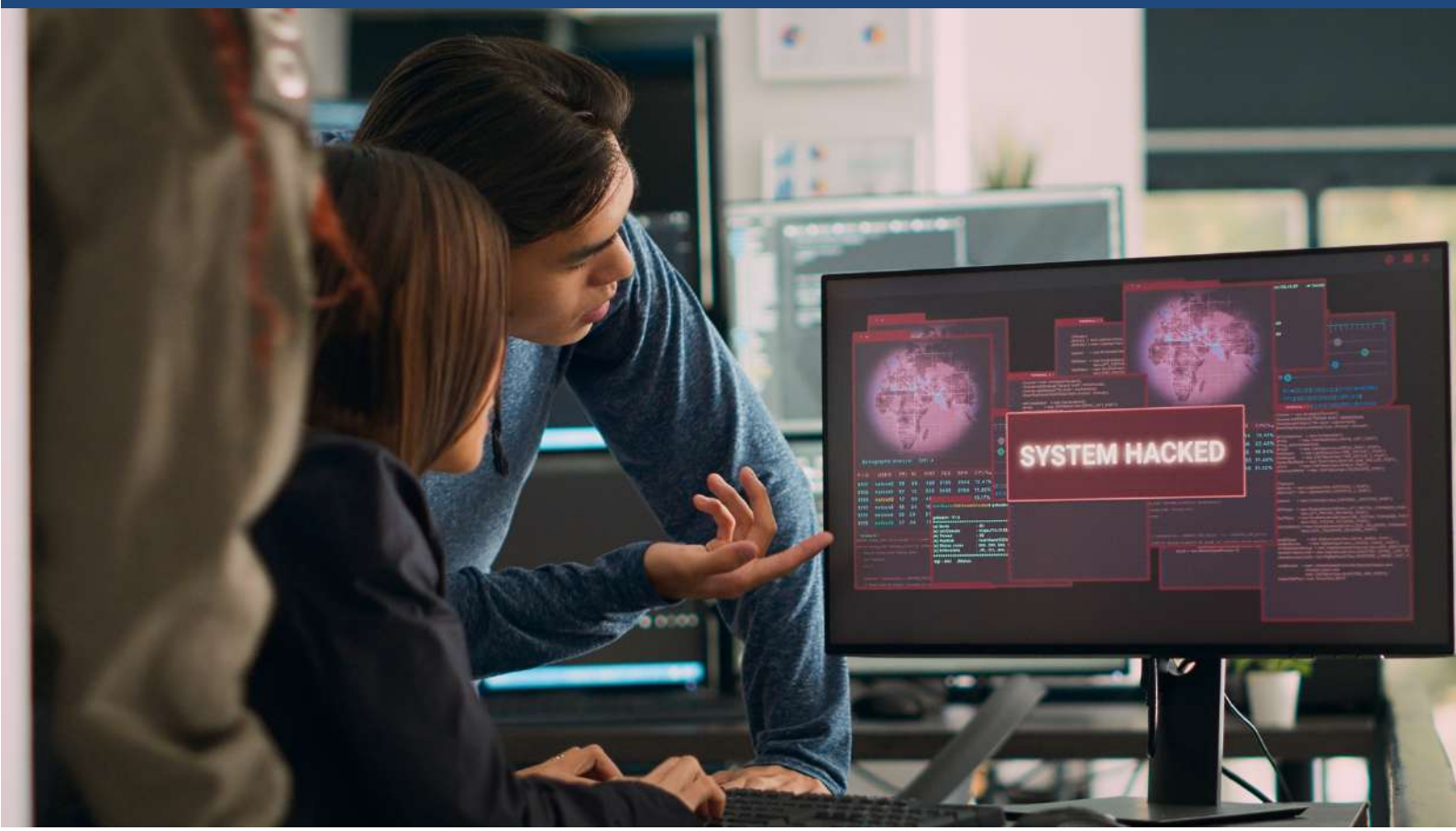
Les personnes sujettes aux théories du complot cliqueront sur ces liens depuis leurs ordinateurs personnels et professionnels et, à terme, les exposeront potentiellement à des infections.

En conséquence, les organisations doivent repenser la meilleure façon de s'organiser en ces temps incertains, de rester en sécurité et de survivre à cette période indéfinie de travail à distance et d'interactions virtuelles.

De nombreuses entreprises ont du mal à adapter leur stratégie de sécurité pour s'adapter à la nouvelle normalité.

Le travail à distance étant désormais une réalité permanente, il y a eu une ruée pour adopter et intégrer une multitude de nouveaux outils et plates-formes cloud pour faciliter la collaboration et maintenir la productivité.

Ceci, associé au fait que s'appuyer uniquement sur un pare-feu d'entreprise n'est plus une bonne stratégie de sécurité, met de nombreuses organisations en danger.



CHAPTITRE 3

Guide sur le piratage et comment l'éviter ?

Guide sur le piratage et comment l'éviter ?

Qu'est-ce que le piratage ?

Le piratage est l'activité consistant à identifier les faiblesses d'un système informatique ou d'un réseau afin d'exploiter la sécurité pour accéder à des données personnelles ou professionnelles.

Un exemple de piratage informatique peut être l'utilisation d'un algorithme de craquage de mot de passe pour accéder à un système informatique.

Les ordinateurs sont devenus obligatoires pour gérer une entreprise. Il ne suffit pas d'avoir des systèmes informatiques isolés ; ils doivent être mis en réseau pour faciliter la communication avec les entreprises externes.

Cela les expose au monde extérieur et au piratage.

Le piratage du système consiste à utiliser des ordinateurs pour commettre des actes frauduleux tels que l'atteinte à la vie privée, le vol de données d'entreprise/personnelles, etc.

Les cybercrimes coûtent des millions de dollars à de nombreuses organisations chaque année. Les entreprises doivent se protéger contre de telles attaques.

Types de pirates et de piratages

Il existe généralement quatre facteurs clés qui conduisent à pirater des sites Web ou des systèmes :

Ce sont :

- Le gain financier par le vol de détails de carte de crédit ou par fraude de services financiers L'espionnage d'entreprise
- La reconnaissance, la notoriété et le respect vis-à-vis des talents de hackeur
- Le piratage orchestré par certains états qui vise à voler des informations commerciales et des renseignements nationaux sensibles

Voici quelques-uns des types de pirates informatiques les plus courants qui mènent ces activités :

Black Hat Hackers

Les Black Hat Hackers sont les "méchants" de la scène du piratage.

Ils travaillent pour découvrir les vulnérabilités des systèmes informatiques et des logiciels afin de les exploiter à des fins financières ou à des fins plus malveillantes, telles que la réputation, l'espionnage commercial ou dans le cadre d'une campagne de piratage d'État.

Les actions de ces individus peuvent infliger de graves dommages à la fois aux utilisateurs d'ordinateurs et aux organisations pour lesquelles ils travaillent.

Ils peuvent voler des informations personnelles sensibles, compromettre les systèmes informatiques et financiers et altérer ou supprimer les fonctionnalités de sites Web et de réseaux critiques.

White Hat Hackers

Les White Hat Hackers peuvent être considérés comme les « bons gars » qui tentent d'empêcher le succès des BHH par le biais d'un piratage proactif.

Ils utilisent leurs compétences techniques pour pénétrer dans les systèmes afin d'évaluer et de tester le niveau de sécurité du réseau, également connu sous le nom de piratage éthique.

Cela permet d'exposer les vulnérabilités des systèmes avant que les pirates informatiques ne puissent les détecter et les exploiter.

Les techniques utilisées par les white hat hackers sont similaires ou même identiques à celles des pirates au BHH, mais ces personnes sont embauchées par des organisations pour tester et découvrir des failles potentielles dans leurs défenses de sécurité.

Grey Hat Hackers

Les Grey Hat Hackers se situent quelque part entre les bons et les méchants.

Contrairement aux BHH, ils tentent de violer les normes et les principes, mais sans avoir l'intention de nuire ou à but financier.

Leurs actions sont généralement menées pour le bien commun. Par exemple, ils peuvent exploiter une vulnérabilité pour faire prendre conscience qu'elle existe, mais contrairement aux pirates informatiques, ils le font publiquement.

Si l'intention peut sembler bonne, la méthode est discutable car, cela alerte les acteurs malveillants de l'existence de la vulnérabilité.

Appareils les plus vulnérables au piratage Appareils intelligents

Les appareils intelligents, tels que les smartphones, sont des cibles lucratives pour les pirates. Les

appareils Android ont un processus de développement logiciel plus open source et incohérent que les appareils Apple, ce qui les expose à un risque de vol ou de corruption de données. Cependant, les pirates ciblent de plus en plus les millions d'appareils connectés à l'Internet des objets (IoT).

Caméras Web

Les webcams intégrées aux ordinateurs sont une cible de piratage courante, principalement parce que leur piratage est un processus simple. Les pirates informatiques accèdent généralement à un ordinateur à l'aide d'un cheval de Troie d'accès à distance (RAT) dans un malware rootkit, ce qui leur permet non seulement d'espionner les utilisateurs, mais aussi de lire leurs messages, de voir leur activité de navigation, de prendre des captures d'écran et de pirater leur webcam.

Routeurs

Le piratage des routeurs permet à un attaquant d'accéder aux données envoyées et reçues à travers eux et aux réseaux auxquels ils accèdent.

Les pirates peuvent également détourner un routeur pour effectuer des actes malveillants plus larges tels que des attaques par déni de service distribué (DDoS), l'usurpation de système de noms de domaine (DNS) ou le minage de crypto.

E-mail

Le courrier électronique est l'une des cibles les plus courantes des cyberattaques.

Il est utilisé pour diffuser des logiciels malveillants et des ransomwares et comme tactique pour les attaques de phishing, qui permettent aux attaquants de cibler les victimes avec des pièces jointes ou des liens malveillants.

Téléphones jailbreakés

Jailbreaker un téléphone signifie supprimer les restrictions imposées à son système d'exploitation pour permettre à l'utilisateur d'installer des applications ou d'autres logiciels non disponibles via sa boutique d'applications officielle.

En plus d'être une violation du contrat de licence de l'utilisateur final avec le développeur du téléphone, le jailbreak expose de nombreuses vulnérabilités.

Les pirates peuvent cibler les téléphones jailbreakés, ce qui leur permet de voler toutes les données de l'appareil, mais également d'étendre leur attaque aux réseaux et systèmes connectés.

Comment fonctionne le piratage ?

Les techniques de piratage évoluent en permanence et il est important de se tenir au courant des nouvelles menaces.

Les pirates informatiques recherchent généralement deux choses dans votre entreprise : des données ou de l'argent.

Ils sont généralement motivés par les deux, car la découverte d'une multitude de données peut être un préliminaire à se remplir les poches.

Comment ces pirates informatiques trouvent-ils les vulnérabilités dans les systèmes, les exploitent-ils et en profitent-ils personnellement ? Trois grands itinéraires règnent en maître :

- ***Ingénierie sociale*** : Le moyen le plus simple de pirater un compte ou un système ? Il suffit de demander à l'utilisateur son mot de passe ! Cela peut prendre la forme d'appels téléphoniques de phishing ou de spam, alors faites attention à qui vous donnez vos informations d'identification.

Une fois qu'un pirate a votre mot de passe, il peut facilement récupérer les informations de votre carte de crédit et de débit, votre numéro de sécurité sociale et d'autres éléments que vous souhaitez garder cachés.

- ***Piratage basé sur la programmation :*** plus avancé que l'ingénierie sociale, le piratage basé sur la programmation exige du pirate qu'il trouve les vulnérabilités d'un système et qu'il s'empare de tous les privilèges administratifs.

- ***Accès physique :*** Bien entendu, le moyen le plus simple de pirater un ordinateur ou un système est d'y avoir un accès physique pendant une longue période.

Pouvons-nous vous implorer de faire attention à vos biens ou même d'investir dans un système de sécurité à domicile ?

Il existe aussi d'autres méthodes de piratage

- ***Dispositifs d'injection de logiciels malveillants :*** les cybercriminels peuvent utiliser du matériel pour introduire des logiciels malveillants sur votre ordinateur.

Vous avez peut-être entendu parler de clés USB infectées, qui peuvent donner aux pirates un accès à distance à votre appareil dès qu'elles sont branchées sur votre ordinateur.

Tout ce qu'il faut, c'est qu'une personne vous donne une clé USB infectée par des logiciels malveillants, et en la branchant simplement sur votre ordinateur, vous êtes infecté.

Les pirates informatiques intelligents utilisent désormais des cordons pour injecter des logiciels malveillants, tels que des câbles USB et des cordons de souris.

Il est donc crucial de toujours réfléchir avant de brancher quoi que ce soit sur un appareil de travail ou dans un conseil personnel avec accès aux données liées au travail.

- ***Correctifs de sécurité manquants :*** les outils de sécurité peuvent devenir obsolètes à mesure que le paysage du piratage évolue et nécessitent des mises à jour fréquentes pour se protéger contre les nouvelles menaces.

Cependant, certains utilisateurs ignorent les notifications de mise à jour ou les correctifs de sécurité, se laissant ainsi vulnérables.

- ***Déni de service distribué (DDoS) :*** cette technique de piratage vise à supprimer un site Web, de sorte qu'un utilisateur ne puisse pas y accéder ou fournir son service.

Les attaques DoS fonctionnent en inondant le serveur de la cible d'importants afflux de trafic.

Le montant est si fréquent et élevé qu'il surcharge le serveur en lui donnant plus de requêtes qu'il ne peut en gérer. En fin de compte, votre serveur tombe en panne et votre site Web tombe en panne avec lui.

Les grandes entreprises peuvent être touchées par une attaque par déni de service distribué (DDoS), qui est une attaque synchronisée sur plusieurs serveurs ou sites Web, susceptible de supprimer de nombreux actifs en ligne.

Utilisez un service de protection dans le cloud ou des services d'atténuation DDoS pour protéger votre entreprise d'un retrait de site.

Pourquoi le piratage est mauvais ?

Comme tout pouvoir, le piratage peut être utilisé pour le bien et le mal. Commençons par le mauvais.

