SOPHOS

Bonnes pratiques pour protéger votre réseau contre les ransomwares

Renforcez votre protection contre les ransomwares et autres attaques réseau

Un livre blanc Sophos. Octobre 2024

Les ransomwares restent une cybermenace majeure

Les ransomwares continuent de figurer parmi les cybermenaces les plus significatives, avec des conséquences de grande ampleur et souvent catastrophiques. 59 % des personnes interrogées dans le cadre de notre enquête 'L'état des ransomwares 2024' ont déclaré que leur organisation avait été victime d'un ransomware au cours de l'année précédente. Dans 70 % de ces cas, les attaquants ont chiffré des données.

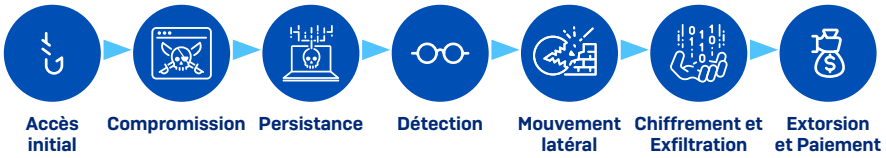
L'augmentation du nombre d'attaques au cours des dernières années reflète probablement le succès croissant du modèle de « ransomware-as-a-service » qui permet aux attaquants même les moins expérimentés de lancer des attaques.

Le coût moyen de remédiation des attaques a maintenant grimpé à 2,73 millions de dollars (une augmentation de 50 % par rapport à l'année dernière), tandis que 34 % des entreprises ont mis plus d'un mois à se rétablir. Cette période de rétablissement prolongée met en évidence la complexité croissante des attaques et la forte pression exercée sur les équipes de sécurité, 95 % d'entre elles rencontrant des difficultés pour gérer les tâches essentielles des opérations de sécurité.[1]

Ces tendances soulignent le besoin urgent de renforcer les défenses contre les ransomwares et les stratégies de rétablissement. Parallèlement à la protection Endpoint, une pile de sécurité réseau optimisée constitue l'une des défenses les plus efficaces contre les ransomwares. Ce livre blanc explore les mécanismes d'attaque des ransomwares, les stratégies de prévention et la façon dont vous pouvez optimiser votre réseau pour une sécurité maximale.

Mode opératoire des attaques de ransomware

Pour mieux nous protéger contre les attaques de ransomware, nous devons d'abord comprendre leur fonctionnement. Une attaque suit typiquement le mode opératoire suivant :



Les auteurs de ransomwares modernes utilisent souvent des outils informatiques légitimes, comme les VPN ou le protocole RDP (Remote Desktop Protocol), pour obtenir un accès initial. Le RDP a joué un rôle dans 90 % des cyberattaques investiguées par l'équipe de Réponse aux incidents de Sophos en 2023, contre 83 % l'année précédente.[2]

Or, ces outils étant utilisés par les salariés dans le cadre de leur travail, cela complique la détection initiale de ces attaques. La source du problème vient du fait qu'une confiance implicite est accordée pour utiliser ces outils : toute personne ayant accès au VPN ou au RDP est supposée être de confiance — une pratique qui s'est avérée à maintes reprises peu judicieuse.

Bonnes pratiques pour protéger votre réseau contre les ransomwares

Maintenant que nous avons fait un rapide tour d'horizon du fonctionnement des attaques de ransomware et des acteurs malveillants, voici trois bonnes pratiques pour renforcer les défenses de sécurité de votre réseau :

1. Réduire votre exposition, c'est-à-dire votre surface d'attaque

2. Inspecter et protéger le trafic réseau lorsqu'il entre dans votre réseau

3. Identifier et bloquer toutes les menaces qui parviennent à s'introduire dans le réseau

1 Remédier à la pénurie de compétences en cybersécurité dans les PME - Sophos

2 Le rapport Sophos Active Adversary du premier semestre 2024 - Sophos

Réduisez votre exposition, c'est-à-dire votre surface d'attaque

Toute infrastructure réseau exposée à l'Internet public devient par nature une cible potentielle pour les attaquants. Par conséquent, la première bonne pratique consiste à minimiser cette exposition autant que possible. Nous vous recommandons fortement de :

