L'approche 360° de Beazley pour la protection contre les ransomwares

L'attaque par ransomware est l'un des actes de malveillance les plus couteux et dommageables que peut subir votre organisation. Ce type d'attaques est en hausse, et rien n'indique que cette tendance pourrait s'atténuer. Au cours des trois derniers mois seulement, Beazley a constaté une augmentation de 37 % du nombre d'incidents signalés impliquant un ransomware, par rapport au trimestre précédent. Les équipes Claims et Breach Response Services de Beazley sont en première ligne pour agir, armées des connaissances et de l'expertise nécessaire pour vous aider à protéger votre entreprise contre ces attaques. En collaboration avec nos prestataires de services d'informatique légale, Lodestone Security et KPMG, nous avons élaboré un guide des bonnes pratiques de prévention contre les ransomwares pour vous permettre de vous prémunir contre ces menaces.

Scenario d'une attaque de Ransomware

1

Contamination initiale de votre environnement

- Votre organisation est la cible d'un groupe criminel qui lance à votre encontre une campagne d'hameçonnage.
- Un logiciel malveillant est transmis à l'un de vos utilisateurs, qui ne se doute de rien, via une pièce jointe ou un lien dans un e-mail.

2

Installation du malware

- L'utilisateur ouvre la pièce jointe et, sans qu'il s'en aperçoive, le programme malveillant est installé sur son ordinateur.
- À l'insu de l'utilisateur, de vos équipes Security et IT, les pirates ont alors un point d'ancrage dans votre environnement.
- Tirant parti de cette situation, ils explorent votre réseau (en restant toujours inaperçus) pour détecter les systèmes vulnérables et les données sensibles. Cela inclut les appareils des autres utilisateurs, mais également les serveurs prenant en charge les applications critiques et le stockage des fichiers.

3

Déploiement du ransomware

- Le groupe criminel a obtenu l'accès dont il a besoin et est maintenant prêt à déclencher son piège.
- Il déploie une souche de ransomware qui se propage sur l'ensemble de votre réseau, cryptant indifféremment les données.
- Les pirates ont à présent chiffré une part significative de vos données, et certaines parties de votre activité sont totalement perturbées, tandis que d'autres le sont partiellement.

4

Extorsion

- Les criminels réclament X millions pour la clé de déchiffrement.
- L'attaque est également rendue publique, entraînant une atteinte à la réputation.
- L'autorité de réglementation cherche par ailleurs à savoir s'il y a eu une utilisation inappropriée des données sensibles de clients. Il existe un risque d'amende substantielle.

Protéger votre organisation contre les ransomwares

Contrôles de base, sans lesquels vous êtes vulnérable

- **Déploiement et maintien d'une solution antivirus bien configurée et gérée de façon centralisée :** un antivirus performant est une composante fondamentale de tout programme de sécurité.
- **Marquage des e-mails :** marquer les e-mails d'expéditeurs externes pour signaler aux collaborateurs qu'ils proviennent de sources extérieures à l'entreprise.
- **Contenu des e-mails et distribution :** mettre en place des contrôles Sender Policy Framework (SPF) stricts pour tous les e-mails entrants afin de vérifier la fiabilité des organisations expéditrices. Filtrer tous les messages entrants pour détecter les contenus malveillants, y compris les exécutables et les documents contenant des macros.
- **Modules complémentaires et configuration Office 365 :** activer l'authentification à deux facteurs (2AF) sur O365 et utiliser la protection avancée contre les menaces.
- **Macros :** désactiver l'exécution automatique des macros. Idéalement, les désactiver totalement si votre organisation n'en a pas besoin.
- **Correctifs :** appliquer rapidement des correctifs en cas de vulnérabilités critiques sur les terminaux et serveurs, en particulier pour les systèmes externes.
- **Contrôles relatifs à l'utilisation des médias :** mettre en place des contrôles concernant l'intégration et/ou l'utilisation de médias qui ne prévoient pas de processus d'authentification/identifiants média appropriés.
- **Processus de réaction aux failles correctement défini et testé :** permet de limiter les pertes et de relancer rapidement les opérations à la suite d'une attaque par ransomware.
- **Sauvegarde des systèmes et bases de données clés :** garantir les sauvegardes régulières, la vérification de ces dernières et la sécurité du stockage en ligne.
- **Formation de vos utilisateurs :** la plupart des attaques découlent d'erreurs commises par les utilisateurs. Former les utilisateurs afin qu'ils puissent identifier les e-mails d'hameçonnage contenant des pièces jointes ou liens malveillants. Les exercices réguliers consistant à identifier les e-mails d'hameçonnage sont une méthode efficace.