Les pirates non éthiques peuvent :

- Voler des informations de carte de crédit, des informations personnelles, des identifiants de connexion, etc.
- Attaquer la sécurité nationale d'autres pays
- Injecter des logiciels malveillants dans les ordinateurs.
- Modifier ou détruire des données.

Les pirates éthiques, en revanche, peuvent utiliser le piratage pour :

- Hacktivisme, c'est-à-dire causes politiques ou sociales.
- Amélioration de la sécurité des sites Web ou des applications.
- Compte tenu des attaques par ransomware et chevaux de Troie actuellement favorisées par les pirates informatiques, la question est maintenant : comment puis-je protéger mon entreprise contre le piratage ?

Voici quelques conseils pour rester en sécurité

- **Mettre en œuvre la segmentation du réseau**

  Répartir vos données sur des sous-réseaux plus petits réduit votre exposition lors d'une attaque. Cela peut aider à contenir les infections sur quelques points de terminaison seulement au lieu de toute votre infrastructure.

- **Appliquer le principe du moindre privilège (PoLP)**

  En donnant uniquement aux utilisateurs le niveau d'accès, ils doivent effectuer leur travail et rien de plus, vous ne pouvez minimiser les dommages potentiels des attaques de ransomware.

- **Sauvegardez toutes vos données**

  Cela vaut également pour tous les points de terminaison de votre réseau et des partages réseau. Si vos données sont archivées, vous pouvez toujours effacer un système infecté et restaurer à partir d'une sauvegarde.

- **Éduquer les utilisateurs finaux sur la façon de détecter les courriels frauduleux**

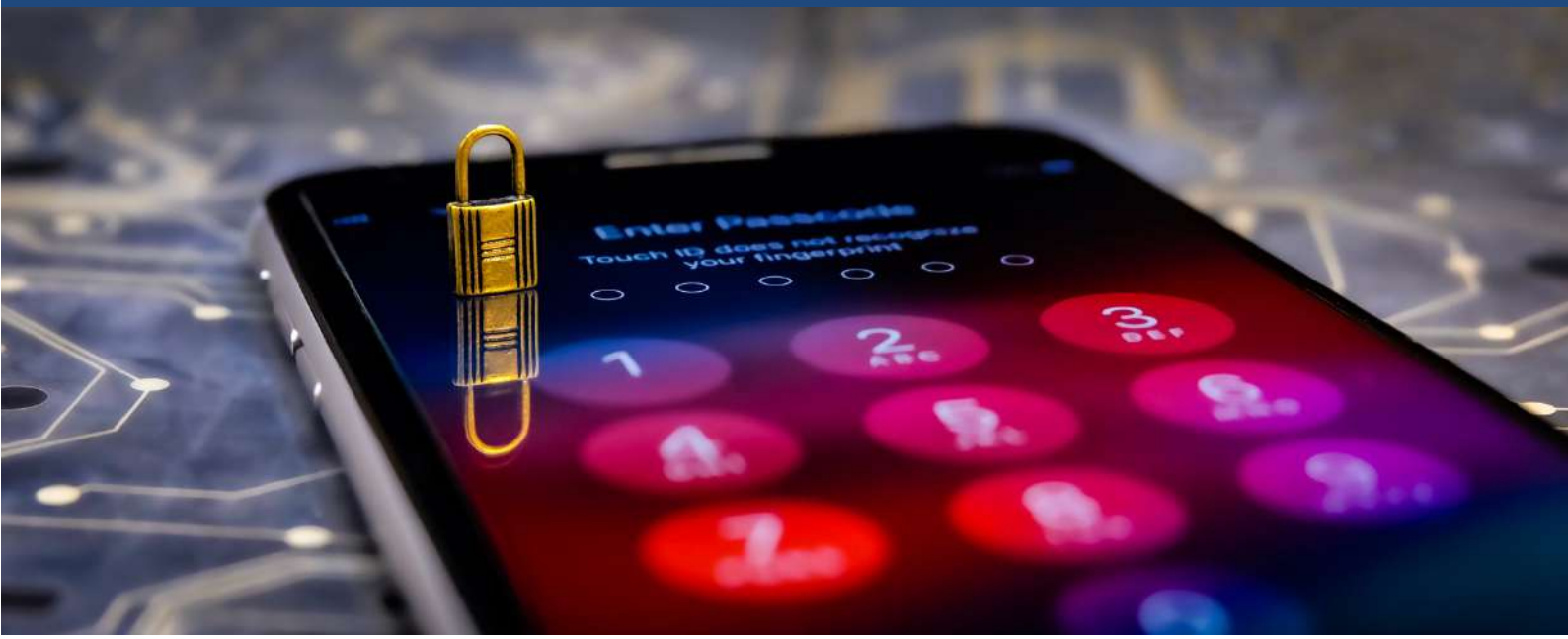
  Les utilisateurs doivent se méfier des e-mails non sollicités et des pièces jointes provenant d'expéditeurs inconnus.

  Entraînez les utilisateurs finaux à se renseigner davantage si des e-mails suspects semblent provenir d'une source fiable. Un simple appel téléphonique ou e-mail permet d'éviter les logiciels malveillants.

- **Former votre personnel**

  Initiez-les à la création de mots de passe forts et imposez-leur de mettre en œuvre une forme d'authentification multifacteur (MFA)— l'authentification à deux facteurs au strict minimum.

  - Corrigez et mettez à jour votre logiciel.
  - Soyez proactif en matière de protection des terminaux.



CHAPTITRE 4

Comment protéger votre smartphone du piratage ?

Comment protéger votre smartphone du piratage ?

Qu'il s'agisse d'écouter un podcast sur le chemin du travail, de faire des calculs rapides car nos compétences en calcul mental se sont presque complètement détériorées, ou de mettre tout, des films aux rendez-vous chez le médecin, dans notre calendrier, vous sollicitez continuellement votre smartphone.

Ainsi, si nous devions être piratés, nous aurions de gros problèmes, risquant de perdre des informations sur nos cartes de crédit et de débit, notre emplacement, notre numéro de sécurité sociale, etc.

Il existe plusieurs façons d'empêcher les pirates d'accéder à votre smartphone, et aucune d'entre elles ne nécessite beaucoup de temps ou d'efforts.

En quelques minutes, vous pouvez passer de zéro à héros en matière de sécurité des smartphones. Commençons !

Ne pas jailbreaker

Non, ce n'est pas un jeu de Monopoly. Jailbreaker votre smartphone signifie que vous avez un contrôle total sur votre smartphone, en évitant les restrictions du fabricant.

Ainsi, sur un iPhone, par exemple, cela signifie que vous pourrez utiliser des applications à partir d'endroits autres que la boutique d'applications officielle d'Apple, et apporter des modifications à l'iOS de votre téléphone.

Cependant, nous ne recommandons pas le jailbreak car la liberté s'accompagne d'un manque de sécurité.

Tout d'abord, vous ne devez pas télécharger d'applications qui ne proviennent pas de l'App Store, car elles n'ont pas été testées contre les logiciels malveillants.

En fait, lorsque vous jailbreakez votre téléphone, vous supprimez essentiellement toutes les mesures de sécurité que le fabricant a intégrées à leurs smartphones. Pensez-y comme à raser la clôture autour de votre maison.

Verrouillez votre smartphone plus tôt

Dans les moments où nous n'avons pas nos smartphones à portée de main, vous avez peut-être remarqué qu'ils se verrouillent, vous obligeant à entrer votre mot de passe ou des données biométriques comme votre empreinte digitale ou votre visage.

Bien qu'il puisse être ennuyeux de devoir se connecter à chaque fois, en fin de compte, cela protège votre appareil, nous vous recommandons donc de régler votre verrouillage automatique sur 30 secondes, ce qui signifie qu'il se verrouillera sans activité pendant 30 secondes.

Et si vous n'avez pas du tout activé le verrou, il va sans dire que vous devriez probablement changer cela.

Effectuer toutes les mises à jour logicielles

Des entreprises comme Google et Apple ont des gens qui travaillent 24 heures sur 24 pour améliorer la sécurité du smartphone, donc s'il y a une mise à jour iOS ou Android, faites-le.

Bien que ces mises à jour puissent être ennuyeuses, elles sont incroyablement nécessaires pour rester à jour avec les logiciels de sécurité les plus récents et les plus performants.

Nous vous recommandons de les faire la nuit, afin que vous ne soyez jamais sans votre smartphone pendant vos heures de veille !

Configurer l'authentification à deux facteurs

Si vous avez fait attention, alors vous savez que c'est une idée intelligente d'activer le verrouillage automatique, vous devrez donc entrer un mot de passe pour accéder à votre smartphone, mais si vous voulez aller plus loin, nous ' d configurer l'authentification à deux facteurs.

De cette façon, si quelqu'un devine votre mot de passe, il ne pourra toujours pas accéder à votre téléphone, car votre compagnie de téléphone vous enverra un autre code par SMS ou appel téléphonique.

Encore une fois, cela rendra l'ouverture de votre smartphone un peu plus fastidieuse, mais c'est une idée fantastique si vous voulez vraiment éviter les pirates.

Créer un code d'accès long

Lors du choix d'un mot de passe, les gens ont tendance à faire quelque chose d'évident, comme leur anniversaire, les numéros dans l'ordre chronologique ou une partie de leur numéro de téléphone. Ce n'est pas la pratique la plus sûre.

Au contraire, les nombres doivent être vraiment aléatoires et assurez-vous d'utiliser un code d'accès à six chiffres, le plus long possible.

Bien qu'il soit un peu plus difficile de se souvenir de ce numéro, il sera également plus difficile à deviner pour les pirates, ce qui est finalement une bonne chose pour la sécurité de votre téléphone.

Activer Effacer les données

Maintenant, que se passe-t-il si votre smartphone est perdu ou volé et que pour une raison quelconque, vos pirates peuvent accéder à votre compte ?

Bien sûr, c'est le pire des cas, mais d'une manière étrange, réfléchir à ce qu'il faut faire dans ces situations est en quelque sorte notre travail.

Ne vous inquiétez pas, il existe une solution, et c'est d'activer Effacer les données, autrement dit configurer votre smartphone pour qu'il s'autodétruise.

L'autre option consiste à faire en sorte que le téléphone s'autodétruise automatiquement après trop de tentatives infructueuses de mot de passe.

Bien sûr, il s'agit d'une mesure plus extrême, mais qui augmentera finalement la sécurité de votre smartphone.

Évitez l'hameçonnage et les fenêtres contextuelles

L'hameçonnage est devenu de plus en plus sophistiqué, envoyant à des personnes férues de technologie des liens et des publicités contextuelles apparemment légitimes.

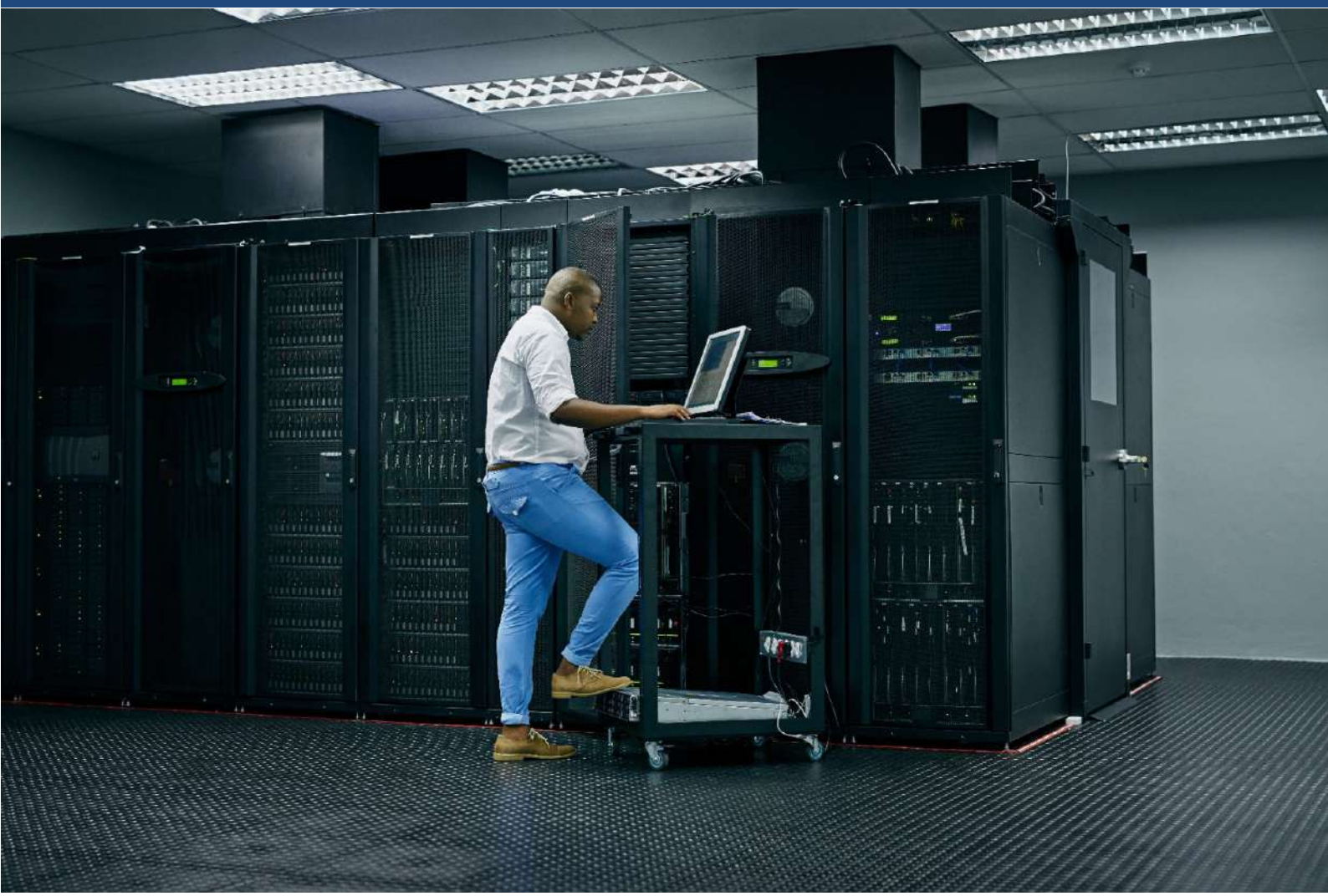
Bien que le phishing soit un sujet, nous avons beaucoup plus à dire, il y a quelques notions de base que nous voulons vous transmettre.

