TENDANCES DE CYBERSÉCURITÉ POUR 2021 :

Comment se protéger en période d'incertitude

TABLE DES MATIÈRES

INTRODUCTION

La pandémie de COVID-19 a provoqué un choc dans le « système », plongeant nombre d'entre nous dans une spirale d'inquiétude et apportant un nouveau sens à la notion de changement permanent. Alors que l'année 2020 touche à sa fin, l'une des grandes questions que tout le monde se pose est la suivante : comment se déroulera l'année 2021?

2020 a été une année comme aucune autre de mémoire d'homme, car pratiquement aucune facette de notre vie n'a été épargnée par les effets de la pire crise de santé publique depuis des décennies. La pandémie de COVID-19 a bouleversé notre quotidien, a exposé notre fragilité collective, et a considérablement accru notre sentiment d'incertitude. Le changement de paradigme aura sans aucun doute des effets profonds et durables, y compris des effets que nous ne pouvons pas encore prévoir.

Certains des bouleversements déclenchés ou accélérés par la pandémie impliquent notre recours à la technologie, car l'urgence mondiale a contribué à dématérialiser certains des « points de contact » qui étaient précédemment hors ligne. En augmentant notre dépendance à la connectivité et en accélérant la transformation numérique, la crise nous a fourni un petit aperçu de ce que sera l'avenir proche, peut-être même après la pandémie.

Cela soulève la question de ce qui pourrait se passer en 2021, notamment en ce qui concerne les menaces et les risques qui sont présents dans le monde numérique. Il est désormais bien établi que les cybercriminels ont su s'adapter rapidement à la nouvelle réalité, en saisissant les opportunités uniques entraînées par l'anxiété générale et la ruée inévitable vers le télétravail. À l'approche de la nouvelle année, nous devons prendre du recul et réfléchir à la manière dont le paysage des menaces a évolué et dont les cyber-risques pourraient être davantage remodelés et exacerbés à l'avenir. Les tendances et les événements récents restent la meilleure base pour s'en faire une idée.

Un aspect de notre vie qui est devenu méconnaissable en 2020 concerne nos habitudes de travail. D'une certaine manière, ce changement a débuté depuis longtemps. La pandémie n'a fait qu'accélérer et intensifier considérablement des tendances préexistantes. Les entreprises et leur main-d'œuvre nouvellement distribuée étaient cependant mal préparées pour faire face aux cyber-risques que le passage quasi instantané à la nouvelle normalité a provoqués ou aggravés. Dans le premier chapitre, Jake Moore se penche sur cette évolution, ainsi que sur la manière dont les entreprises, en particulier celles qui ne veulent pas revenir aux anciennes méthodes, et leur personnel peuvent continuer de se protéger. Point tout aussi important, il se demande ce que l'avenir proche réserve aux modes de travail et si nous allons bientôt revenir à la vie de bureau d'avant la pandémie.

Il serait négligent de notre part de ne pas considérer au moins certaines des menaces les plus pressantes posées par les malwares. Tony Anscombe s'intéressera plus particulièrement à l'évolution des ransomwares. Cette menace est très présente depuis des années, mais de plus en plus d'opérateurs de ransomwares augmentent la pression sur leurs victimes en combinant extorsion et exfiltration de données, menaçant ainsi de publier, vendre ou mettre aux enchères les données volées si aucun paiement de rançon n'est effectué. Tony évoquera également la hausse des sommes demandées comme autre tendance qui s'est manifestée récemment, avant d'examiner la situation dans son ensemble et de noter que ces changements sont un moyen pour les pirates de maximiser le retour sur investissement de leurs attaques. Comment la situation évoluera-t-elle en 2021, avec peut-être même une implication quant à la définition de ce que sont les ransomwares?

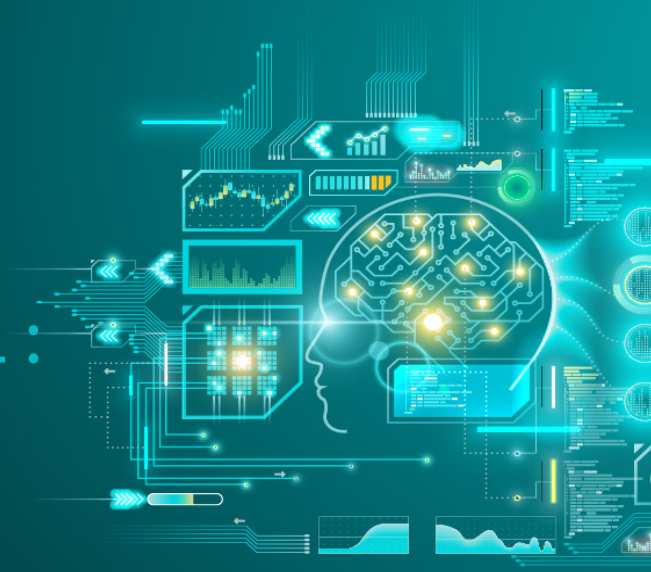
Tandis que les pirates continuent de déployer des moyens de plus en plus complexes et souvent innovants pour piéger leurs victimes, Camilo Gutiérrez se penchera sur une tactique particulièrement évasive qui, bien qu'elle ne soit pas entièrement nouvelle, a gagné en popularité au cours des dernières années. Les attaques de type « living off the land » exploitent des applications légitimes sur le système ciblé, pour minimiser le risque d'être détectées tout en maximisant la furtivité et l'efficacité des incursions. Il peut donc être difficile de les détecter et les empêcher, ce qui devrait rappeler aux entreprises qu'elles doivent évaluer leur niveau de préparation face à ces attaques.

Le fait que la technologie imprègne presque toutes les facettes de notre vie a été, naturellement, rendu encore plus évident au cours d'une année où tout ce qui est numérique a façonné plus que jamais notre quotidien. Dans notre quête d'une application pratique de la technologique, nous utilisons des objets connectés depuis des années, y compris pour le bien-être sexuel. Les jouets pour adultes n'ont certainement pas échappé à la révolution intelligente, et pendant la pandémie, les ventes de sex toys intelligents ont fait un bond. Ce qui a peut-être moins retenu l'attention, cependant, ce sont lesimplications de ces dispositifs sur la vie privée et la sécurité. Denise Giusto et Cecilia Pastorino précisent que cette technologie est un foyer potentiel de préoccupations en matière de confidentialité et de sécurité, qui pourrait au final exposer certaines des données les plus sensibles des utilisateurs à des cybercriminels.

Il est certain que de nombreux problèmes de longue date ne disparaîtront pas, car la priorité sera d'émerger des tréfonds de la pandémie. Néanmoins, s'il y a une lueur d'espoir au bout du tunnel que représente COVID-19, ce sont les précieux enseignements à tirer de cette calamité. Ils nous rappellent notamment qu'il faut être prêt à faire face à l'adversité, et que s'armer de connaissances est un premier pas vers la « vaccination » contre différents types de menaces.

1

L'AVENIR DU TRAVAIL : ADOPTION D'UNE NOUVELLE RÉALITÉ



2020 a été l'année où les entreprises sont passées au télétravail, mais qui a vraiment conduit ces entreprises à accélérer leur numérisation? Était-ce le PDG, le DSI, ou plus franchement COVID-19 ? Et à quoi ressemblera le travail après la pandémie?

