SOPHOS

LES BONNES PRATIQUES DE PARE-FEU POUR BLOQUER LES RANSOMWARES

Livre blanc Sophos Août 2020

Les bonnes pratiques de pare-feu pour bloquer les ransomwares

Les ransomwares continent d'empoisonner les entreprises, comme le montre une étude récente où plus de la moitié des entreprises interrogées ont révélé avoir été touchées par un ransomware au cours de l'année passée*.

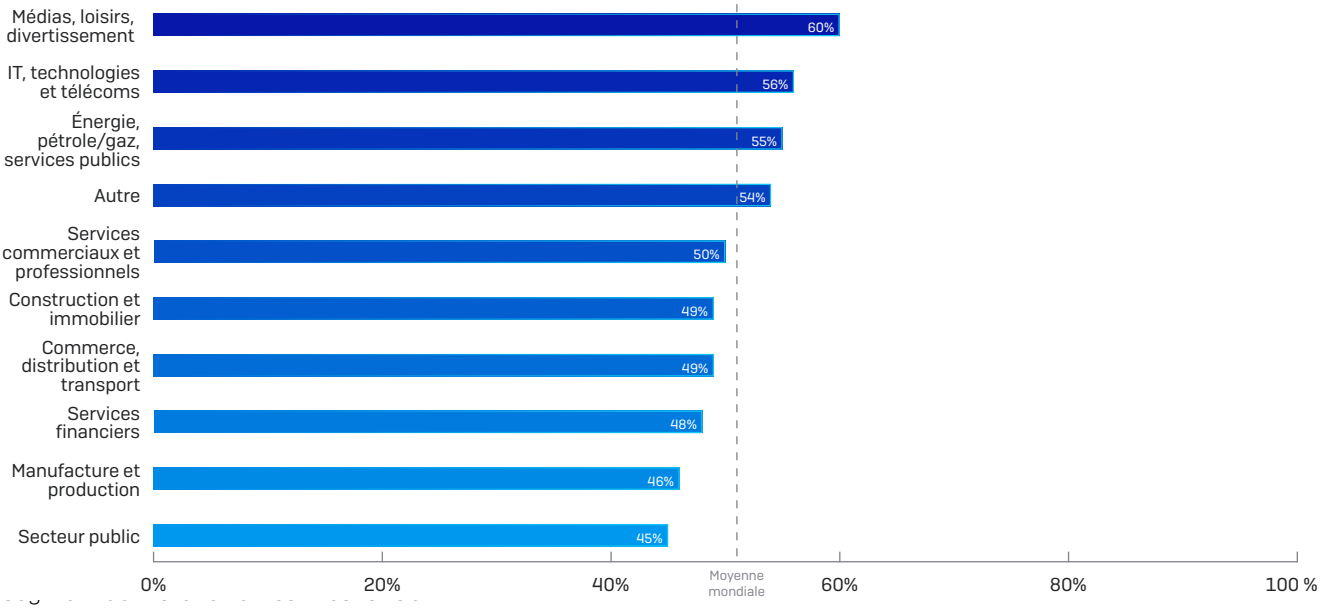
De telles attaques sont toujours plus complexes et exploitent toujours plus efficacement les vulnérabilités des réseaux et des systèmes, au grand désespoir des entreprises qui en paient les frais :

le coût moyen à l'échelle mondiale est de 680 000 € (761 100 $).

Les pare-feu modernes sont particulièrement efficaces pour bloquer ces types d'attaques, mais il faut pour cela respecter de bonnes pratiques d'utilisation. Dans ce livre blanc, nous analysons le mode opératoire de ces attaques et les moyens nécessaires pour les bloquer, et nous passons en revue les bonnes pratiques pour configurer votre pare-feu et votre réseau afin de vous doter de la meilleure protection possible.

Quelles sont les cibles des hackers

Qui les hackers ciblent-ils ? La réponse courte est : tout le monde. Dans une étude récente, 51 % des répondants ont déclaré avoir été touchés par un ransomware au cours de l'année passée, et il semble que la taille de l'entreprise ne soit pas un facteur significatif. En effet, 47 % des entreprises touchées avaient moins de 1 000 employés, tandis que 53 % en avaient plus de 1 000. Aucun pays, aucune région géographique, ni aucun



Pourcentage des entreprises touchées par un ransomware au cours de l'année passée

Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Base : 5 000 répondants.

