TANIUM

Points de vue de cadres dirigeants :

Pourquoi la gestion des endpoints est plus que jamais essentielle

TANIUM

Points de vue de cadres dirigeants :

Pourquoi la gestion des endpoints est plus que jamais essentielle

Les endpoints constituent le nouveau périmètre du réseau informatique. Il est essentiel de les défendre.

Les architectures cloud et le télétravail ont contribué à éclater le périmètre du réseau informatique, la ligne de défense traditionnelle pour la sécurité IT. Cette absence de frontière déterminée a modifié le travail des équipes de sécurité. Aujourd'hui, pour se protéger contre les violations de données, les ransomwares et d'autres types de cybermenaces, la protection des endpoints du réseau est plus importante que jamais.

Mais la protection des endpoints représente une tâche ardue, compte tenu de l'ampleur du travail nécessaire. Les endpoints englobent tout ; des ordinateurs portables, postes de travail, et tablettes des employés aux serveurs sur site, conteneurs et applications dans le cloud. Une solide stratégie de sécurité des endpoints requiert une stratégie plus globale et flexible que par le passé, lorsque les actifs informatiques étaient presque tous sur site et protégés par un pare-feu.

Dans cet eBook, nous abordons les plus importantes cyber menaces actuelles, leurs impacts sur les endpoints et la gestion des endpoints, et proposons quelques bonnes pratiques partagées par des responsables de la sécurité informatique.

L'évolution du paysage des menaces

Les rançongiciels et autres menaces continuent d'évoluer, échappant aux stratégies de défense auparavant efficaces.

Les rançongiciels continuent d'être une menace majeure pour les organisations de toutes tailles. En baisse pendant quelques années, les attaques de rançongiciel sont de nouveau en hausse. Elles ont augmenté de 23 % entre 2021 et 2022.

Les attaques sont non seulement plus fréquentes, mais elles sont aussi plus perturbatrices. En 2021, 26 % des attaques ont entraîné des perturbations qui ont duré une semaine ou plus. En 2022, ce chiffre a grimpé à 43 %.[1]

En moyenne, chacune de ces attaques coûte 4,54 millions USD aux organisations, en incluant le paiement de rançon et les coûts de remédiation.[2]

Aussi alarmants que soient ces chiffres, ils devraient s'aggraver. En effet, au cours de l'année passée, les attaquants ont adopté de nouveaux modèles pour extorquer de l'argent à leurs victimes.

L'idée initiale derrière le rançongiciel était de chiffrer les données des victimes et d'empêcher le déchiffrement jusqu'au paiement d'une rançon en crypto monnaie. Une meilleure segmentation du réseau et des sauvegardes sécurisées ont diminué l'efficacité de ce mode d'attaque. Les entreprises pouvaient ignorer la rançon, restaurer plus ou moins leurs données à leur état initial et continuer à opérer normalement.

Face à cette résistance, les attaquants ont modifié leur stratégie.[3] A la menace de laisser les données indéfiniment cryptées s'ajoute celle de divulguer au public les données récupérées s'agissant d'informations personnelles, de dossiers financiers, de journaux d'assistance, de code source, de dépôts de brevets et toute autre donnée sensible.

Ce second niveau d'extorsion est même plus facile à gérer pour les attaquants, parce qu'il est difficile de chiffrer de grandes quantités de données. Les

attaquants s'appuient souvent sur des sous-traitants experts en chiffrement. Malgré cette expertise, le chiffrement ne fonctionne pas toujours comme prévu. Les données ne sont pas toujours chiffrées correctement, et peuvent même se retrouver corrompues. Cette situation rend le déchiffrement impossible même avec le paiement de la rançon.

Si d'autres entreprises apprennent que le logiciel de décryptage d'un groupe de rançongiciels ne fonctionne pas, elles refuseront probablement de payer la rançon si leurs propres données sont cryptées dans le cadre d'une de ses attaques.

Toutefois, les criminels n'ont pas nécessairement besoin de s'appuyer sur le chiffrement si leur plan consiste simplement à exfiltrer les données dérobées. Aucune société ne veut que ses données internes soient divulguées au public. Ces données pourraient détériorer les relations avec les clients et les partenaires, et compliquer la gestion de perte de réputation de la marque. La fuite de données pourrait également révéler des secrets commerciaux, érodant à jamais l'avantage concurrentiel.

