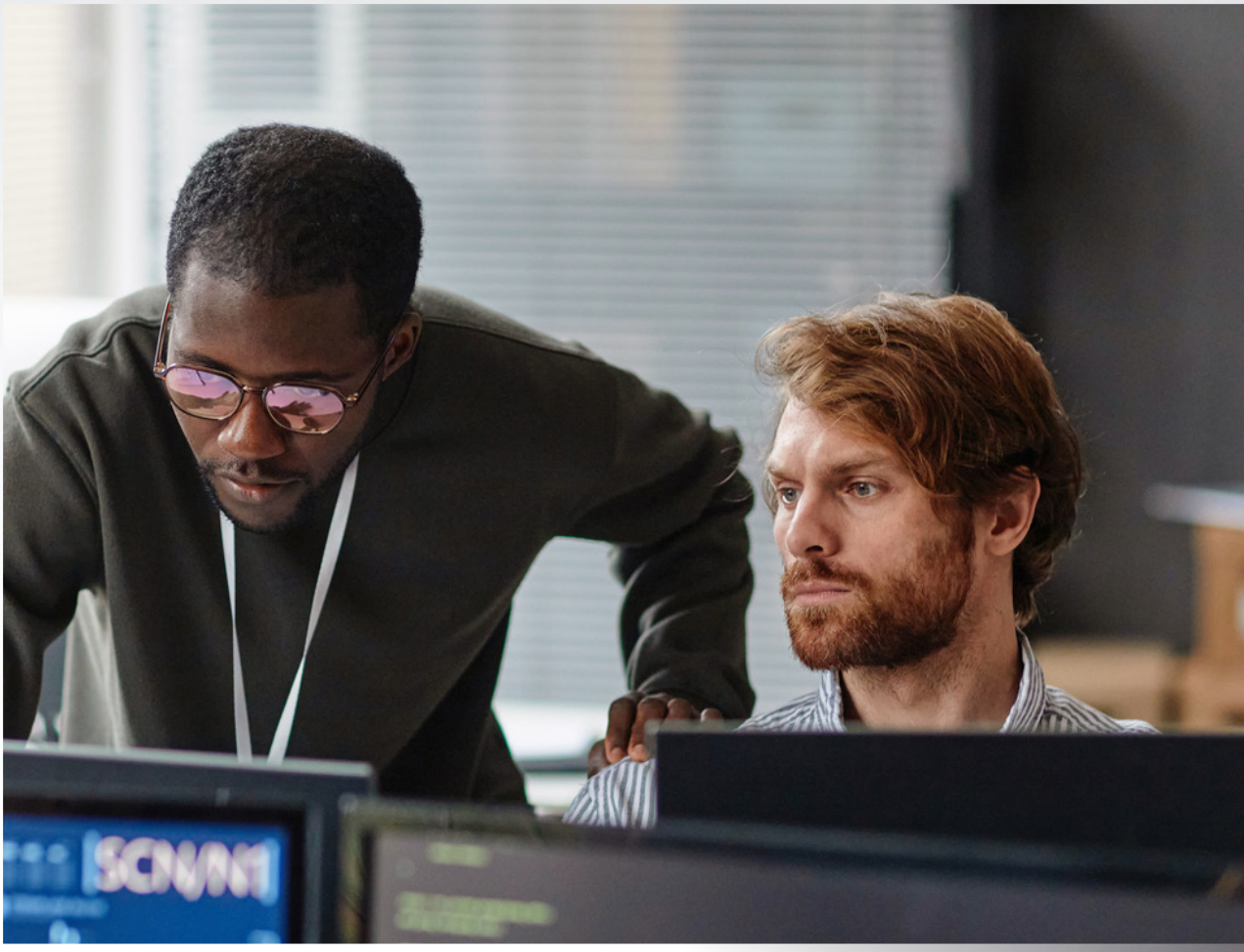