Si vous cherchez des articles consacrés aux attaques de ransomware dans la presse, vous vous rendrez compte que des entreprises sont attaquées, avec succès, chaque jour. Et les effets sont dévastateurs : des demandes de rançon exorbitantes, des pannes et un gel des activités significatifs, des répercussions sur la réputation de l'entreprise, des fuites de données, et de plus en plus souvent, une mise aux enchères des données sensibles volées.

*L'état des ransomwares 2020 — Une enquête indépendante commandée par Sophos et menée par le cabinet Vanson Bourne auprès de 5 000 responsables informatiques dans 26 pays différents.

Comment les attaques de ransomware entrent sur le réseau

En 2020, nous avons observé une hausse des attaques de serveurs. Il s'agit d'attaques hautement ciblées et sophistiquées, qui sont plus complexes à déployer. Mais elles sont généralement beaucoup plus dangereuses, car elles chiffrent des ressources de haute valeur et peuvent paralyser les entreprises avec des demandes de rançons pouvant aller jusqu'à plusieurs millions d'euros. Heureusement, ce type d'attaques peut être évité grâce à la mise en place de bonnes pratiques de sécurité.

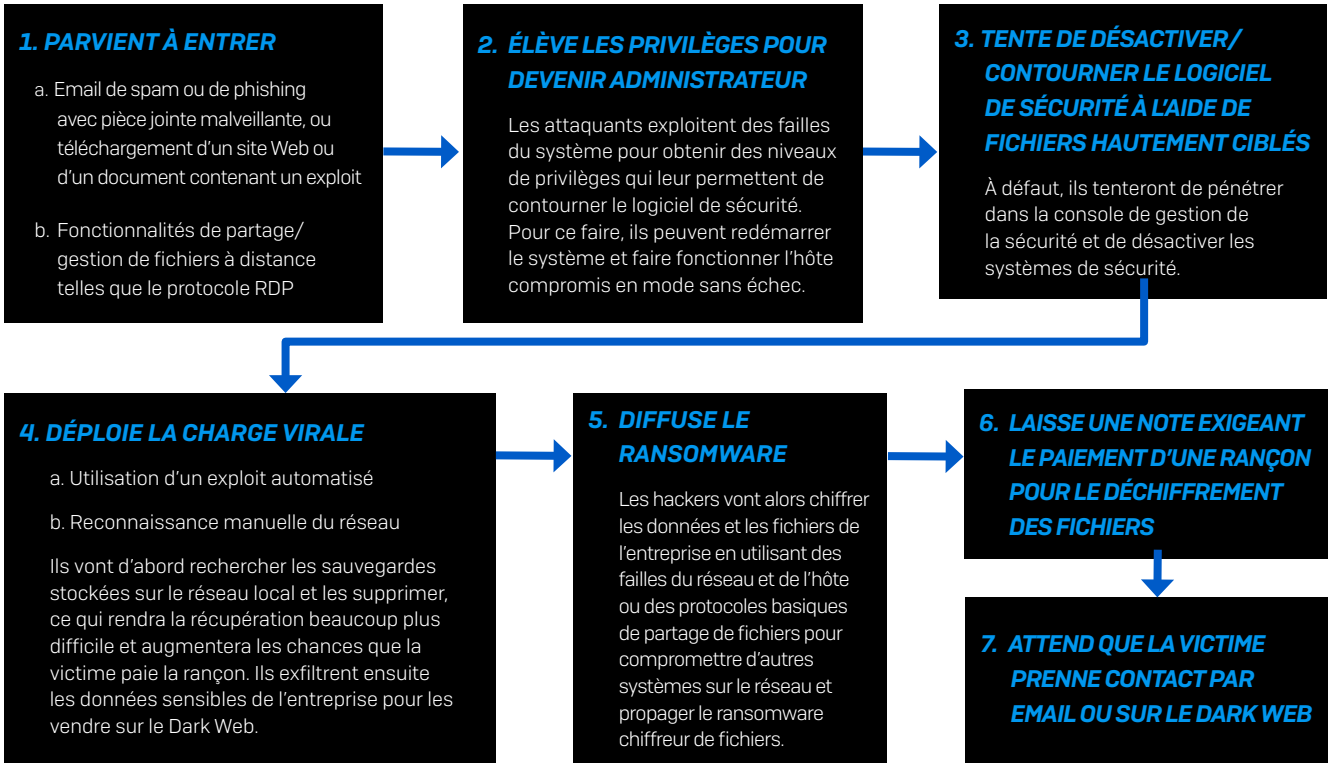
COMMENT LE RANSOMWARE EST ENTRÉ DANS L'ENTREPRISE	% D'INCIDENTS
Via un fichier téléchargé/email avec PJ malveillante	29%
Via une attaque à distance du serveur	21%
Via un email avec pièce jointe malveillante	16%
Instances de Cloud public mal configurées	9%
Via le protocole RDP (Remote Desktop Protocol)	9%
Via un prestataire avec qui nous collaborons	9%
Via une clé USB/support amovible	7%
Autre	0%
Ne sait pas	0%
Total	100 %

