SOPHOS
Security made simple.

Comment bien se protéger contre les ransomwares ?

Ce document explique comment réagir rapidement et efficacement aux menaces posées par les ransomwares tels que CryptoWall, TeslaCrypt et Locky.

Il détaille en premier lieu les mécanismes que ces infections utilisent pour pouvoir pénétrer les entreprises puis démontre pourquoi un grand nombre de nouvelles infections continuent de se produire en dépit des mesures de protection existantes.

Il fournit ensuite des recommandations pratiques pour s'en protéger et explique comment faire face à ces menaces en utilisant des mesures techniques et organisationnelles à court et long terme.

Il présente également les paramètres de configuration optimale pour les solutions Sophos conçues pour protéger contre les ransomwares.

Introduction

Les ransomwares sont devenus l'une des menaces les plus répandues et les plus nocives auxquelles les internautes sont confrontés. Depuis la première apparition du fameux Cryptolocker en 2013, on assiste à une nouvelle ère de variantes de ransomwares de chiffrement de fichiers distribués via les messages de spam et les kits d'exploits, conçus pour extorquer de l'argent aux particuliers et aux entreprises.

L'origine des différentes familles de ransomwares actuelles peut remonter aux premiers jours de FakeAV (faux antivirus), en passant par des variantes de « Locker » ou des variantes de chiffrement de fichiers qui prévalent aujourd'hui. Cela dit, chaque catégorie de malwares partage un objectif commun : extorquer de l'argent aux victimes grâce à l'ingénierie sociale et à l'intimidation pure et simple. Et les sommes exigées augmentent en force à chaque itération.

D'où vient la vague actuelle d'infections par ransomwares ?

Même si la plupart des entreprises ont plusieurs mécanismes de sécurité en place - analyse antivirale, pare-feu, systèmes IPS, passerelles de messagerie antivirus/antispam et filtrage Web - on assiste à un grand nombre d'infections de ransomwares, tels que CryptoWall, TeslaCrypt et Locky actuellement à travers le monde. L'un des effets de ces infections est de chiffrer les fichiers sur les ordinateurs et les lecteurs réseau. Les utilisateurs se retrouvent ainsi piégés et obligés de payer une somme d'argent, habituellement autour des 200-500 dollars, pour obtenir l'outil de déchiffrement.

Voici un scénario d'infection courant :

- Un utilisateur reçoit un email pouvant provenir d'un expéditeur apparemment plausible avec une pièce jointe, d'un service d'expédition avec des informations de livraison en pièce jointe ou encore d'une société externe avec une facture jointe.
- La pièce jointe contient un document Word ou Excel avec une macro intégrée. Si le destinataire ouvre le document, une macro tente alors de s'exécuter automatiquement, lançant les actions suivantes :
    - Elle essaie de télécharger la charge de ransomware à partir d'une série d'adresses Web qui existent uniquement de manière temporaire. Si une adresse Web ne peut pas être atteinte, elle passe à la prochaine jusqu'à ce que la charge ait été téléchargée avec succès.
    - La macro exécute le ransomware.
    - Le ransomware contacte le serveur de Commande & Contrôle de l'attaquant, envoie des informations sur l'ordinateur infecté et télécharge une clé publique de chiffrement individuelle pour cet ordinateur.
    - Les fichiers de certains types (documents Office, les fichiers de base de données, fichiers PDF, documents CAO, HTML, XML, etc.) sont alors chiffrés sur l'ordinateur local et sur tous les lecteurs réseau accessibles avec cette clé publique.
    - Les sauvegardes automatiques du système d'exploitation Windows (copies masquées) sont souvent supprimées pour éviter ce type de récupération de données.

- Un message apparaît alors sur le bureau de l'utilisateur, expliquant comment la rançon (souvent sous la forme de Bitcoins) doit être payée dans un délai de 72 heures par exemple pour obtenir l'envoi d'un outil de déchiffrement approprié avec la clé privée qui est disponible uniquement dans le système de l'attaquant.
- Le ransomware s'autosupprime, laissant seulement les fichiers chiffrés et les notes de rançon derrière lui.