Désactiver le remplissage automatique

Le remplissage automatique, qui remplit automatiquement les formulaires avec vos informations personnelles et financières, est à la fois incroyablement pratique et incroyablement dangereux si votre téléphone tombe entre de mauvaises mains.

Qu'est-ce qui empêche un pirate informatique ou un voleur d'utiliser les informations de votre carte de crédit pour s'acheter une nouvelle garde-robe ?

Bien que cela puisse vous rendre la vie un peu plus fastidieuse, c'est l'idée la plus sûre de désactiver le remplissage automatique sur votre smartphone.



CHAPTITRE 5

Un registre sur les types de malwares et comment les gérer

Un registre sur les types de malwares et comment les gérer

Un malware est un logiciel indésirable sur votre ordinateur qui, souvent, est conçu pour causer des dommages.

Depuis les débuts de l'informatique, un large éventail de types de logiciels malveillants dotés de fonctions variées a vu le jour.

À la base, les logiciels malveillants exploitent les vulnérabilités existantes du réseau, des appareils ou des utilisateurs, posant aussi peu de risques que des publicités ennuyeuses.

En revanche, il existe des "malwares" bien plus dangereux et agressifs qui pourraient causer des dégâts bien plus dommageables. On parle de, potentiellement, des milliers voire des millions d'euros de rançon.

Voici quelques menaces de logiciels malveillants courantes et moins courantes et comment s'en défendre.

Ce sont :

Logiciels publicitaires

Les logiciels publicitaires, également connus sous le nom de publicité malveillante, adware, sont un type de programme qui télécharge ou affiche des publicités sur l'interface utilisateur.

Plutôt que de voler des données, les logiciels publicitaires sont plutôt un irritant forçant les utilisateurs à voir des publicités indésirables.

La plupart des utilisateurs sont habitués aux logiciels publicitaires sous la forme de fenêtres contextuelles de navigateur impossibles à fermer.

Les utilisateurs s'infectent parfois sans le savoir avec des logiciels publicitaires installés par défaut lorsqu'ils téléchargent et installent d'autres applications.

Comment se défendre contre les logiciels publicitaires ?

Installez une solution antivirus qui inclut des fonctionnalités anti-adware. Désactivez les fenêtres contextuelles sur vos navigateurs et faites attention au processus d'installation lors de l'installation de nouveaux logiciels, en vous assurant de décocher toutes les cases qui installeront des logiciels supplémentaires par défaut.

Portes dérobées

Une porte dérobée est un cheval de Troie qui offre à un attaquant un accès à distance à l'appareil de la victime.

La plupart des fabricants d'appareils ou de logiciels placent des portes dérobées dans leurs produits intentionnellement et pour une bonne raison.

Si nécessaire, le personnel de l'entreprise ou les forces de l'ordre peuvent utiliser la porte dérobée pour accéder au système en cas de besoin.

Cependant, entre les mains d'un pirate, une porte dérobée peut faire tout ce que l'utilisateur fait. Les portes dérobées peuvent également être installées par d'autres types de malwares, tels que des virus ou des rootkits.

Comment se défendre contre une porte dérobée ?

Les portes dérobées sont parmi les types de menaces les plus difficiles à protéger. Les experts disent que la meilleure défense est une stratégie de sécurité réseau à plusieurs volets qui comprend un pare-feu, un logiciel anti-malware, une surveillance du réseau, une détection et prévention des intrusions (IDPS) et une protection des données.

Bots et botnets

Les bots sont des logiciels effectuant des tâches automatisées, rendant les attaques connues sous le nom de « botnets » mortelles pour les victimes. En cybersécurité, un bot fait généralement référence à un appareil infecté contenant un logiciel malveillant.

À l'insu ou sans la permission de l'utilisateur, un bot peut corrompre l'appareil. Les attaques de botnets sont des efforts ciblés d'une armée de bots, dirigée par leur bot herder.

Comment se défendre contre les botnets ?

Les organisations peuvent empêcher que leurs ordinateurs ne fassent partie d'un botnet en installant un logiciel anti-malware, en utilisant des pares-feux, en gardant les logiciels à jour et en forçant les utilisateurs à utiliser des mots de passe forts.

Un logiciel de surveillance de réseau peut également aider à déterminer quand un système fait partie d'un botnet.

Modifiez toujours les mots de passe par défaut pour tous les appareils IoT que vous installez avant une utilisation prolongée.

Pirate de navigateur

Un pirate de navigateur également appelé « piratage » modifie sensiblement le comportement de votre navigateur Web.

Ce changement peut vous envoyer vers une nouvelle page de recherche, ralentir le chargement, modifier votre page d'accueil, installer des barres d'outils indésirables, vous diriger vers des sites que vous n'aviez pas l'intention de visiter et afficher des publicités indésirables.

Les attaquants peuvent gagner de l'argent grâce aux frais de publicité, voler des informations aux utilisateurs, espionner ou diriger les utilisateurs vers des sites Web ou des applications qui téléchargent davantage de logiciels malveillants.

Comment se défendre contre un pirate de navigateur ?

Soyez prudent lorsque vous installez un nouveau logiciel sur votre système. De nombreux pirates de navigateur se greffent sur des logiciels recherchés, un peu comme le font les logiciels publicitaires.

Assurez-vous d'installer et d'exécuter un logiciel anti-malware sur votre système et de maintenir des paramètres de haute sécurité pour l'activité du navigateur.

Parce que le hijackware est lié à votre navigateur, c'est là que réside la solution pour exterminer un pirate de navigateur.

Si votre logiciel antivirus ne détecte pas une nouvelle souche, vous pouvez réinstaller le navigateur. Si cela ne fonctionne pas, il peut être nécessaire d'effacer le contenu de l'appareil.

Bug

Les bogues sont un terme générique pour les failles dans les segments de code. Tous les logiciels comportent des bogues, et la plupart passent inaperçus ou ont un impact modéré sur l'utilisateur.

Parfois, cependant, un bogue représente une grave faille de sécurité, et l'utilisation d'un logiciel avec ce type de bogue peut ouvrir votre système à des attaques.

Comment se défendre contre les bugs ?

La meilleure façon de minimiser les bogues potentiellement désagréables consiste à mettre à jour votre logiciel de manière cohérente.

Les vulnérabilités étant au cœur des préoccupations des éditeurs de logiciels, ils publient rapidement des correctifs pour éviter d'endommager les systèmes des utilisateurs.

Pour les organisations qui écrivent ou configurent leur code, il est impératif de suivre les meilleures pratiques pour un code sécurisé et éventuellement de demander un examen par un tiers.

Crimeware

Certains fournisseurs utilisent le terme « crimeware » pour désigner des logiciels malveillants exécutés de manière criminelle et qui profitent souvent financièrement à l'attaquant.

Tout comme les logiciels malveillants, il s'agit d'une catégorie inclusive qui englobe une grande variété de logiciels malveillants.

Contrairement aux ransomwares, il peut s'agir d'une opération criminelle qui n'implique pas la collecte d'une rançon.

En tant que terme, les logiciels malveillants englobent la plupart des types de logiciels malveillants répertoriés dans cet article.

Comment se défendre contre les logiciels criminels ?

Les meilleures pratiques de sécurité réseau sont essentielles, notamment l'utilisation d'anti- programmes malveillants, de pare-feu, de prévention et de détection des intrusions (IPDS), de surveillance du réseau et des journaux, de la protection des données, de la gestion des informations et des événements de sécurité (SIEM) et des renseignements sur les menaces.

Les fournisseurs de cybersécurité comme Panda Security suggèrent que le meilleur moyen de se défendre contre les logiciels criminels consiste à utiliser une combinaison d'antivirus, d'anti- spyware, de pare-feu et de technologie de détection des menaces.

Enregistreurs de frappe

Un keylogger est un logiciel qui enregistre toutes les touches qu'un utilisateur touche. Ces données exposées incluent tout, des e-mails et documents saisis aux mots de passe saisis à des fins d'authentification.

En obtenant un accès d'authentification sensible, les attaquants peuvent s'introduire dans le réseau du fournisseur ou le compte utilisateur.

Comment se défendre contre un keylogger ?

Une bonne hygiène des mots de passe est l'un des meilleurs moyens d'empêcher l'accès aux enregistreurs de frappe.

L'utilisation de mots de passe forts que vous mettez à jour régulièrement peut grandement contribuer à votre sécurité. Vous devez également utiliser un pare-feu réseau et une solution anti-malware.

Applications mobiles malveillantes

Dans la mer d'applications disponibles aujourd'hui, toutes ne sont pas souhaitables, et le problème est encore plus aigu avec les magasins d'applications tiers.

Alors que les fournisseurs de magasins d'applications tentent d'empêcher la disponibilité d'applications malveillantes, certaines passent inévitablement à travers.

Ces applications peuvent voler des informations sur les utilisateurs, tenter d'extorquer de l'argent aux utilisateurs, accéder aux réseaux d'entreprise, forcer les utilisateurs à afficher des publicités indésirables ou se livrer à d'autres types d'activités indésirables.

Prévenir les dommages causés par une application mobile malveillante

L'éducation des utilisateurs est l'un des outils les plus puissants pour empêcher les applications mobiles malveillantes.

En évitant les magasins d'applications tiers et en examinant les données des applications avant le téléchargement, les utilisateurs peuvent considérablement atténuer ce risque.

Le déploiement d'un anti-malware mobile et d'un plan de sécurité mobile à l'échelle de l'entreprise est essentiel pour les grandes organisations.

Phishing et ingénierie sociale

L'hameçonnage et l'ingénierie sociale sont un type d'attaque par courrier électronique qui tente d'amener les utilisateurs à divulguer des mots de passe, à télécharger une pièce jointe ou à visiter un site Web qui installe des logiciels malveillants sur leurs systèmes.

Des efforts plus ciblés sur des utilisateurs ou des organisations spécifiques sont connus sous le nom de spear phishing.

Parce que le but est de tromper l'utilisateur, les attaquants rechercheront la victime pour maximiser le potentiel de tromperie.

Prévenir une attaque de phishing

Étant donné que le phishing repose sur l'ingénierie sociale – incitant les utilisateurs à faire quelque chose – la formation des employés est l'une des meilleures défenses contre ces attaques.

Les utilisateurs doivent déployer des solutions anti-spam et anti-malware, et le personnel doit savoir qu'il ne doit pas divulguer d'informations personnelles ou de mots de passe dans les e-mails.

Une formation sur le téléchargement de pièces jointes ou le clic sur des liens de sites Web dans les messages, même s'ils semblent provenir d'une source connue, est impérative étant donné que les attaquants de phishing prétendent souvent être une entreprise ou une personne connue de la victime.

Le courrier électronique est également généralement le mode de fonctionnement des ransomwares.

Malware RAM

Le malware RAM scraper, également connu sous le nom de malware de point de vente (POS), récupère les données temporairement stockées dans la mémoire d'un système, également appelée mémoire vive (RAM).

Ce type de malware cible les systèmes de point de vente tels que les caisses enregistreuses ou les portails de fournisseurs où un attaquant peut accéder à des numéros de carte de crédit non cryptés.

Bien que ces données de paiement sensibles ne soient disponibles que quelques millisecondes avant de transmettre les numéros cryptés aux systèmes dorsaux, les attaquants peuvent toujours accéder à des millions d'enregistrements.

Empêcher un malware de RAM

Les organisations peuvent aider à prévenir les attaques de malware RAM en utilisant des systèmes de point de vente renforcés et en séparant les systèmes liés au paiement des systèmes de non- paiement.

Les précautions habituelles telles que les logiciels anti-malware, les pares-feux, le cryptage des données et le respect de toutes les normes ou réglementations pertinentes pour la protection des données des clients sont indispensables.

Ransomware

Ces dernières années, les ransomwares sont rapidement devenus l'un des types de malwares les plus répandus.

Les variantes de logiciels malveillants les plus courantes chiffrent un système ou des fichiers spécifiques, suspendant tout travail jusqu'à ce que la victime paie une rançon à l'attaquant.

D'autres formes de ransomware menacent de publier des informations sensibles dans les données cryptées.

Empêcher un ransomware

Souvent, les organisations peuvent atténuer les attaques de ransomware en disposant de sauvegardes à jour.

Si leurs fichiers sont verrouillés, ils peuvent simplement effacer le système et redémarrer à partir d'une sauvegarde hors ligne.

Les organisations doivent former les utilisateurs à la menace, corriger leurs logiciels si nécessaire et installer toutes les solutions de sécurité habituelles.

Certains cas de ransomware semblent si graves que de nombreuses organisations et individus ont recours au paiement de la rançon.

Rootkit

Les rootkits sont l'un des types de logiciels malveillants les plus insidieux, car ils permettent aux attaquants d'avoir un accès de niveau administrateur aux systèmes à l'insu des utilisateurs.

Une fois qu'un attaquant a un accès root à un réseau, il peut presque tout faire avec le système, y compris enregistrer une activité, modifier les paramètres du système, accéder aux données et monter des attaques sur d'autres systèmes.

Empêcher un rootkit

Vous pouvez empêcher la plupart des infections de rootkit en installant un logiciel de sécurité approprié (anti-malware, pare-feu, surveillance des journaux) et en gardant votre système d'exploitation et autres logiciels à jour avec des correctifs.

Vous devez être prudent lorsque vous installez un logiciel sur votre système et lorsque vous cliquez sur des pièces jointes ou des liens d'e-mails.

Si un rootkit infecte votre système, il peut être presque impossible à détecter et à supprimer ; dans de nombreux cas, vous devrez peut-être nettoyer votre disque dur et recommencer à zéro pour vous en débarrasser.

Logiciels espions

Un logiciel espion est tout type de logiciel qui recueille des informations sur une personne à son insu ou sans son consentement. Par exemple, les cookies de suivi de site Web qui surveillent l'historique de navigation d'un utilisateur sont considérés comme une forme de logiciel espion.