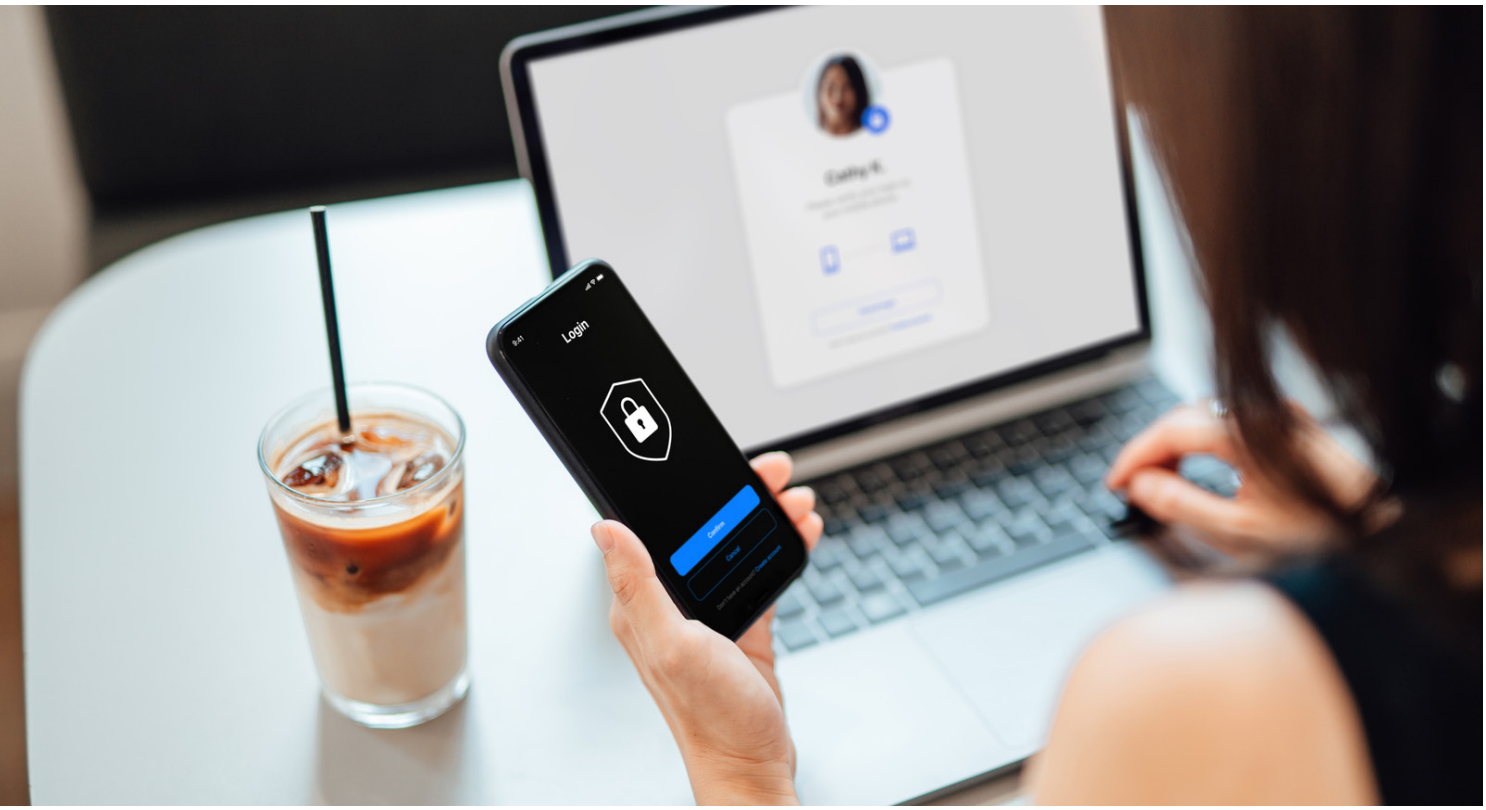