Ceci est juste un exemple de la façon dont un scénario d'infection peut opérer. En effet, bien que l'email reste une technique courante pour diffuser ces menaces, il est loin d'être le seul vecteur. Les kits d'exploits sont également fréquents : Angler, par exemple, est largement utilisé pour distribuer CryptoWall.

Pourquoi les attaques de ransomwares rencontrent-elles un tel succès ?

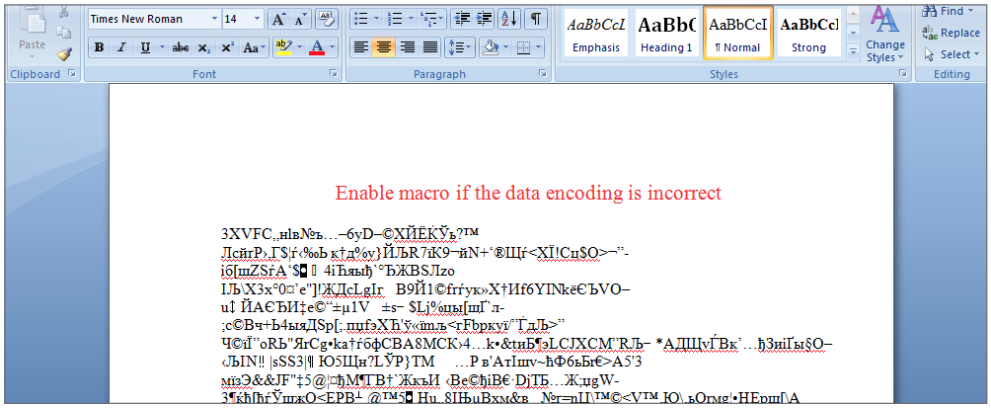
Voici les principales raisons expliquant le succès de ces infections :

1. Technologie d'attaque sophistiquée

- Les créateurs de ransomwares opèrent de manière très professionnelle. Ils conçoivent et fournissent généralement un véritable outil de déchiffrement après le paiement de la rançon (mais il n'y a aucune garantie).
- Ils utilisent intelligemment l'ingénierie sociale pour demander à l'utilisateur d'exécuter la procédure d'installation du ransomware. Par exemple, vous pouvez recevoir un email énonçant quelque chose du style : « Si l'encodage du document Word joint semble incorrect, veuillez activer les macros. Pour ce faire, procédez ainsi... »

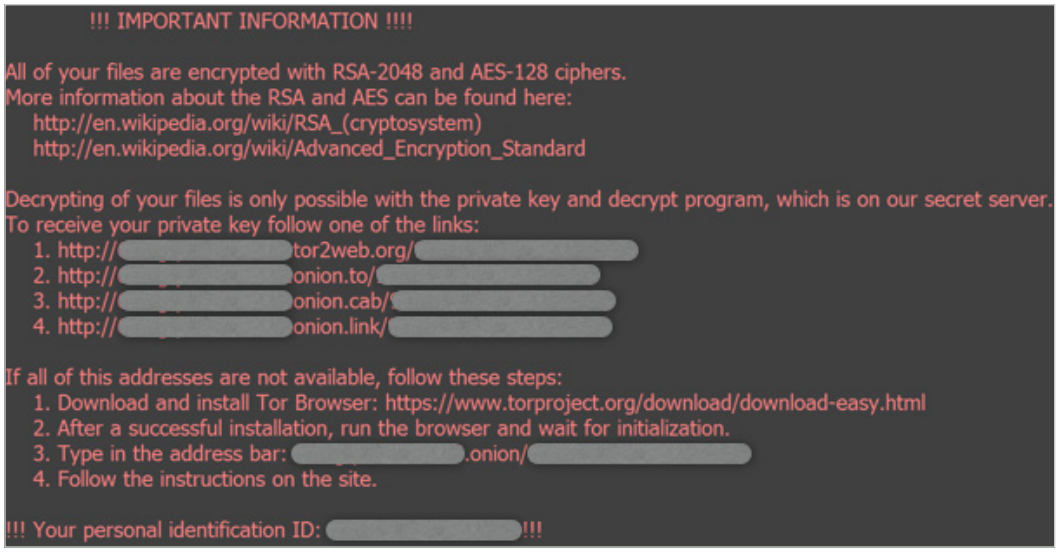
Locky se propage généralement de la manière suivante :

- Vous recevez un email contenant une pièce jointe.
- Le document ressemble à du charabia.
- Le document conseille d'activer les macros « si l'encodage de données est incorrect ».
- Les pirates veulent que vous cliquiez sur le bouton « Options » en haut de la page.