D'autres types de logiciels espions peuvent tenter de voler des informations personnelles ou d'entreprise.

Les agences gouvernementales et les forces de l'ordre utilisent souvent des logiciels espions pour enquêter sur des suspects nationaux ou des acteurs internationaux menaçants.

Il est difficile pour l'utilisateur de détecter les symptômes des logiciels espions allant des problèmes de performances à l'activité inhabituelle du modem.

Empêcher un logiciel espion

Installez un logiciel anti-espion sur votre ordinateur. Heureusement, les capacités anti-spyware sont incluses dans la plupart des packages antivirus ou anti-malware de nos jours.

L'utilisation d'un pare-feu et la prudence lors du téléchargement de logiciels sont indispensables. Et enfin, rechercher les menaces potentielles au moins une fois par semaine peut vous sauver la vie.

Cheval de Troie

En matière de sécurité informatique, un cheval de Troie est un logiciel malveillant qui prétend être autre chose mais sert un objectif malveillant.

Par exemple, un cheval de Troie peut sembler être un jeu gratuit, mais une fois installé, il peut détruire votre disque dur, voler des données, installer une porte dérobée ou effectuer d'autres actions nuisibles.

Empêcher un cheval de Troie

Étant donné que les chevaux de Troie utilisent l'ingénierie sociale pour des attaques ciblées, il est impératif d'éduquer les utilisateurs.

Les organisations peuvent se défendre contre la plupart des chevaux de Troie avec des logiciels de sécurité tels qu'un logiciel anti-malware et des pares-feux suffisants.

Virus

Alors que certains se réfèrent indifféremment aux logiciels malveillants et aux virus, un virus est un type spécifique de logiciel malveillant qui nécessite une activation humaine - un clic sur une pièce jointe, une image, un lien ou même un fichier auquel vous accédez tous les jours.

Souvent caché, un clic du personnel pourrait inconsciemment déclencher un virus.

Les virus infectent un appareil, puis tentent de se propager à d'autres appareils et systèmes. En ce qui concerne les dommages causés à l'utilisateur, un virus peut exécuter plusieurs commandes indésirables.

Ceux-ci inclus :

- Intégration de systèmes dans un botnet
- Envoi de spam aux contacts
- Vol d'informations sensibles
- Verrouillage du système
- Fichiers et programmes manquants

Prévenir un virus

Tout système connecté à Internet sur votre réseau doit avoir un logiciel antivirus installé et à jour. Le déploiement d'un pare-feu est essentiel, mais soyez prudent lorsque vous cliquez sur des pièces jointes ou des liens URL.

L'inspection de la sécurité du site Web par son SSL est impérative pour éviter de visiter des sites Web inconnus ou non fiables.

Les principaux fournisseurs de logiciels antivirus incluent Avast, AVG, Bitdefender, ESET, Kaspersky, Norton, Panda et Sophos, et Microsoft offre une protection Windows gratuite sous la forme de Microsoft Defender.

Vers

Un ver est comme un virus car il se propage, mais un ver n'a pas besoin de l'autorisation d'un attaquant pour être activé.

Au lieu de cela, il s'agit d'un malware autonome qui s'étend au sein d'un système ou d'un réseau. Comme les virus, il peut causer autant de dommages à l'appareil.

Comment se défendre contre les vers ?

Comme pour les virus, le meilleur moyen de prévenir les infections par les vers est d'utiliser un logiciel antivirus ou anti-malware.

Et comme toujours, les utilisateurs ne doivent cliquer sur les liens ou les pièces jointes des e-mails que lorsqu'ils sont sûrs du contenu.

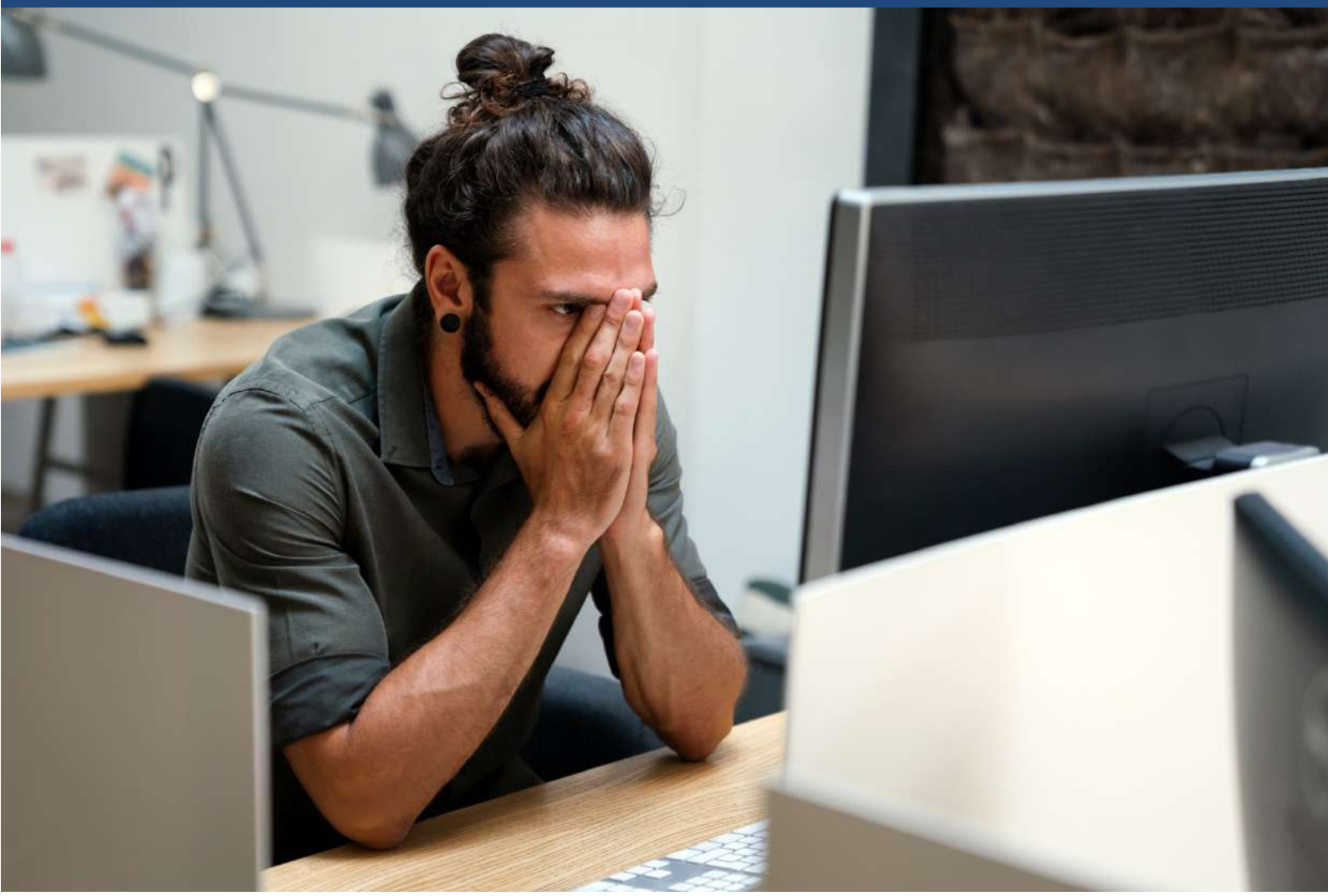
Préparez-vous à tous les types de logiciels malveillants

Si vous êtes arrivé jusqu'ici, vous savez que la forêt de logiciels malveillants est sombre et profonde. La ligue actuelle des acteurs malveillants ne s'appuie pas sur les formes traditionnelles de logiciels malveillants.

Ils recherchent constamment des souches plus robustes qui peuvent surpasser la sécurité de votre réseau et les solutions anti-malware ou antivirus actuelles.

Être conscient des dangers inhérents aux différents types de logiciels malveillants passe avant tout.

En tant que professionnel de la cybersécurité, il est de votre responsabilité de rester attentif aux tendances des logiciels malveillants et de répondre activement aux vulnérabilités pertinentes.



CHAPTITRE 6

Comment vous prémunir contre la visite de sites Web dangereux

Comment vous prémunir contre la visite de sites Web dangereux

Étant donné le nombre de fois que nous utilisons Internet dans une journée, nous passons probablement relativement peu de temps à réfléchir aux sites Web à utiliser en toute sécurité.

Bien sûr, aller sur un mauvais site Web peut entraîner des conséquences majeures comme le phishing, les virus, les logiciels malveillants, le vol d'identité, etc.

Mais comment êtes-vous censé savoir quand un site Web est dangereux et que pouvez-vous faire pour vous assurer que vous ne visitez que des sites Web légitimes ?

Voici quelques signes rapides d'un site Web qui peut être utilisé :

- Symbole de cadenas à côté de l'URL
- HTTPS dans l'URL plutôt que HTTP
- Politique de confidentialité sur le site Web
- Le site Web accepte tous les principaux modes de paiement.
- Lorsque vous surfez sur le Web, il est important de rechercher les drapeaux rouges

Tels que :

- Le navigateur vous indique que le site Web n'est pas sûr.
- De nombreuses fenêtres contextuelles ou des redirections vers d'autres sites Web louches.
- Le site Web accepte uniquement les virements bancaires ou les paiements électroniques.
- Aucune politique de retour ou politique de confidentialité sur le site Web. Plongeons un peu plus loin.

1. Outils intégrés au navigateur pour la sécurité des sites Web

Il y a de fortes chances que votre navigateur fasse déjà beaucoup pour vous pour savoir quels sites Web sont sûrs. Personnellement, nous utilisons Chrome, qui :

- Bloque les fenêtres contextuelles
- Envoie des demandes « ne pas suivre » aux sites Web pour protéger nos données.
- Désactive le contenu flash dangereux.
- Arrête les téléchargements malveillants.
- Contrôle quels sites peuvent accéder à notre haut-parleur, microphone et caméra. Allez simplement dans les paramètres de votre navigateur et vérifiez dans la section
- « Confidentialité et sécurité » pour voir comment votre navigateur filtre le mauvais.
- Bien entendu, ces outils de sécurité intégrés au navigateur ne capturent pas tout, c'est pourquoi il est important d'effectuer d'autres tests.

2. Autres tests de sécurité du site Web

Si vous n'êtes pas sûr qu'un site Web est sûr, la chose la plus simple à faire est de l'entrer dans un vérificateur de site Web comme le rapport de transparence Google, Norton Safe Web Checker ou URLVoid ou tout autre outil.

Il vous dira si le site Web est sûr ou non en moins de deux secondes !

Bien sûr, vous ne voulez pas avoir à saisir tous les sites Web sur lesquels vous vous rendez dans un vérificateur en ligne, car cela prendrait du temps et serait peu pratique.

Il y a donc quelques éléments que vous pouvez analyser par vous-même pour voir si un site est légitime.

3. Utilisez des sites de confiance

Celui-ci peut sembler évident, mais surtout si vous faites des achats en ligne, essayez d'utiliser des détaillants dont vous avez entendu parler, Amazon étant le choix le plus évident.

N'oubliez pas que vous donnez à ce site les informations de votre carte de crédit ou de débit ainsi que votre nom, votre adresse e-mail et votre adresse, ce qui pourrait être dangereux s'il tombait entre de mauvaises mains.

4. Vérifiez les URL

Parfois, les escrocs orthographient mal les noms d'URL de confiance ou remplacent l'une des lettres par un nombre, par exemple en écrivant go0gle.com au lieu de google.com.

Dans la précipitation, c'est quelque chose que vous pouvez facilement manquer, et avec de faux sites Web imitant de vrais sites Web aussi bien qu'eux, il est assez facile de donner vos informations personnelles aux méchants.

Heureusement, si vous utilisez Firefox ou Chrome, vous pouvez simplement passer votre souris sur le « texte d'ancrage » (AKA le texte qui est lié), pour voir l'URL avant de cliquer dessus ; il apparaîtra dans le coin inférieur gauche de votre navigateur.

5. Remarque sur les méthodes de paiement

Vérifiez que le site Web accepte toutes les principales cartes de crédit et de débit.

Tout site Web normal aura des méthodes de paiement normales des principales sociétés de cartes de crédit/débit, comme Mastercard, Visa, American Express - vous obtenez l'exercice.

Si un site Web accepte uniquement les virements bancaires ou les paiements électroniques, évitez.

6. Vérifiez les sites d'avis comme Trustpilot.

L'Internet est l'endroit idéal pour que les gens expriment leurs problèmes au plus grand nombre de personnes qui veulent écouter.

Il y a de fortes chances que, s'il y a un sujet, les gens l'aient examiné sur le Web, des restaurants aux sites de commerce électronique.

Profitez du besoin insatiable des gens de tout évaluer publiquement et de consulter des sites d'avis comme TrustPilot, surtout s'il s'agit d'un site de commerce électronique.

Vous n'avez même pas nécessairement besoin d'utiliser un site d'examen. Demandez simplement à Google si le site Web/l'entreprise est une arnaque et voyez ce que les gens ont dit.

Si plusieurs personnes disent qu'il s'agit d'une arnaque, elles ont probablement raison.

7. Vérifiez HTTPS

Maintenant, ce n'est pas infaillible à 100 %, mais la plupart des sites Web réputés auront des URL qui commencent par HTTPS plutôt que par HTTP ; et oui, si vous vous posez la question, le S signifie sécurisé.

Fondamentalement, cette toute petite lettre fait la différence entre un site Web sécurisé qui crypte vos données et un site Web frauduleux qui les vole (à quelques exceptions près, bien sûr).

Si le site Web est sécurisé, vous verrez un cadenas à gauche de l'URL, mais notez que certains sites Web dangereux ont HTTPS, il n'est donc pas garanti qu'il soit sûr.

Cependant, une règle stricte et rapide que vous pouvez suivre est de ne jamais entrer votre mot de passe ou vos informations financières sur un site Web sans cadenas.

8. Recherchez une politique de confidentialité

La vérité est que la plupart des sites Web réputés ont des politiques de confidentialité, car de nombreux pays l'exigent par la loi, alors assurez-vous d'en rechercher une sur un site Web.