Comment le ransomware est-il entré dans votre entreprise ? Question posée aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée. Base : 2 538 répondants.

Toutefois, comme vous pouvez le voir dans les réponses ci-dessus issues de notre enquête, le principal point d'entrée des ransomwares est un fichier téléchargé par les utilisateurs ou envoyé dans un email de spam ou de phishing. Ne laissez pas la sécurité entre les mains de vos utilisateurs. Pour ce type d'attaques, il est préférable de protéger votre entreprise avec des technologies de pare-feu robustes.

Comment fonctionne une attaque de ransomware

Une attaque ciblée de ransomware suit ce mode opératoire :



RDP : Protocole RDP ou Protocole de déploiement de ransomware ?

Le protocole RDP (Remote Desktop Protocol) ainsi que d'autres outils de partage de bureau, comme Virtual Network Computing (VNC), sont des fonctionnalités de la plupart des systèmes d'exploitation qui sont très pratiques et inoffensives et qui permettent aux employés d'accéder et de gérer des systèmes à distance. Malheureusement, en l'absence de mesures de protection adéquates, elles constituent également des points d'entrée aisés pour les attaquants et sont couramment exploitées par les ransomwares.

Ne pas sécuriser correctement le protocole RDP et d'autres protocoles de gestion à distance similaires derrière un réseau privé virtuel (VPN), ou au moins restreindre les adresses IP qui peuvent se connecter via des outils d'accès à distance, peut vous laisser en proie à des attaques. Les attaquants utilisent souvent des outils de piratage par force brute qui vont essayer des centaines de milliers de combinaison de noms d'utilisateurs et de mots de passe jusqu'à ce qu'ils trouvent la bonne.

Comment se protéger contre les ransomwares

Pour protéger votre entreprise efficacement contre les ransomwares, vous devriez mettre en place trois grandes initiatives.

1. Renforcez votre sécurité informatique

Votre pare-feu et votre sécurité Endpoint empêchent en premier lieu les attaques d'entrer sur votre réseau, et si une attaque parvient à y pénétrer, ils peuvent l'empêcher de se propager et d'infecter les autres systèmes. Mais tous les pare-feu et les solutions de sécurité Endpoint n'y parviennent pas efficacement, c'est pourquoi vous devez vous assurer d'avoir en place un système de sécurité informatique qui réponde à ces besoins.

Pour cela, dotez-vous de :