Jake Moore
Spécialiste de la sécurité d'ESET

Depuis que les gouvernements du monde entier ont mis en place des mesures de confinement en raison de COVID-19, le monde du travail a considérablement changé, d'une manière que la plupart des gens n'auraient pas pu imaginer. Le résultat? Le recours en masse au télétravail qui s'appuie encore plus fortement que jamais sur la technologie, ainsi qu'une déstructuration des infrastructures technologiques de nombreuses entreprises. Les systèmes informatiques centraux ont été remplacés par un réseau d'individus disparates, tous ayant une plus grande responsabilité quant à leur propre utilisation de la technologie et à leurs besoins en matière de sécurité. Non seulement un système de sécurité défaillant laisse les entreprises vulnérables, mais la confiance des employés dans la gestion de la cybersécurité est également un risque sérieux.

À une époque où les entreprises comptent sur la résilience, des acteurs malveillants exploitent continuellement les vulnérabilités de sécurité qui accompagnent le télétravail. Il existe bien sûr des moyens d'améliorer la sécurité de nos nouveaux environnements. Des mesures simples peuvent être mises en place pour réduire les risques de cyberattaque, mais passer d'un ou deux bureaux à des dizaines, voire des centaines de bureaux à domicile, a généralement un coût.

CE QUE LA COVID-19 NOUS A ENSEIGNÉ

La pandémie nous a non seulement appris qu'il est possible de travailler à domicile, mais également que les entreprises peuvent créer et appliquer des politiques de sécurité en quelques semaines. La délocalisation de l'ensemble de la main-d'œuvre prend généralement des mois de planification, de consultations et encore plus de planification, avant d'être approuvée par les parties prenantes. Mais lorsque votre gouvernement vous dit que vous n'êtes plus autorisé à entrer dans vos bureaux (lorsque c'est possible), il est fascinant de voir à quelle vitesse ces changements peuvent être mis en œuvre, voire même dès le moment venu.

Il reste cependant certaines questions en suspens : Comment pouvons-nous protéger les télétravailleurs? Le travail à domicile est-il aussi sûr qu'au bureau? Reviendrons-nous un jour à la vie de bureau de 2019?

Afin de résister aux cyberattaques, de nombreuses entreprises ont mis en place de robustes politiques de sécurité et des évaluations des risques. Nombre d'entre elles sont équipées pour résister à la grande majorité des menaces qui pèsent sur toute entreprise normale, mais il est peu probable qu'aucune entreprise dans le monde n'ait été entièrement préparée à ce changement énorme et rapide du travail entraîné par COVID-19. Les murs physiques des bureaux agissent comme un grand pare-feu et toute anomalie sur le réseau peut souvent être facilement étudiée. Mais lorsque la totalité du personnel se connecte désormais au réseau depuis l'extérieur du périmètre de sécurité habituel, le responsable de la sécurité de l'information (RSSI) et les autres parties prenantes peuvent être confrontés à des tâches pour le moins intimidantes.

Le télétravail, sous une forme ou une autre, a clairement de beaux jours devant lui, mais pour fonctionner efficacement, il nécessite une excellente gestion, ainsi qu'une sécurité fondamentale. Pour qu'elles fonctionnent normalement et avec un minimum de perturbations, les entreprises doivent s'assurer que les pratiques de gestion et de sécurité jouent un rôle à parts égales dans leur protection et celle de leur personnel. Certaines entreprises ont été désorientées lorsqu'on les a obligées à renvoyer leurs collaborateurs chez eux, mais d'autres ont adopté cette nouvelle normalité et ont même découvert comment dégager plus de productivité (c'est le cas d'ESET!).

Des formations peuvent contribuer grandement à la protection du personnel, particulièrement quand elles sont administrées souvent et à petites doses. Cela peut se faire, par exemple, via des rappels rapides dans les produits autour de l'importance des réseaux privés virtuels (VPN) et par la sensibilisation aux emails d'hameçonnage, pour que les gens restent vigilants sans pour autant les frustrer ou les effrayer.

AVANT / APRÈS

Avant COVID-19, le nombre de cyberattaques était déjà en hause. La pandémie et le confinement qui en ont résulté n'ont fait qu'accroître ce risque. Les cybercriminels ont utilisé des tentatives d'hameçonnage et des malwares sur le thème de COVID-19 pour tirer parti des vulnérabilités innées de la main-d'œuvre dispersée et de leurs systèmes informatiques afin de trouver des failles à exploiter.

Le télétravail a permis une certaine flexibilité, mais il a également modifié considérablement les systèmes et les processus métiers afin de répondre aux besoins d'une main-d'œuvre distribuée. L'accès des salariés aux services informatiques, et vice versa, a changé. La collaboration et le travail d'équipe sont facilités virtuellement, et l'absence de communication en face à face peut entraver les canaux de communication directs. Certaines des mesures de sécurité courantes dans un bureau doivent être compensées à domicile, notamment l'obligation pour les télétravailleurs d'utiliser une authentification multifacteurs ou un VPN pour accéder aux réseaux internes. Rappeler aux télétravailleurs d'activer les mises à jour automatiques et de vérifier la sécurité de leurs propres réseaux Wifi est une première ligne de défense cruciale contre les cybercriminels. Idéalement, les télétravailleurs utiliseront toujours des appareils fournis par l'entreprise et seront pleinement vigilants face aux menaces persistantes.

Le passage au télétravail, qui s'est opéré du jour au lendemain, a été essentiel pour de nombreuses entreprises afin de prouver qu'il est efficace et qu'elles pourront continuer d'y recourir. Cependant, nous ne devons jamais nous reposer sur nos lauriers. Quand reprendrons-nous les discussions à la machine à café ou pendant le déjeuner, pour évoquer les dernières tentatives d'hameçonnage ou recevoir des conseils pratiques de sécurité qui nous aident souvent à faire les bons choix?

ASSURER LA PÉRENNITÉ DE L'ENTREPRISE

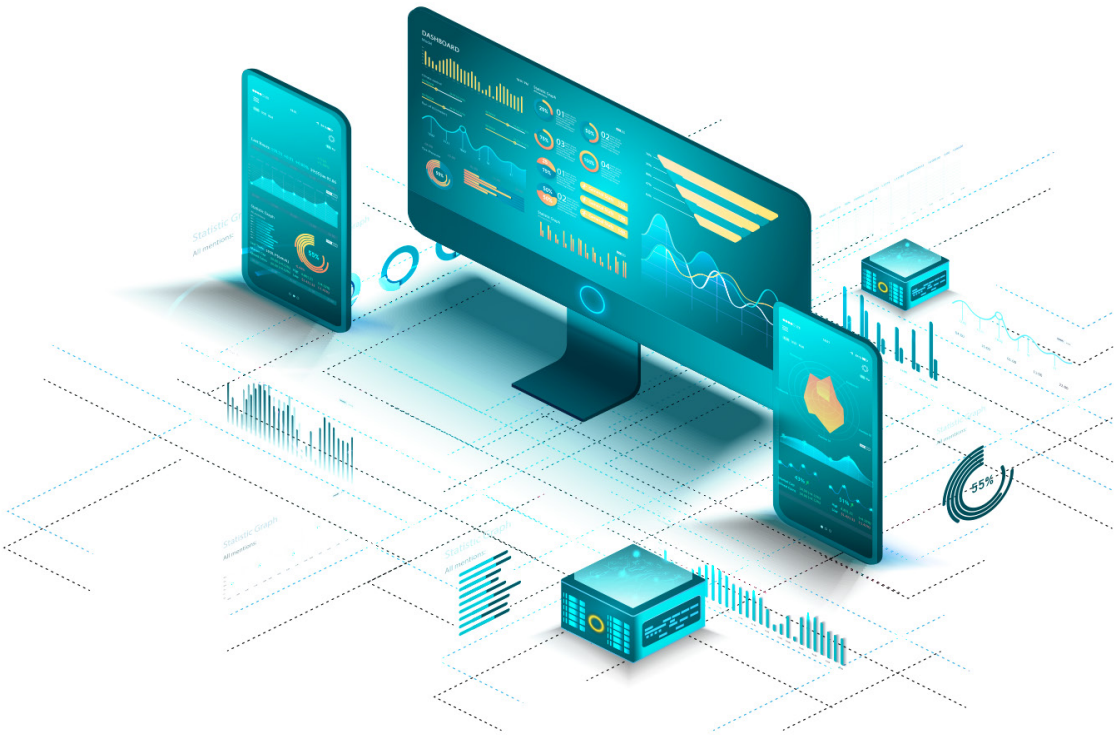
Les entreprises entièrement numériques étaient clairement mieux adaptées et mieux organisées pour le télétravail, mais toutes les entreprises n'ont pas eu cette chance. Il convient de rappeler que des milliers d'entreprises exigent que leurs collaborateurs travaillent depuis leur domicile. Si la sécurité est au cœur de la politique organisationnelle, il n'y a donc aucune raison pour que la majorité des entreprises ne puissent pas continuer de travailler à l'extérieur du bureau en toute sécurité.