Face à la résurgence des ransomwares, les entreprises ont besoin de nouvelles stratégies pour élaborer des défenses intelligentes et accélérer leur reprise

Les experts suggèrent de plus en plus de s'intéresser plutôt à réduire les dommages qu'à assurer une détection à toute épreuve.



Les ransomwares sont de retour !

Les entreprises comme les particuliers ont bénéficié d'un peu de répit en 2022 en raison de la diminution considérable des attaques par ransomware qui a débuté fin 2021. Malheureusement, cette tendance s'est inversée depuis : les attaques par ransomware augmentent à nouveau et atteignent désormais un niveau record, en hausse de 72 % sur un an au deuxième trimestre 2023[1].

« Nous assistons à une augmentation effrénée des ransomwares cette année, et je m'attends à ce que cela se poursuive jusqu'en 2024 », déclare Chris Rogers, évangéliste technologique senior chez HPE Zerto Software.

En grande partie, cette résurgence est imputable à l'essor de l'intelligence artificielle. Le temps des messages de hameçonnage évidents, bourrés de fautes de grammaire et d'images médiocres, est bel et bien révolu. Désormais, les attaques par hameçonnage générées par l'IA sont bien plus sophistiquées et ressemblent de plus en plus à la réalité.

« Les pirates peuvent envoyer un e-mail approximatif via une IA pour lui donner l'allure d'un message authentique, sans fautes de grammaire ou d'orthographe, avec la bonne image de marque », explique Chris. « Il aura l'air de provenir d'une entreprise réputée. » Chaque e-mail sera individualisé pour chaque destinataire, ce qui le rendra encore plus difficile à détecter.

Chris ajoute que l'IA va également conduire à un nouveau type d'attaque : le deepfake de la voix. Par exemple, votre patron vous appelle et vous demande de retirer de l'argent du compte bancaire de la société ou d'acheter 100 cartes-cadeaux à offrir aux employés en guise de primes de vacances. Mais la voix n'est qu'une simulation informatique, entraînée pour imiter le modèle de locution exact de votre patron, sur la base d'un webinaire YouTube™ accessible au public auquel il a participé.

Selon Chris, il y a de quoi s'inquiéter, mais il ajoute qu'au cours des derniers mois, il a constaté un changement notable d'attitude parmi les clients, les partenaires et les prospects. « La plupart des personnes disent soit qu'elles n'ont pas été touchées par une attaque, soit que l'attaque qu'elles ont subie n'a pas été aussi grave qu'elles ne le pensaient », explique Chris. Cela signifie que beaucoup pourraient baisser leur garde prématurément.

« Les personnes pensent qu'elles s'en sortent plutôt bien en matière de cybersécurité, même si les statistiques confirment le fait que la plupart des entreprises vont être attaquées et qu'une de ces attaque finira par atteindre sa cible et faire des dégâts. »

Le message est clair : il est impératif de bien se préparer pour renforcer la sécurité.

[1] « Q2 Ransomware Report: Global Attacks At All-Time High », Corvus, 31 juillet 2023

De nouveaux conseils pour moderniser vos défenses de sécurité

Compte tenu des sombres perspectives concernant les ransomwares et autres attaques, que pouvez-vous faire pour vous préparer et vous protéger contre une future attaque ?

Chris affirme que les meilleurs conseils donnés ces dernières années continuent de s'appliquer, mais que les entreprises doivent être réalistes quant à leur capacité à détecter des attaques. « Les ransomwares sont plus difficiles que jamais à détecter », dit-il. « Le temps d'exposition tend également à diminuer. »

Le temps d'exposition est la durée pendant laquelle un attaquant peut consacrer du temps à son méfait avant que l'attaque ne soit détectée ou que la charge utile ne soit activée, causant des dommages à la victime. Selon un rapport de Cyberint, le temps médian d'exposition des ransomwares au niveau mondial était de neuf jours en 2022[2]. Il est tombé à seulement cinq jours au premier semestre 2023. En d'autres termes, les victimes disposent de moins de temps que jamais pour détecter les programmes malveillants sur leur réseau avant que des dégâts ne soient causés. « Moins vous disposez de temps, moins vous avez de chances de détecter l'attaque », ajoute Chris.