1. Consolider votre infrastructure réseau

La plupart des entreprises disposent d'un pare-feu protégeant leur réseau. Beaucoup disposent également d'un concentrateur VPN ou de passerelles réseau supplémentaires. Réduisez cette infrastructure autant que possible. Évoluez vers un pare-feu qui intègre l'accès à distance, pour remplacer au minimum tout concentrateur VPN que vous utilisez, mais idéalement pour passer à l'accès réseau Zero Trust (ZTNA) — vous trouverez plus d'informations à ce sujet dans la suite de ce document.

2. Corriger le firmware et le maintenir à jour

Le saviez-vous ?

Même si toutes les attaques de ransomware ont des conséquences négatives, celles qui commencent par l'exploitation de vulnérabilités non corrigées sont particulièrement agressives. Les organisations touchées par des attaques ayant commencé de cette manière ont signalé des coûts de rétablissement 4 fois plus élevés et des délais de rétablissement plus longs par rapport à celles ayant commencé avec des identifiants compromis.[3]

Les vulnérabilités non corrigées ont été la principale cause des attaques de ransomware en 2024.[4] Il est essentiel de maintenir votre pare-feu et tout autre firmware de votre infrastructure à jour. Vérifiez régulièrement (au moins une fois par mois) si des mises à jour de firmware sont disponibles et programmez leur application à des moments opportuns.

3 Vulnérabilités non corrigées : le vecteur d'attaque de ransomware le plus agressif - Sophos
4 L'état des ransomwares 2024 - Sophos

3. Veiller à ce que votre infrastructure réseau soit sécurisée dès sa conception

Veillez à ce que tous les produits d'infrastructure réseau exposés à Internet, tels que votre pare-feu, soient sécurisés dès leur conception. Optez pour un pare-feu spécialement conçu et renforcé pour résister aux attaques. Les principales caractéristiques à rechercher sont les suivantes :

- **Pas d'accès à Internet par défaut** : le pare-feu ne doit pas proposer d'accès à Internet par défaut et doit offrir des contrôles d'accès granulaires pour gérer ce qui est exposé.
- **Une conception renforcée** : elle doit intégrer des mécanismes de sécurité tels que l'authentification multifacteur (MFA) et la conteneurisation de tout service ou portail exposé, empêchant ainsi les attaquants d'exploiter les vulnérabilités potentielles.
- **Des correctifs automatisés** : dans le paysage actuel des menaces, qui évolue rapidement, les correctifs automatisés sont essentiels. Pour faire face aux menaces émergentes, le pare-feu doit être capable de recevoir des mises à jour instantanément, sans nécessiter de mises à jour majeures du firmware.
- **Une surveillance proactive** : La surveillance par l'éditeur de l'ensemble de sa base de clients déployée peut permettre d'identifier les attaques et d'y répondre beaucoup plus rapidement.

4. Minimiser l'exposition des serveurs et des applications à Internet

Si vous utilisez des outils de bureau à distance (RDP ou VNC) ou si un système de votre réseau est directement accessible via Internet pour la gestion à distance, désactivez immédiatement cet accès. Comme nous l'avons mentionné, ce type d'exposition est l'un des principaux moyens utilisés par les attaquants pour pénétrer dans les réseaux. Examinez les règles NAT de votre pare-feu et assurez-vous de ne pas exposer ce qui n'est pas absolument essentiel. Utilisez une solution ZTNA pour protéger vos serveurs et vos systèmes admin et les rendre invisibles aux attaquants tout en fournissant un accès à distance sécurisé à ceux qui en ont besoin.