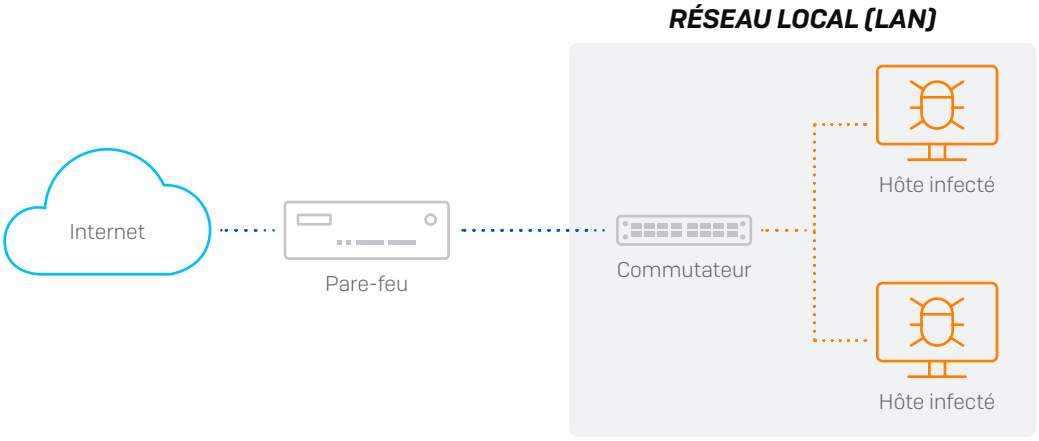
- Une technologie de sandboxing abordable pour analyser le comportement des fichiers avant qu'ils n'entrent dans votre réseau.
- La dernière technologie de Machine Learning pour identifier les nouvelles variantes zero-day de tous les fichiers traversant le pare-feu.
- Un IPS (Intrusion Prevention System) avec mise à jour des signatures en direct pour bloquer les exploits réseau.
- Un VPN d'accès à distance gratuit et facile à utiliser pour pouvoir gérer à distance votre réseau sans compromettre la sécurité.
- Une protection Endpoint avec des capacités anti-ransomware.

2. Verrouillez l'accès et la gestion à distance

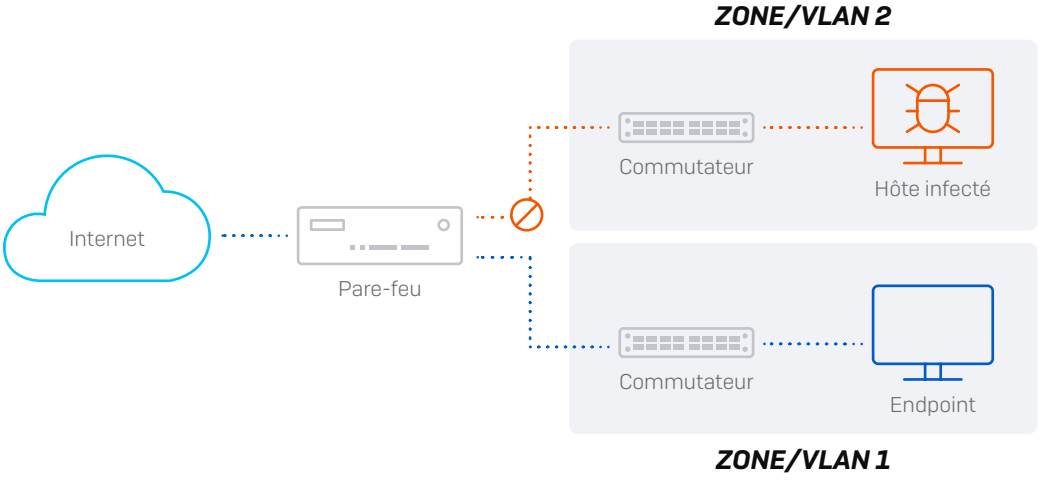
En ce qui concerne les réseaux, chaque ouverture sur le monde extérieur est une vulnérabilité potentielle qui attend d'être exploitée par une attaque de ransomware. Verrouiller le protocole RDP, les ports ouverts et les autres protocoles de gestion de votre entreprise est l'une des mesures les plus efficaces pour vous protéger contre les attaques ciblées des ransomwares. Vous pouvez y parvenir de nombreuses manières. Une méthode courante consiste à exiger que tous les utilisateurs soient sur un VPN avant de pouvoir accéder à des ressources telles que le protocole RDP et à limiter l'accès au VPN aux seules adresses IP connues. De plus, sécurisez et renforcez correctement vos serveurs, utilisez des mots de passe complexes qui sont fréquemment modifiés, et exploitez l'authentification multifacteur.

