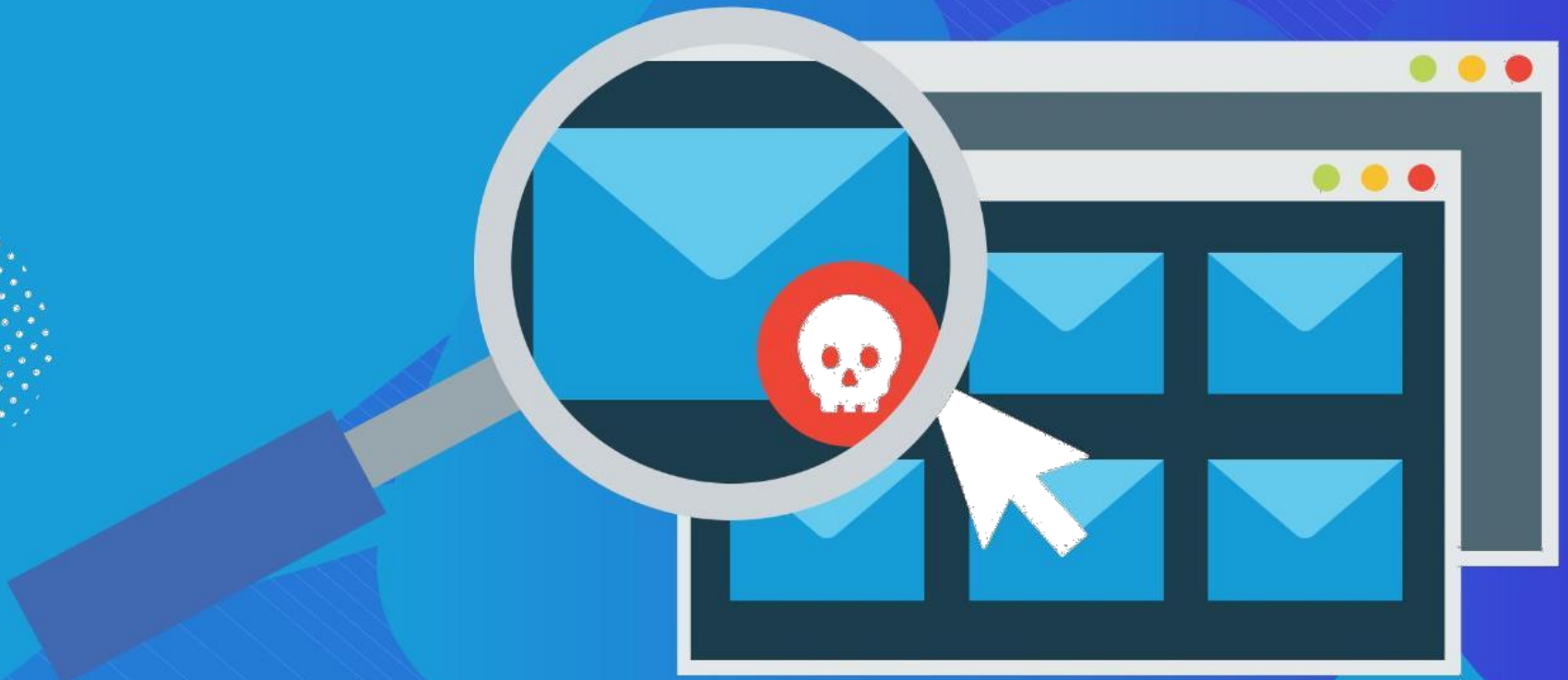
Livre blanc

Le Guide du Ransomware pour l'Entreprise

Tout savoir pour garder votre entreprise en bon état



Introduction

Le ransomware a émergé de plus en plus comme une menace majeure pour les particuliers comme pour les entreprises. Il s'agit d'un type de logiciel malveillant qui crypte les données sur les systèmes infectés, il est devenu une pratique lucrative pour les cyber-extorqueurs. Lorsque le logiciel malveillant est exécuté, il verrouille les fichiers de la victime et permet aux criminels d'exiger le paiement d'une rançon pour les libérer.