Et s'il existe un vaccin? Est-ce que tout va revenir à la normale? Je ne pense pas. Nous avons tous appris que le télétravail peut être bénéfique aux entreprises et que la transition peut se faire en toute sécurité. Je ne pense pas, cependant, que nous continuerons de télétravailler cinq jours par semaine. Nous avons constaté qu'à mesure que cela fonctionne, nous continuerons de travailler à domicile quand cela nous conviendra... Ce qui sera sans aucun doute bénéfique pour notre santé et notre bien-être.

Personnellement, j'ai trouvé que ce passage au télétravail améliorait énormément ma vie de famille. Je n'ai jamais passé autant de temps avec mes jeunes enfants, et ils m'ont dit à plusieurs reprises combien il est agréable de m'avoir à la maison plus souvent. Cette comédie du lundi au vendredi de 9h à 18h est révolue. Nous devons à COVID-19 d'avoir accéléré un processus qui aurait probablement pris des années à être mis en place, voire pas du tout. De plus en plus de salariés vont naturellement et sans effort se diriger vers ce qui fonctionne le mieux pour eux et leur entreprise. Le fait que cela puisse être pris au sérieux et réalisé en toute sécurité permettra d'améliorer l'environnement pour tout le monde.

Indépendamment de ce que l'avenir nous réserve, deux choses sont certaines : notre façon de travailler a été irrévocablement transformée et les cyberattaques ne vont pas disparaître. La pandémie de COVID-19 n'a fait qu'accélérer la mise en œuvre de la technologie dans tous les domaines de la vie, et comme nos vies professionnelles et personnelles sont de plus en plus numérisées, la cybersécurité restera le pilier de la sécurité des entreprises.

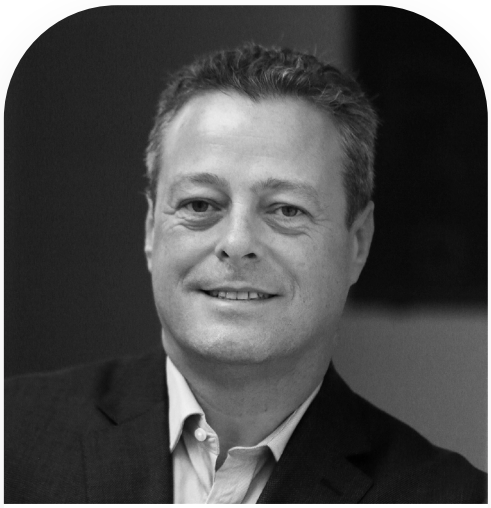
Les cyberattaques sont une menace constante pour les entreprises, qui doivent mettre en place des équipes et des systèmes informatiques résistants pour éviter les conséquences des attaques sur leurs finances et leur réputation. La sensibilisation de la main-d'œuvre joue un rôle essentiel dans la stratégie de cybersécurité de toute entreprise, pour améliorer l'efficacité des formations et inciter les collaborateurs à s'investir davantage dans leurs propres compétences. Comprendre que l'élément humain de la cybersécurité est tout aussi important que l'élément technique est la première étape de l'implémentation de protocoles holistiques qui tiennent compte des forces et des points faibles des individus.



2

DES RANSOMWARES DIFFÉRENTS : PAYEZ OU VOS DONNÉES SERONT DIVULGUÉES

Avec des attaques de ransomwares demandant des sommes de plus en plus importantes, et des pirates qui cherchent des moyens de forcer les entreprises à payer, les enjeux sont clairement élevés pour les victimes. À quoi ressemblera l'année prochaine dans le paysage des ransomwares?



Tony Anscombe
Évangéliste de la sécurité chez ESET

Une chose qui d'après moi devrait changer en 2021 est la définition du mot ransomware :

> « Un ransomware est un logiciel informatique illégal qui empêche un ordinateur de fonctionner ou qui empêche l'utilisateur d'accéder à des informations tant qu'il n'a pas payé une certaine somme d'argent. »
>
> (Dictionnaire anglais Collins)

Pourquoi cette définition devrait-elle être modifiée?

On se souvient des années 1980 pour beaucoup de choses : les mixtapes, les épaulettes, le Rubik's Cube et le concert Live Aid pour n'en citer que quelques-unes, mais peu d'entre nous associent cette décennie avec les ransomwares. En 1989, le cheval de Troie AIDS infectait de s appareils via une disquette, cachait des répertoires et chiffrait les noms et les extensions des fichiers stockés sur le disque dur. L'utilisateur recevait ensuite un message lui demandant de renouveler sa licence afin de résoudre le problème en envoyant 189 dollars à une boîte postale au Panama. Trente et un ans plus tard, avec plusieurs rebondissements dans son évolution, le terme « ransomware » est couramment utilisé dans le monde entier.

Les ransomwares sont aujourd'hui principalement associés au chiffrement des fichiers et des données, et au verrouillage de l'accès jusqu'à ce qu'une rançon soient payée et qu'une méthode de déchiffrement soit fournie. C'est du moins ce que vous espérez. Au cours de leur évolution, les ransomwares ont adopté différentes formes, notamment en verrouillant l'ensemble de l'appareil sans rien chiffrer et en affichant un message exigeant un paiement pour récupérer l'accès, ou en verrouillant seulement l'écran, en affichant des images pornographiques avec l'exigence d'un paiement par SMS surtaxé pour récupérer l'accès et empêcher l'affichage des images.

La part de marché de Microsoft Windows crée un environnement cible naturel pour les cybercriminels qui veulent soutirer de l'argent à leurs victimes. Il est cependant important de noter que d'autres plateformes ne sont pas à l'abri, avec des exemples d'attaques de ransomwares sur le système OS X d'Apple et sur le système d'exploitation Android de Google.