Maintenant, nous ne disons pas que vous serez en mesure de comprendre ces politiques, car elles sont souvent écrites dans ce que nous, dans l'industrie, appelons « juridique ».

Mais pour avoir une bonne idée de la façon dont le site Web utilisera vos données, appuyez sur Ctrl F et recherchez des éléments tels que « tiers », « données », « stocker » et « conserver ».

Si un site Web n'a pas du tout de politique de confidentialité, vous ne lui ferez pas confiance.

9. Ne donnez pas une foi absolue aux badges de « confiance »

Savez-vous à quel point il est facile d'obtenir l'un de ces soi-disant « badges de confiance » sur votre site Web ?

C'est si facile que vous pouvez littéralement taper des « badges de confiance » sur des images Google et les faire glisser sur votre site.

Bien que ces sceaux puissent sembler légitimes, n'importe qui pourrait littéralement les ajouter à leur site Web, des grandes entreprises comme Barnes & Noble au « prince étranger » le plus louche du Web.

Nous ne disons pas que ces badges de confiance renseignent automatiquement un site non digne de confiance. Cependant, vous ne devez pas les confondre avec la sécurité.

10. Recherchez ces drapeaux rouges

Il existe plusieurs signaux d'alarme qui non seulement font d'un site Web une expérience utilisateur médiocre, mais peuvent également indiquer que quelque chose ne va pas.

Attention à :

- Avertissements instantanés
- Fenêtres contextuelles
- Trop de points d'exclamation !!!!!
- Des redirections vers d'autres sites qui semblent dangereux.
- Avertissements de moteur de recherche de votre navigateur ou moteur de recherche
- Mauvaise orthographe et grammaire
- Texte illogique
- Des images étranges
- Pas d'espace pour laisser des commentaires sur les produits.
- Aucune politique de retour ou politique de confidentialité sur le site
- Des prix trop beaux pour être vrais.
- Même si nous détestons juger un livre par sa couverture, ce sont tous des signes d'un site Web qui n'est pas très sûr.

11. Rechercher le propriétaire du domaine

La plupart des sites Web réputés, en particulier pour les entreprises, auront un propriétaire de domaine, facilement consultable sur la recherche de données d'enregistrement de nom de domaine de l'ICANN.

Ce site Web vous indiquera également la date d'expiration de ce registre, l'organisation et l'adresse postale du déclarant, ainsi que les données auxquelles le registre a été créé.

12. Appeler l'entreprise

Nous savons que cela semble démodé, mais même les robots les plus avancés ont du mal à imiter exactement les humains.

Par conséquent, si vous n'êtes pas sûr qu'un site Web provient d'une véritable entreprise, un moyen simple de le savoir est simplement de l'appeler par téléphone !

En règle générale, la plupart des sites Web fournissent un numéro de téléphone sur leurs pages Contact ou À propos de nous.

Si vous ne le trouvez pas, vous pouvez également essayer de le rechercher exactement de la même manière qui est recherché ci-dessus ou essayer de les contacter via le support client.

13. Outils de sécurité Web supplémentaires

Enfin, un moyen simple d'éviter d'accéder à des sites Web nuisibles consiste à utiliser des outils de sécurité Web qui vous protègent des virus. Voici quelques exemples phares :

- Antivirus AVG
- Sécurité Premium d'Avast
- Norme Norton 360
- Avec ces logiciels téléchargés, vous n'aurez pas à vous soucier de donner vos données personnelles à des sites dangereux. Il effectuera le travail pour vous, vous n'avez donc pas à vous en soucier du tout !

14. VPN

Les VPN sont des réseaux privés virtuels qui cryptent votre trafic Web dans un tunnel, masquant complètement votre activité Web et remplaçant votre adresse IP.

Ils sont particulièrement utiles si vous êtes sur un réseau public comme un café, ou si vous souhaitez simplement accéder au serveur d'un autre pays afin de profiter de Netflix Italie.

Les VPN rendent beaucoup moins probable que votre appareil soit piraté, et vous pouvez facilement les télécharger sur votre téléphone, tablette, ordinateur ou même votre routeur.

15. Services de surveillance d'identité

Se faire voler votre identité peut être l'une des choses les plus épuisantes émotionnellement et financièrement que vous puissiez vivre, c'est pourquoi il est important d'employer un service de surveillance d'identité.

Bien qu'aucun d'entre eux ne soit garanti pour empêcher complètement le vol d'identité, ils peuvent surveiller les domaines clés qui pourraient indiquer que vos informations d'identification ont été volées, telles que vos rapports de crédit, vos comptes bancaires, de carte de crédit et d'investissement, ainsi que le dark web et d'autres criminels. zones d'activités.

Si votre identité est volée, la plupart des services de surveillance d'identité vous rembourseront vos pertes.

16. Gestionnaires de mots de passe

Les gestionnaires de mots de passe facilitent l'accès à vos comptes en mémorisant vos mots de passe pour vous, de manière sécurisée bien sûr.

Ils sont également parfaits pour stocker des informations importantes ou sensibles, et même pour remplir automatiquement des formulaires Web pour vous !

L'une des choses les plus ennuyeuses à propos de la technologie est de devoir mémoriser autant de mots de passe différents pour différents comptes.

De plus, chaque compte a probablement ses propres règles, comme vous devez avoir des caractères spéciaux, vous ne pouvez pas avoir de chiffres, pas de lettres répétées, et plus encore, ce qui rend encore plus difficile de se souvenir de tout.

Et le processus de réinitialisation de votre mot de passe est loin d'être amusant, surtout parce que vous allez probablement l'oublier à nouveau !

Pour conclure, être en ligne ne doit pas être effrayant. Il existe de nombreux outils qui peuvent vous protéger en ligne, comme les VPN, les gestionnaires de mots de passe, les services de surveillance de l'identité et simplement le réglage des paramètres de vos appareils.

Savoir comment surfer en ligne en toute sécurité est la première étape pour protéger vos informations d'identification personnelles, et en suivant les étapes ci-dessus, vous serez sûrement en sécurité.

CHAPTITRE 7

Comprendre le phishing et le ransomware et savoir comment les prévenir

Comprendre le phishing et le ransomware et savoir comment les prévenir

Les attaques de ransomware par e-mail sont à nouveau en augmentation. Plusieurs formes nouvelles de ransomware ont récemment été observées dans les messages de phishing.

Le courrier électronique était autrefois le moyen le plus prolifique d'infecter les victimes avec des ransomwares.

Mais ces dernières années, les hackers ont réussi à utiliser des ports distants, des serveurs publics non sécurisés et d'autres vulnérabilités dans les réseaux d'entreprise pour chiffrer des réseaux entiers.

Cela leur permettant d'exiger souvent des centaines de milliers de dollars en paiement pour rendre à nouveau les données accessibles.

Définition du ransomware

Le ransomware est une forme de malware qui crypte les fichiers d'une victime. L'attaquant réclame alors une rançon à la victime pour restaurer l'accès aux données lors du paiement.

Les utilisateurs reçoivent des instructions sur la façon de payer des frais pour obtenir la clé de déchiffrement. Les coûts peuvent aller de quelques centaines de dollars à des milliers de dollars, payables aux cybercriminels en Bitcoin.

Comment fonctionne le ransomware ?

Il existe plusieurs vecteurs que les ransomwares peuvent utiliser pour accéder à un ordinateur. L'un des systèmes de diffusion les plus courants est le spam par hameçonnage.

C'est-à-dire utiliser les pièces jointes envoyées à la victime dans un e-mail comme appât

Généralement, le mail est une copie très bien exécutée d'un site connu et crédible. Ceci afin de ne pas susciter la méfiance du destinataire. Le piège se referme aussitôt la pièce jointe ouverte.

Une fois téléchargés et ouverts, ils peuvent prendre le contrôle de l'ordinateur de la victime, en particulier s'ils disposent d'outils d'ingénierie sociale intégrés qui incitent les utilisateurs à autoriser un accès administratif.

D'autres formes de ransomware plus agressives, comme NotPetya, exploitent les failles de sécurité pour infecter les ordinateurs sans avoir besoin de tromper les utilisateurs.

Dans certaines formes de logiciels malveillants, Le pirate peut prétendre être un site "justicier" qui prend le contrôle de l'ordinateur de la victime en raison de la présence de pornographie ou d'autres contenus illégaux.

Le hacker exige le paiement d'une « amende », en arguant du fait que la victime pourrait être dénoncée aux autorités si elle n'obtempère pas.

Mais la plupart des attaques ne s'embarrassent pas de ce prétexte. Il existe également une variante, appelée leakware ou doxware, dans laquelle l'attaquant menace de publier des données sensibles sur le disque dur de la victime à moins qu'une rançon ne soit payée.

Mais parce que trouver et extraire de telles informations est une proposition très délicate pour les attaquants, le ransomware de chiffrement est de loin le type le plus courant.

Qui est une cible pour les ransomwares ?

Il existe plusieurs façons pour les attaquants de choisir les sites qu'ils ciblent avec les ransomwares.

Parfois, c'est une question d'opportunité : par exemple, les attaquants peuvent cibler les universités car elles ont tendance à avoir des équipes de sécurité plus réduites et une base d'utilisateurs disparate qui partage beaucoup de fichiers, ce qui facilite la pénétration de leurs défenses.

En revanche, certaines organisations sont des cibles tentantes car elles semblent plus susceptibles de payer une rançon rapidement.

Par exemple, les agences gouvernementales ou les établissements médicaux ont souvent besoin d'un accès immédiat à leurs dossiers.

Les cabinets d'avocats et autres organisations disposant de données sensibles peuvent être disposés à payer, pour garder secrets et confidentiels, leurs dossiers avec les données de leurs clients.

C'est pourquoi, ces organisations peuvent être particulièrement sensibles aux attaques de pirates.

Comment prévenir les attaques de ransomware ?

Pour vous protéger et protéger votre système contre les ransomwares, suivez les conseils ci- dessous.

Ce sont :

- Évitez d'ouvrir des e-mails non vérifiés ou de cliquer sur les liens qui y sont intégrés.
- Sauvegardez les fichiers importants à l'aide de la règle 3-2-1 : créez trois copies de sauvegarde sur deux supports différents avec une sauvegarde dans un emplacement distinct.
- Mettez régulièrement à jour les logiciels, programmes et applications pour les protéger des dernières vulnérabilités.
- Créer une culture de sécurité et doter le personnel des connaissances adéquates sur les ransomwares et autres menaces qui utilisent le phishing et les comptes non sécurisés dans leurs campagnes.
- Appliquer le principe du moindre privilège pour empêcher les utilisateurs d'exécuter certains programmes pouvant être utilisés par des variantes de ransomware.
- Limitez l'accès aux lecteurs partagés ou en réseau et désactivez le partage de fichiers. Cela minimise le risque de propagation d'une infection par un ransomware à d'autres appareils.
- Gardez votre système d'exploitation à jour pour vous assurer d'avoir moins de vulnérabilités à exploiter.
- N'installez pas de logiciel et ne lui accordez pas de privilèges administratifs à moins que vous ne sachiez exactement de quoi il s'agit et à quoi il sert.

- Installez un logiciel antivirus, qui détecte les programmes malveillants comme les ransomwares dès leur arrivée, et un logiciel de liste blanche, qui empêche l'exécution d'applications non autorisées en premier lieu.
- Les organisations peuvent également atténuer les effets de la honte publique infligée par les conditions du programme de double extorsion de ransomware en étant responsables et en prenant les mesures suivantes :
- Informez les forces de l'ordre de l'attaque et de l'étendue de la violation de données.
- Suivre les protocoles de réglementation des données tels que le Règlement général sur la protection des données (RGPD) et effectuer les divulgations et notifications nécessaires.
- Empêchez des attaques similaires de réussir en résolvant les problèmes de sécurité exploités par l'attaque.

Définition de l'hameçonnage

Le phishing est une cyberattaque qui utilise un e-mail déguisé comme une arme.

L'objectif est de faire croire au destinataire de l'e-mail que le message est quelque chose qu'il veut ou dont il a besoin - une demande de sa banque, par exemple, ou une note d'un membre de son entreprise - et de cliquer sur un lien ou de télécharger une pièce jointe.

Ce qui distingue vraiment le phishing, c'est la forme que prend le message : les attaquants se font passer pour une entité de confiance quelconque, souvent une personne réelle ou vraisemblablement réelle, ou une entreprise avec laquelle la victime pourrait faire des affaires.

C'est l'un des types de cyberattaques les plus anciens, datant des années 1990, et c'est toujours l'un des plus répandus et des plus pernicieux, les messages et les techniques de phishing devenant de plus en plus sophistiqués.

Il utilise des techniques d'ingénierie sociale et de programmation informatique pour inciter les destinataires de courrier électronique et les internautes à croire qu'un site Web frauduleux est légitime.

Lorsque la victime d'hameçonnage clique sur le lien d'hameçonnage, elle découvre que des informations vitales sur son identité personnelle ont été volées.

De l'argent peut aussi être soustrait aux victimes par ce moyen.

Le coût moyen d'une escroquerie par hameçonnage est de 1,6 million de dollars. C'est aujourd'hui une préoccupation majeure en matière de sécurité pour les entreprises.

Quelques statistiques :

- 70,2 milliards de dollars sont le coût estimé pour les marques 28,1 milliards de dollars pour les entreprises.
- Les professionnels de l'événementiel sont une proie de choix pour les pirates.

Cela leur coûte :

- 3 milliards chaque mois 36 milliards par an

Le taux de réussite :

- 1 entreprise sur 3 est concernée.
- 30 % des e-mails de phishing sont ouverts.
- 100 millions de messages de phishing transitent chaque jour.
- L'hameçonnage est désormais le moyen n°1 pour propager les ransomwares et les malwares. Il est beaucoup plus sophistiqué et ciblé qu'auparavant. Le phishing est populaire parmi les cybercriminels car le taux de "réussite " est élevé.

10 messages litigieux peuvent obtenir :

- 90 % de chances d'obtenir un clic.
- 8% de chances que les utilisateurs cliquent sur une pièce jointe.
- 8% de chances que les utilisateurs remplissent un formulaire Web.
- 18% de chances que les utilisateurs cliquent sur un lien malveillant dans un e-mail.