Mesures de référence pour une protection renforcée

- **Mise en place d'une configuration de base sécurisée :** les logiciels malveillants reposent sur l'exploitation de failles. Une configuration de base conforme aux normes techniques telles que les normes du Center for Internet Security (CIS) peuvent aider à combler les lacunes.
- **Filtrage du trafic de navigation sur Internet :** les outils de filtrage aideront à empêcher les utilisateurs d'accéder à des sites malveillants.
- **Utilisation de DNS de protection :** aide à empêcher l'accès aux adresses IP connues pour être malveillantes.
- **Gestion efficace de l'accès :** l'attaque par ransomware peut ne pas nécessairement se propager dans toute l'entreprise. Prendre les mesures appropriées pour l'accès général des utilisateurs et l'accès au système dans l'ensemble de l'organisation. Prendre les mesures appropriées pour l'accès privilégié aux actifs critiques (serveurs, terminaux, applications, bases de données, etc.). Mettre en place l'authentification multifactorielle lorsque nécessaire, par exemple : accès à distance/VPN, applications externes, etc.
- **Test régulier des sauvegardes :** limite la durée d'interruption et les pertes de données en cas de restauration à partir de sauvegardes après une attaque par ransomware fructueuse.
- **Déconnexion des sauvegardes du réseau de l'organisation :** empêche l'accès aux sauvegardes et leur cryptage par un ransomware en cas d'attaque fructueuse sur le réseau principal d'une organisation.
- **Identifiants de sauvegarde uniques et conservés séparément :** empêche l'accès aux données de sauvegarde et le cryptage de ces dernières par des criminels.

Pratiques offrant la meilleure protection

- **Outils EDR (Endpoint Detection and Response) :** les solutions d'EDR ciblent la surveillance des serveurs, ordinateurs portables et de bureau et dispositifs mobiles administrés afin de détecter les menaces et activités suspectes. Ces outils permettent également une réponse quasi immédiate par des experts en sécurité qualifiés. Lorsqu'ils sont efficacement déployés et contrôlés, les outils EDR constituent l'une des meilleures défenses contre les ransomwares et autres attaques par logiciel malveillant.
- **Surveillance complète et centralisée des registres :** la collecte et la surveillance centralisées des registres, idéalement au moyen d'un système de gestion des événements et informations de sécurité, permettent d'identifier les menaces qui percent vos défenses internes.
- **Souscription de services de veille externe sur les menaces informatiques :** fournit un accès à des services externes qui peuvent communiquer des détails sur les méthodes, techniques et procédures d'attaque en développement. Ces services permettent également l'accès aux bases de données des pièces jointes d'e-mail et sites malveillants connus, etc.
- **Sauvegardes cryptées :** empêche l'utilisation de données de sauvegarde par des criminels en cas d'accès non autorisé.
- **Segmentation réseau :** mise en place de contrôles dans l'environnement réseau pour limiter l'accès et/ou le flux de trafic. Un ensemble de règles de pare-feu bien configuré garantira que seul le trafic requis passe d'un segment à l'autre.

KPMG

KPMG offre une large gamme de services pour aider les organisations à se défendre contre les attaques par ransomware et à réagir de façon adaptée.
Pour trouver la solution qui correspond le mieux à vos besoins, contactez :
Matthew Martindale – Partner, Cyber Security
cyber@kpmg.co.uk

beazley

BZCER034_FR_12/19