SONICWALL®

TYPES DE CYBERATTAQUES ET MOYENS DE PRÉVENTION

Actuellement, les cybercriminels utilisent plusieurs techniques complexes pour infiltrer discrètement les réseaux d'entreprise sans être détectés, et voler la propriété intellectuelle ou s'emparer de fichiers contre une rançon. Pour éviter toute détection, ils chiffrent souvent leurs menaces.

Une fois que leur cible est atteinte, les pirates tentent de télécharger et d'installer des logiciels malveillants sur le système compromis. Dans la plupart des cas, les logiciels malveillants utilisés sont des nouvelles versions évoluées que les solutions antivirus classiques ne sont pas encore en mesure d'identifier.

Cet e-book présente les stratégies et les outils utilisés par les cybercriminels pour infiltrer votre réseau ainsi que les moyens de les stopper.

Les cybercriminels travaillent 24h/24, 7j/7 pour exploiter vos faiblesses.

Stratégie de cyberattaque n°1

Bombarder les réseaux de logiciels malveillants, sans interruption

Les attaques sont véhiculées par tous les vecteurs : messagerie, appareils mobiles, trafic Web mais aussi exploits automatisés. Et peu importe la taille de votre entreprise : pour les pirates, vous êtes une adresse IP, une adresse e-mail ou un prospect susceptibles d'être une cible intéressante. Jour et nuit, les agresseurs utilisent des outils automatisés pour exécuter les exploits ou pour lancer des messages de phishing.

Pour de nombreuses entreprises, le problème réside dans le fait qu'elles ne possèdent pas les outils appropriés pour réagir. Des outils automatisés leur permettraient de nettoyer le trafic, de protéger les terminaux et de filtrer les e-mails indésirables. Certaines utilisent des pare-feux incapables de détecter les menaces dissimulées dans le trafic chiffré ou font confiance à une mémoire système intégrée limitée pour stocker les signatures des programmes malveillants.

SONICWALL®

Contre-attaque n°1

Protéger votre réseau, chaque jour et chaque minute

Avec des centaines de nouvelles variantes de logiciels malveillants développées toutes les heures, les entreprises ont besoin d'une protection à jour et en temps réel contre les menaces les plus récentes. Une solution de sécurité efficace doit être mise à jour en continu, 24h/24, 7j/7. En outre, la mémoire disponible sur les pare-feux est insuffisante pour prendre en charge le nombre considérable de types et de variantes de logiciels malveillants.

Pour être efficaces, les pare-feux doivent utiliser une sandbox réseau et le cloud afin d'offrir une visibilité étendue sur les menaces, de détecter les variantes les plus récentes et d'améliorer leur identification. Par ailleurs, veillez à ce que votre solution de sécurité propose également une protection avec mise à jour dynamique au niveau de la passerelle du pare-feu mais aussi au niveau des terminaux mobiles et distants, sans oublier votre messagerie.

Optez pour une plate-forme de sécurité qui tire parti de la puissance du cloud et fournit une protection en temps réel contre les menaces les plus récentes.

Stratégie de cyberattaque n°2

Infecter les réseaux avec différents types de programmes malveillants

Les cybercriminels utilisent différents types de vecteurs d'attaque et de programmes malveillants pour compromettre les réseaux. Les cinq types de menaces les plus répandus sont les virus, les vers, les chevaux de Troie, les logiciels espions et les ransomewares.

Les virus informatiques se répandaient à l'origine par le partage de disquettes infectées. Avec l'évolution de la technologie, les modes de transmission se sont perfectionnés. Aujourd'hui, les virus sont généralement transmis via le partage de fichiers, les téléchargements Web et les pièces jointes des courriers électroniques.

Les vers informatiques existent depuis la fin des années 1980, mais ont peu été utilisés, jusqu'à ce que les infrastructures réseau soient largement adoptées par les entreprises. Contrairement aux virus, les vers peuvent infiltrer les réseaux sans aucune interaction humaine.