Même les cadres supérieurs sont abusés et n'hésitent pas à partager des noms d'utilisateur et des mots de passe.

Qu'est-ce qu'un kit de phishing ?

La disponibilité des kits d'hameçonnage permet aux cybercriminels, même ceux ayant des compétences techniques minimales, de lancer facilement des campagnes d'hameçonnage.

Un kit d'hameçonnage regroupe des ressources et des outils de site Web d'hameçonnage qui ne doivent être installés que sur un serveur.

Une fois installé, tout ce que l'attaquant doit faire est d'envoyer des e-mails aux victimes potentielles.

Des kits de phishing ainsi que des listes de diffusion sont disponibles sur le dark web.

Quelques sites pour contrer les hackers

Phishtank et OpenPhish conservent des listes de kits d'hameçonnage connus provenant du web.

Phishtank et OpenPhish sont des plateformes autonomes entièrement automatisées conçues pour déceler les sites de phishing.

Elles identifient ceux-ci et effectuent des analyses de renseignement en temps réel sans intervention humaine et sans utiliser de ressources externes, telles que des listes noires.

Certains kits de phishing permettent aux attaquants d'usurper des marques de confiance, augmentant ainsi les chances qu'une personne clique sur un lien frauduleux.

L'analyse des kits de phishing permet aux équipes de sécurité de savoir qui les utilise.

L'une des choses les plus utiles que nous pouvons apprendre de l'analyse des kits de phishing est l'endroit où les informations d'identification sont envoyées.

En suivant les adresses e-mail trouvées dans les kits de phishing, nous pouvons corréler les acteurs à des campagnes spécifiques et même à des kits spécifiques.

Types d'hameçonnage

S'il y a un dénominateur commun entre les attaques de phishing, c'est la faculté d'usurper la crédibilité d'un site.

Les attaquants falsifient leur adresse e-mail, donnant l'impression que celui-ci provient d'un site connu.

Ils créent de faux sites Web qui ressemblent à ceux auxquels la victime fait confiance et utilisent des jeux de caractères étrangers pour masquer les URL.

Cela dit, il existe une variété de techniques qui relèvent du phishing. Il existe plusieurs façons de diviser les attaques en catégories.

L'un est le but de la tentative de phishing. Généralement, une campagne de phishing tente d'amener la victime à faire l'une des deux choses suivantes :

Ce sont :

Transmettre des informations sensibles

Ces messages visent à inciter l'utilisateur à révéler des données importantes - souvent un nom d'utilisateur et un mot de passe que l'attaquant peut utiliser pour violer un système ou un compte.

La version classique de cette arnaque consiste à envoyer un e-mail conçu pour ressembler à un message d'une grande banque ; en diffusant le message à des millions de personnes, les attaquants s'assurent qu'au moins certains des destinataires seront des clients de cette banque.

La victime clique sur un lien dans le message et est redirigée vers un site malveillant conçu pour ressembler à la page Web de la banque, puis, entrer son nom d'utilisateur et son mot de passe.

L'attaquant peut désormais accéder au compte de la victime.

Télécharger des logiciels malveillants

Comme beaucoup de spam, ces types d'e-mails de phishing visent à amener la victime à infecter son propre ordinateur avec des logiciels malveillants.

Souvent, les messages sont « ciblés » : ils peuvent être envoyés à un membre du personnel des RH avec une pièce jointe qui prétend être le curriculum vitae d'un demandeur d'emploi, par exemple.

Ces pièces jointes sont souvent des fichiers .zip ou des documents Microsoft Office contenant du code malveillant intégré.

Il existe différentes méthodes d'hameçonnage pour pousser l'internaute à cliquer sur le lien.

Ce sont :

- Spear phihing

Lorsque les attaquants créent un message pour faire appel à un individu spécifique, cela s'appelle le spear phishing. (L'image est celle d'un pêcheur visant un poisson spécifique, plutôt que de simplement jeter un hameçon appâté dans l'eau pour voir qui mord.)

Les hameçonneurs identifient leurs cibles (parfois en utilisant des informations sur des sites comme LinkedIn) et utilisent des adresses falsifiées pour envoyer des e-mails qui pourraient vraisemblablement sembler provenir de collègues.

Par exemple, le harponnage peut cibler quelqu'un du service financier et prétendre être le responsable de la victime en demandant un virement bancaire important dans un court délai.

- Chasse à la baleine

Whale phishing, ou chasse à la baleine, est une forme de spear phishing visant les très gros poissons.

— PDG ou autres cibles de grande valeur. Beaucoup de ces escroqueries ciblent les membres du conseil d'administration, qui sont considérés comme particulièrement vulnérables.

Ils ont une grande autorité au sein d'une entreprise, et, ils utilisent souvent des adresses e-mail personnelles pour la correspondance commerciale, qui ne bénéficie pas des protections offertes par l'e-mail d'entreprise.

D'autres types de phishing incluent le phishing par clone, le vishing, les raquettes.

Comment prévenir les attaques de phishing ?

Voici 10 étapes simples pour identifier et prévenir les escroqueries par hameçonnage.

1. Sachez à quoi ressemble une arnaque par hameçonnage

Il existe de nombreux sites en ligne qui vous tiendront informé des dernières attaques de phishing et de leurs identifiants clés.

Plus tôt vous découvrez les dernières méthodes d'attaque et les partagez avec vos utilisateurs grâce à une formation régulière de sensibilisation à la sécurité, plus vous avez de chances d'éviter une attaque potentielle.

2. Ne cliquez pas sur n'importe quel lien

Il est généralement déconseillé de cliquer sur un lien dans un e-mail ou un message instantané, même si vous connaissez l'expéditeur. Le strict minimum que vous devriez faire est de survoler le lien pour voir si la destination est la bonne.

Certaines attaques de phishing sont sophistiquées et l'URL de destination peut ressembler à une copie carbone du site authentique, configurée pour enregistrer les frappes au clavier ou voler les informations de connexion/de carte de crédit.

S'il vous est possible d'accéder directement au site via votre moteur de recherche, plutôt que de cliquer sur le lien, alors vous devriez le faire.

3. Obtenez des logiciels anti-hameçonnage gratuits

De nos jours, la plupart des navigateurs vous permettent de télécharger des logiciels qui détectent les signes d'un site Web malveillant ou vous alertent sur les sites de phishing connus.

Ils sont généralement entièrement gratuits, il n'y a donc aucune raison de ne pas les installer sur tous les appareils de votre entreprise ou société.

4. Ne donnez pas vos informations à un site non sécurisé

Si l'URL du site Web ne commence pas par "https", ou si vous ne voyez pas d'icône de cadenas fermé à côté de l'URL, n'entrez aucune information sensible ou téléchargez des fichiers à partir de ce site.

Les sites sans certificat de sécurité ne sont peut-être pas destinés aux escroqueries par hameçonnage, mais il vaut mieux prévenir que guérir.

5. Changez régulièrement les mots de passe

Si vous avez des comptes en ligne, vous devriez prendre l'habitude de changer régulièrement vos mots de passe afin d'empêcher un attaquant d'obtenir un accès illimité.

Vos comptes peuvent avoir été compromis à votre insu. Par conséquent, l'ajout d'une couche de protection supplémentaire via la rotation des mots de passe peut empêcher les attaques en cours et bloquer les attaquants potentiels.

6. N'ignorez pas ces mises à jour

Recevoir de nombreux messages de mise à jour peut être énervant et il peut être tentant de les reporter ou de les ignorer complètement.

Ne faites pas cela. Les correctifs et mises à jour de sécurité sont publiés pour une raison, le plus souvent pour se tenir au courant des méthodes modernes de cyberattaque en corrigeant les failles de sécurité.

Si vous ne mettez pas à jour votre navigateur, vous pourriez être exposé à des attaques de phishing via des vulnérabilités connues qui auraient pu être facilement évitées.

7. Installer des pares-feux

Les pares-feux sont un moyen efficace de prévenir les attaques externes, agissant comme un bouclier entre votre ordinateur et un attaquant.

Les pares-feux de bureau et les pare-feu réseau, lorsqu'ils sont utilisés ensemble, peuvent renforcer votre sécurité et réduire les risques qu'un pirate informatique s'infiltre dans votre environnement.

8. Ne vous laissez pas tenter par les pop-ups

Les pop-ups ne sont pas seulement irritants ; ils sont souvent liés à des logiciels malveillants dans le cadre de tentatives d'attaques de phishing.

La plupart des navigateurs vous permettent désormais de télécharger et d'installer un logiciel gratuit de blocage des publicités qui bloquera automatiquement la plupart des fenêtres contextuelles malveillantes.

Si les pop-ups parviennent à échapper au bloqueur de publicités, ne soyez pas tenté de cliquer ! Parfois, des fenêtres contextuelles essaieront de vous tromper avec l'emplacement du bouton

« Fermer », alors essayez toujours de rechercher un « x » dans l'un des coins.

9. Ne donnez pas d'informations importantes

En règle générale, à moins que vous ne fassiez confiance à 100% au site sur lequel vous vous trouvez, vous ne devriez pas volontairement donner les informations de votre carte.

Assurez-vous, si vous devez fournir vos informations, que vous vérifiez que le site Web est authentique, que l'entreprise est réelle et que le site lui-même est sécurisé.

10. Disposez d'une plate-forme de sécurité des données pour détecter les signes d'une attaque

Si vous avez la malchance d'être victime d'une attaque de phishing réussie, il est alors important que vous puissiez détecter et réagir en temps opportun.

La mise en place d'une plate-forme de sécurité des données permet d'alléger une partie de la pression de l'équipe informatique/sécurité en alertant automatiquement sur le comportement anormal des utilisateurs et les modifications indésirables apportées aux fichiers.

Si un attaquant a accès à vos informations sensibles, les plates-formes de sécurité des données peuvent aider à identifier le compte concerné afin que vous puissiez prendre des mesures pour éviter d'autres dommages.

CHAPRITRE 8

Conseils pour concevoir un budget cyber sécurité post covid-19

Conseils pour concevoir un budget cyber sécurité post covid-19

Alors que les organisations commencent à planifier leurs budgets de cybersécurité, il est immédiatement évident que cette année entraînera des coûts nouveaux et inattendus.

Le passage mondial au travail à domicile au cours de ces deux dernières années a obligé de nombreuses organisations à réorganiser la cyber sécurité pour protéger le personnel travaillant à distance et potentielles victimes de menaces accrues en matière de piratage.

Dans ce chapitre, nous examinerons plusieurs éléments clés (mais peut-être inattendus) qui devraient figurer dans votre budget de cybersécurité.

Évaluation de la menace

Chaque budget de cybersécurité doit être basé, en fin de compte, sur le niveau et les types de menaces auxquelles vous êtes confronté.

La pandémie de COVID-19 a entraîné une augmentation notable de la cybercriminalité, tout en forçant simultanément les employés à travailler à domicile, où ils sont plus vulnérables.

L'essentiel est donc que la cybersécurité coûtera beaucoup plus cher au cours de l'année à venir que l'année dernière, et peut-être plus que jamais auparavant.

Nonobstant ce titre, il est plus important que jamais de mener une analyse approfondie des menaces pour votre organisation - en suivant de nouvelles et meilleures pratiques

Le budget cyber sécurité devrait être celui qui bénéficie de la meilleure attention. Ce sont les fondements même de votre entreprise qui sont concernés.

Cette évaluation des menaces aidera également à justifier votre budget de cybersécurité cette année, si la direction se demande pourquoi il est tellement plus élevé que les années précédentes.

Frais de personnel et de formation

Avant la pandémie, de nombreuses entreprises encourageaient déjà le travail à distance. L'une des forces motrices de ce changement était la perception que le personnel en télétravail permettait de réduire les coûts.

Si cela est avéré, financièrement parlant, vrai, ce n'est absolument pas le cas en matière de cybersécurité.

En effet, les membres du personnel qui travaillent à domicile ont besoin d'une formation supplémentaire importante pour assurer leur sécurité et celle des actifs numériques de l'entreprise.

Compte tenu de la pénurie généralisée de compétences qui caractérise toujours le monde de la cybersécurité, cela est susceptible de s'appliquer à toutes les équipes.

Pire encore – si le personnel n'est pas formé de manière adéquate, vous devrez payer pour nettoyer après ses erreurs, ce qui coûtera encore plus cher.

Réponse aux incidents

Deuxièmement, vous devez tenir compte de votre tolérance au risque, faire une estimation raisonnable du nombre d'incidents auxquels vous êtes susceptible de devoir répondre cette année et combien cela vous coûtera.

Dans de nombreuses organisations, ces coûts sont négligés, car les consultants en cybersécurité commettent toujours l'erreur de penser que dépenser suffisamment en prévention leur permettra de réduire à zéro les coûts de réponse aux incidents.

Ne commettez pas cette erreur. Cela ne fonctionne tout simplement pas comme ça.

Remplacement et mise à niveau des ressources

Vous devriez également envisager de remplacer et de mettre à niveau vos ressources matérielles et logicielles en réponse au passage au travail à domicile.

Les ordinateurs portables plus anciens dotés de logiciels de sécurité obsolètes peuvent être (à peine) suffisamment sécurisés pour protéger vos employés et vos données s'ils restent derrière le pare-feu de votre entreprise, mais une fois qu'ils quittent le bureau, ils sont exposés à un niveau de risque beaucoup plus élevé à l'extérieur.

Pour cette raison, le moment est peut-être venu de remplacer le matériel vieillissant par des machines plus récentes qui intègrent la biométrie, ou d'installer le chiffrement matériel sur des machines plus anciennes.

Également, cette année est le bon moment pour revoir tout logiciel gratuit mais non sécurisé que vous utilisez.

Consultants

Cela peut sembler un mauvais moment pour dépenser des milliers de dollars en consultants, mais les tests redhats sont un excellent moyen de comprendre les menaces auxquelles vous êtes confronté et de comprendre comment les atténuer.

Wikipedia : Redhats

Un test d'intrusion réussi est un excellent moyen de concentrer tout le monde sur le même objectif.