Les attaquants peuvent également tenter un troisième niveau d'extorsion : contacter directement les clients, les partenaires et les employés d'une organisation pour les informer que leurs données ont été secrètement copiées, et les encourager à exhorter l'entreprise à payer la rançon, afin que les données ne soient pas divulguées. Ils peuvent aussi demander aux parties prenantes d'effectuer leurs propres paiements de rançon pour protéger leurs données personnelles. Le gang criminel Clop a adopté cette stratégie en 2021, exigeant deux rançons : l'une pour le décryptage des données, et l'autre pour empêcher la publication de ces données.[4]

Avec trois niveaux d'extorsion désormais possibles, les enjeux liés aux rançongiciels sont plus élevés que jamais.

Pour se protéger contre ces nouvelles formes d'extorsion, il ne suffit pas d'avoir des sauvegardes de vos données. Vous devez protéger vos données, où qu'elles se trouvent. Cela signifie que vous devez sécuriser tous vos endpoints, où qu'ils se trouvent, afin qu'ils ne deviennent pas des passerelles pour une attaque.

Comment les rançongiciels atteignent les endpoints

Comment les rançongiciels atteignent-ils les endpoints ? Dans ses rapports de recherche récents, le cabinet d'analystes IDC a identifié les voies suivantes :

- Ouvrir une pièce jointe malveillante ou cliquer sur un lien dans un e-mail d'hameçonnage
- Tomber victime d'un exploit furtif qui mène les adversaires malveillants à accéder à un endpoint au cours d'une navigation Internet normale
- Accéder à des périphériques ou à des supports amovibles infectés par des logiciels malveillants[5]

Les vulnérabilités sont désormais l'une des principales sources de violations de données. L'application de correctifs est plus importante que jamais. Mais l'application de correctifs nécessite une visibilité sur tous les endpoints, ce qui fait défaut dans la plupart des organisations.

« Plus les criminels ont de difficultés à pirater les systèmes d'authentification, plus ils s'appuieront sur les vulnérabilités logicielles pour leurs attaques. Les vulnérabilités seront toujours présentes. C'est pourquoi vous devez les trouver et les corriger si rapidement. C'est également la raison pour laquelle vous constatez une telle augmentation des entreprises qui mettent en place des programmes de primes pour détecter les bogues. Les équipes internes et les fournisseurs de logiciels eux-mêmes savent que les enjeux n'ont jamais été aussi élevés. »

Tim Morris,
Conseiller en sécurité, Amériques
Tanium

Attaques de compromission de messagerie d'entreprise (Business email compromise, BEC)

Une autre forme d'attaque courante est la compromission des messageries professionnelles (BEC). Dans ce type d'attaque, les criminels envoient un e-mail usurpant l'identité d'un contact professionnel de confiance, tel qu'un PDG de l'entreprise, un directeur des RH ou un responsable des achats. L'e-mail, souvent écrit pour transmettre un sentiment d'urgence, demande au destinataire de payer une facture, de transférer de l'argent, d'envoyer des informations d'imposition W-2, d'envoyer des numéros de série de cartes-cadeaux ou de prendre une autre mesure qui semble légitime, même si elle est inhabituelle. Si le destinataire suit ces instructions, l'argent ou les données demandés sont effectivement envoyés aux criminels, et non au prétendu destinataire. Les fonds peuvent être subrepticement convertis en cryptomonnaies au cours de l'opération, rendant leur récupération presque impossible.

Entre juin 2016 et décembre 2021, le FBI a enregistré plus de 240 000 plaintes nationales et internationales concernant les attaques BEC, ce qui a entraîné des pertes cumulées de 43 milliards USD. Les rançongiciels peuvent faire les gros titres, mais les attaques BEC sont 64 fois plus coûteuses.[6] Et elles deviennent plus fréquentes, augmentant de 65 % entre 2019 et 2021.[7]

Les attaques BEC sont très difficiles à détecter, car les criminels sont devenus experts en usurpation d'identité de PDG et d'autres dirigeants d'entreprise. Elles peuvent recueillir beaucoup d'informations sur ces cadres et leur vie personnelle - comme leurs activités sociales, leurs familles, leur travail philanthropique et leurs calendrier des déplacements - à partir de comptes de réseaux sociaux, d'articles d'actualités et d'autres sources. Elles permettent d'inclure des informations visant à instaurer un climat de confiance avec les destinataires .