- Ils utilisent diverses technologies pour propager des infections qui sont permises dans de nombreuses entreprises et dans lesquelles le code malveillant peut être facilement déguisé (macros de Microsoft Office, JavaScript, VBScript, CHM, Flash, Java).

- Une fois que vous cliquez sur Options, Locky commence à s'exécuter sur votre ordinateur. Dès qu'il est prêt à vous demander la rançon, il change votre fond d'écran :



2. Faiblesses de sécurité dans les entreprises affectées

- Stratégie de sauvegarde insuffisante (pas de sauvegarde en temps réel, pas de sauvegarde hors ligne / hors site)
- Les mises à jour/correctifs pour le système d'exploitation et les applications ne sont pas mis en œuvre assez rapidement
- Autorisations des droits/utilisateurs dangereuses (les utilisateurs travaillent comme administrateurs et/ou ont plus de droits d'accès aux fichiers sur les lecteurs réseau que nécessaire pour accomplir leur travail)
- Manque de formation à la sécurité auprès des utilisateurs ("Quels documents puis-je ouvrir et de qui ?", "Quelle est la procédure à suivre si un document semble malveillant ?", "Comment puis-je reconnaître un email de phishing ?")
- Les systèmes de sécurité (antivirus, pare-feu, IPS, passerelles email /Web) ne sont pas actifs ou ne sont pas configurés correctement. La segmentation inadéquate du réseau peut également être incluse ici (serveurs et postes de travail sur le même réseau)
- Manque de connaissances de la part des administrateurs dans le domaine de la sécurité informatique (les fichiers .exe peuvent être bloqués dans les emails sans empêcher les macros Office ou tout autre contenu actif)
- Conflits de priorités (« Nous savons que cette méthode n'est pas sûre, mais nos employés doivent travailler... »)

Définition des priorités

Le dernier point précédemment cité se rapportant aux priorités mérite d'être approfondi. L'argument selon lequel « La sécurité perturbe les utilisateurs ... ils ne doivent pas être dérangés dans leur travail » empêche souvent l'implémentation de nombreuses mesures utiles de sécurité. Dans de nombreux cas, cet argument ne s'applique pas si les mesures relatives à la sécurité sont prévues dans les temps et adaptées à la situation des employés et de l'entreprise.

Dans certains cas, comme par exemple lorsqu'il reçoit un email ou lorsque les documents Office avec des macros sont utilisés en interne, l'employé doit savoir ce qui est plus important pour l'entreprise :

Exemple 1 :

Chaque utilisateur peut recevoir des documents Office depuis le Web et peut également les exécuter avec des macros sur les ordinateurs de l'entreprise.

Exemple 2 :

Seuls les utilisateurs des services spécialisés devant travailler avec des macros Office (traitement des commandes, comptabilité, ventes) ont l'autorisation d'exécuter des macros Office en accord avec la politique globale de l'entreprise.

Si un partenaire commercial envoie un courriel avec un document Office à des destinataires au sein de l'entreprise, alors ce message est mis en quarantaine. Le destinataire en est informé et est invité à confirmer avec l'expéditeur de l'email qu'il l'a bien envoyé. Après avoir fait cela, l'employé peut alors libérer cet email de la quarantaine automatiquement.

Alternativement, il peut demander au partenaire de réunir tous les documents futurs dans une archive ZIP protégée par un mot de passe créé ensemble au cours de cette conversation. Ces archives ZIP protégées par mot de passe ne sont jamais placées dans la quarantaine ; les emails futurs arriveront toujours immédiatement et le transfert par email des fichiers sera maintenant aussi chiffré.