Les chevaux de Troie sont spécialement conçus pour extraire des données confidentielles d'un réseau. Plusieurs types de chevaux de Troie prennent le contrôle d'un système infecté, créant ainsi une brèche que les pirates utilisent ensuite pour accéder au système. Les chevaux de Troie sont souvent utilisés pour créer des botnets.

Les logiciels espions ne sont pas fondamentalement malveillants, mais constituent une nuisance de taille, car ils infectent souvent les navigateurs Web et les empêchent de fonctionner normalement. Ils ont parfois été présentés comme des applications autorisées offrant des avantages aux utilisateurs, alors qu'en réalité ils consignaient secrètement des informations sur leur comportement et leurs habitudes d'utilisation.

Les ransomwares attaquent via le chiffrement des fichiers au niveau d'un terminal ou d'un serveur et demandent à l'utilisateur final, s'il veut recevoir la clé de chiffrement, de payer une rançon sous la forme de bitcoins. Lorsque l'attaque vise des systèmes vitaux, le coût de la rançon peut s'élever à des centaines de milliers de dollars.

Les cybercriminels utilisent plusieurs types de programmes malveillants pour vous prendre au dépourvu.

Contre-attaque n°2

Veiller à protéger votre réseau contre tous types de programmes malveillants

Tous les pare-feux doivent protéger les entreprises contre les virus, vers, chevaux de Troie, logiciels espions et ransomewares. Le meilleur moyen d'y parvenir est d'adopter une approche à faible latence et en un seul passage, qui intègre toutes ces protections, et qui bloque les vecteurs d'attaque au niveau de la passerelle ainsi qu'au niveau des terminaux, au-delà du périmètre habituel. Privilégiez les fonctionnalités suivantes :

- **Protection contre les programmes malveillants** basée sur le réseau empêchant les pirates de télécharger ou de répandre ces logiciels sur un système compromis.
- **Mises à jour continues et immédiates** permettant de protéger les réseaux 24h/24, 7j/7, contre des millions de nouvelles variantes de programmes malveillants, dès qu'elles sont identifiées.
- **Service de prévention des intrusions (IPS)** empêchant les pirates d'exploiter les vulnérabilités d'un réseau.
- **Sandboxing réseau** envoyant le code suspect à un environnement cloud isolé afin de le déclencher et de l'analyser pour identifier les programmes malveillants d'un type entièrement nouveau.
- **Sécurité des accès** appliquant des contre-mesures de protection au niveau des terminaux mobiles et distants, à l'intérieur et à l'extérieur du périmètre réseau.
- **Sécurisation de messagerie** bloquant attaques par phishing, spam, chevaux de Troie et ingénierie sociale transmises par le biais des e-mails.

En veillant à ce que chaque appareil qui accède à votre réseau dispose d'un logiciel antivirus à jour, vous renforcez votre protection contre les programmes malveillants. Les entreprises peuvent éliminer la plupart des outils utilisés par les pirates pour compromettre un réseau en associant un antivirus exécuté par un ordinateur à des pare-feux réseau.

Anticipez les menaces avec une protection multi-couche contre les programmes malveillants.

Stratégie de cyberattaque n°3

Identifier et compromettre les réseaux les plus vulnérables

Nombreux sont les distributeurs de pare-feux qui prétendent assurer une protection haut de gamme, mais bien peu parviennent à prouver l'efficacité de leurs solutions. Les entreprises qui utilisent des pare-feux moins avancés pensent que leurs réseaux sont protégés. Et ce, même si des cybercriminels expérimentés sont capables d'infiltrer des réseaux en contournant le système de prévention des intrusions à l'aide d'algorithmes complexes qui leur permettent de compromettre le système en échappant à toute détection.

Comme certains pare-feux privilégient la protection aux dépens des performances, les entreprises qui les utilisent peuvent être tentées de suspendre ou de réduire leurs mesures de sécurité afin d'assurer des performances réseau élevées. Cette pratique extrêmement risquée est à proscrire.