PRESSION SUPPLÉMENTAIRE

L'exfiltration combinée à l'extorsion n'est peut-être pas une technique nouvelle, mais c'est certainement une tendance qui se développe. Lors de ces attaques, les pirates exfiltrent un exemplaire des données sensibles vers leur propre environnement, puis chiffrent et verrouillent l'accès aux données sur les serveurs des victimes. Les pirates menacent alors de publier, vendre ou mettre aux enchères les données sensibles si aucune rançon n'est payée. Cette technique est généralement un scénario à long terme pour les pirates, puisqu'ils doivent obtenir l'accès au réseau, identifier les données sensibles et en exfiltrer un exemplaire.

Considérons pour un instant l'incursion du point de vue des cybercriminels : les entreprises deviennent plus intelligentes, déploient des technologies qui contrecarrent les attaques, créent des processus de sauvegarde et de restauration résilients, et sont beaucoup moins susceptibles de payer une rançon. Les pirates ont donc besoin d'un « plan de secours » pour monétiser leurs efforts et augmenter l'impact de leurs attaques, au lieu de dépendre d'une seule forme de menace : infecter et chiffrer. En ajoutant le « vol d'un exemplaire des données » à leur panoplie, ils renforcent leur résilience et obtiennent un argument de vente unique afin de conclure l'affaire avec leur « client », la victime. Maze est l'un de ces groupes de cybercriminels qui se distingue par des attaques d'exfiltration et d'extorsion. Fin 2019, le groupe a publié des détails sur des données qu'il prétend avoir volées à Southwire, un fabricant de câbles américain, qui a refusé de payer une rançon de 6 millions de dollars. Maze a poursuivi sa sale besogne en publiant une liste d'entreprises qui refusaient de coopérer, en menaçant de publier leurs documents et leurs données sensibles. En mars 2020, pendant que le monde était plongé dans le chaos de la pandémie de COVID-19, le groupe a annoncé par tweet qu'en raison de la crise mondiale, il offrirait une réduction à toutes les entreprises qui refusaient de coopérer, et s'abstiendrait d'attaquer les entreprises médicales jusqu'à ce que la situation s'améliore.

Ce scénario de longue haleine d'exfiltration et d'extorsion exige des pirates qu'ils possèdent des compétences différentes et une certaine patience. Tandis que de nombreuses attaques de ransomwares se sont contentées de refuser l'accès, soit par verrouillage, soit par chiffrement, cette tendance croissante à voler un exemplaire des données oblige les pirates à infiltrer un réseau et l'explorer sans être détectés afin que des données sensibles puissent être identifiées puis exfiltrées. Il ne s'agit plus d'un simple lien ou d'une pièce jointe dans un email qu'un employé ou un consommateur sans méfiance ouvre et qui déclenche involontairement une attaque. Il faut un point d'entrée initial, utilisant des techniques pour exploiter le protocole RDP (accès à distance), ou des attaques de « credential stuffing » ou des mécanismes plus traditionnels d'hameçonnage et d'ingénierie sociale.

Une fois dans le réseau, il faut pouvoir échapper à toute détection, recueillir des informations et collecter des identifiants et des mots de passe supplémentaires pour s'assurer que même si la porte initiale se referme, cet accès est conservé. Le travail préparatoire et les renseignements requis pour cartographier un réseau prennent du temps et nécessitent des ressources qualifiées pour atteindre l'objectif ultime d'identifier les ressources précieuses de l'entreprise, qui, si elles sont verrouillées ou divulguées, causeraient à l'entreprise le maximum de perturbations. Ce n'est qu'une fois les données furtivement exfiltrées que les pirates peuvent passer au déploiement plus traditionnel de ransomwares. Grâce à l'accès privilégié existant, ils peuvent même en avoir profité pour désactiver la protection afin d'assurer la réussite de leur attaque.

L'ÉVOLUTION DES DEMANDES

Les compétences et le temps supplémentaires requis doivent être financés, comme le montre l'évolution des exigences des cybercriminels. En 2018, la ville d'Atlanta a subi une attaque de ransomware traditionnel. Des serveurs clés de l'infrastructure ont été chiffrés et les pirates ont exigé 51 000 dollars pour fournir la méthode déchiffrement. La ville d'Atlanta a fait ce qu'il fallait faire; elle a refusé de payer et a reconstruit ses systèmes, ce qui lui aurait coûté 9,5 millions de dollars.

Les 18 derniers mois ont vu les demandes augmenter, malheureusement pas au taux d'inflation normal. Lake City et Riviera Beach City en Floride ont payé 500 000 et 600 000 $ respectivement. Lion, une entreprise australienne de boissons, a refusé de payer une rançon d'un million de dollars, et l'Université de Californie à San Francisco a reçu une demande de 3 millions de dollars et a payé 1,1 million de dollars. Aujourd'hui deux ans plus tard, les demandes faites à la ville d'Atlanta semblent minuscules, et cette tendance malvenue à la hausse des sommes d'argent demandées va très probablement se poursuivre.

Les demandes de paiement en bitcoins ne sont pas le seul indicateur qui démontrent un changement dans le paysage. Coalition, une société de cyberassurance qui compte 25 000 petites et moyennes entreprises clientes en Amérique du Nord, a récemment publié un rapport résumant les demandes d'indemnisation au cours du premier semestre 2020, qui couvre bien entendu le début de la pandémie. Le rapport indique que « la gravité moyenne des sinistres déclarés par les assurés de Coalition a augmenté de 65 % entre 2019 et 2020, en grande partie en raison de la hausse du coût des attaque de ransomwares. » Le rapport précise que 41 % de toutes les demandes d'indemnisation sont liées à des ransomwares et indique que « depuis peu, un certain nombre d'opérateurs de ransomwares volent désormais les données d'une entreprise avant de les chiffrer, puis menacent de révéler publiquement les données volées si une rançon n'est pas payée. » Les données indépendantes contenues dans le rapport de Coalition confirment ce changement de mode opératoire des cybercriminels ainsi que l'augmentation des montants demandés.

LES ENJEUX SONT PLUS IMPORTANTS

Intéressons-nous maintenant au mois d'août 2020, avec une autre histoire de fuites de données : Blackbaud, un prestataire de services dans le Cloud qui fournit des logiciels de collecte de fonds à des entreprises du monde entier, a annoncé avoir réussi à se défendre contre une attaque de ransomware. En coopération avec un analyste expert et les forces de police, l'équipe de cybersécurité de Blackbaud a empêché un cybercriminel de chiffrer ses données et de les verrouiller sur ses propres systèmes. Le pirate a cependant rapidement mis en œuvre son plan de secours, proposant contre paiement de supprimer les données sensibles des clients qu'il avait exfiltrées des systèmes Blackbaud avant leur protection par l'équipe de cybersécurité.

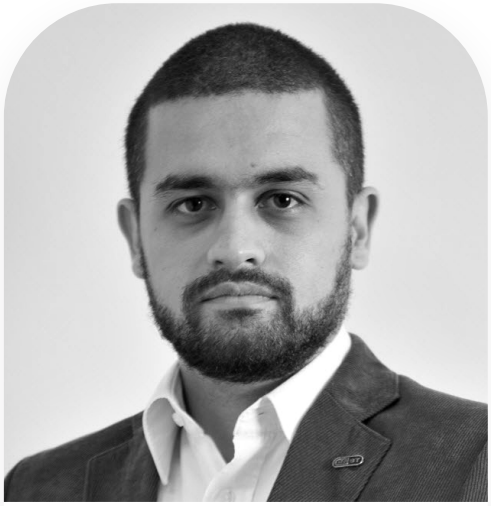
Étonnamment, Blackbaud a payé une somme non révélée au pirate à condition qu'une preuve de la suppression soit fournie. Le plan de secours a porté ses fruits pour le cybercriminel, malgré les efforts héroïques des équipes qui ont contrecarré l'attaque. Si l'attaque s'était limitée au scénario plus traditionnel d'infection et de chiffrement, nous n'aurions peut-être même jamais entendu parler de cette faille de sécurité. Néanmoins, comme les données volées comprenaient des informations permettant d'identifier des personnes, l'entreprise a été obligée par la législation locale sur la protection de la confidentialité, d'informer les clients et les autorités de régulation qu'une fuite de données s'était produite.