L'exemple 1 est certainement le plus simple du point de vue de l'administration. Dans l'exemple 2, vous devez d'abord savoir quels services spécialisés peuvent recevoir des documents Office des partenaires commerciaux par email; vous devez fournir les instructions pour les groupes appropriés et former les employés des départements spécialisés. Néanmoins, l'exemple 2 est bien sûr l'étape la plus logique à mettre en œuvre si vous voulez améliorer la sécurité de manière significative en utilisant des mesures techniques et en réduisant au minimum les changements au niveau des habitudes de travail des employés.

Dans cet exemple, les mesures recommandées suivantes doivent toujours être prises en compte, en considérant ce que seraient les conséquences d'un manquement et comment ces mesures pourraient être mises en œuvre afin d'affecter l'utilisateur le moins possible.

Les meilleures pratiques à appliquer immédiatement

- **Sauvegardez régulièrement et conservez une copie de sauvegarde récente hors site.** Il existe de multiples raisons - autres que les ransomwares - pouvant être à l'origine de la disparition d'un fichier : un incendie, une inondation, un vol, un ordinateur portable qui tombe en panne ou encore une suppression accidentelle. En chiffrant votre sauvegarde, vous n'aurez plus à vous inquiéter que le système de sauvegarde tombe entre de mauvaises mains.
- **N'activez pas les macros dans les pièces jointes de documents reçus par courrier électronique.** Microsoft a délibérément désactivé l'auto-exécution de macros par défaut il y a plusieurs années comme mesure de sécurité. Un grand nombre d'infections par malwares consistent à vous persuader d'activer les macros, alors ne le faites pas !
- **Soyez prudent avec les pièces jointes non sollicitées.** Les pirates comptent sur le dilemme qui consiste à ne pas ouvrir un document avant d'être sûr qu'il soit légitime, mais comment le savoir si on ne l'ouvre pas.... En cas de doute, abstenez-vous.
- **Ne vous autorisez pas plus de privilèges que nécessaire.** Surtout, ne restez pas connecté en tant qu'administrateur plus longtemps que ce dont vous avez strictement besoin, et évitez la navigation, l'ouverture de documents ou autres activités de « travail régulier » alors que vous avez des droits d'administrateur.
- **Envisagez d'installer les visionneuses Microsoft Office.** Ces applications de visualisation vous permettent de voir à quoi ressemblent les documents sans avoir à les ouvrir dans Word ou Excel. En particulier, les visionneuses ne prennent pas du tout en charge les macros, donc vous ne pouvez pas activer les macros par erreur !
- **Mettez à jour les correctifs régulièrement et souvent.** Les malwares qui ne sont pas distribués via les macros des documents reposent souvent sur des failles dans les applications courantes telles qu'Office, votre navigateur Web ou encore Flash. Plus tôt vous installerez les correctifs, moins les pirates auront de vulnérabilités à exploiter.

Paramètres de configuration pour les solutions Sophos

Les technologies Sophos protègent et bloquent les fichiers malveillants et le trafic Web utilisés par les ransomwares. Pour que votre protection fonctionne efficacement, il est important de configurer vos solutions de manière optimale.

Sophos Endpoint Protection

Si vous administrez Sophos Endpoint Security and Control via la Sophos Enterprise Console, assurez-vous que les paramètres suivants aient bien été configurés dans la politique AV de tous les postes de travail et les serveurs:

- Analyse sur accès : activé
  - Vérification des fichiers en lecture/écriture/modification : activé
  - Analyse mémoire: activé
- Analyse des téléchargements : activé
- Blocage de l'accès aux sites Web malveillants : activé
- Sophos Live Protection : activé
- Surveillance des comportements : activé
  - Détection des comportements malveillants : activé

- Détection du trafic malveillant : activé
- Détection des dépassements de la mémoire tampon : activé

Si vous utilisez **Sophos Cloud Endpoint Protection,** les paramétrages suivants doivent être effectués pour tous les utilisateurs :

- Analyse en temps réel : activé

Si vous utilisez **Sophos Cloud Server Protection**, configurez votre serveur de la manière suivante :

- Analyse en temps réel - fichiers locaux ...: tous les paramètres activés
- Analyse en temps réel - Internet : tous les paramètres activés
- Analyse en temps réel - Options :
  - Détection des comportements malveillants : activé
  - Live protection : activé
- Activez la fonction « Serveur Lockdown »

Configuration de la passerelle de messagerie

Une analyse antivirus et antispam de tous les emails entrants et sortants doit d'abord être mise en place sur la passerelle de messagerie, configurée selon les meilleures pratiques de l'éditeur.