5. Remplacer le VPN d'accès à distance par le ZTNA

Le modèle d'accès réseau Zero Trust, ou ZTNA (Zero Trust Network Access), remplace aujourd'hui le VPN d'accès à distance. Il élimine la confiance inhérente et l'accès large qu'offre le VPN, en utilisant plutôt les principes du Zero Trust (confiance zéro) : « ne faites confiance à rien ni personne, vérifiez tout ». Le ZTNA améliore la sécurité, facilite la gestion et procure une meilleure visibilité et une meilleure expérience utilisateur que le VPN d'accès à distance.

Il élimine les clients VPN vulnérables, s'appuie sur l'authentification multifacteur (MFA) et l'intégrité de l'appareil pour contrôler les accès. Et il ne donne accès qu'à des applications réseau spécifiques, permettant ainsi de micro-segmenter votre réseau. Recherchez un pare-feu qui intègre le ZTNA afin d'obtenir une solution de passerelle unique — gérée depuis une console unique, et idéalement avec un agent unique sur l'appareil de l'utilisateur qui combine protection Endpoint et ZTNA.

6. Utiliser des mots de passe forts et l'authentification multifacteur (MFA)

Les mots de passe faibles et l'absence d'authentification multifacteur (MFA) restent des vulnérabilités majeures, permettant la réussite d'un nombre important de cyberattaques. Assurez-vous que tous les systèmes de votre réseau, même ceux qui ne sont pas exposés vers l'extérieur, utilisent des mots de passe forts et sont protégés par une solution MFA pour empêcher les attaques par force brute.

Inspectez votre trafic réseau et protégez-le dès son entrée dans votre réseau

Autre vecteur d'attaque couramment utilisé par les adversaires : s'implanter sur votre réseau par le biais du trafic web et de messagerie quotidien qui traverse votre infrastructure. Si les outils web et de messagerie sont essentiels pour toute entreprise et ne peuvent être tout bonnement isolés, il est toutefois possible de s'assurer que ce trafic est inspecté et protégé de manière adéquate. Voici quelques bonnes pratiques recommandées pour sécuriser le trafic de votre réseau :

1. Inspecter le trafic chiffré

Plus de 90 % du trafic réseau est chiffré. C'est une bonne chose pour le respect de la confidentialité, mais c'est aussi un défi pour la sécurité, car la détection des menaces classique ne peut pas voir à l'intérieur des flux de trafic chiffrés. Les attaquants profitent de cet angle mort de la sécurité. La plupart des pare-feux peineront sous la charge supplémentaire que représente le déchiffrement et l'inspection de ces 90 % de trafic chiffré. Choisissez un pare-feu spécialement adapté au monde fortement chiffré d'aujourd'hui, qui est capable de déterminer intelligemment les flux de trafic qui nécessitent un déchiffrement et ceux qui n'en ont pas besoin. Il doit déchiffrer et inspecter efficacement le trafic sans compromettre les performances globales du réseau, tout en étant capable d'identifier les menaces chiffrées.

2. Utiliser un système de prévention des intrusions (IPS)

De nombreux systèmes de votre réseau peuvent présenter des vulnérabilités non corrigées. Il peut s'agir de systèmes Windows ou Linux, d'appareils connectés (IoT) comme des caméras, de systèmes de contrôle industriel, ou de tout ce qui se connecte à votre réseau — avec ou sans fil. Chaque pare-feu comprend une technologie permettant de détecter les attaques réseau qui tentent d'exploiter les vulnérabilités : c'est ce qu'on appelle un système de prévention des intrusions ou IPS. Malheureusement, de nombreuses organisations ne l'utilisent tout simplement pas. Assurez-vous d'utiliser un IPS sur tous les flux de trafic de votre réseau, en particulier ceux qui proviennent d'Internet, mais aussi en interne pour détecter les attaquants potentiels qui peuvent déjà se trouver sur votre réseau.