Déjouer des attaques ou implémenter des processus de sauvegarde et de restauration efficaces peuvent ne plus suffire à repousser les cybercriminels qui exigent le paiement d'une rançon. Changer de technique pour réussir à monétiser les attaques, même si cela nécessite plus de ressources et de patience, permet aux cybercriminels d'améliorer leurs chances de générer un retour sur investissement (ROI), exactement comme une entreprise légitime qui serait jugée sur son ROI. Dans le scénario Blackbaud, l'attaque de ransomware ne déployait pas de logiciel malveillant et ne verrouillait pas l'accès aux systèmes ou aux données. C'est une autre évolution du terme « ransomware ». Je suis sûr que c'est une tendance que nous verrons malheureusement davantage en 2021.

3

AU-DELÀ DE LA PRÉVENTION : SUIVRE LE RYTHME DES CYBERMENACES ATS

Les acteurs de la menace cherchent toujours des moyens de rendre leurs attaques plus difficiles à détecter et à contrecarrer, notamment en cooptant les outils légitimes d'un système à des fins malveillantes. Comment les cyberdéfenseurs peuvent-ils suivre la cadence?



Camilo Gutiérrez Amaya
ESET Senior Security Researcher

Depuis l'apparition du concept de « virus informatique », il y a plus de 30 ans, les menaces de cybersécurité n'ont cessé d'évoluer. En effet, selon le rapport Global Risks Report 2020 du Forum économique mondial, les cybermenaces figurent parmi les risques les plus importants pour l'humanité au cours des dix prochaines années. Ajoutons à cela la pandémie COVID-19, qui, en plus de toutes ses conséquences désastreuses, a également augmenté les risques de subir un incident de sécurité. Cela a été confirmé par l'augmentation des tentatives de cyberattaques au début de cette année, comme l'ont souligné de nombreuses organisations, dont l'Organisation des nations unies et le National Cyber Security Centre (NCSC) du Royaume-Uni.

Dans ce contexte, nous avons vu, au cours des dernières années, comment les groupes cybercriminels se sont tournés vers l'utilisation de techniques de plus en plus complexes pour perpétrer des attaques de plus en plus ciblées. Il y a quelque temps, la communauté de la sécurité a commencé à parler d'attaques de « logiciels malveillants sans fichiers » (ou « fileless malwares »), qui s'appuient sur les outils et les processus du système d'exploitation lui-même et les exploitent à des fins malveillantes. En d'autres termes, les incursions co optent des applications pré-installées sans qu'il soit nécessaire de déposer des exécutables supplémentaires sur le système de la victime. Ces exécutables ont été surnommés LOLBaS (« Living Off the Land Binaries and Scripts »). Depuis la fin de 2017, le terme a commencé à être utilisé pour désigner les techniques où les attaquants utilisent des binaires exécutables déjà préinstallés sur un système.

Comme ces attaques peuvent être difficiles à détecter, les adversaires adoptent ces techniques afin de maximiser la furtivité et l'efficacité de leurs attaques.

LÀ OÙ TOUT A COMMENCÉ

Il est important de noter que l'utilisation de ces techniques n'est pas quelque chose de nouveau. Nous avons vu comment certaines familles de logiciels malveillants ont commencé à abuser de ces caractéristiques dès 2001, lorsque le ver Code Red est apparu. Ces dernières années, cependant, ces techniques ont gagné en popularité, ayant été employées dans diverses campagnes de cyberespionnage et par divers acteurs malveillants, principalement pour toucher des cibles de fichiers de haut niveau telles que des entités gouvernementales. C'est notamment le cas de l'Opération In(ter)ception, qui a impliqué des attaques contre des entreprises militaires et aérospatiales en Europe et au Moyen-Orient, ainsi que du groupe EvilNum et de ses attaques contre le secteur financier.

Nombre des tactiques, techniques et procédures (TTP) utilisées par ces groupes sont décrites dans le cadre de l'initiative MITRE ATT&CK®. Parmi les TTP les mieux documentées figurent sans doute celles d'APT34, également connu sous le nom de groupe Lazarus, qui s'est fait un nom dans la cybercriminalité avec des incursions telles que l'attaque contre Sony Pictures de 2014, les attaques contre un casino en ligne en Amérique centrale de 2017 et, plus récemment, les attaques visant des institutions financières en Europe. Comme l'ont constaté les chercheurs d'ESET, le Groupe Invisimole fonde également ses opérations sur l'utilisation de techniques de type « living of the land », avec un ensemble complet d'outils pour mener des campagnes de cyberespionnage. Les incursions profitent, par exemple, d'applications vulnérables telles que Total Video Player ou speedfan.sys, en plus de composants légitimes comme rundll32 et womapiexec, afin de rester sous le radar.

Ceci dit, même une recherche rapide dans le cadre de MITRE ATT&CK® sur l'utilisation malveillante de binaires tels que certutil, esentutl ou regsvr32, pour n'en citer que quelques-uns, fait ressortir un grand nombre d'acteurs de la menace utilisant ces techniques. Même un examen superficiel des groupes qui utilisent ces trois binaires révèle plus de 100 acteurs de menace différents, dont certains des groupes APT les plus notoires au monde, y compris Turla, Machete, Fancy Bear et Cobalt Group.

Compte tenu de tout ce qui précède, on peut donc raisonnablement s'attendre à ce que 2021 soit une année où les incidents utilisant ces techniques auront un impact plus important. Des secteurs tels que les infrastructures critiques ou le secteur financier figureront probablement parmi les plus visés

COMPRENDRE LES MODÈLES D'ATTAQUE POUR RENFORCER VOS DÉFENSES

Grâce à leur utilisation de programmes légitimes, l'une des principales caractéristiques de ces attaques est qu'elles réduisent considérablement les traces d'activité criminelle, car les actions malveillantes sont chargées et exécutées à partir de la mémoire de l'ordinateur, sans affecter le système de fichiers. Par conséquent, ces attaques génèrent peu ou pas d'éléments d'analyse que les cyberdéfenseurs peuvent utiliser.

Ceci peut évidemment entraver la détection et, par extension, la prévention de ces attaques. Les attaques sont également particulièrement efficaces lorsque la sécurité d'une organisation est axée sur des technologies de détection basées sur la liste blanche ou lorsqu'elle ne dispose pas d'une heuristique offrant des capacités de détection avancées.

Comme ces attaques cherchent à échapper à la plupart des solutions de sécurité et à contrecarrer l'analyse des experts en cybercriminalité, une autre caractéristique principale qui sous-tend ces techniques est la furtivité. Les attaquants s'appuient sur les outils natifs d'un système tels que PowerShell et WMI (Windows Management Instrumentation), qui sont conçus pour faciliter l'automatisation des tâches et la gestion des paramètres du système d'exploitation.