Sauf si vous avez vécu à l'écart, vous savez sans doute que le ransomware est le sujet brûlant du moment. Des organisations de tous types et tailles ont été touchées, mais les petites entreprises peuvent être particulièrement vulnérables aux attaques. Et le ransomware est à la hausse.

Dans le McAfee Labs de Juin 2018 Rapport Threat, le nombre de nouvelles souches de ransomwares a augmenté de 62% au cours des quatre derniers trimestres. Cette augmentation porte le nombre total de souches identifiées par McAfee à environ 16 millions. Le ransomware est distribué de façons très variées et il est difficile de s'en protéger parce qu'il il est en constante mutation tout comme le virus de la grippe.

Il existe des moyens pour protéger votre entreprise contre les attaques de ransomwares. Dans ce livre blanc, vous apprendrez comment le logiciel malveillant se propage, les différents types de ransomwares qui prolifèrent aujourd'hui, et ce que vous pouvez faire pour éviter ou récupérer vos données après une attaque. Vous cacher la tête dans le sable ne fonctionnera pas, parce que les demandeurs de rançon d'aujourd'hui ne jouent pas. Assurez-vous que votre entreprise est prête.

Le ransomware utilise HTML et JavaScript pour identifier le navigateur de la victime et les plug-ins installés, ce qui permet au pirate de sélectionner une attaque qui est susceptible d'être le plus couronnée de succès.

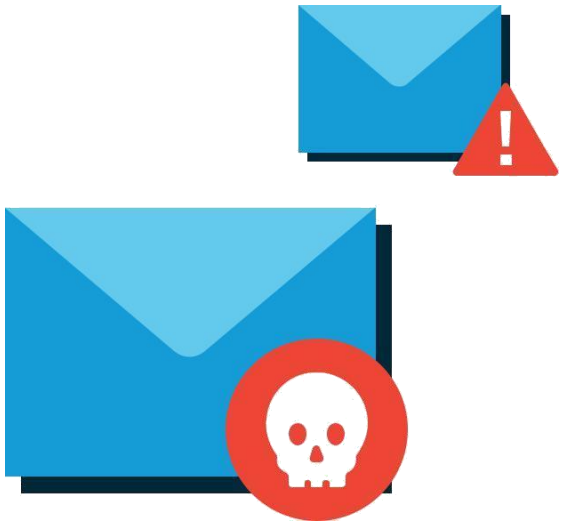
Le Ransomware Aujourd'hui

Il existe quelques types dominants, ou familles de ransomwares. Chaque type a ses propres variantes. Il est prévu que de nouvelles familles apparaissent au fil du temps. Dans le passé, Microsoft Office, les fichiers PDF et les images d'Adobe ont été ciblées, mais comme les ransomwares continuent d'évoluer, McAfee prévoit que d'autres types de fichiers deviendront des cibles.

La plupart des ransomwares utilisent l'algorithme AES pour chiffrer les fichiers, bien que certains utilisent des algorithmes alternatifs. Pour décrypter les fichiers, les cybercriminels demandent généralement le paiement sous forme de bons de paiement Bitcoins ou en ligne, tels que Ukash ou Paysafecard. La demande classique est d'environ 500 $, bien que nous ayons vu récupéré beaucoup plus élevé. Lors des campagnes de ransomware, les cybercriminels concentrent généralement leurs attaques vers les pays riches et les villes où les gens et les entreprises peuvent se permettre de payer la rançon. Lors de certaines périodes, nous avons remarqué des attaques répétées sur des secteurs spécifiques comme dans les collectivités locales.

Comment se transmet le ransomware

Le spam est la méthode la plus courante pour la distribution de ransomware. Il se propage généralement en utilisant une forme subtile de communication ; les victimes sont dupées et incitées à télécharger une pièce jointe par courriel ou à cliquer sur un lien. Les faux messages électroniques ressemblent à une note d'un ami ou collègue qui demande par exemple à l'utilisateur de consulter un fichier joint, ou à un e-mail provenant d'une institution de confiance (comme une banque) qui vous demande d'effectuer une tâche de routine. Parfois, les ransomwares utilisent des tactiques de peur, comme prétendre que l'ordinateur a été utilisé pour des activités illégales afin de contraindre les victimes à agir. Une fois que l'utilisateur fait l'action, le malware s'installe sur le système et commence chiffrer les fichiers. Cela peut arriver d'un coup en un seul clic.