Le facteur humain constitue un autre maillon faible de la sécurité réseau. Les agresseurs utilisent le phishing pour obtenir des informations d'identification et d'autorisation qui leur permettent tout simplement de se soustraire aux protections des pare-feux et de lancer des attaques depuis l'intérieur. Il arrive également que les employés perdent leur appareil mobile ou l'expose à une brèche lorsqu'ils l'utilisent en dehors du périmètre de sécurité du pare-feu.

Les cybercriminels ciblent souvent leurs victimes en fonction des faiblesses de leur réseau.

Contre-attaque n°3

Choisir une plate-forme de sécurité complète qui fournit à la fois une protection avancée contre les menaces et des performances élevées

Optez pour des solutions de sécurité testées par le groupe indépendant ICSA Labs et certifiées pour offrir une protection contre les programmes malveillants basée sur le réseau.

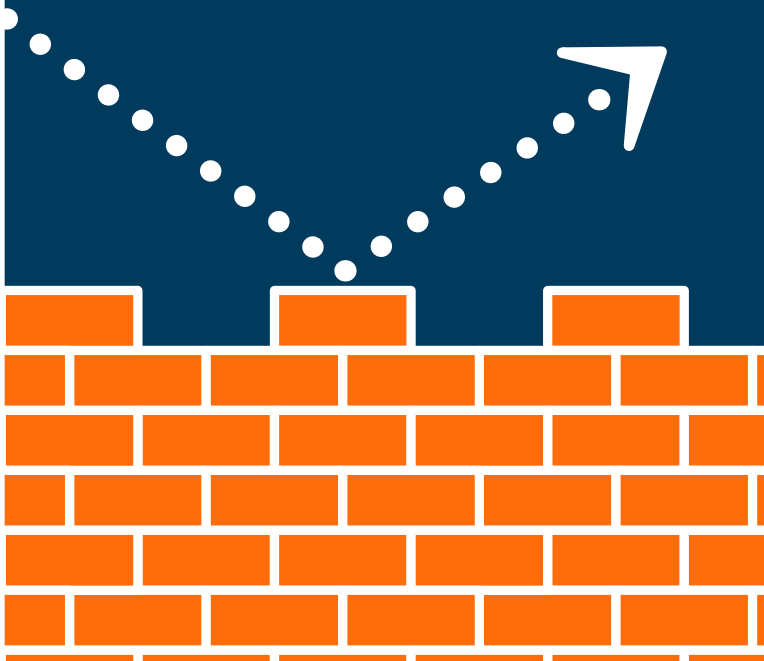
Privilégiez une plate-forme multi-cœur capable d'analyser des fichiers de toute taille et de tout type pour répondre à l'évolution des flux du trafic. Tous les pare-feux ont besoin d'un moteur pouvant protéger les réseaux contre les attaques internes et externes, sans affecter les performances.

Choisissez un pare-feu qui offre une sandbox réseau permettant de détecter les programmes malveillants les plus récents susceptibles de cibler votre environnement. Cela pet faire la différence entre un jour de travail sans problème et une journée lors de laquelle vos fichiers sont retenus en otage.

Votre stratégie de sécurité doit inclure une protection des terminaux mobiles et distants, à l'intérieur comme à l'extérieur du périmètre.

Elle doit aussi protéger la messagerie du phishing, des spams, des virus, de l'ingénierie sociale et des autres menaces transmises via e-mail.

Tous les pare-feux ont besoin d'un moteur pouvant protéger les réseaux contre les attaques internes et externes, sans affecter les performances.



De nouvelles menaces émergent toutes les heures sur tous les continents.

Stratégie de cyberattaque n°4

Changer constamment et attaquer globalement

La réussite de nombreux cybercriminels repose sur leur capacité à réinventer continuellement les programmes malveillants et à les partager avec leurs pairs dans le monde entier. De fait, de nouvelles menaces émergent toutes les heures sur tous les continents. La plupart des pirates emploient une approche semblable à celle des cambrioleurs : ils s'infiltrent, prennent tout ce qu'ils peuvent et sortent avant que quelqu'un ne déclenche l'alarme. Puis ils reproduisent cette attaque sur un autre système.