Si votre passerelle de messagerie fournit une technologie de sandboxing pour analyser les pièces jointes, alors activez cette fonction. **Sophos Email Appliance** fournit cette fonction dans la version 4.0 ; **Sophos UTM** la fournit dans la version 9.4.

Configurez également votre passerelle de messagerie de manière à ce qu'aucune pièce jointe exécutable ne soit autorisée dans les emails entrants depuis le Web, y compris les documents Office, VBS, JavaScript, Java, ActiveX et CHM.

Sophos recommande en particulier la mise en quarantaine des types de fichiers ayant les extensions suivantes : .ade, .adp, .bas, .bat, .chm, .cla, .class, .cmd, .com, .cpl, .exe, .hlp, .hta, .inf, .ins, .js, .jse, .lnk, .msc, .msi, .mst, .ocx, .pcd, .pif, .reg, .scr, .sct, .shb, .shs , .url, .vb, .vbs, .vbe, .wsf, .wsh et .wsc. Il est également important de scanner les archives pour ces fichiers et de les placer en quarantaine si nécessaire.

Il existe une règle prédéfinie pour cela avec la **Sophos Email Appliance** : « Threat Protection -> SophosLabs Suspect Attachments to all ».

Les emails avec ces types de pièces jointes doivent être placés en quarantaine et le destinataire doit être informé de cette action (par exemple en remplaçant la pièce jointe originale par un message expliquant que la pièce jointe est en quarantaine et comment procéder).

Si vous utilisez Sophos Email Appliance, activez l'option «Delay queue " dans " Policy -> SMTP Options -> Delay Queue ". Lorsque cette option est activée, l'appliance retardera le spam suspecté qui n'a pas été détecté lors de la première analyse de 10 à 60 minutes et effectuera une autre analyse ultérieure. Cela permet d'empêcher les campagnes de spam d'être distribuées dès leur arrivée.

Selon la solution de messagerie, l'organisation et la formation que les employés ont reçue, les emails peuvent être libérés de la quarantaine, soit par les administrateurs de messagerie soit par les destinataires originaux de l'email - après que le destinataire en question ait vérifié (par exemple en appelant l'expéditeur de l'email) qu'il s'agit bien d'un expéditeur valide.

Configuration de la passerelle Web

Configurez votre passerelle Web de façon à analyser tous les téléchargements à la recherche de virus et bloquez les adresses Web connues et les mécanismes de communication avec les serveurs Command & Control. Activez l'analyse des connexions SSL dans chaque cas. Si votre passerelle Web fournit une technologie de **sandboxing** pour analyser les téléchargements, alors activez cette fonction.

Configurez **Sophos UTM** comme suit :

- ATP : Protection réseau -> Advanced Threat Protection : activé
- Profil filtrage Web -> Action de filtrage -> Antivirus -> Analyse antivirus : Double analyse
- Profil filtrage Web -> Action de filtrage -> Antivirus -> Sandstorm : activé (depuis UTM 9.4)
- Filtrage Web -> HTTPS -> Déchiffrer et analyser
- Bloquez des catégories de filtrage Web :
  - Anonymizeurs
  - Exploits du navigateur
  - Téléchargements dangereux
  - Sites malveillants
  - Phishing
  - URL de spam
  - Les données sur les programmes sont anonymisées (anonymisation des utilitaires également)

Configurez **Sophos XG/SF-OS Firewall** comme suit :