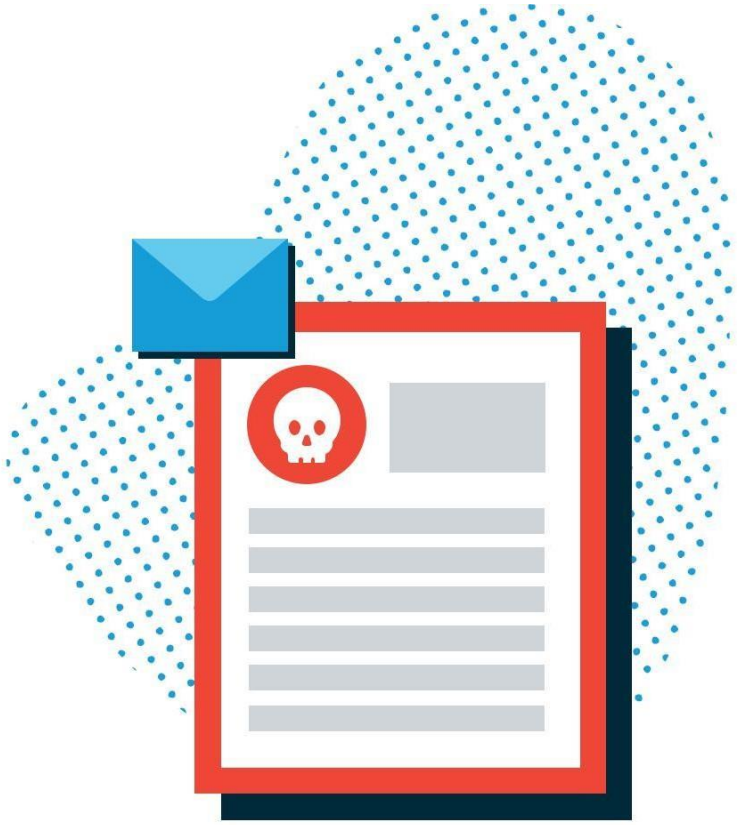


Il existe également des solutions disponibles pour les pirates en herbe disposant d'un minimum de compétences informatiques. Selon McAfee, il y a des offres ransomware-as-a-service hébergées sur le Tor Network permettant à tout un chacun de réaliser ces types d'attaques malveillantes.

Une autre méthode commune pour la diffusion de ransomware est un logiciel connu sous le nom d'Exploit Kit. Ces packages sont conçus pour identifier les vulnérabilités et les exploiter afin d'installer les ransomwares. Pour ce type d'attaque, les pirates installent le code sur un site Web légitime qui redirige les utilisateurs d'ordinateurs vers un site malveillant. Contrairement à la méthode du spam, cette approche ne nécessite parfois aucune action supplémentaire de la victime. Cette attaque est appelée « drive-by download ».

Angler était un Exploit Kit couramment utilisé en 2015. Une étude menée par le fournisseur de logiciels de sécurité Sophos a montré que des milliers de nouvelles pages Web exécutant Angler étaient créés chaque jour. L'exploit Kit Angler utilise HTML et JavaScript pour identifier le navigateur de la victime et les plug-ins installés, ce qui permet au pirate de sélectionner l'attaque qui est le plus susceptible d'avoir du succès. Au début de 2018, une nouvelle souche de ransomware appelé GandCrab a été diffusée en utilisant deux kits distincts qui exploitent les vulnérabilités d'Internet Explorer et de Flash Player pour lancer des attaques basées sur JavaScript, Flash et VBscript.

Les Spam botnets et Exploit Kit sont relativement faciles à utiliser, mais nécessitent un certain niveau de compétence technique. Cependant, il existe également des solutions disponibles pour les pirates en herbe disposant d'un minimum de compétences informatiques. Selon McAfee, il y a des offres ransomware-as-a-service hébergées sur le TorNetwork, permettant à tout un chacun de mener ce type d'attaques.