Même si les organisations continueront naturellement de s'appuyer sur des outils tiers pour détecter les attaques entrantes, Chris affirme que cette stratégie échoue finalement avec des attaques de type zero-day, qui exploitent de tout nouveaux exploits. « La plupart des entreprises se retrouvent dans une situation où elles ne savent rien de ce qui s'est passé jusqu'à ce qu'un utilisateur appelle pour leur dire qu'il ne peut plus accéder à tout un tas de fichiers », poursuit-il.

Divers outils de sécurité utilisent désormais l'IA pour les aider à détecter des attaques, mais désormais, ils sont loin d'être la panacée. « Je ne pense pas qu'il existe un produit d'IA qui puisse empêcher les personnes de cliquer sur des liens malveillants », déclare Chris. « Et je ne pense pas que les produits de cybersécurité aient rattrapé les attaquants en ce qui concerne l'utilisation de l'IA. » C'est parce qu'il n'y a aucune pénalité si un attaquant échoue. S'il n'atteint pas sa cible, il peut toujours réessayer. D'après Chris, un outil de cybersécurité basé sur l'IA devrait être presque parfait. Une promesse encore loin d'être réalisée pour cette technologie émergente.

Aujourd'hui, HPE Zerto adopte une approche plus fondamentale de la sécurité en analysant les données en temps réel et en en faisant une copie sécurisée au fur et à mesure de leur écriture sur un périphérique de stockage. « Nous sommes en retard d'environ cinq secondes par rapport au temps réel », explique Chris. « Nous sommes donc en mesure d'émettre rapidement une alerte et d'informer l'équipe de sécurité si quelque chose ne va pas dans l'environnement. » Cette approche peut limiter le rayon d'action d'une attaque et aider les analystes à identifier son origine avant qu'elle n'ait une chance de se propager à d'autres systèmes.

Des sauvegardes plus imbriquées que jamais

Le revers de la médaille de la détection est la préparation. Maintenant plus que jamais, cela signifie adopter une approche intelligente en matière de sauvegardes. L'époque où l'on déposait un lecteur de bande dans un coin de la salle des serveurs en le configurant pour qu'il fonctionne pendant la nuit est révolue depuis longtemps. Même la règle 3-2-1, reconnue depuis longtemps, avec trois copies de vos données sur deux types de supports distincts, dont une stockée hors site, ne suffit plus.

« Il suffit de manquer un correctif » pour qu'une attaque réussisse, explique Paul Lloyd, stratège en sécurité chez HPE. « Vous devez le faire correctement à chaque fois. Il leur suffit d'avoir de la chance une fois. Cela devient ennuyeux de continuer à entendre cela dans ce métier, mais le fait est que c'est inévitablement vrai. »

Les dernières directives de sauvegarde suggèrent aux entreprises de suivre une routine de sauvegarde 3-2-1-1-0 plus agressive. Les mêmes règles que le 3-2-1 continuent de s'appliquer, mais le 1 supplémentaire fait référence à une sauvegarde isolée qui est physiquement déconnectée du réseau principal. Cela la rend immunisée contre des attaques par ransomware qui pourraient se propager à partir du réseau principal.

L'isolation est aujourd'hui cruciale. « Si vous pouvez accéder à la sauvegarde depuis chez vous, cela signifie qu'un pirate informatique peut aussi le faire », explique Paul. Le nouveau 0 souligne l'importance de vérifier que ces sauvegardes soient fiables, précises et complètes, sans aucune erreur lors des tests de reprise.

