Présentation abrégée

Cisco Ransomware Defense

Les bénéfices

- **Une réduction des risques** d'attaques par ransomware grâce à une solution de sécurité qui bloque les menaces avant qu'elles affectent votre système.
- **Une protection immédiate** contre les ransomwares qui vous permet de vous concentrer sur votre cœur de métier.
- **Un système de défense multicouche** pour une visibilité et une réactivité inégalées, depuis la couche DNS jusqu'au réseau en passant par le terminal.
- **Une segmentation dynamique** pour isoler le ransomware sur le réseau.
- **Des informations de sécurité adaptative de pointe** grâce au groupe de sécurité adaptative et de recherche Cisco Talos.

La montée en puissance des ransomwares

Un ransomware est un programme malveillant, ou malware, qui chiffre les données présentes sur un ordinateur, comme des documents, des photos et de la musique. L'utilisateur ne peut débloquer ou récupérer ses fichiers que contre le paiement d'une rançon.

Le ransomware est rapidement devenu le type de malware le plus rentable, représentant un marché annuel approchant le milliard de dollars.

Il infiltre généralement un ordinateur ou un réseau par le web ou par e-mail. Les ransomwares peuvent infiltrer un site web par le biais de publicités malveillantes, des publicités infectées qui transmettent des malwares. Lorsqu'un utilisateur navigue sur un site contenant des publicités malveillantes, ces dernières téléchargent automatiquement les malwares ou le redirigent vers des kits d'exploit. Les ransomwares peuvent également s'infiltrer sur un ordinateur par le biais d'e-mails d'hameçonnage et de spams. Il suffit que l'utilisateur clique sur un lien contenu dans ce type d'e-mail ou ouvre une pièce jointe pour télécharger le ransomware et le signaler à son serveur de contrôle-commande.

Les ransomwares peuvent également prendre le contrôle des systèmes à l'aide de kits d'exploits. Les kits d'exploits sont des kits logiciels conçus pour identifier les vulnérabilités logicielles des systèmes des utilisateurs. Ils téléchargent et exécutent ensuite un programme malveillant, tel qu'un ransomware, sur ces systèmes vulnérables.

À l'avenir, ces ransomwares ne cibleront pas uniquement des utilisateurs individuels, mais des réseaux tout entiers. Alors que les méthodes de propagation semi-automatiques se multiplient, les développeurs de ransomwares ont davantage d'opportunités d'infiltrer le réseau et d'en prendre progressivement le contrôle, ce qui maximise l'impact des attaques et les chances d'obtenir un paiement.

Réduisez les risques d'attaques par ransomware grâce à une sécurité renforcée

Étant donné que les ransomwares peuvent s'infiltrer dans l'entreprise sous de nombreuses formes, le meilleur moyen de réduire les risques d'infection est d'adopter un ensemble de solutions de sécurité plutôt qu'un produit unique. Il est essentiel d'empêcher les ransomwares d'accéder à vos systèmes, de les détecter s'ils parviennent à s'infiltrer et de limiter les dégâts qu'ils peuvent causer.

« Nous avons grandement réduit notre surface d'exposition aux ransomwares issus du web et avons pu améliorer l'expérience de nos utilisateurs en matière de connectivité Internet. »

Octapharma

La solution Cisco® Ransomware Defense s'appuie sur l'architecture de sécurité de Cisco pour protéger l'entreprise à l'aide de systèmes de défense qui couvrent l'ensemble de l'infrastructure : les réseaux, la couche DNS, la messagerie et les terminaux. Elle s'appuie sur les recherches de pointe du centre Cisco Talos sur les menaces afin de garantir une réactivité optimale face aux ransomwares.

Notre solution inclut les composants suivants :

- **Cisco Umbrella**, qui protège les appareils utilisés sur le réseau de l'entreprise et en dehors. Ce composant bloque les requêtes DNS avant qu'un appareil ne puisse se connecter à des sites hébergeant des ransomwares.
- **Cisco Advanced Malware Protection (AMP) for Endpoints**, qui empêche l'exécution des ransomwares sur les terminaux.
- **La solution de sécurisation de la messagerie Cisco avec Advanced Malware Protection (AMP)**, qui bloque les spams et les messages d'hameçonnage, ainsi que les URL et les pièces jointes malveillantes. La technologie AMP est identique à celle appliquée au niveau du terminal, mais elle est déployée sur la passerelle de messagerie.
- **Le pare-feu de nouvelle génération Cisco Firepower** avec Cisco AMP et la technologie de sandboxing Threat Grid, qui bloque les menaces connues et les instructions de type contrôle-commande, tout en fournissant des fonctions analytiques dynamiques pour détecter les menaces et les malwares inconnus.
- **Cisco ISE via le réseau Cisco**, qui permet de segmenter le réseau de façon dynamique afin de sécuriser l'accès aux services et aux applications et d'éviter que les ransomwares ne se propagent latéralement sur le réseau.
- **Les services de sécurité Cisco** supervisent instantanément le processus de riposte en cas d'attaque. Ils rationalisent les déploiements de la solution AMP, des pare-feu de nouvelle génération et d'autres produits.

Étapes suivantes

Laissez-nous vous aider à vous concentrer sur votre cœur de métier : contactez votre conseiller Cisco pour en savoir plus sur la solution Cisco Ransomware Defense.

C45-737465-00 07/16