SONICWALL

PRÉSENTATION : POURQUOI LES MENACES SOPHISTIQUÉES NÉCESSITENT UNE SÉCURISATION DE MESSAGERIE ÉVOLUÉE

Les ransomwares et autres menaces inconnues font de la sécurisation de messagerie un enjeu plus important que jamais.

Résumé

Dans le monde actuel, hyperconnecté, les communications par courrier électronique ne jouent pas un rôle banal. Elles sont devenues un facteur d'efficacité fondamental dans l'activité des entreprises. Selon les prévisions, le volume total d'e-mails envoyés chaque jour dans le monde devrait augmenter d'au moins 5 % par an. Étant donné leur nature omniprésente, les e-mails constituent un vecteur stratégique que l'entreprise doit protéger.

L'utilisation des e-mails toujours en hausse

Malgré la multiplication des médias textuels et sociaux, les communications par courrier électronique continuent de croître à un rythme soutenu. Selon une récente étude réalisée par The Radicati Group, le volume total d'e-mails envoyés et reçus chaque jour dans le monde a atteint les 205 milliards et ce chiffre devrait augmenter d'au moins 5 % par an.[1] Un fait qui n'est pas inconnu des pirates informatiques, toujours en quête de failles dans les entreprises.

1 The Radicati Group, Inc., Email Statistics Report, 2015-2019

Anatomie d'une attaque par e-mail :

- Un directeur financier reçoit un message du PDG l'autorisant à procéder en urgence à un transfert de fonds. L'e-mail provient en fait d'un cybercriminel.
- Un employé doté de droits administratifs relatifs à des systèmes clés reçoit un message urgent du service informatique lui demandant d'actualiser son mot de passe réseau. Résultat : il dévoile son mot de passe à un pirate.
- Un employé reçoit un message lui demandant de lire une pièce jointe importante sur un fournisseur de prestations. En ouvrant la pièce jointe, il active à son insu un cheval de Troie.

Les menaces électroniques qui touchent les entreprises

Les hackers utilisent les e-mails pour véhiculer diverses vulnérabilités, dont voici les plus courantes :

- **Ransomwares :** c'est une forme particulièrement néfaste de logiciel malveillant. Une fois la pièce jointe activée, le code s'embarque sur le réseau où il chiffre ou bloque les fichiers et systèmes vitaux. Les hackers forcent alors l'organisation à payer une rançon pour déchiffrer ou débloquer les fichiers ou systèmes. Les e-mails représentent un support privilégié pour la diffusion des ransomewares via des pièces jointes infectées ou des URL malveillantes.
- **Spear phishing/whaling :** cette variante de phishing vise des individus importants, responsables informatiques/réseau ou cadres dirigeants, en leur envoyant des messages semblant venir d'une source de confiance, en vue d'accéder aux systèmes et données internes. Plus de 90 % des cyberattaques commencent par une campagne de phishing réussie.
- **Business Email Compromise/arnaque au président/e-mail d'imposteur :** au cours des quelques dernières années, les fraudes BEC (Business Email Compromise) ont causé au moins 5,3 milliards de pertes pour environ 22 000 entreprises du monde entier, si l'on en croit les derniers chiffres du FBI[2]. Le FBI définit ce type de fraude comme une arnaque sophistiquée ciblant des entreprises qui travaillent avec des partenaires étrangers qui effectuent régulièrement des virements.
- **Phishing :** tactique courante consistant à envoyer des e-mails intégrant des liens pour pirater des sites. Lorsque les utilisateurs crédules se rendent sur ces sites, ils doivent saisir leurs identifiants, qui serviront dès lors à voler des identités, compromettre des données ou accéder à d'autres systèmes vitaux.
- **Logiciels malveillants :** le courrier électronique est l'un des mécanismes de choix pour distribuer des logiciels malveillants, connus ou inconnus, généralement intégrés aux pièces jointes, dans l'espoir que celles-ci soient ouvertes ou téléchargées sur un ordinateur ou un réseau, permettant ainsi d'accéder aux ressources, de voler des données ou de paralyser des systèmes.
- **Spam :** des messageries sont utilisées pour envoyer du spam ou des messages non sollicités, susceptibles d'engorger les boîtes de réception et les ressources du réseau, de diminuer la productivité et d'accroître les coûts d'exploitation.
- **Détournement de messages sortants :** les entreprises sont soumises à des règles internes et à des réglementations gouvernementales, qui les tiennent responsables des e-mails sortants et de garantir la protection des identifiants de leurs clients. Les attaques de zombies et le détournement d'adresse IP peuvent propager les identifiants de clients et ruiner la réputation d'une entreprise.

Conclusion

Aujourd'hui, les e-mails sont un moyen de communication essentiel dans les entreprises. Les pirates le savent parfaitement. Face aux attaques sophistiquées et ciblées modernes, il est primordial que les organisations déploient une solution de sécurité multicouche, incluant une protection de messagerie avancée et dédiée. Pour combattre efficacement les menaces émergentes, il est fortement recommandé de mettre en place une solution de sécurisation de messagerie de nouvelle génération assurant la prévention des brèches en temps réel.

Pour en savoir plus sur les moyens de protéger la messagerie de votre organisation, lisez notre dossier « Ce dont votre sécurisation de messagerie nouvelle génération a besoin pour contrer les menaces sophistiquées ».

1 www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2 www.ic3.gov/media/2016/160614.aspx

À propos de nous

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.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com