3. Utiliser une protection contre les menaces zero-day

De nombreuses attaques utilisent des logiciels malveillants incorporés dans des fichiers que des utilisateurs vont télécharger à leur insu sur le web. Ces menaces inédites sont appelées « zero-day ». Vous ne pouvez pas compter sur l'analyse antivirus traditionnelle pour détecter ce type de menaces. Vous avez besoin d'une analyse des menaces qui exploite l'IA ou le Machine Learning formés sur des millions d'échantillons afin d'identifier les menaces nouvelles et émergentes. Assurez-vous que l'inspection de votre pare-feu inclut l'analyse zero-day. Idéalement, elle devrait être effectuée en temps réel dans le Cloud pour décharger votre pare-feu de ce traitement intensif et pour bénéficier instantanément du partage mondial des renseignements sur les menaces.

4. Implémenter des mesures de sécurité robustes pour la messagerie et apprendre aux utilisateurs à repérer les emails de phishing

Nous connaissons tous quelqu'un qui a un jour cliqué sans le savoir sur un lien malveillant dans un email qui semblait légitime. Bien que cela reste un vecteur d'attaque populaire pour les cybercriminels, il existe des protections efficaces et des mesures éducatives pour lutter contre ce problème.

Recherchez une solution de sécurité des messageries capable de filtrer de manière proactive les emails malveillants des boîtes de réception des utilisateurs. Même si certains emails parviennent à passer, la solution doit permettre de les supprimer rétroactivement ou de réécrire les URL pour permettre des vérifications au moment du clic. En outre, recherchez un produit de sécurité des messageries qui inclut des fonctions permettant de tester la capacité des utilisateurs à reconnaître les attaques de phishing et qui propose une formation sur les éléments à surveiller.

Identifiez et bloquez toutes les menaces qui parviennent à s'introduire dans le réseau

Malgré tous vos efforts, il est prudent de partir du principe qu'un jour ou l'autre, un attaquant s'introduira dans votre réseau. C'est là que l'identification et le temps de réponse deviennent critiques, et pourtant, c'est là que la plupart des solutions de sécurité réseau laissent à désirer. Vous devriez rechercher des solutions qui peuvent vous aider à :

1. Segmenter votre réseau

Si un attaquant parvient à pénétrer votre réseau, l'une des choses qu'il cherchera à faire sera de se déplacer. Pour limiter tout mouvement et détecter un attaquant le plus tôt possible, il vous faudra micro-segmenter votre réseau. Assurez-vous que votre réseau est segmenté en plusieurs zones réduites ou VLAN qui sont connectés via des switchs et des points d'accès gérés, et via votre pare-feu où l'IPS inspecte ce flux de trafic. Utilisez également le ZTNA pour l'accès à distance pour micro-segmenter efficacement vos applications.

2. Identifier instantanément les adversaires à travers de multiples vecteurs

Lorsqu'un attaquant s'introduit dans votre réseau, une détection rapide est essentielle. Sachant que 91 % des attaques de ransomware se produisent en dehors des heures de bureau habituelles[5], vous avez besoin d'une solution de cybersécurité qui fonctionne 24 h/24 pour détecter les adversaires en temps réel et partager immédiatement les renseignements sur les menaces. Cette capacité doit faire plus que simplement alerter les administrateurs, elle doit permettre une communication transparente entre tous les produits de sécurité afin de garantir une réponse et un confinement rapides et coordonnés.

Optez pour une suite de solutions entièrement intégrées, comprenant des pare-feux, des solutions Endpoint, des switchs, des réseaux sans fil, le ZTNA et la sécurité des messageries. Ces outils doivent pouvoir partager des renseignements sur les menaces avec votre équipe de sécurité mais aussi entre eux, afin de mettre en œuvre des réponses automatisées pour neutraliser les attaques, même au plein milieu de la nuit.