D'autres avancent lentement mais sûrement en espérant accéder à davantage de données sur une plus longue période. Certains attaques s'infiltrent via le Web, d'autres via les e-mails ou le réseau d'appareils infectés pendant leur itinérance hors du périmètre de sécurité.

SONICWALL®

Contre-attaque n°4

Choisir un pare-feu qui protège votre réseau des menaces mondiales

Pour assurer une protection efficace, il convient de réagir rapidement aux menaces. Pour déployer plus rapidement des contre-mesures sur votre pare-feu et faire face aux menaces émergentes, faites appel à un fournisseur de solutions de sécurité qui dispose d'une équipe interne et réactive d'experts en systèmes de protection. Cette équipe doit en outre collaborer avec la vaste communauté de spécialistes en sécurité afin d'étendre son rayon d'action.

Une solution à large spectre utilise un catalogue complet, basé sur le cloud, qui répertorie les programmes malveillants à l'échelle mondiale et permet d'améliorer l'analyse du pare-feu local.

Enfin, tandis qu'un simple pare-feu peut identifier et bloquer des menaces d'après leur provenance, un pare-feu sophistiqué intègre des fonctions de filtrage des botnets afin de réduire toute exposition aux menaces mondiales connues. Pour ce faire, le pare-feu bloque le trafic issu de domaines dangereux ou les connexions établies à partir d'un endroit spécifique ou vers celui-ci.

Pour contrer les menaces mondiales les plus récentes, investissez dans une solution de sécurité à portée internationale.

Conclusion

Les cyberattaques sont en pleine expansion, mais il existe des moyens de défense efficaces. Si vous souhaitez en savoir plus et évaluer les solutions de contre-attaque adaptées à votre environnement réseau, téléchargez notre livre blanc Achieving Deeper Network Security (Renforcer la sécurité réseau).

About Us

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

© 2017 SonicWall Inc. TOUS DROITS RÉSERVÉS.

SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives.

Les informations contenues dans ce document sont fournies en relation avec les produits SonicWall et/ou ses filiales. Aucune licence, expresse ou implicite, par préclusion ou un autre moyen, quant à un quelconque droit de propriété intellectuelle n'est accordée par le présent document ou en lien avec la vente de produits SonicWall. SAUF DISPOSITION CONTRAIRE DANS LES CONDITIONS DU CONTRAT DE LICENCE, LA SOCIÉTÉ SONICWALL ET/OU SES FILIALES DÉCLINENT TOUTE RESPONSABILITÉ QUELLE QU'ELLE SOIT ET REJETTENT TOUTE GARANTIE EXPRESSE, IMPLICITE OU STATUTAIRE CONCERNANT SES PRODUITS, Y COMPRIS ET SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE NON-CONTREFAÇON. EN AUCUN CAS, SONICWALL ET/OU SES FILIALES NE SERONT RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, PUNITIFS, SPÉCIAUX OU FORTUITS (Y COMPRIS, SANS LIMITATION, LES DOMMAGES POUR PERTE DE PROFITS, INTERRUPTION DE L'ACTIVITÉ OU PERTE D'INFORMATIONS) PROVENANT DE L'UTILISATION OU L'IMPOSSIBILITÉ D'UTILISER CE DOCUMENT, MÊME SI SONICWALL ET/OU SES FILIALES ONT ÉTÉ INFORMÉES DE L'ÉVENTUALITÉ DE TELS DOMMAGES. SonicWall et/ou ses filiales ne font aucune déclaration ou ne donnent aucune garantie en ce qui concerne l'exactitude ou l'exhaustivité du contenu de ce document et se réservent le droit d'effectuer des changements quant aux spécifications et descriptions des produits à tout moment sans préavis. SonicWall Inc. et/ou ses filiales ne s'engagent en aucune mesure à mettre à jour les informations contenues dans le présent document.

© 2017 SonicWall, Inc. TOUS DROITS RÉSERVÉS. SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives.

Ebook-TypesOfCyberAttacks-EU-IMAG-24644

SONICWALL®