Assurance

Vous avez probablement remarqué que vos primes d'assurance cybersécurité ont augmenté au cours de la dernière année, et il y a une bonne raison à cela.

Les compagnies d'assurance ont examiné les statistiques et ont décidé que les employés à distance présentaient un risque énorme.

Ils facturent donc plus pour les assurer, et vous devez intégrer ce surcoût dans votre budget de cybersécurité.

Si, en revanche, vous n'avez actuellement aucune assurance cybersécurité, vous devriez sérieusement envisager de la souscrire.

Alors qu'une dépense supplémentaire peut sembler être un lourd fardeau à supporter maintenant, les économies en cas d'attaque réussie dépassent de loin ce coût prévisible et répétitif.

Sécurité en tant que service

Enfin, et en particulier si le nombre de facteurs ci-dessus semble augmenter votre budget à des niveaux ingérables cette année, il est peut-être temps d'envisager une aide extérieure.

Il existe des solutions de sécurité tierces sur le marché depuis des décennies, certaines ont été développées en plates-formes de sécurité en tant que service à spectre complet.

Ces plateformes promettent de prendre en charge votre cybersécurité dans son intégralité, vous laissant libre de vous concentrer sur des choses plus importantes.

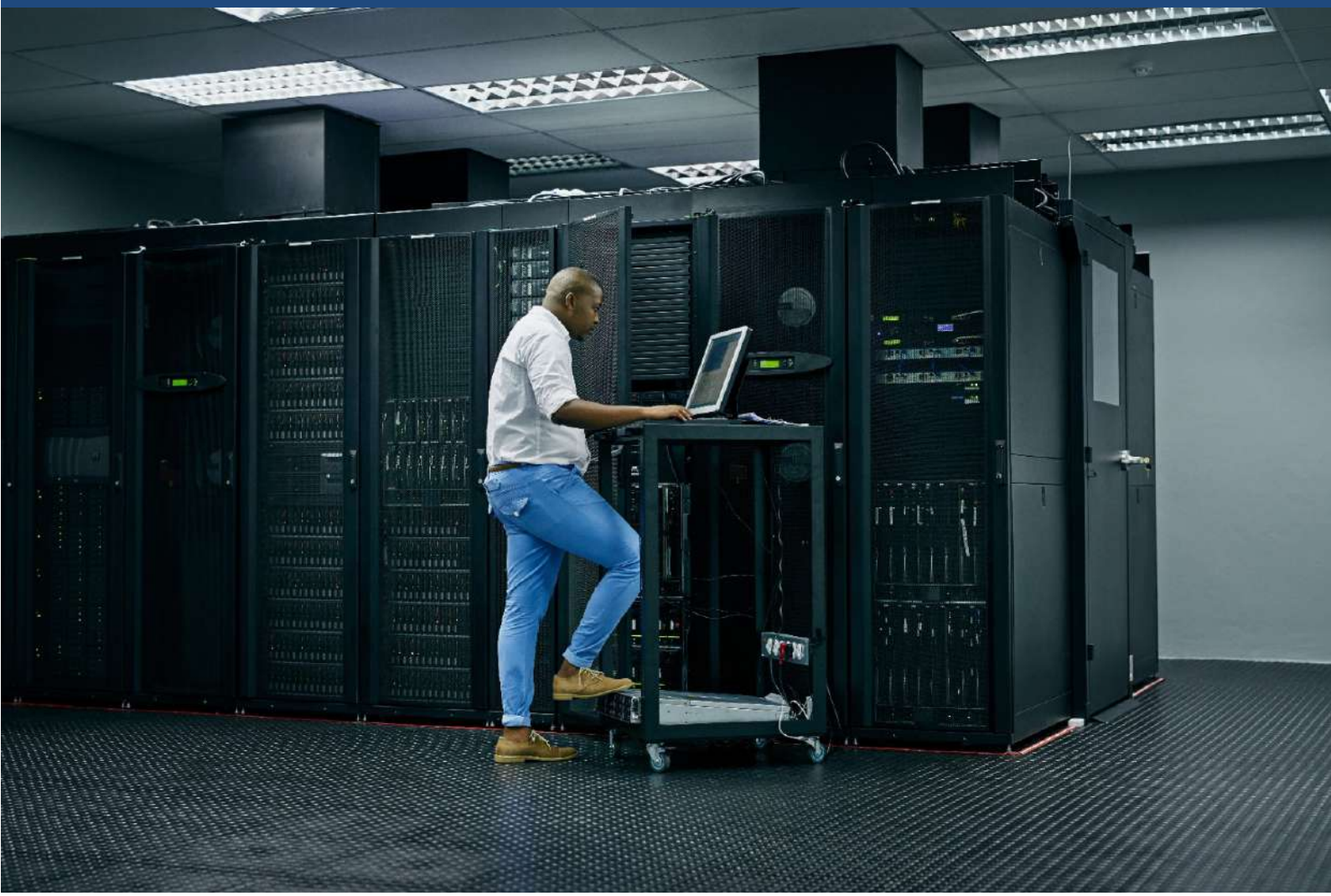
Attendez-vous à l'inattendu

Bien que cela puisse ne pas en avoir l'air pour le moment, le type d'évaluation en profondeur des budgets de cybersécurité nécessité par la pandémie pourrait, dans l'ensemble, être une évolution positive.

De nombreuses entreprises n'ont pas examiné leurs budgets et les hypothèses sur lesquelles ils se fondent depuis de nombreuses années. Cette critique était attendue depuis longtemps.

Même si vous constatez que vous êtes déjà bien préparé pour l'année à venir, le processus de réexamen de votre budget peut être instructif.

La capacité à évaluer les risques et le budget en conséquence est l'une des compétences en cybersécurité qui connaît la croissance la plus rapide et le développement d'une expertise dans ce domaine pourrait à terme donner un coup de fouet à une carrière.



CHAPITRE 9

Comment les entreprises adapteront-elles leurs nouvelles stratégies de cyber sécurité post pandémie ?

Comment les entreprises adapteront-elles leurs nouvelles stratégies de cyber sécurité post pandémie ?

De nombreuses entreprises ont du mal à adapter leur stratégie de sécurité pour s'adapter à la nouvelle normalité.

Le travail à distance étant désormais une réalité permanente, il y a eu une ruée pour adopter et intégrer une multitude de nouveaux outils et plates-formes cloud pour faciliter la collaboration et maintenir la productivité.

Cependant, dans la course pour connecter tout le monde, les implications en matière de sécurité sont souvent négligées.

Ceci, associé au fait que s'appuyer uniquement sur un pare-feu d'entreprise n'est plus une bonne stratégie de sécurité, met de nombreuses organisations en danger.

Alors, que doivent faire les entreprises maintenant pour ajuster leur stratégie de sécurité ? Voici cinq facteurs à respecter qui empêcheront les cybercriminels de profiter de l'environnement commercial virtuel.

1. Adoptez une approche Zéro Trust

Les organisations doivent adopter cet état d'esprit maintenant qu'il n'y a plus de périmètre de sécurité bien défini.

Tous les systèmes doivent être correctement sécurisés et nécessitent un accès authentifié à partir d'un périphérique autorisé, qu'ils résident sur le réseau interne ou externe.

Les entreprises devraient également exiger que les employés distants utilisent un VPN pour accéder aux ressources de l'entreprise lorsqu'ils ne sont pas physiquement au bureau. Cela aidera à atténuer les problèmes de sécurité.

2. Vérifiez la sécurité avant d'ajouter des outils

Il y a eu une augmentation de l'adoption d'outils de collaboration et de services cloud pour soutenir l'engagement dans notre monde dépendant du numérique.

La plupart des organisations ont donné la priorité à la résilience sur les problèmes de sécurité.

Cependant, plutôt que de se précipiter pour adopter de nouveaux outils, les équipes informatiques doivent auditer chaque solution pour détecter les vulnérabilités de sécurité potentielles et savoir comment les configurer en toute sécurité avant qu'elles ne soient activées.

En outre, les équipes doivent ajuster leur approche de l'application de la sécurité à l'incarnation d'un conseiller en risques, aidant ainsi l'entreprise à comprendre les vulnérabilités de sécurité tout en soutenant une réponse plus agile au nouvel environnement de travail.

3. Rendre l'authentification multi facteur obligatoire

Les mots de passe restent un maillon faible et sont à l'origine de nombreuses failles de cybersécurité. Les systèmes et données sensibles nécessitent plus qu'un simple mot de passe pour la sécurité.

Les organisations doivent ajouter des couches supplémentaires, même si cela peut sembler contraignant dans l'expérience utilisateur plutôt que d'espérer qu'une seule suffira.

4. Exploitez les technologies intelligentes

Avec la pénurie de ressources de cybersécurité et l'escalade des menaces, il n'a jamais été aussi essentiel d'exploiter la puissance des technologies intelligentes.

La capacité de ces solutions à traiter de vastes volumes de données pour identifier et prévoir les menaces est une ressource inestimable pour les organisations qu'elles ne peuvent ignorer.

L'apprentissage automatique et la détection de bots sont des outils essentiels pour les équipes de sécurité maintenant et en période post-pandémique.

5. Formation pratique à la sécurité pour les télétravailleurs

La formation à la sécurité est essentielle pour que les employés comprennent le nouveau paysage des risques.

La formation devrait viser à aider à protéger les données professionnelles et personnelles, car la plupart des réseaux domestiques sont surchargés d'une gamme d'appareils différents.

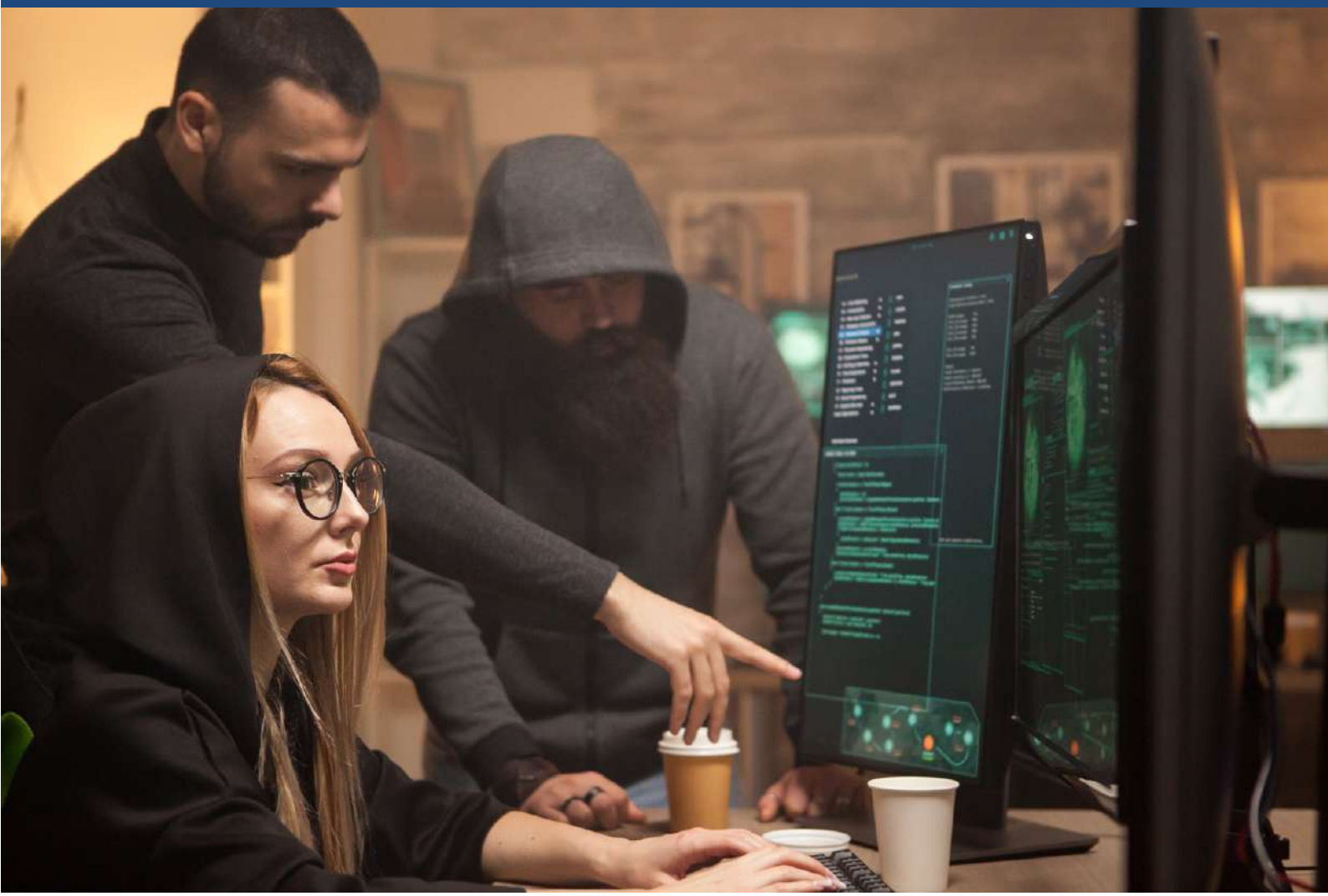
Les employés seront plus réceptifs si vous présentez une vision globale des menaces.

Il doit y avoir des trucs et astuces réguliers qui informent sur les dernières cyber-escroqueries et attaques de phishing pour empêcher les employés de tomber dans le piège.

La configuration d'un chatbot pour répondre aux questions fréquemment posées par les travailleurs à distance fournira aux employés les informations dont ils ont besoin quand ils en ont besoin sans ajouter de charge inutile à l'équipe informatique.

L'environnement de travail a changé pour toujours et les organisations doivent adopter une approche agile pour faire face au nouveau paysage des menaces.

Rester enraciné à ce qui a fonctionné dans le passé a le potentiel d'être une recette pour un désastre cette année en matière de sécurité.



CHAPITRE 10

Étude de cas

Étude de cas

Les ransomwares, le phishing et l'écrémage des guichets automatiques ne sont que quelques-unes des menaces de cybersécurité assez courantes et très dommageables auxquelles les petites entreprises doivent faire attention.