3. Segmentez votre réseau

Malheureusement, de nombreuses entreprises fonctionnent avec une topologie de réseau simple : tous leurs systèmes d'extrémité sont connectés à un seul commutateur. Cette topologie compromet la protection en facilitant les mouvements latéraux et la propagation des attaques au sein du réseau local, car le pare-feu n'a aucune visibilité ni contrôle sur le trafic traversant le commutateur.



Une bonne pratique est de segmenter le LAN en sous-réseaux plus petits, en zones ou VLAN, puis de les connecter ensemble à travers le pare-feu pour mettre en place une protection antimalware et un IPS entre les segments. Cela permet d'identifier et de bloquer les menaces tentant de se déplacer latéralement sur le réseau.



Que vous utilisiez des zones ou des VLAN dépend de votre stratégie de segmentation du réseau, mais ces deux méthodes offrent des capacités de sécurité similaires en donnant la possibilité d'appliquer une sécurité et un contrôle adéquats au mouvement du trafic entre les segments. Les zones sont idéales pour les stratégies de segmentation ou pour les réseaux moins importants dotés de commutateurs non administrés. Les VLAN sont souvent la méthode privilégiée pour segmenter les réseaux internes, car ils offrent une flexibilité et une évolutivité incomparables. Mais ils nécessitent l'utilisation (et la configuration) de commutateurs de couche 3 administrés.

Bien que la segmentation du réseau soit une bonne pratique, il n'existe pas de « meilleure » façon de procéder. Vous pouvez segmenter votre réseau par type d'utilisateurs (internes, contractuels, invités), par département (ventes, marketing, ingénierie), par service, appareil ou rôle (VoIP, Wi-Fi, IoT, ordinateurs, serveurs) ou toute autre combinaison qui vous parait logique pour l'architecture de votre réseau. En général, vous choisirez de segmenter les parties les moins fiables et les plus vulnérables du reste de votre réseau. Vous réduirez également de grands réseaux en plus petits segments afin de réduire les risques de pénétration et de propagation d'une menace.

Bonnes pratiques pour configurer le pare-feu et le réseau

- **Assurez-vous de disposer de la meilleure protection**, notamment d'un pare-feu Next-Gen moderne et performant avec IPS, inspection TLS, technologie de sandboxing zero-day et protection anti-ransomware par Machine Learning.
- **Verrouillez le protocole RDP et d'autres services** avec votre pare-feu. Ce dernier devrait être capable de restreindre l'accès aux utilisateurs du VPN et de mettre sur liste d'autorisation les adresses IP autorisées.
- **Réduisez autant que possible la surface d'attaque** en réévaluant toutes les règles de redirection de ports afin d'éliminer tous les ports ouverts inutiles. Chaque port ouvert est potentiellement une porte ouverte sur votre réseau. Pour accéder aux ressources du réseau interne depuis l'extérieur, utilisez si possible un VPN plutôt que la redirection de ports.
- **Veillez à sécuriser tous les ports ouverts** en appliquant une protection IPS adaptée aux règles gouvernant le trafic.
- **Activez l'inspection TLS** avec la prise en charge des dernières normes TLS 1.3 sur le trafic Web pour vous assurer que les menaces n'entrent pas dans votre réseau par des flux de trafic chiffrés.
- **Réduisez le risque de mouvement latéral** à l'intérieur du réseau en segmentant les LAN en plusieurs réseaux secondaires protégés individuellement par le pare-feu. Appliquez ensuite des politiques IPS adéquates aux règles gouvernant le trafic traversant ces segments LAN, afin d'éviter la propagation de vers et de bots entre segments.
- **Isolez automatiquement les systèmes infectés.** En cas d'infection, il est important que votre solution de cybersécurité soit capable d'identifier rapidement les systèmes compromis et de les isoler automatiquement jusqu'à leur nettoyage (comme le fait la Sécurité Synchronisée de Sophos).
- **Utilisez des mots de passe forts et l'authentification multifacteur** pour vos outils de gestion à distance et de partage de fichiers pour qu'ils ne puissent pas être facilement compromis par des outils de piratage par force brute.