3. S'adapter et répondre automatiquement aux menaces actives

Lorsqu'une menace est détectée — que ce soit par vous, un analyste de sécurité, vos postes, votre pare-feu ou tout autre élément de votre système de cybersécurité — vous avez besoin d'une réponse immédiate et coordonnée pour la contenir et la neutraliser. Pour y parvenir, choisissez un pare-feu (et des solutions de sécurité intégrées) capable de :

- **Répondre automatiquement aux menaces actives** sans intervention manuelle, en contenant l'attaque dès sa découverte.
- **Bloquer les menaces de manière dynamique** sans nécessiter de nouvelles règles de pare-feu ou l'intervention d'un administrateur.
- **Travailler en toute transparence avec d'autres outils de sécurité**, tels que des solutions Endpoint ou ZTNA, garantissant une défense coordonnée qui empêche les mouvements latéraux et isole la menace.

5 Par « heures de bureau normales », nous entendons de 8 h à 18 h, du lundi au vendredi | Comment stopper les adversaires actifs : les leçons tirées de la ligne de front de la cybersécurité – Sophos

Utilisez plusieurs couches de technologies de sécurité pour vous protéger contre les ransomwares

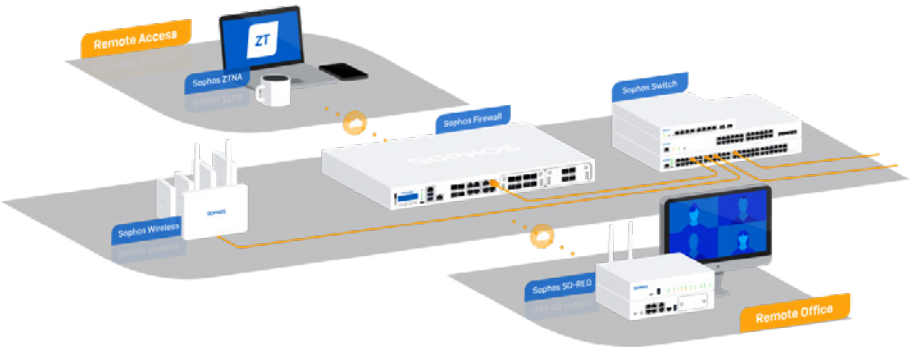
Comme dit le proverbe : «*mieux vaut prévenir que guérir*». Il est bien plus facile de stopper les problèmes à un stade précoce que de réparer les dégâts ultérieurement. La protection de votre organisation contre les ransomwares bénéficie d'une approche de sécurité informatique en couches, où plusieurs technologies travaillent ensemble pour créer une défense et une visibilité. En commençant par un pare-feu et une protection Endpoint, les organisations peuvent ajouter des couches supplémentaires en fonction de l'évolution des besoins, renforçant ainsi la protection et la visibilité au fil du temps.

Par exemple :

- **Un produit NDR (Network Detection and Response)** peut détecter les appareils non protégés et identifier les adversaires qui se déplacent latéralement dans votre réseau. La solution NDR offre une visibilité sur le trafic du réseau interne que les pare-feux ne peuvent pas voir.
- **Une plateforme XDR (Extended Detection and Response)** peut fournir des capacités de chasse aux menaces, d'investigation et de neutralisation. Elle peut également s'intégrer à vos autres solutions de sécurité informatique, offrant ainsi une visibilité sur l'ensemble des contrôles de sécurité à partir d'une plateforme unique.
- **Un service MDR (Managed Detection and Response)** fournit la chasse aux menaces 24 h/24 et 7 j/7, orchestrée par des experts spécialisés dans la détection et la réponse aux cyberattaques, que les solutions technologiques seules ne peuvent pas empêcher. Votre service MDR doit offrir une réponse complète aux incidents pour intercepter, contenir et éliminer complètement les adversaires sans coûts supplémentaires. Un service MDR doit s'intégrer à vos outils de cybersécurité existants pour une visibilité complète sur l'ensemble de votre environnement. Il offre également le plus haut niveau de protection contre les attaques de ransomware pilotées par des humains.
- **Une solution de gestion de la surface d'attaque externe (EASM) ou de gestion des vulnérabilités (VM)** peut être utilisée pour identifier et prioriser les vulnérabilités. Cela vous permet d'identifier et d'appliquer les correctifs manquants avant que les adversaires ne puissent les exploiter.