Les criminels peuvent également intercepter des fils de discussion légitimes par e-mail, puis envoyer un message qui semble être une réponse à une partie du fil de discussion. Étant donné que les autres messages du fil de discussion sont légitimes, les destinataires supposent que le message BEC est également légitime. Ils agissent ensuite sur les instructions incluses dans le message.

Avec le télé-travail, les employés sont encore plus susceptibles de succomber à ces formes d'attaque. [8]

Dans les attaques BEC, les endpoints eux-mêmes ne sont pas nécessairement compromis. Au contraire, les endpoints deviennent la base de lancement des attaques. Dans ce contexte, ils fournissent des informations contextuelles précieuses aux équipes de sécurité pour comprendre comment l'attaque a eu lieu et quelles autres menaces connexes pourraient exister.

Stratégies de gestion des endpoints

Comment les équipes de sécurité informatique doivent-elles répondre à ces menaces en constante évolution ? Voici 10 suggestions.

1

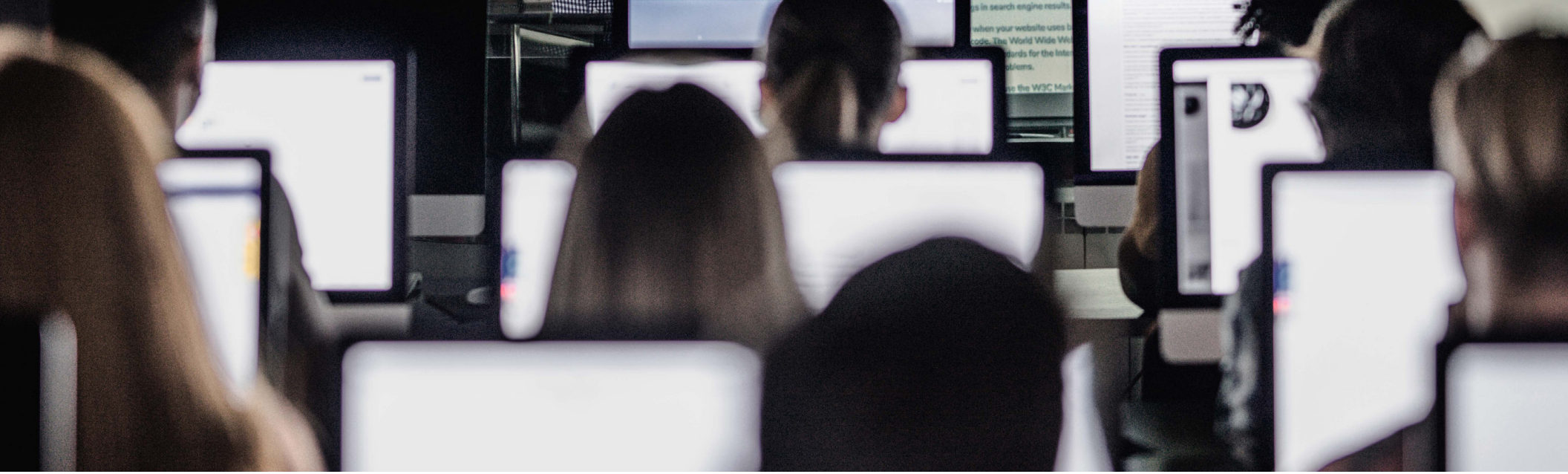
Traitez les endpoints comme la nouvelle périphérie du réseau.

Avec autant de personnes travaillant à distance et 48 % des applications exécutées dans le cloud, il est temps de reconnaître que la nouvelle ligne de défense concerne chaque endpoint, où qu'il se trouve et quel que soit le type de connexion réseau, VPN ou non, avec lequel il opère.

2

Assurez-vous d'avoir un moyen d'identifier tous les appareils connectés au réseau, même les appareils personnels qui ne sont pas officiellement autorisés.

« Vous ne pouvez pas sécuriser ce que vous ne pouvez pas gérer », déclare Tim Morris, Conseiller en sécurité pour les Amériques chez Tanium. « Vous ne pouvez pas gérer ce que vous ne connaissez pas. » Les centres d'opérations de sécurité (Security Operations Centers, SOC) doivent s'assurer qu'ils connaissent tous les endpoints dont ils sont responsables. Des audits approfondis de réseaux d'entreprises révèlent régulièrement que les systèmes de gestion des endpoints manquent environ 20 % des endpoints. Les équipes SOC doivent mettre en place des outils et des processus pour s'assurer qu'elles disposent d'un inventaire complet des endpoints et peuvent surveiller l'état de ces endpoints en temps réel.