Les ransomwares courants

Comme indiqué plus haut, le ransomware est en constante évolution et de nouvelles variantes font leur apparition tout le temps. Ainsi, il serait difficile, voire impossible, de dresser une liste de tous les types de ransomwares qui prolifèrent aujourd'hui. Bien que ce qui suit ne soit pas une liste complète des ransomwares du moment, cela donne une idée des principaux acteurs existants et de leur variété.

Cryptolocker

Le ransomware existe sous une forme ou une autre depuis deux décennies, mais il s'est vraiment fait connaitre en 2013 avec le cryptolocker. L'original Botnet cryptolocker a été éliminé en mai 2014, mais les pirates ont tout de même réussi à extorquer près de 3 millions $ à leurs victimes.

Depuis lors, bien que les variantes d'exploitation d'aujourd'hui ne soient pas directement liées à l'original, l'approche cryptolocker a été largement copiée. Le mot cryptolocker, un peu comme Xerox et Kleenex dans leur domaine respectif, est devenu presque synonyme de ransomware.

Le cryptolocker est distribué par les Exploit-kits et le spam. Lorsque le logiciel malveillant est exécuté, il s'installe dans le dossier du profil utilisateur Windows et crypte les fichiers à travers les disques durs locaux et les lecteurs réseau mappés. Il crypte uniquement les fichiers avec des extensions spécifiques, y compris Microsoft Office, OpenDocument, images et fichiers AutoCAD. Une fois que le mal est fait, un message s'affiche sur l'écran de l'utilisateur l'informant que ses fichiers ont été chiffrés et lui exigeant un paiement en Bitcoin pour pouvoir récupérer ceux-ci.

CryptoWall

CryptoWall a gagné en notoriété après la chute du cryptolocker d'origine. Il a émergé au début de 2014 et des variantes sont apparues avec une variété de noms tels que : Cryptorbit, CryptoDefense, CryptoWall 2.0 et 3.0 CryptoWall, entre autres. Comme cryptolocker, CryptoWall est distribué via le spam ou l'Exploitkit.

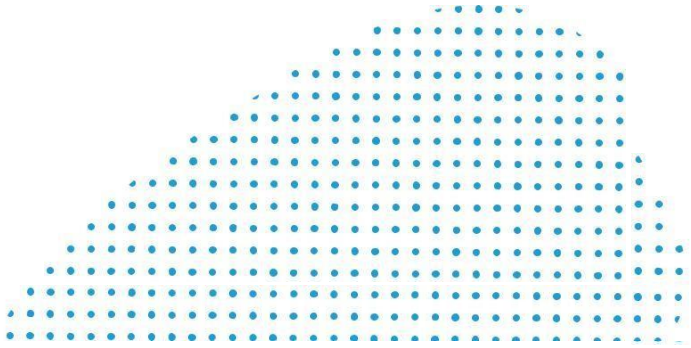
La version initiale de CryptoWall utilise une clé de chiffrement publique RSA, mais les versions ultérieures (y compris la dernière CryptoWall 3.0) utilisent une clé AES privée qui est masquée avec une clé AES publique. Quand on ouvre la pièce jointe les logiciels malveillants, les CryptoWALL binaires se copient dans le dossier temporaire Microsoft et commencent à encoder les fichiers. CryptoWall encrypte une plus grande variété de types de fichiers que cryptolocker et lorsque le chiffrement est terminé, il affiche également un message de rançon exigeant le paiement sur l'écran de l'utilisateur.

CTB-Locker

Les criminels qui sont derrière CTB-Locker adoptent une approche différente de la distribution d'un virus. Ils prennent une page des Playbooks de Girl Scout Cookies et Mary Kay Cosmetics, puis ces pirates sous-traitent le processus d'infection à ces partenaires en échange d'une part des bénéfices. C'est une stratégie qui a fait ses preuves pour réaliser plus rapidement de grands volumes d'infections via logiciels malveillants.