- ATP : Dans le tableau de bord -> allez à la colonne de droite et cliquez sur "Advanced Threat Protection" -> Configurer -> "Advanced Threat Protection : activé »
- Filtrage du contenu Web -> Analyse : Double antivirus
- Pour chaque règle de politique correspondante-> Analyser les malwares -> Déchiffrer et analyser le trafic HTTPS : activé
- Pour chaque règle de politique correspondante-> politique de filtrage Web avec catégories bloquées :
  - Anonymizeurs
  - Command & Control
  - Phishing & fraude
  - URL de spam

Configurez la **Sophos Web Appliance** comme suit :

- Politique globale-> Analyse HTTPS : activé
- Politique globale-> Sandstorm : activé
- Bloquez des catégories de filtrage Web : Proxies & traducteurs

Toutes les autres URL malveillantes (sites à haut risque, phishing, spyware, spam) sont bloquées par défaut et l'analyse antivirus est activée.

Configurez le pare-feu/système de prévention des intrusions (IPS)

Un IPS dédié ou un IPS intégré au pare-feu/UTM doit être configuré de telle manière que la communication Command & Control soit bloquée.

Dans **Sophos UTM** , voici comment utiliser la politique IPS pour bloquer la communication :

- Protection réseau -> Prévention des intrusions -> Modèle d'attaque
  - Malware

Dans **Sophos XG/SF-OS Firewall**, voici comment utiliser la politique IPS pour bloquer la communication :

- Politiques -> Catégorie Prévention des intrusions
  - Communication Malware

Mesures supplémentaires pour lutter contre les ransomwares

Sensibiliser/former les employés

En plus des mesures immédiates décrites ci-dessus, il est important que tous les employés reçoivent une formation régulière sur la sécurité informatique. L'efficacité de ces mesures devrait également être vérifiée régulièrement.

Sophos fournit un certain nombre d'outils gratuits pour aider à sensibiliser les employés sur les menaces à la sécurité, comme le document **Recommandations de sécurité informatique** ou encore son **Threatsaurus**. Reportez-vous à la section « Lectures complémentaires » à la fin de ce livre blanc pour obtenir les liens vers ces ressources.

Segmenter le réseau d'entreprise

Les mesures de sécurité à la passerelle sont rendues inutiles si un ordinateur, se connectant au réseau sans autorisation (ordinateur portable privé, ordinateur appartenant à un prestataire de services, portable de l'entreprise avec protection antivirus obsolète), est autorisé à infiltrer ces mesures. Les solutions de NAC (contrôle d'accès réseau), par exemple, peuvent aider à lutter contre la menace d'un système non autorisé sur le réseau en permettant uniquement aux ordinateurs connus d'accéder au réseau.

Par conséquent, le principe selon lequel chaque système a seulement accès aux ressources nécessaires pour effectuer les tâches requises devrait également s'appliquer à la conception réseau.

Au niveau du réseau, cela signifie aussi que vous sépariez les zones fonctionnelles avec un pare-feu, par exemple pour les réseaux client et serveur. Les systèmes et les services concernés ne seront alors accessibles que si cela est vraiment nécessaire. Les serveurs de sauvegarde peuvent uniquement être accessibles depuis les postes de travail, par exemple, via le port requis par la solution de sauvegarde et non via l'accès au système de fichiers Windows.

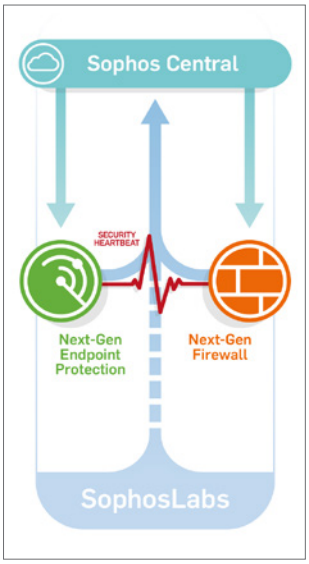
Par conséquent, vous devez également envisager d'appliquer un pare-feu client aux postes de travail et aux serveurs, car il n'y a généralement aucune raison pour que les postes de travail ou les serveurs communiquent entre eux, à moins que ce soit pour des services connus. Cette méthode peut également empêcher la propagation d'infections au sein d'un réseau.