Comment Sophos peut vous aider

Sophos offre la solution de sécurité informatique ultime pour vous protéger contre les derniers ransomwares. Non seulement vous obtenez la meilleure protection à tous les niveaux, mais vous bénéficiez également d'années d'expérience d'intégration entre pare-feu et protection Endpoint. Cela offre d'énormes avantages en matière de visibilité sur la sécurité du réseau et la capacité à répondre automatiquement aux incidents de sécurité.

Avec notre pare-feu XG primé, l'objectif est avant tout d'empêcher les attaques de pénétrer sur le réseau. Mais si un ransomware parvenait à s'y introduire, vous seriez doublement couvert. XG Firewall bloque automatiquement les ransomwares grâce à l'intégration avec Sophos Intercept X, notre plateforme de protection Endpoint leader du marché. C'est comme si vous mettiez votre réseau en pilote automatique, un extraordinaire multiplicateur de force pour votre équipe.

C'est ce que nous appelons la Sécurité Synchronisée. La Sécurité Synchronisée fusionne nos fonctionnalités de protection Endpoint et Réseau en un système de cybersécurité puissant et profondément intégré. Et le meilleur : tout cela est extrêmement aisé à administrer, comme tous vos autres produits Sophos, depuis Sophos Central, notre console de gestion dans le Cloud.

Technologies clés de Sophos et XG Firewall conçues spécifiquement pour lutter contre les ransomwares

- La technologie de sandboxing Sandstorm de XG Firewall et l'analyse par Machine Learning des fichiers entrant dans le réseau empêchent même les variantes jusqu'alors inconnues de ransomwares, d'exploits et de malwares de se propager pas par le biais d'emails de spam, de phishing ou de téléchargements sur le Web.
- Le système de prévention des intrusions (IPS) de XG Firewall détecte les exploits et les attaques de réseau les plus récents que les hackers utilisent pour trouver des failles dans vos défenses.
- Les options VPN étendues mais simples de XG Firewall permettent de combler toutes les failles de votre réseau et de ne plus dépendre des connexions RDP vulnérables, tout en offrant un accès complet à votre réseau aux utilisateurs autorisés.
- XG Firewall offre l'inspection TLS 1.3 Xstream haute performance avec des contrôles de politiques flexibles qui vous permettent de trouver le parfait équilibre entre confidentialité, protection et performances, et de vous assurer que les menaces ne pénètrent pas dans votre réseau cachées dans un flux de trafic chiffré.
- La Sécurité Synchronisée de Sophos intègre XG Firewall à notre protection Endpoint Intercept X pour répondre automatiquement aux attaques de ransomware en détectant les premiers signes de compromission, en les bloquant et en vous notifiant.
- La protection Endpoint Sophos Intercept X avec CryptoGuard peut détecter automatiquement une attaque de ransomware en cours, la bloquer et restaurer les fichiers affectés. XG Firewall inclut la technologie CryptoGuard dans l'environnement de sandboxing pour identifier les ransomwares avant qu'ils n'arrivent sur votre réseau.

Conclusion

Bien qu'ils soient déjà bien implantés dans le paysage actuel des cybermenaces, les ransomwares ne cesseront jamais d'évoluer. Nous ne parviendrons peut-être jamais à les éradiquer complètement, mais en suivant les bonnes pratiques de pare-feu décrites dans ce document, votre entreprise aura les meilleures chances de se protéger contre les derniers ransomwares et autres menaces malveillantes.

En résumé :

- Assurez-vous d'avoir la meilleure protection
- Verrouillez le protocole RDP et d'autres services avec votre pare-feu
- Réduisez autant que possible la surface d'attaque
- Sécurisez tous les ports ouverts en appliquant une protection IPS adaptée
- Appliquez l'analyse de la technologie de sandboxing et du Machine Learning aux téléchargements et aux pièces jointes
- Réduisez les risques de mouvement latéral à l'intérieur du réseau en segmentant les LAN
- Isolez automatiquement les systèmes infectés
- Utilisez des mots de passe forts et l'authentification multifacteur pour vos outils de gestion à distance et de partage de fichiers

Essayez Sophos XG Firewall gratuitement sur www.sophos.fr/xgfirewall

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

200806 WPFR (TN)

SOPHOS