Lorsque CTB-Locker opère, il se copie dans le répertoire temp Microsoft. Contrairement à la plupart des formes de ransomwares aujourd'hui, CTB-Locker utilise Elliptic Curve Cryptographie (ECC) pour crypter les fichiers. CTB-Locker impacte plus de types de fichiers que cryptolocker. Une fois que les fichiers sont cryptés, CTB-Locker affiche, vous l'aurez deviné, un message exigeant le paiement d'une rançon en Bitcoins.

Les campagnes de spam Locky fonctionnent à une échelle massive. Le malware se propage en utilisant le spam, généralement sous la forme d'un message électronique déguisé en une facture. Lors de l'ouverture, la facture est brouillée et la victime doit activer les macros pour lire le document.



Locky

Locky est relativement nouveau parmi les types de ransomware, mais son approche est familière. Le malware se propage en utilisant le spam, généralement sous la forme d'un message électronique déguisé en une facture. Lors de l'ouverture, la facture est brouillée, et la victime est chargé d'activer les macros pour lire le document. Lorsque les macros sont activées, Locky commence à chiffrer un large éventail de types de fichiers en utilisant le cryptage AES. La rançon en Bitcoin est exigée lorsque le chiffrement est terminé. Est-ce plaisant ?

La campagnes de spam Locky fonctionnent à une échelle massive. Une entreprise reçoit cinq millions de courriels de blocage associés à des campagnes LOCKY en deux jours.

TeslaCrypt

TeslaCrypt est un nouveau type de ransomware. Comme la plupart des autres exemples, il utilise un algorithme AES pour chiffrer les fichiers. Il est généralement distribué par l'Exploitkit qui attaque spécifiquement les vulnérabilités d'Adobe. Une fois qu'une vulnérabilité est exploitée, TeslaCrypt s'installe dans le dossier temp Microsoft. Lorsque la victime doit payer, TeslaCrypt donne un peu de choix pour le paiement : Bitcoin, PaySafeCard et Ukash. Vous appréciez les options ?

TorrentLocker

TorrentLocker est généralement distribué via des campagnes de spam par courriels et est géographiquement ciblé, avec des messages électroniques livrés sur des régions spécifiques. TorrentLocker est souvent appelé cryptolocker et il utilise un algorithme AES pour chiffrer les types de fichiers. En plus de l'encodage des fichiers, il recueille également les adresses e-mail du carnet d'adresses de la victime pour propager des logiciels malveillants au-delà de l'ordinateur/réseau infecté initialement ce qui est unique à TorrentLocker.

Parce que le ransomware est en constante évolution, même le meilleur logiciel de sécurité peut être violé. Voilà pourquoi une couche de défense secondaire est essentielle pour les entreprises afin de s'assurer de la récupération de leurs données en cas d'attaque de logiciels malveillants : la sauvegarde.

TorrentLocker utilise une technique appelée processus de perçage, dans lequel un processus système Windows est mis en suspens, le code malveillant est installé puis le processus reprend. Il utilise explorer.exe pour le processus de perçage. Ce malware supprime également des copies Microsoft Volume Shadow pour empêcher l'aide d'outils de restauration, récupération de fichiers Windows. De même que pour les autres méthodes de ransomware décrites ci-dessus, le Bitcoin est la monnaie préférée pour le paiement de la rançon.

KeRanger

Selon ArsTechnica, le ransomware KeRanger a été découvert sur un client BitTorrent. KeRanger n'est pas largement diffusé actuellement, mais il est important de noter qu'il est le premier ransomware entièrement fonctionnel conçu pour verrouiller les applications Mac OS X.

Petya

Au lieu de crypter des fichiers sur l'ordinateur d'une victime, Petya écrase le master boot, ne permettant plus au système d'exploitation de démarrer. Petya s'appuie souvent sur des e-mails de phishing pour se diffuser.

NotPetya

Les premiers rapports ont classé NotPetya comme une variante de Petya, une souche de ransomware apparue en 2016. Cependant, les chercheurs pensent maintenant que NotPetya est plutôt un malware qui n'a qu'un seul but, détruire les données et ne pas obtenir de rançon.