Les attaquants utilisent aussi souvent ces méthodes pour obtenir la persistance, l'escalade des privilèges et même l'exfiltration des données, alors que l'accès initial est encore couramment associé à l'exploitation de vulnérabilités ou à des campagnes d'ingénierie sociale. Il est donc nécessaire d'envisager d'autres stratégies de gestion de la sécurité qui vont au-delà des technologies de prévention et prennent en compte la détection et la réponse aux incidents.

LES DÉFIS EN MATIÈRE DE SÉCURITÉ POUR LES ENTREPRISES

L'élément clé de l'approche de toute organisation pour lutter contre les logiciels malveillants sans fichiers en 2021 consiste à renforcer les processus et les procédures internes qui permettent d'intégrer les technologies et les personnes afin de surveiller l'ensemble du cycle de vie d'une menace, depuis le moment où un attaquant cherche un accès initial à un système jusqu'à l'exfiltration des données ou tout autre type d'action néfaste. Par conséquent, il est essentiel d'envisager plusieurs couches de technologies qui permettent une visibilité avant, pendant et après une attaque.

Ces types de capacités sont obtenus grâce à des technologies telles que la détection et la réponse des terminaux (EDR), qui améliorent la visibilité des défenseurs sur ce qui se passe au sein d'un réseau informatique. En tandem avec les technologies de détection, l'EDR peut augmenter la capacité d'une organisation à détecter des activités suspectes et à mettre fin à des comportements considérés comme dangereux, tout en permettant d'enquêter sur des incidents potentiels qui peuvent faire partie d'une attaque plus importante et d'isoler les dispositifs qui pourraient être compromis.

Les menaces sans fichier ont évolué rapidement et l'on s'attend à ce qu'en 2021, ces méthodes soient utilisées dans des attaques de plus en plus complexes et de plus grande envergure. Cette situation souligne la nécessité pour les équipes de sécurité de développer des processus exploitant des outils et des technologies qui non seulement empêchent le code malveillant de compromettre les systèmes informatiques, mais qui disposent également de capacités de détection et de réaction - avant même que ces attaques ne remplissent leur mission. Les changements induits par les pandémies ont accéléré la transformation numérique en 2020, mais l'année qui vient annonce de nouveaux défis pour les organisations, qui devraient continuer à adopter des technologies leur permettant d'accroître leur visibilité et leur surveillance des comportements anormaux. Il est donc vital que les organisations soient équipées des outils techniques appropriés et d'une équipe de personnes formées qui aident à détecter les incidents à un stade précoce et à y répondre rapidement.

4

MAUVAISES VIBRATIONS: FAILLES DE SÉCURITÉ DANS LES JOUETS SEXUELS INTELLIGENTS

À quel point les sex toys sont-ils sécuritaires? Les vendeurs en font-ils suffisamment pour protéger les données et la vie privée des gens? Et pourquoi la sécurité est-elle si importante lorsqu'on parle de jouets pour adultes?

Cecilia Pastorino

Chercheuse en cybersécurité d'ESET

Denise Giusto Bilić

Chercheuse en cybersécurité d'ESET

Personne ne s'étonnera d'apprendre que les appareils connectés via l'Internet des objets (IoT) présentent des vulnérabilités. ESET a analysé les graves failles trouvées dans de nombreux hubs de maisons intelligentes et caméras intelligentes. De plus, les chercheurs d'ESET ont récemment découvert KRØØK, une grave vulnérabilité Wi-Fi. Bien que les dispositifs IdO aient fait l'objet d'innombrables failles de sécurité entraînant l'exposition des données de connexion, des informationsfinancières et de la localisation géographique des personnes, entre autres, il existe peu de types de données plus susceptibles de nuire à un utilisateur, si elles sont publiées, que celles relatives à leurs activités sexuelles.

Avec l'apparition régulière sur le marché de nouveaux modèles de jouets intelligents pour adultes, on peut imaginer que des progrès sont réalisés dans le renforcement des mécanismes visant à garantir de bonnes pratiques dans le traitement des informations des utilisateurs. Cependant, de nombreuses recherches ont montré que nous sommes loin de pouvoir utiliser des sex toys intelligents sans nous exposer au risque d'une cyberattaque. Ces conclusions sont aujourd'hui plus pertinentes que jamais, car nous constatons une croissance rapide des ventes de sex toys, reflet de la crise sanitaire mondiale et des mesures de distanciation sociale liées à COVID-19.

On peut donc se questionner sur la sécurité des jouets pour adultes à l'heure actuelle et sur ce que nous réserve l'avenir. Les précautions nécessaires ont-elles été prises pour protéger les données et la vie privée des gens? Pourquoi la sécurité est-elle si importante en ce qui concerne les jouets sexuels?

EN QUOI LA SÉCURITÉ ENTRE EN JEU

Comme on peut l'imaginer, les informations traitées par les sex toys intelligents sont extrêmement sensibles : noms, préférences et orientations sexuelles, liste de partenaires sexuels, informations sur l'utilisation des appareils, photos et vidéos intimes, etc. Toutes ces informations peuvent avoir des conséquences désastreuses si elles tombent entre de mauvaises mains.

Qui pourrait être intéressé par ce type d'informations? De nombreux pays ont des lois qui interdisent expressément à leurs citoyens de se livrer à certaines pratiques sexuelles. Que se passerait-il si les autorités locales lançaient une campagne d'oppression fondée sur l'expropriation forcée des données des entreprises qui les traitent, ou sur l'exploitation des bugs ou des faiblesses des appareils sexuels comme moyen d'identifier, de localiser et de persécuter les homosexuels, les adultères ou toute autre personne appartenant à une minorité ou à un groupe social en raison de leurs pratiques et préférences sexuels? En outre, les jouets sexuels ne sont pas à l'abri de la possibilité d'être compromis par des cyber-attaquants. De nouvelles formes de sextorsion pourraient surgir, si l'on considère le matériel intime accessible par les applications qui contrôlent ces dispositifs.

Outre les préoccupations relatives à la confidentialité des données, nous devons envisager la possibilité que les vulnérabilités de l'application permettent d'installer des logiciels malveillants sur le téléphone ou de modifier les microprogrammes des jouets. Ces situations pourraient conduire à des attaques par déni de service (DoS) qui bloqueraient toute commande. Ce fût notamment le cas d' une cage de chasteté masculine intelligente, qui s'est récemment révélée vulnérable à l'exploitation par des attaquants pouvant les barrer en série, piégeant potentiellement des milliers d'utilisateurs. Un dispositif pourrait également être armé pour effectuer des actions malveillantes et propager des logiciels malveillants, ou même être délibérément modifié pour causer des dommages physiques à l'utilisateur, par exemple en surchauffant et en explosant.

Parallèlement, nous ne pouvons pas parler des implications d'une attaque sur un appareil sexuel sans réévaluer également l'importance des abus sexuels dans le contexte de la transformation numérique que connaît la société. Quelles sont les conséquences de la possibilité pour une personne de prendre le contrôle d'un appareil sexuel sans son consentement? Cela pourrait-il être considéré comme une agression sexuelle? La notion de cybercriminalité prend une autre apparence si nous l'examinons sous l'angle de l'atteinte à la vie privée, de l'abus de pouvoir et de l'absence de consentement à un acte sexuel. Le consentement obtenu par fraude n'est pas un consentement du tout, et cette lacune dans les lois actuelles devra être comblée afin de garantir la sécurité sexuelle, physique et psychologique des utilisateurs dans l'arène numérique.