Sophos protège votre réseau contre les ransomwares

Sophos fournit tout ce dont vous avez besoin pour sécuriser votre réseau contre les ransomwares et toute autre attaque. Avec Sophos, vous bénéficiez d'une pile de cybersécurité intégrée qui comprend des solutions de pare-feu, ZTNA, switch, sans fil, RED (Remote Edge Device), une protection de la messagerie et une protection Endpoint Next-Gen pour tous vos appareils et serveurs.



Et tout est géré à partir d'une seule plateforme de gestion dans le Cloud : Sophos Central, qui rassemble les informations sur les menaces provenant de nos solutions et de nos experts, pour une réponse aux menaces automatique.

Ce niveau d'intégration et de synchronisation est unique à Sophos, vous ne le trouverez nulle part ailleurs, et c'est sans doute le composant le plus critique de toute réponse à une attaque active.

La Sécurité Synchronisée en action

Lorsqu'un hôte compromis est détecté, Sophos Firewall l'isole immédiatement tandis que vos postes sains gérés par Sophos ignorent automatiquement le trafic provenant de cet appareil. De plus, vos Switch et points d'accès abandonneront les paquets provenant de l'hôte compromis, et Sophos ZTNA empêchera tout appareil compromis de se connecter à vos appareils. Une menace active est immédiatement et automatiquement isolée sur le réseau, et n'aura nulle part où aller.

Aperçu de la sécurité réseau de Sophos

Sophos Firewall

Sophos Firewall et les appliances de la série XGS vous aident à protéger votre réseau contre les ransomwares en implémentant de bonnes pratiques dès le départ :

- **La sécurité dès la conception (*Secure by design*)** : Non seulement nous avons investi massivement pour que Sophos Firewall soit le pare-feu le plus sécurisé sur le marché, mais nous travaillons sans relâche pour en faire une cible des plus difficiles à atteindre pour les cybercriminels, tout en protégeant votre réseau et votre organisation contre les attaques futures grâce à une surveillance proactive.
- **ZNTA intégré** : Sophos Firewall comprend une passerelle ZTNA intégrée, qui vous permet d'évoluer aisément du VPN traditionnel vers le Zero Trust sans avoir à déployer quoi que ce soit de plus. En outre, la solution ZTNA est gérée depuis la même console Cloud que votre pare-feu, pour faciliter la sécurisation et la segmentation de vos applications et de vos accès à distance.
- **Protection contre les menaces zero-day optimisée par IA** : Sophos Firewall intègre des technologies d'IA avancées pour identifier les attaques de ransomwares sophistiquées et les bloquer avant qu'elles n'entrent dans votre réseau. Nous utilisons une combinaison d'IA avancée et de Machine Learning qui ont été entraînés sur des millions d'échantillons, ainsi qu'une technologie de sandboxing en temps réel pour identifier des menaces inédites.
- **Réponse active aux menaces** : Sophos Firewall peut identifier instantanément un adversaire actif sur le réseau en se basant sur diverses sources de renseignements sur les menaces et coordonner une réponse aux menaces synchronisée afin d'isoler automatiquement une menace active avant qu'elle ne devienne un véritable problème.

Sophos ZTNA

Sophos ZTNA connecte de manière transparente vos utilisateurs aux applications et aux systèmes dont ils ont besoin pour faire leur travail, tout en offrant une segmentation, une sécurité et une visibilité accrues par rapport aux VPN d'accès à distance traditionnels.