3

Gardez à l'esprit que même si vous fournissez aux employés des équipements durcis, la plupart d'entre eux continueront également à utiliser des équipements personnels.

L'ère du BYOD n'est pas encore révolue. Lorsqu'IDC a demandé aux utilisateurs s'ils continueraient à utiliser des équipements personnels pour le travail même si leur employeur leur en fournissait, la plupart ont répondu qu'ils continueraient à utiliser occasionnellement des équipements personnels. Les stratégies de sécurité des endpoints doivent considérer que de nombreux endpoints se connectant au réseau et traitant des données sensibles seront des appareils personnels sur lesquels l'équipe de sécurité n'a qu'un contrôle partiel.

4

Appliquez des correctifs en continu.

L'application de correctifs a toujours été importante pour s'assurer que les endpoints ont accès aux dernières fonctionnalités et corrections de bogues. A présent que les vulnérabilités logicielles représentent un point d'entrée majeur pour les pirates, au même titre que le vol des identifiants d'accès pour l'exfiltration de données, il est plus important que jamais de vous assurer que les correctifs sont appliqués rapidement. Les entreprises ne peuvent pas espérer répondre aux attaques de la chaîne logistique comme Log4j sans solutions automatisées pour la gestion de bibliothèques logicielles et l'application de correctifs .

5

Obtenez une meilleure visibilité sur les composants logiciels installés sur les endpoints, afin de prévenir la prochaine attaque de la chaîne logistique.

Les attaques de la chaîne logistique tirent parti des vulnérabilités des composants logiciels qui sont largement utilisés dans les entreprises aujourd'hui, à la fois dans les applications commerciales et les applications développées en interne. Lorsque la vulnérabilité Log4j a été annoncée, les criminels n'ont pas perdu de temps à développer de nouvelles attaques pour tirer parti des faiblesses de Log4j, sachant qu'ils gardaient l'avantage tant que les entreprises luttaient à identifier les applications vulnérables et à les corriger. Pour se défendre contre de futures attaques comme celles-ci, les équipes SOC ont besoin d'une visibilité en temps réel sur tous les composants logiciels installés sur les endpoints, afin que les dangereuses failles de sécurité puissent être rapidement remédiées. Il est temps pour les équipes de sécurité d'ajouter la nomenclature logicielle (SBOM) dans les besoins standards des outils du SOC.

6

Imposez l'authentification multifacteur pour essayer d'empêcher les attaquants de tirer parti des endpoints compromis.

Les attaques d'hameçonnage continuent d'inciter les employés à divulguer leurs identifiants de connexion. Les criminels peuvent également accéder aux identifiants de connexion en piratant les serveurs de répertoires, en exfiltrant les données ou encore en les récupérant auprès de collaborateurs malveillants. Pour essayer d'empêcher les criminels de tirer parti de ces informations d'identification, il est judicieux d'appliquer l'authentification multifacteur (AMF) dans la mesure du possible, en particulier pour les systèmes et consoles back-office de gestion du réseau et autres fonctions informatiques. L'authentification multifacteur exige qu'un utilisateur utilise différents facteurs de vérification pour s'authentifier. Ces facteurs sont généralement décrits comme quelque chose que vous connaissez (par exemple, un mot de passe), quelque chose dont vous disposez (par exemple, un jeton matériel) et quelque chose que vous êtes (par exemple, un indicateur biométrique tel qu'une empreinte digitale).

7

Obtenez le contexte du endpoint.

Lorsque des attaques se produisent, il est important de réagir le plus rapidement possible. Pour répondre efficacement, les équipes de sécurité doivent comprendre ce qui se passe sur les endpoints affectés, où qu'ils se trouvent dans le monde. Quels processus sont en cours d'exécution ? Quel est le trafic réseau en cours ? Quels fichiers ont été récemment téléchargés ? Quel était l'état de conformité ? Il était plus facile d'effectuer ce type de recherche lorsque tous les endpoints étaient sur site. Désormais, les analystes peuvent nécessiter qu'un endpoint situé à des milliers de kilomètres réponde en quelques minutes. Et ils n'ont pas le temps d'installer un nouveau logiciel ou ils espèrent que l'utilisateur à distance pourra les aider à configurer une connexion. Les équipes de sécurité doivent disposer d'un système déjà en place pour analyser les endpoints et collecter ces données, de sorte que lorsqu'un type d'attaque se produit (même les attaques comme les attaques BEC), elles peuvent collecter les informations contextuelles nécessaires pour comprendre précisément ce qui s'est passé et quelles menaces restent encore actives. Assurez-vous surtout que votre organisation a la possibilité d'obtenir les informations contextuelles de tout endpoint, à tout moment et n'importe où.

