SOPHOS
Security made simple.

Checklist anti-ransomware

Technologies clés et bonnes pratiques de sécurité

Les attaques de ransomwares ont deux points de départs principaux : un email piégé avec pièce jointe malveillante ou un site web compromis. De là, les ransomwares vont s'installer sur vos systèmes d'extrémité et vos serveurs. Pour être en mesure de les bloquer, il est indispensable d'avoir installé des technologies de protection avancées capables d'agir à chaque stade de l'attaque, mais également de mettre en place de bonnes pratiques de sécurité.

Sécuriser vos systèmes et vos serveurs

Si un ransomware parvient à s'infiltrer dans vos systèmes et vos serveurs, il est vital que vous le bloquiez et le supprimiez le plus rapidement possible. Dotez-vous des technologies suivantes :

☐ CryptoGuard (Sophos Intercept X)

Il sécurise vos systèmes d'extrémité et vos serveurs grâce à sa technologie unique qui stoppe les ransomwares dans leur élan. Il complète votre solution de sécurité traditionnelle en place, en bloquant les processus tentant de modifier vos données sans autorisation.

- Efficace contre CryptoLocker, Locky, Zepto, Cerber etc.
- Protège contre le chiffrement local ou à distance.
- Restaure automatiquement les modifications, sans aucune perte de données.

☐ Prévention des exploits (Sophos Intercept X)

Bloque les ransomwares exploitant les failles présentes dans d'autres logiciels.

☐ Analyse HIPS du comportement / des fichiers

Examine les composants et la structure des fichiers à la recherche d'éléments malveillants et vérifie s'ils contiennent du code tentant de modifier le registre.

☐ Sécurité du Web

Analyse le contenu web pour détecter tout code associé à un ransomware.

☐ Détection du trafic malveillant (MTD)

Détecte et bloque le trafic vers les serveurs de Commande et de Contrôle du ransomware.

☐ Contrôle des applications

Restreint ce que les applications peuvent exécuter et peut bloquer Wscript (souvent utilisé par les ransomwares).

☐ Listes blanches d'applications

Établit une politique de « blocage par défaut » sur les serveurs pour que seules les applications fiables puissent s'exécuter, empêchant les ransomwares de s'implanter.

Stopper les menaces diffusées par email

Une **passerelle de messagerie** est votre première ligne de défense contre les emails piégés. Assurez-vous qu'elle inclut :

☐ Technologie anti-spam/antivirus

Bloque les emails contenant un ransomware, notamment les pièces jointes avec macros, et stoppe les autres menaces diffusées par email.

☐ Protection Time-of-Click

Empêche les utilisateurs de cliquer sur des liens renvoyant vers des sites web hébergeant des ransomwares, même si le lien était sûr au moment de son arrivée dans la boîte de réception.

☐ Sandboxing dans le Cloud

Détecte les menaces zero-day, dont les ransomwares, en testant les fichiers dans un environnement sécurisé avant que l'utilisateur ne les exécute.

Stopper les menaces Web

Une **passerelle Web** bloque les ransomwares issus du web avant qu'ils n'atteignent les systèmes de vos utilisateurs. Recherchez les technologies suivantes :

☐ Filtrage des URL

Bloque les sites web hébergeant des ransomwares et empêche les ransomwares de communiquer avec leurs serveurs Commande et Contrôle.

☐ Filtrage du Web

Applique des contrôles stricts sur les types de fichiers apparentés aux ransomwares, empêchant leur téléchargement.

☐ Sandboxing dans le Cloud

Détecte les menaces zero-day, dont les ransomwares, en testant les fichiers dans un environnement sécurisé avant que l'utilisateur ne les exécute.

Neuf bonnes pratiques de sécurité à appliquer maintenant

De bonnes pratiques de sécurité informatique sont indispensables dans toute stratégie de sécurité. Suivez ces neuf bonnes pratiques :

☐ Sauvegardez régulièrement et conservez une copie récente hors ligne et hors site

Les ransomwares ne peuvent pas atteindre ce qui est hors ligne et hors site. Avec des sauvegardes récentes, les pertes de données peuvent être réduites.

☐ Affichez l'extension des fichiers

Afficher les extensions permet de détecter plus facilement les types de fichiers que vous et vos utilisateurs n'avez pas l'habitude de recevoir (tels que le JavaScript).

☐ Ouvrez les fichiers JavaScript (.JS) dans Notepad

Ouvrir un fichier JavaScript dans Notepad l'empêche d'exécuter un script malveillant et vous permet d'examiner son contenu.

☐ N'activez pas les macros des pièces jointes reçues par email

Une des techniques majeures des infections consiste à vous persuader d'activer les macros, alors ne le faites pas !

☐ Soyez prudent avec les pièces jointes non sollicitées

Si vous avez un doute, ne l'ouvrez pas ! Si possible, renseignez-vous auprès de l'expéditeur.

☐ N'ayez pas plus de privilèges que nécessaire

Avec des droits d'administrateur, une infection localisée peut vite se transformer en une catastrophe sur le réseau.

☐ Envisagez d'installer les visionneuses Microsoft Office

Ces applications vous permettent de voir à quoi ressemblent les documents sans avoir à les ouvrir dans Word ou Excel.

☐ Mettez à jour les correctifs régulièrement et souvent

Plus tôt vous installerez les correctifs, moins les ransomwares auront de vulnérabilités à exploiter.

☐ Restez informé des dernières fonctionnalités de sécurité de vos applications professionnelles

Par exemple, Office 2016 inclut désormais un contrôle appelé « Bloquer l'exécution des macros dans les fichiers Office provenant d'Internet ».

Protégez-vous avec Sophos

Sophos Intercept X est doté de la technologie CryptoGuard, qui stoppe les ransomwares avant qu'ils ne chiffrent vos fichiers. Vous pouvez également les bloquer avant qu'ils n'atteignent vos systèmes d'extrémité en utilisant des technologies anti-ransomware au niveau de votre passerelle de messagerie, de votre passerelle web, de votre pare-feu et de vos serveurs. Ensemble, elles vous offrent la meilleure défense pour empêcher un ransomware de prendre vos données - et votre entreprise - en otage.

Comment se protéger contre les ransomwares ?

Découvrez-le sur sophos.fr/ransomware

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

08/09/2016 CL-FR (RP)