SURFACE D'ATTAQUE DES SMARTS SEX TOYS

En termes d'architecture, la plupart de ces appareils peuvent être contrôlés via Bluetooth Low Energy (BLE) à partir d'une application installée sur un smartphone. De cette façon, les sex toys agissent comme des capteurs, qui ne font que collecter des données et les envoyer à l'application pour qu'elle les traite. L'application est alors chargée de régler les options de l'appareil et de contrôler le processus d'authentification de l'utilisateur. Pour ce faire, elle se connecte par Wi-Fi à un serveur dans le nuage, qui stocke les informations sur le compte de la personne. Dans certains cas, l'application sert également d'intermédiaire entre les différents utilisateurs qui souhaitent utiliser des fonctionnalités telles que le chat, la vidéoconférence et les transferts de fichiers, ou s'ils veulent donner le contrôle de leur appareil à des utilisateurs distants en partageant des tokens d'identifications avec ces derniers.

Certains fournisseurs offrent aux utilisateurs la possibilité de se connecter à leur appareil en installant un logiciel sur leur ordinateur et en utilisant un dongle BLE spécial. Vous pouvez également utiliser l'API BLE dans certains navigateurs pour vous connecter aux sex toys à l'aide d'une application web. Les différentes façons de se connecter aux appareils offrent plus de flexibilité, mais augmentent également la surface d'attaque.

Qu'est-ce qui pourrait mal tourner? Cette architecture présente plusieurs points faibles qui pourraient être utilisés pour compromettre la sécurité des données traitées : intercepter la communication locale entre l'application de contrôle et l'appareil, entre l'application et le cloud, entre le téléphone distant et le cloud, ou attaquer directement le backend. Bien entendu, toutes les attaques ne se font pas par le biais de connexions réseau et certains scénarios malveillants pourraient être lancés en utilisant des logiciels malveillants préalablement installés sur le téléphone ou en exploitant des bogues dans le système d'exploitation.

De nombreux chercheurs en sécurité ([1], [2], [3] et [4], entre autres) ont montré que ces dispositifs contiennent des failles de sécurité qui pourraient menacer la sécurité des données stockées ainsi que la sécurité de l'utilisateur. Ces failles vont de procédures d'authentification médiocres à des dispositifs qui rendent leur présence constamment publique, permettant à quiconque de s'y connecter.

En 2016, deux chercheurs ont présenté une conférence intitulée « Hacking the Internet of Vibrating Things ». Ils ont montré comment des informations telles que l'intensité, les modèles, la température et les habitudes des utilisateurs étaient collectées par l'application We-Connect et renvoyées aux serveurs sans aucun anonymat. L'année dernière, un chercheur a montré à quel point il pouvait être facile pour un attaquant de pirater une fiche de connexion contrôlée par le BLE. C'était également la première preuve de concept où un appareil sexuel intelligent pouvait être utilisé comme arme et nuire à la personne qui l'utilisait.

Cette année, l'équipe de chercheurs d'ESET en Amérique latine a présenté à DEF CON IoT Village de nouveaux résultats de recherche sur les jouets sexuels intelligents non sécuritaires. L'enquête était basée sur deux dispositifs : un dispositif portable appelé Jive, fabriqué par We-Vibe, et le masturbateur masculin Max de Lovense.

Nous avons découvert que les deux dispositifs présentaient des vulnérabilités dans la mise en œuvre des communications BLE, permettant aux attaquants d'intercepter les données envoyées et de contrôler à distance les dispositifs par le biais d'attaques BLE MitM (man-in-the-middle). Cela implique que n'importe qui pourrait utiliser un simple scanner Bluetooth pour localiser et contrôler ces sex toys intelligents à proximité, comme l'a fait le chercheur Alex Lomas en 2017 en se promenant dans les rues de Berlin et en détectant des sex toys. Cette vulnérabilité est très courante dans les appareils IdO, car la plupart des modèles disponibles sur le marché ne mettent pas en œuvre le paring sécurisé, ce qui permet à n'importe qui de se connecter et de les contrôler.

En ce qui concerne l'application Lovense Remote, nous avons trouvé quelques choix de conception controversés qui peuvent menacer la confidentialité des images intimes envoyées par les utilisateurs. Il n'y avait pas de chiffrement de bout en bout, les captures d'écran n'étaient pas désactivées, l'option « supprimer » du chat n'effaçait pas réellement les messages du téléphone distant, et les utilisateurs pouvaient télécharger et transférer le contenu d'autres personnes sans avertissement. En outre, les utilisateurs malveillants pouvaient découvrir les adresses électroniques associées à un nom d'utilisateur donné et vice versa. Ces constatations constituent de sérieux problèmes de protection de la vie privée, en particulier dans le cas d'une application spécifiquement conçue pour partager des contenus à caractère sexuel.

L'application permet aux utilisateurs d'accorder le contrôle à distance de leurs appareils via une URL, qui comprend un token à 4 chiffres. Nous avons également rencontré des problèmes de sécurité avec ce jeton qui permettrait aux attaquants de détourner des dispositifs à distance aléatoires sans consentement.

Quant à l'application We-Connect, nous nous sommes rendus compte que les métadonnées sensibles n'étaient pas supprimées des fichiers avant leur envoi. Cela signifie que des utilisateurs pourraient envoyer par inadvertance des informations sur leurs appareils et leur géolocalisation exacte lorsqu'ils se sont envoyés des sextos avec d'autres utilisateurs. Cela pourrait être très dangereux, car de nombreux utilisateurs donnent le contrôle de leur appareil à de parfaits inconnus en partageant leurs tokens en ligne, que ce soit par préférence personnelle ou dans le cadre de services de type « cam girl/boy ».

LES MEILLEURES PRATIQUES POUR PRÉVENIR LES RISQUES

Les sex toys intelligents gagnent en popularité dans le cadre du concept de « sexnologie », formé de la combinaison des mots sexe et technologie. Ces pratiques pourraient bien être là pour rester, mais nous ne devons pas oublier les menaces potentielles pour la vie privée et l'intimité des utilisateurs.

Pour minimiser les risques liés à l'utilisation de dispositifs sexuels intelligents, nous vous recommandons de garder à l'esprit les conseils suivants :

1. Certaines applications offrent la possibilité de contrôler les appareils localement par BLE sans créer de compte utilisateur. Si vous ne prévoyez pas de laisser d'autres utilisateurs contrôler votre appareil à distance via Internet, recherchez l'un de ces appareils.

2. Dans la mesure du possible, évitez de partager des photos ou des vidéos dans lesquelles vous pouvez être identifié et ne publiez pas vos tokens de contrôle à distance sur Internet.

3. Évitez de vous inscrire à des applications sexuelles en utilisant un nom officiel ou une adresse électronique qui pourrait vous identifier.

4. Lisez toujours les conditions générales des applications et des sites web pour lesquels vous vous inscrivez.

5. Utilisez les sex toys intelligents dans un environnement protégé et évitez de les utiliser dans des lieux publics ou des zones de passage (comme les hôtels).

6. Télécharger les applications et essayer leurs fonctionnalités avant d'acheter l'appareil peut vous donner un aperçu du degré de sécurité du produit. Utilisez les moteurs de recherche pour vérifier si le modèle que vous envisagez d'acheter a déjà présenté des vulnérabilités dans le passé.