Les études de cas suivantes ont été créées par la National Cyber Security Alliance, avec une subvention du NIST, et devraient s'avérer utiles pour stimuler l'apprentissage continu pour tous les propriétaires d'entreprise et leurs employés.

Cas 1 : Un voyage d'affaires en Amérique du Sud

SCÉNARIO :

Un cabinet de conseil de 10 personnes a envoyé une petite équipe en Amérique du Sud pour mener à bien un projet client. Pendant leur séjour, un employé a utilisé une carte de débit professionnelle à un guichet automatique local.

Un mois après son retour aux États-Unis, l'entreprise a reçu des avis de découvert de sa banque. Ils ont identifié des retraits frauduleux de 13 000 $, tous provenant d'Amérique du Sud. Il y avait des frais de découvert supplémentaires de 1 000 $.

ATTAQUE :

Les criminels ont installé un dispositif d'écumoire ATM pour enregistrer les informations d'identification du compte de carte. De nombreuses fausses cartes de débit ont été fabriquées et utilisées dans les guichets automatiques de différentes villes d'Amérique du Sud.

Qu'est-ce que l'écrémage ? L'écrémage se produit lorsque des criminels installent des appareils sur des guichets automatiques, des terminaux de point de vente (POS), des pompes à carburant, etc. pour capturer des données ou enregistrer les codes PIN des titulaires de carte.

Les criminels utilisent les données pour créer de fausses cartes de débit ou de crédit, puis volent les comptes des victimes.

RÉPONSE :

Se rendant compte qu'ils avaient été escroqués, l'entreprise a contacté sa banque et a immédiatement fermé le compte concerné. Leurs tentatives pour obtenir le remboursement de la banque ont été infructueuses.

Le compte commercial utilisé au guichet automatique pour la monnaie locale avait des protections différentes des comptes des consommateurs et la banque n'était pas tenue de les rembourser pour leurs pertes.

La banque a ensuite déduit les frais de découvert de 1 000 $ du compte personnel du propriétaire de l'entreprise.

L'entreprise a rompu les liens avec cette banque. La nouvelle banque offrait des garanties complètes de protection contre la fraude.

L'entreprise a créé deux comptes professionnels :

- un pour recevoir des fonds et effectuer de petits virements.
- un pour les petits paiements
- L'entreprise a mis à jour les protocoles de voyage, interdisant l'utilisation des cartes de débit fournies par l'entreprise.
- Les employés prépayent désormais les dépenses par voie électronique, paient en espèces ou utilisent une carte de crédit reconnue, si nécessaire.

IMPACT :

La totalité de la réserve de trésorerie de la petite entreprise a été anéantie, enregistrant des pertes nettes de près de 15 000 $.

LEÇONS APPRISES :

- Utilisez les principales cartes de crédit lorsque vous voyagez - elles offrent une meilleure protection contre la fraude aux consommateurs que les cartes de débit.

- Recevez une notification - configurez des alertes de transaction avec vos sociétés de cartes de crédit et de débit pour surveiller la fraude.
- Vérifiez fréquemment votre compte bancaire.
- Créer des alertes de retrait.
- Comprenez les politiques de votre banque concernant la couverture des pertes dues à la fraude.

Cas 2 : Une entreprise de construction se fait piéger par un enregistreur de frappe SCÉNARIO :

Une petite entreprise de construction familiale a largement utilisé les services bancaires en ligne

et les virements automatisés. Les employés se sont connectés avec un identifiant et un mot de passe spécifiques à l'entreprise et à l'utilisateur.

Deux questions devaient être posées pour les transactions de plus de 1 000 $.

Le propriétaire a été informé qu'un transfert automatique de 10 000 $ avait été initié par une source inconnue.

Ils ont contacté la banque et identifié qu'en une semaine seulement, les cybercriminels avaient effectué six virements à partir des comptes bancaires de l'entreprise, totalisant 550 000 $.

Comment ? L'un de leurs employés avait ouvert un e-mail provenant de ce qu'ils pensaient être un fournisseur de matériaux, mais il s'agissait plutôt d'un e-mail malveillant contenant des logiciels malveillants provenant d'un compte imposteur.

ATTAQUE :

Les cybercriminels ont pu installer des logiciels malveillants sur les ordinateurs de l'entreprise, en utilisant un enregistreur de frappe pour capturer les informations d'identification bancaires.

Un enregistreur de frappe est un logiciel qui surveille silencieusement les frappes de l'ordinateur et envoie les informations à un cybercriminel.

Ils peuvent ensuite accéder aux services bancaires et autres services financiers en ligne, en utilisant des numéros de compte et des mots de passe valides.

RÉPONSE :

La banque n'a pu récupérer que 200 000 $ de l'argent volé au cours des premières semaines, laissant une perte de 350 000 $.

La banque a même tiré plus de 220 000 $ sur la marge de crédit de l'entreprise pour couvrir les virements frauduleux. L'absence de plan de cybersécurité a retardé la réponse de l'entreprise à la fraude.

L'entreprise a également recherché une société d'expertise judiciaire en cybersécurité pour :

- les aider à effectuer un examen complet de la cybersécurité de leurs systèmes.
- identifier la source de l'incident.
- recommander des mises à niveau de leur logiciel de sécurité.

IMPACT :

L'entreprise a fermé son compte bancaire et a intenté une action en justice pour recouvrer ses pertes. L'entreprise a récupéré les 350 000 $ restants avec intérêts. Aucun argent pour le temps et les frais juridiques n'a été récupéré.

LEÇONS APPRISES :

- Recevez une notification - configurez des alertes de transaction sur toutes les cartes de crédit, de débit et les comptes bancaires.
- Limitez l'accès aux comptes sensibles aux seuls employés qui ont besoin d'y accéder, changez souvent les mots de passe.
- Les entreprises devraient évaluer leur risque et évaluer les options d'assurance responsabilité civile.
- Choisissez des banques qui offrent plusieurs niveaux d'authentification pour accéder aux comptes et aux transactions.
- Créer, maintenir et mettre en pratique un plan de réponse aux cyber incidents rapidement réalisable.

- Les cybercriminels livrent et installent des logiciels malveillants par courrier électronique. Former les employés à la sécurité des e-mails.

Cas 3 : Un ordinateur portable volé dans une voiture SCÉNARIO :

Un cadre du système de santé a laissé son ordinateur portable de travail, qui avait accès à plus de

40 000 dossiers médicaux, dans une voiture verrouillée alors qu'il faisait une course. La voiture a été cambriolée et l'ordinateur portable volé.

ATTAQUE :

Vol physique d'un appareil non crypté. Le chiffrement est le processus de brouillage du texte lisible afin qu'il ne puisse être lu que par la personne qui possède la clé de déchiffrement.

Il crée une couche de sécurité supplémentaire pour les informations sensibles.

RÉPONSE :

L'employé a immédiatement signalé le vol à la police et au service informatique du système de santé qui a désactivé l'accès à distance de l'ordinateur portable et a commencé à surveiller l'activité.

L'ordinateur portable était équipé d'outils de sécurité et d'une protection par mot de passe.

Les données stockées sur le disque dur n'étaient pas cryptées – cela incluait les données sensibles et personnelles des patients.

Le département américain de la Santé et des Services sociaux a été informé. Personnellement, les données d'informations identifiables et d'informations de santé protégées nécessitent des processus et des normes de reporting rigoureux.

Après le vol et la violation, le système de soins de santé a commencé un examen approfondi des politiques internes ; ils ont créé une procédure disciplinaire pour les employés qui violent les normes de sécurité.

Un examen approfondi des mesures de sécurité avec le personnel informatique interne et les fournisseurs informatiques auxiliaires a révélé des vulnérabilités.

IMPACT :

Le système de santé a dépensé plus de 200 000 $ en mesures correctives, en surveillance et en améliorations opérationnelles. Une violation de données a un impact négatif sur une marque et la confiance doit être rétablie.

LEÇONS APPRISES :

- Les entreprises doivent établir et former des employés sur la manipulation sécurisée des appareils émis par le travail.
- Les appareils doivent être rangés en toute sécurité lorsqu'ils ne sont pas en présence immédiate de l'employé.
- Les entreprises doivent prendre des mesures pour crypter les données partout où elles sont stockées ou transmises. Les employés doivent avoir une compréhension claire de l'importance du cryptage et de la façon de l'utiliser.
- Les entreprises doivent comprendre et connaître leurs responsabilités en vertu des lois sur la notification des violations de données des États dans lesquels elles opèrent.
- Un examen régulier des pratiques de sécurité de l'entreprise est impératif dans les organisations modernes pour prévenir les incidents, découvrir les vulnérabilités et réduire l'impact des incidents.

Cas 4 : le PDG d'un hôtel trouve du contenu indésirable dans un compte de messagerie

SCÉNARIO :

Le PDG d'un hôtel de charme s'est rendu compte que son entreprise était victime d'une fraude électronique lorsque le comptable a commencé à recevoir des notifications de fonds insuffisants pour des factures récurrentes.

Un examen des registres comptables a révélé un grave problème.

À un moment donné, quelques semaines auparavant, le PDG avait cliqué sur un lien dans un e- mail qu'ils pensaient provenir de l'IRS. Ce n'était pas.

Lorsqu'ils ont cliqué sur le lien et saisi leurs informations d'identification, les cybercriminels ont capturé les informations de connexion du PDG, leur donnant un accès complet aux informations commerciales et personnelles intimes.

ATTAQUE :

Ingénierie sociale, attaque de phishing.

Une attaque de phishing est une forme d'ingénierie sociale par laquelle les cybercriminels tentent de tromper les individus en créant et en envoyant de faux e-mails qui semblent provenir d'une source authentique, telle qu'une entreprise ou un collègue.

L'e-mail peut vous demander de confirmer des informations de compte personnel telles qu'un mot de passe ou vous inviter à ouvrir une pièce jointe malveillante qui infecte votre ordinateur avec des logiciels malveillants.

RÉPONSE :

Les réserves de trésorerie de l'hôtel étaient épuisées. Les transferts frauduleux s'élevaient à plus d'un million de dollars.

L'hôtel a également contacté une entreprise de cybersécurité pour l'aider à atténuer le risque d'une attaque répétée.

IMPACT :

L'entreprise a perdu 1 million de dollars sur un compte en Chine. Les fonds n'ont pas été récupérés.

LEÇONS APPRISES :

- Enseignez au personnel les dangers de cliquer sur des liens et des pièces jointes d'e-mails non sollicités, et la nécessité de rester attentif aux signes avant-coureurs d'e-mails frauduleux.
- Participez à une formation régulière sur la sécurité des e-mails.
- Mettre en œuvre des protocoles de virement électronique stricts et inclure une forme secondaire de validation.
- Ayez un plan de réponse aux cyber incidents prêt à être mis en œuvre !

Cas 5 : Le dark web SCÉNARIO :

Le PDG d'une entreprise contractante du gouvernement a été informé qu'une vente aux enchères sur le dark web vendait l'accès aux données commerciales de son entreprise, qui comprenait l'accès à la base de données de son client militaire.

Le PDG a rapidement établi que les données « vendues » étaient obsolètes et n'étaient liées à aucun client d'une agence gouvernementale.

Comment est-ce arrivé ? L'entreprise a identifié qu'un employé senior avait téléchargé une pièce jointe malveillante, pensant qu'elle provenait d'une source fiable.

ATTAQUE :

Une attaque de phishing où un malware se trouve dans la pièce jointe de l'e-mail.

Une attaque de phishing est une forme d'ingénierie sociale par laquelle les cybercriminels tentent de tromper les individus en créant et en envoyant de faux e-mails qui semblent provenir d'une source authentique, telle qu'une entreprise ou un collègue.

L'e-mail peut vous demander de confirmer des informations de compte personnel telles qu'un mot de passe ou vous inviter à ouvrir une pièce jointe malveillante qui infecte votre ordinateur avec un virus ou un logiciel malveillant.

RÉPONSE :

La direction informatique de l'entreprise a immédiatement coupé les communications avec le serveur concerné et a mis le système hors ligne pour exécuter des analyses de cybersécurité du réseau et identifier toute violation supplémentaire.

La direction de l'entreprise a embauché un cabinet d'expertise judiciaire en cybersécurité réputé. Chaque agence gouvernementale potentiellement touchée a été notifiée. Les services secrets américains ont participé à l'enquête médico-légale.

IMPACT :

L'impact opérationnel et financier de la brèche a été considérable – coûtant plus d'un million de dollars : l'entreprise a été hors ligne pendant plusieurs jours, perturbant les activités ; de nouvelles licences de logiciels de sécurité et un nouveau serveur ont dû être mis en place.

LEÇONS APPRISES :

- Vous n'êtes jamais trop petit pour être une cible. Une cyberattaque peut arriver à n'importe qui.
- Enseignez au personnel les dangers de cliquer sur des liens et des pièces jointes de courrier électronique non sollicités et insistez sur la nécessité de rester attentif aux signes avant-coureurs de courriers électroniques frauduleux.
- Installez et mettez régulièrement à jour des outils antivirus, de pare-feu réseau et de chiffrement des informations pour rechercher et contrer les virus et les programmes nuisibles.
- Effectuer des tests de vulnérabilité et des évaluations des risques continus sur les réseaux informatiques.

CONCLUSION

Alors que nous enquêtons sur une année incertaine, une chose reste claire : les cybermenaces non seulement resteront, mais prendront de plus en plus d'ampleur.

Les cyberattaques ont également gagné en sophistication et en complexité.

L'époque où l'on se fiait simplement au logiciel antivirus intégré de votre ordinateur est révolue.

Les entreprises ont besoin du meilleur logiciel de sécurité des terminaux pour rester protégées.

Les organisations devront rester vigilantes sur les politiques de travail à distance, l'accès aux données et le perfectionnement des compétences, et elles devront s'appuyer sur des technologies éprouvées telles que l'IA et la sécurité du cloud.

Les défis sont là, mais les opportunités aussi.

Avec les stratégies et les connaissances fournies dans ce guide, vous savez tout pour protéger votre entreprise et vos proches contre les menaces en ligne et assurer toujours la protection numérique.