- **Micro-segmentez et sécurisez vos applications** : Sophos ZTNA fournit une micro-segmentation de pointe pour offrir un accès sécurisé aux applications — qu'elles soient hébergées sur site, dans un datacenter ou dans votre infrastructure de Cloud public — en les rendant invisibles au monde extérieur.
- **Bloquez les ransomwares et autres menaces** : Avec le ZTNA, les ransomwares et autres menaces ne peuvent plus se propager sur le réseau à partir d'un appareil utilisateur compromis. Les utilisateurs et les appareils ne disposent que d'un accès explicite, basé sur des politiques de sécurité, à des applications spécifiques. Cela élimine le problème de confiance implicite et d'accès large au réseau inhérent au VPN.
- **Bloquez l'accès aux sites web compromis** : Sophos ZTNA permet à vos travailleurs distants d'accéder de manière sécurisée et transparente aux applications et aux données dont ils ont besoin. Si l'appareil d'un utilisateur est compromis, son accès aux applications sera automatiquement coupé pour empêcher les mouvements latéraux, et ce jusqu'à ce qu'il soit nettoyé.

Sophos Switch et points d'accès sans fil

Sophos Switch et les points d'accès Sophos sont étroitement intégrés à Sophos Firewall et au reste de la plateforme de cybersécurité Sophos, offrant une réponse aux menaces automatisée et une gestion à partir d'une console unique :

- **Réponse active aux menaces** : Sophos Switch et les points d'accès Sophos prennent également en charge la réponse active aux menaces (Actice Threat Response) pour stopper net les adversaires actifs. Un appareil compromis peut être instantanément bloqué au niveau du switch ou du point d'accès pour empêcher les mouvements latéraux, même sur le même segment de LAN.
- **Console de gestion unique** : Sophos Switch et les points d'accès Sophos sont tous gérés à partir de Sophos Central, tout comme vos pare-feux, ZTNA et d'autres solutions Sophos, afin d'offrir une visibilité optimale et une gestion aisée.

Sophos Email

Sophos Email sécurise les messageries et offre une protection avancée contre le phishing pour empêcher les menaces de s'infiltrer par le biais des emails :

- **Protection anti-phishing** : Sophos Email utilise le traitement du langage naturel (NLP) optimisé par IA pour identifier les tentatives d'usurpation d'identité qui visent à tromper les utilisateurs en leur faisant croire à la légitimité d'une tentative de phishing. La solution inclut également une analyse multicouche des malwares et des URL malveillantes avec une protection au moment du clic qui réécrit les URL, forçant une vérification supplémentaire si les liens sont cliqués. Sophos Email utilise plusieurs technologies pour identifier les expéditeurs suspects en s'appuyant sur les méthodes d'authentification SPF, DKIM et DMARC, ainsi que sur l'analyse des anomalies de l'entête des emails.
- **Formation des employés avec Phish Threat** : Sophos Phish Threat permet de simuler des attaques et de former vos employés. La solution peut être extrêmement utile pour former les employés à identifier les emails suspects et les attaques de phishing, et peut être utilisée pour tester et identifier les utilisateurs qui ont besoin d'une formation supplémentaire.

Conclusion

Les ransomwares continuent d'évoluer et sont toujours aussi efficaces pour forcer les organisations touchées à payer une rançon. Votre objectif est d'empêcher les adversaires de pénétrer dans votre organisation, et de les détecter et de les éjecter rapidement s'ils y parviennent. Veillez à suivre les bonnes pratiques de sécurité réseau décrites dans le présent rapport, assurez la formation continue des utilisateurs et restez vigilant face aux menaces et aux adversaires présents dans votre environnement. Une approche multicouche de la cybersécurité, avec une détection et une réponse 24/7, donne à votre organisation les meilleures chances de se protéger contre les ransomwares et les menaces les plus récentes.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site www.sophos.fr

2024-10-14 (WP-PC)

SOPHOS