Chiffrez les données de l'entreprise

En chiffrant intelligemment les documents de l'entreprise, vous pouvez empêcher que des malwares gagnent un accès non chiffré à des documents confidentiels, évitant ainsi de nombreux dommages causés par le flux des documents professionnels.

Pensez à la sécurité comme un système intégré

Dans de nombreuses entreprises, les divers composants de sécurité (pare-feu, VPN, IPS, sécurité Endpoint, chiffrement, sécurité Web, sécurité de la messagerie, gestion des mobiles, gestion du WLAN) fonctionnent indépendamment chacun de leur coté, sans communiquer entre eux, sans corréler de résultats ni être capables de déclencher des contre-mesures automatiques en cas d'incidents de sécurité potentiels.



Mais si tous ces composants pouvaient communiquer entre eux et déclencher des actions automatiques pour protéger l'ensemble du système en cas d'incident de sécurité - c'est-à dire fonctionner comme un système à part entière - alors la sécurité globale de l'infrastructure en serait grandement renforcée.

L'approche de Sophos avec sa sécurité synchronisée vous permet de partager l'intelligence en temps réel entre vos systèmes d'extrémité et votre pare-feu. En automatisant l'identification, l'investigation et la réponse aux menaces, la sécurité synchronisée vous offre une protection inégalée contre les menaces avancées. Pour en savoir plus, visitez notre site à la page www.sophos.fr/heartbeat

Déployez les fonctions de détection de trafic malveillant

Il est essentiel de réagir rapidement aux nouvelles menaces. La détection du trafic malveillant, qui est disponible dans Sophos Endpoint Protection, détecte les communications entre un système d'extrémité compromis et les serveurs d'un attaquant. La détection du trafic malveillant identifie automatiquement le logiciel fautif et l'empêche de fonctionner pour éviter tout dommage ou perte de données potentiels.

Utilisez des outils d'analyse de la sécurité

Même si vous implémentez toutes les mesures mentionnées ci-dessus, vous ne pouvez jamais garantir à 100% que des incidents de sécurité/infections n'affecteront pas les ordinateurs de l'entreprise à l'avenir. Néanmoins, si un incident se produit, il est vital que la source de l'infection et ses effets potentiels sur d'autres systèmes de l'entreprise soient identifiés et maîtrisés aussi vite que possible. Cela peut aider à réduire le temps et les efforts nécessaires pour identifier et corriger les systèmes affectés, et rétablir le bon fonctionnement de l'infrastructure informatique de manière drastique. De plus, en identifiant la source et la méthode d'infection, les vulnérabilités potentielles dans le dispositif de sécurité peuvent être mises en évidence et éliminés.

Bonnes pratiques de sécurité informatique

Bon nombre des mesures proposées dans le présent document sont des « bonnes pratiques » en matière de sécurité informatique et devraient en fait être établies depuis longtemps dans l'entreprise, tout comme d'autres mesures qui ne sont pas mentionnées ici, comme l'application de mots de passe forts par exemple. Nous recommandons des contrôles/ audits de sécurité réguliers afin d'identifier les défaillances potentielles et d'être à jour en termes d'options technologiques et organisationnelles pour protéger au mieux votre infrastructure informatique

Les ransomwares représentent un risque bien réel pour toutes les organisations et les statistiques donnent à penser que cela n'est pas prêt de s'arrêter. Il est donc essentiel de prendre des mesures immédiates pour sécuriser votre entreprise contre ce type d'attaque. En suivant les recommandations à court et à long terme décrites dans le présent document, les organisations prendront des mesures importantes pour se protéger contre les infections de ransomwares.

Lectures complémentaires :

Livre blanc Sophos sur les ransomwares

Publication du blog Sophos sur Locky

Publication du blog Sophos sur les ransomwares

Recommandations de sécurité informatique

Threatsaurus

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

Oxford (Royaume-Uni) | Boston (États-Unis)
© Copyright 2016. Sophos Ltd. Alle Rechte vorbehalten.
Immatriculée en Angleterre et au Pays de Galles No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Royaume-Uni
Sophos est une marque déposée de Sophos Ltd. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

03/16.NP.wpfr.simple

SOPHOS