7. Protégez toujours les appareils mobiles que vous utilisez pour contrôler ces gadgets, tenez-les à jour et faites installer une solution de sécurité sur eux.

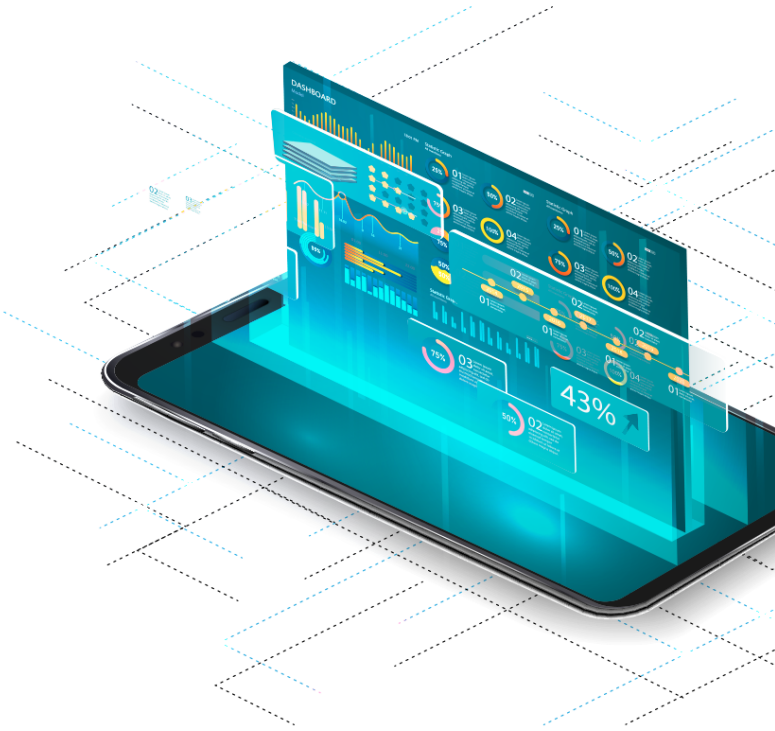
8. Protégez le réseau Wi-Fi domestique que vous utilisez pour la connexion avec des mots de passe forts, des algorithmes chiffrés sécuritairement et en effectuant la mise à jour régulière du micrologiciel du routeur.

ET LA SUITE?

L'ère des sex toys intelligents ne fait que commencer. Les dernières avancées de l'industrie comprennent des modèles dotés de capacités de RV (réalité virtuelle) et des robots sexuels alimentés par l'IA qui comprennent des caméras, des microphones et des capacités d'analyse de la voix basées sur des techniques d'intelligence artificielle. L'utilisation de ces robots pour remplacer les travailleurs du sexe dans les maisons closes est déjà une réalité.

Ces jouets sexuels ne sont qu'une petite expression de la sexualité dans le monde numérique, un domaine qui, selon nous, comprend également les applications de rencontre et d'autres dispositifs tels que les « petites amies virtuelles », la manifestation technologique d'un phénomène sociologique plus vaste qui transforme notre société à mesure que les dispositifs IdO s'infiltrent dans nos vies.

Comme cela a été prouvé à maintes reprises, un développement sûr et la sensibilisation du public seront essentiels pour garantir la protection des données sensibles, permettant aux utilisateurs les moyens de devenir des consommateurs intelligents, capables d'exiger des vendeurs de meilleures pratiques afin de garder le contrôle de leur intimité numérique dans les années à venir.



CONCLUSION

Alors que les vents et marées commencent à tourner et que nous reprenons une certaine vie pré-pandémique, nous ne devons pas baisser la garde. La complaisance, dit-on, est l'ennemi du progrès. Il s'avère qu'elle est également l'ennemie de la sécurité.

Quand la pandémie COVID-19 a initialement frappé, une grande partie de la vie normale s'est arrêtée net et une nouvelle réalité s'est installée. Même la Terre elle-même est soudainement devenue plus silencieuse moins turbulente. À ce moment, nous nous sommes repliés sur nous-mêmes, en nous taillant des espaces de travail dans nos maisons et en apprenant à vivre en réclusion chez soi. Le confinement et d'autres aspects de ce que l'on appelle désormais la nouvelle normalité ont entraîné des changements dans nos habitudes de vie et même dans notre perception du temps et de l'espace.

Le monde étant en proie à la pire crise depuis des décennies, nous avons dû faire face à une incertitude accrue en matière de santé, de relations, de finances et d'avenir. La pandémie et ses effets en chaîne nous ont permis d'apprendre une foule de nouveaux termes scientifiques et ont amené nombre d'entre nous à se réinventer. Mais surtout, la pandémie nous a appris d'importantes leçons de vie, mettant en évidence ce qui est important et ce qui ne l'est pas.

Avec la mise en place des mesures de confinement à domicile, nos vies ont basculé dans le monde en ligne et la transformation numérique a été poussée à l'extrême. La technologie nous aide à maintenir un certain bien-être social et émotionnel et à soutenir la réponse de santé publique à la pandémie. Les habitudes de travail ont également été bouleversées, car de nombreuses entreprises ont fait des pieds et des mains pour maintenir leurs activités en ligne et en se tournant vers une main-d'œuvre évoluant presque du jour au lendemain à distance. Internet est pratiquement devenu notre seule fenêtre sur le monde.

Ces éléments ont également permis de créer une tempête de cyber-risques presque parfaite. Les organisations et la main-d'œuvre nouvellement répartie ont dû nager (ou couler) dans les eaux largement inexplorées du travail à distance, révélant souvent sans le vouloir des fissures dans leurs armures de défense. Les cybercriminels ont rapidement adapté leurs tactiques pour tirer parti de la surface d'attaque en expansion et de l'environnement riche en cibles, notamment en capitalisant sur la peur du virus dans la population.

La tendance à se concentrer sur le travail à distance a également permis de découvrir et de résoudre certains problèmes de confidentialité et de sécurité sur des plates-formes qui, après une forte hausse de popularité, ont suscité une vague d'intérêt. Ces évolutions ont à leur tour contribué à montrer clairement que la sécurité doit être une priorité absolue pour tout le monde, un fait d'autant plus important que la technologie a joué un rôle essentiel dans la gestion de la perturbation sociale généralisée.

En outre, une longue liste de menaces familières, comme les rançongiciels, n'ont pas pour autant disparu cette année. Au contraire, elles ont continué à évoluer, ce qui est leur habitude, et ont frappé les victimes plus durement que jamais auparavant. Notre examen des récents développements majeurs sur la scène des rançongiciels a montré que les enjeux sont de plus en plus importants pour les victimes, et que ces attaques sont une réalité persistante qui, aussi cliché que cela puisse paraître, continuera d'évoluer.

Nous voilà donc à période de l'année où nous prenons un temps d'arrêt pour revenir sur les thèmes qui ont défini l'année qui s'achève, ainsi que pour réfléchir à ce qui nous attend. Bien que ce processus conserve un côté familier, beaucoup de choses semblent – et sont – différentes cette fois-ci. Nous devons néanmoins nous tourner vers l'avenir, y compris vers l'avenir post-pandémique. Et même lorsque le vent tournera et que nous reprendrons une certaine vie normale, nous ne devons pas baisser la garde, que ce soit en ligne ou hors ligne. La complaisance, disent-ils, est l'ennemi du progrès. Il s'avère qu'elle est également l'ennemie de la sécurité.

CYBERSECURITY
EXPERTS ON YOUR SIDE