[2] « Ransomware Trends Q3 2023 Report », Cyberint, 11 octobre 2023

« Les criminels veulent entrer, récupérer leur argent et passer à la cible suivante », détaille Paul. D'après la société de cybersécurité Mandiant, le délai moyen pour exploiter des vulnérabilités nouvellement découvertes est passé de 63 jours en 2018 et 2019 à 44 jours en 2020 et début 2021[3]. En 2022, le délai moyen est tombé à 32 jours.

Paul poursuit : « Les attaquants sont de plus en plus rapides et les entreprises de plus en plus lentes à installer des correctifs, ce qui les rend de plus en plus vulnérables aux attaques. Nous continuons à nous tromper sur les fondamentaux, et ces mauvaises habitudes datent de plusieurs décennies », dit-il. « Cela signifie que dans certains cas, limiter la propagation d'une attaque réussie est probablement la meilleure chose que vous puissiez faire. »

Un accent sur l'accélération et l'amélioration de la reprise

La bonne nouvelle est qu'en matière de reprise après une attaque, la situation semble plus brillante que jamais. « Nous en sommes arrivés au point où vous pouvez vous remettre d'une attaque en quelques minutes, avec seulement une seconde de perte de données », explique Chris.

L'astuce ne consiste pas à récupérer les données rapidement, mais proprement. À cet égard, il est crucial de comprendre quand une attaque a commencé. La restauration d'une sauvegarde déjà infectée ne fait qu'aggraver le problème.

La mise en œuvre de salles blanches et de coffres-forts numériques constitue un élément clé de cet effort. Autrefois réservés aux entreprises disposant de ressources confortables telles que les grandes sociétés financières ou de soins de santé, ces environnements deviennent de plus en plus accessibles au grand public à mesure que les coûts diminuent et que les systèmes soient plus conviviaux.

Une salle blanche est une zone d'infrastructure déconnectée du réseau de production, et un coffre-fort numérique est une architecture qui stocke les données dans un format immuable. En les combinant, vous obtenez un réseau fonctionnellement isolé de tout autre environnement, ce qui rend l'intrusion d'un attaquant pratiquement impossible. Avec uniquement des sauvegardes vérifiées stockées dans le coffre-fort numérique de la salle blanche, l'utilisateur est bien plus certain que tous les fichiers restaurés à partir de cet environnement ne seront pas infectés, mais plutôt sécurisés.

Une vérification efficace des sauvegardes comprend l'examen des données pendant le processus de reprise pour garantir qu'elles n'aient pas été cryptées ou autrement compromises par un programme malveillant. Cela implique également de restaurer les données et les applications individuellement, de les vérifier et de les approuver à la volée. Si un problème survient au cours de ce processus, la restauration peut être suspendue et une copie plus ancienne des données ou de l'application peut être récupérée à la place. Les plateformes de sécurité modernes comme celle de HPE Zerto peuvent effectuer tout ce travail beaucoup plus rapidement que la génération précédente d'outils de récupération. Elles permettent à la plupart des environnements de redevenir opérationnels en quelques heures au lieu de quelques semaines.

Aujourd'hui, il est presque obligatoire de disposer d'une architecture de sauvegarde et de restauration telle que celle-ci. « Si vous n'êtes pas prêt à investir dans ces domaines, vous ajoutez des risques à votre organisation », explique Chris.

Ne vous laissez pas non plus décourager par la complexité de l'environnement de sécurité moderne. Chris poursuit : « Recherchez l'expertise dont vous avez besoin et faites appel à des prestataires de services de sécurité qui peuvent vous aider à gérer ces choses à votre place ».

[3] « Analysis of Time-to-Exploit Trends: 2021-2022 », Mandiant, 28 septembre 2023

Visit HPE.com

Pour en savoir plus, rendez-vous sur

HPE.com/data

Live Chat

a50010074FRE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com