« La surveillance des endpoints n'arrêtera pas une attaque BEC, mais elle pourrait vous en dire un peu plus sur la personne qui a réellement ouvert l'e-mail, puis sur ce qu'elle en a fait et où elle est allée ou sur ce qui se passait au même moment. Le contexte peut vous donner les indices dont vous avez besoin pour déterminer si cette attaque ne fait pas partie d'une campagne plus large, vouée à contacter d'autres destinataires avec des messages trompeurs. »

Tim Morris,
Conseiller en sécurité, Amériques
Tanium

8

Pensez comme un premier intervenant.

Pouvez-vous agir rapidement à la fois pour diagnostiquer les problèmes et les contenir ? Votre équipe dispose-t-elle des outils, de la formation et des processus dont elle a besoin ? Assurez-vous que votre équipe peut passer à l'action lorsque les endpoints sont attaqués de n'importe où. Les minutes comptent. Une réponse rapide peut contenir des menaces avant qu'elles ne se propagent à d'autres endpoints et sites, ce qui permet potentiellement à une organisation d'économiser des millions de dollars.

« Soyez prêt pour ne pas avoir à vous préparer. »

Tim Morris, Conseiller en sécurité, Amériques

9

Exercez-vous.

Une fois que vous avez un plan de cybersécurité, un ensemble d'outils de cybersécurité et un personnel formé, il est important de vous entraîner à détecter les menaces et à répondre aux attaques de tout type. Il est utile d'adopter une approche Équipe rouge/Équipe bleue, en mettant en place une équipe d'analystes de sécurité de confiance chargée d'infiltrer un réseau contre une équipe d'autres analystes de sécurité de confiance chargée de le défendre.[9] Quelle que soit l'organisation, ces exercices révèlent presque toujours des lacunes en matière de sécurité, soulignant le besoin de nouveaux outils ou processus. Les exercices aident également les équipes à apprendre à bâtir la confiance et à travailler ensemble plus efficacement.

10

Pensez grand.

Le nombre d'endpoints ne va qu'augmenter. Les équipes de sécurité doivent déployer des outils et des processus dès maintenant, afin de disposer de stratégies et contrôles de sécurité efficaces lorsqu'elles auront beaucoup plus de endpoints à surveiller, gérer et protéger.

Conclusion

Les cybermenaces telles que les rançongiciels augmentent, et les endpoints sont plus hétérogènes, plus nombreux et plus distribués que jamais. En suivant les stratégies décrites dans cet eBook, les équipes de sécurité peuvent réduire le risque de cyberattaques et s'assurer que lorsque des attaques se produisent, celles-ci peuvent être contenues rapidement et efficacement.

Pour en savoir plus sur la solution Converge Endpoint Management (XEM) de Tanium, rendez-vous sur www.tanium.com.

Notes de fin

1 IDC, Michael Suby, Présentation de Tanium Converge, 2022.

2 *Rapport sur le coût d'une violation de données 2022,* IBM. https://www.ibm.com/reports/data-breach

3 https://www.darkreading.com/vulnerabilities-threats/fool-me-thrice-how-to-avoid-double-and-triple-ransomware-extortion-

4 https://krebsonsécurité.com/2021/04/ransom-gangs-emailing-victim-customers-for-leverage/

5 *Enquête sur la résilience et les dépenses futures des entreprises,* mars 2022, citée par Michael Suby, VP d'IDC

6 https://www.lifars.com/bec-attacks-account-for-losses-64-times-worse-than-ransomware/

7 https://www.techrépublique.com/article/fbi-43-billion-losses-are-business-email-compromise-fraud-between-2016-2021/

8 Compromission d'e-mails professionnels : L'escroquerie de 43 milliards USD, Annonce du service public du FBI, Alerte I-050422-PSA, 4 mars 2022, https://www.ic3.gov/Media/Y2022/PSA220504

9 https://csrc.nist.gov/glossary/term/red_team_blue_team_approach