WannaCry

WannaCry est une campagne de ransomware généralisée qui affecte les organisations à travers le monde. Plus de 125 000 organisations dans plus de 150 pays ont été impactées. La souche ransomware est également connue sous le nom WCry ou WanaCrypt0r, elle affecte actuellement les machines Windows à travers une faille Microsoft connue sous le nom EternalBlue

Se Protéger contre les ransomwares

Les cybercriminels armés avec ces ransomwares sont des adversaires redoutables. Alors que les PME ne sont pas spécifiquement ciblées dans les campagnes de ransomware, elles peuvent être plus susceptibles de souffrir lors d'une attaque. Souvent, les effectifs informatiques des PME sont limités et celles-ci se basent sur des technologies dépassées en raison de contraintes budgétaires. C'est le contexte parfait en terme de vulnérabilité ransomware. Heureusement, il existe de véritables moyens pour protéger votre entreprise contre les attaques de ransomwares. Le logiciel de sécurité est essentiel, cependant, vous ne pouvez pas compter sur lui uniquement. Une bonne stratégie de protection de ransomware nécessite une approche à trois volets, comprenant l'éducation, la sécurité et la sauvegarde.

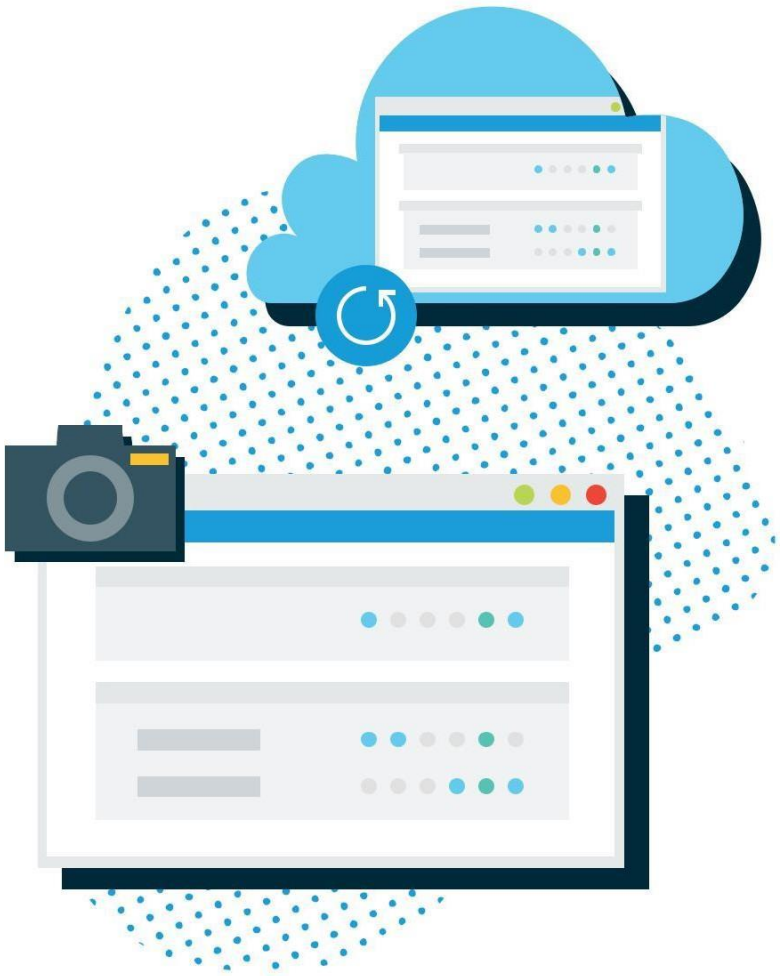
Éducation : Tout d'abord, l'éducation est essentielle pour protéger votre entreprise contre le ransomware. Il est essentiel que votre personnel comprenne ce qu'est un ransomware et les menaces qu'il engendre. Fournissez à votre équipe des exemples précis d'e-mails suspects avec des instructions claires sur ce qu'il faut faire si elle rencontre un leurre potentiel de ransomware (ne pas ouvrir les pièces jointes, si vous voyez quelque chose, avertissez en cas de doute, etc.).

Proposer une formation officielle 2 fois par an pour informer le personnel sur le risque de ransomware et autres cybermenaces. Lorsque de nouveaux employés se joignent à l'équipe, s'assurer de leur transmettre un e- mail pour mettre à jour les meilleures pratiques cyber. Il est important de veiller à ce que le message soit communiqué clairement à tout le monde dans l'organisation et ne pas communiquer uniquement par oral. Enfin, tenir les managers au courant lorsque de nouveaux ransomwares entrent sur le marché.

Sécurité : Le logiciel antivirus doit être considéré comme essentiel pour toute entreprise afin de se protéger contre les ransomwares et autres risques. Assurez-vous que le logiciel de sécurité est à jour afin de vous protéger contre les menaces nouvellement identifiées. Faites toutes les mises à jour et patchs de vos applications commerciales afin de minimiser les vulnérabilités.

Certains logiciels antivirus offrent des fonctionnalités spécifiques aux ransomwares. Sophos, Webroot par exemple, proposent une technologie qui surveille les systèmes pour détecter les activités malveillantes telles que l'extension de fichier ou modifications du Registre. Si le ransomware est détecté, le logiciel a la capacité de bloquer et alerter les utilisateurs.

Cependant, étant donné que le ransomware est en constante évolution, même le meilleur logiciel de sécurité peut être violé, c'est pourquoi une couche secondaire de défense est essentielle pour les entreprises afin d'assurer la récupération des fichiers en cas d'attaque des logiciels malveillants : la sauvegarde.



La Sauvegarde : solutions de protection des données totales modernes comme Datto, Faire des snapshot, des sauvegardes incrémentielles au rythme de toutes les cinq minutes pour créer une série de points de récupération. Si votre entreprise souffre d'une crise de ransomware, cette technologie vous permet de revenir en arrière juste avant que la corruption ait eu lieu. En ce qui concerne le ransomware, l'avantage est double, tout d'abord, vous n'êtes pas obligé de payer la rançon pour récupérer vos données et en second lieu, puisque vous restaurez à un point juste avant que le ransomware ait infecté votre système, vous pouvez être certain que tout est propre et que le malware ne peut pas être déclenché à nouveau. Voici un exemple sur la manière dont Datto a sauvé une journée de la chaîne internationale de l'hôtel Crowne Plaza.

En outre, certains produits de protection des données d'aujourd'hui permettent aux utilisateurs d'exécuter des applications à partir de sauvegardes basées sur des images de machines virtuelles. Cette capacité est communément appelée « récupération en place » ou « récupération instantanée. » Cette technologie peut être utile lors d'une attaque de ransomware car elle vous permet de poursuivre vos activités pendant que vos systèmes primaires sont en cours de restauration, sans temps d'arrêt. Cette technologie Datto est appelée businesssaving, la virtualisation instantanée, qui virtualise les systèmes localement ou à distance dans un nuage sécurisé en quelques secondes. Cette solution permet aux entreprises de rester opérationnelles en cas de catastrophe.

Conclusion

En utilisant le ransomware, les Cyber-extorqueurs sont une menace certaine pour les entreprises aujourd'hui, de la boutique locale de pizza au classement CAC 40. Cependant, un peu d'éducation et de bonnes solutions sont possibles. Assurez-vous que vos employés comprennent ce qu'il faut surveiller et vous pourrez bien dormir.
Il ne faut jamais sous-estimer la détermination ou l'expertise des pirates informatiques d'aujourd'hui. Ils s'adaptent et améliorent leurs armes en permanence. Voilà pourquoi vous avez besoin d'un logiciel de sécurité et de sauvegarde haut de gamme. Gardez votre entreprise en toute sécurité et restez serein.

Pour résumer, la diffusion des connaissances et des logiciels de sécurité peut vous aider à éviter les cyber-attaques. La gestion des correctifs est essentielle. Assurez-vous que vos logiciels sont à jour et sécurisés. En final, la sauvegarde vous aidera à redémarrer quand tout le reste échoue. Pensez à utiliser un produit de sauvegarde moderne qui offre des fonctionnalités qui vous permettent de limiter voire d'éliminer les temps d'arrêt.

Pour plus d'information:

Quietic
Nous gérons, vous grandissez.

HUB CREATIC, 6 rue Rose Dieng Nantes,, 44300
www.quietic.fr

Téléphone:02 85 52 88 00

Email: contact@quietic.fr