Recommander des mesures d’atténuation des menaces

Objectifs

Partie 1: Analyser un incident dans une entreprise de production vidéo

Partie 2: Analyser un incident dans une entreprise de vente au détail

Contexte/scénario

La connaissance des vulnérabilités et des attaques du réseau n'est qu'une partie de la lutte. La réduction des menaces est l'objectif final du personnel de sécurité du réseau.

Dans cet atelier, vous allez lire deux études de cas qui décrivent des incidents liés à la sécurité du réseau. Il vous incombe de recommander des mesures d'atténuation des menaces pour faire face à chaque incident.

Ressources requises

- Accès à Internet

Instructions

Partie 1: Analyser un incident dans une entreprise de production vidéo

All Time Video Inc. est une entreprise qui produit des vidéos pour plusieurs clients. Ils utilisent des méthodes de production vidéo numériques et stockent leur contenu sur des serveurs de gestion de contenu spécialisés. Ils sont très fiers de leurs bibliothèques de contenu qui incluent un large éventail de séquences d'archives pouvant être utilisées dans des vidéos sur de nombreux sujets.

La direction de l'entreprise a reçu un e-mail d'un groupe de hackers. Dans l'e-mail, les hackers affirment avoir été en mesure de voler plusieurs téraoctets de ressources vidéo et de projets sur les serveurs de gestion de contenu. Les hackers menacent de télécharger les ressources vidéo sur divers serveurs sur Internet, à moins que l'entreprise ne paie une somme d'argent. La direction d'All Time Video craint de perdre un avantage concurrentiel si ses ressources sont rendues publiques.

L'entreprise a fait appel à une équipe de sécurité externe pour enquêter sur l'incident. L'enquête a révélé qu'un lot de clés USB disponibles lors d'un récent salon de la vidéo était infecté par des malwares. Le malware a infecté plusieurs hôtes sur le réseau All Time Video et s’est également propagé sur le réseau à d’autres machines. Le malware a analysé le réseau à la recherche de plusieurs types de logiciels de gestion de contenu et a déterminé la version du logiciel. Le malware a ensuite exploité les vulnérabilités d'une ancienne version non corrigée du logiciel pour y accéder. Une fois l'accès obtenu, le malware a informé les hackers qui ont ensuite pu installer un logiciel utilisant la tunnellisation DNS pour voler progressivement les données des serveurs. Cela a été utilisé pour échapper à la détection. Pendant plusieurs mois, les hackers stockent des téraoctets de ressources vidéo.

Étape 1: Analyser l'attaque.

En tant que membre de l'équipe de sécurité "**All Time Video**", vous devrez nous faire part de vos idées sur la manière de limiter une telle attaque. Commencez par identifier les conditions qui ont conduit à l'attaque.

Que devait-il se passer pour que cette attaque se produise ?

Pour que cette attaque puisse arriver, plusieurs éléments ont posé problème :

- Les employés ont utilisé des clés USB contaminées qu'ils avaient récupéré dans un salon, sans faire de vérification avant.
- Le logiciel de gestion de contenu tournait sur une version trop ancienne, qui n'avait pas été patchée
- Le réseau interne n'était pas vraiment bien sécurisé, donc le malware a pu scanner et infecter d'autres postes.
- Le pare-feu n'a pas stoppé la tunnellisation DNS, ce qui a rendu possible l'exfiltration des données

Étape 2: Recommander des techniques d'atténuation.

Pour chaque événement qui s'est produit au cours de cet incident, utilisez votre accès Internet pour étudier les techniques d'atténuation possibles. Vous êtes libre d'utiliser toutes les sources d'informations que vous pouvez trouver afin de recommander des techniques de réduction des menaces exploitables.

Pour éviter que ça se reproduise :

- Gestion des supports externes : Interdire les clés USB inconnues ou obliger un scan antivirus automatique dès qu'on les branche.
- Mise à jour (patching) : Garder absolument les logiciels à jour pour corriger les failles de sécurité.
- Segmentation réseau : Séparer les serveurs critiques du reste du réseau pour éviter que le malware se balade partout.
- Surveillance DNS : Configurer le pare-feu pour analyser le trafic DNS et bloquer les tunnels suspects afin d'empêcher la fuite de données.

Partie 2: Analyser un incident dans une entreprise de vente au détail

Une entreprise de vente au détail de taille moyenne est spécialisée dans la vente de pièces détachées personnalisées. Un client a appelé l'entreprise pour informer l'entreprise que ses données personnelles et les informations relatives à sa carte bancaire se trouvaient sur Internet. Une enquête a montré que des hackers ont pu infiltrer le réseau de l'entreprise via la connexion réseau d'un fournisseur d'équipement. Le but de la connexion est de surveiller un outil de travail du bois contrôlé par ordinateur qui est utilisé pour créer des cous et des corps de guitare. Le faible niveau de sécurité chez le fournisseur a permis aux hackers d'exploiter cette connexion. Les hackers ont pu localiser et accéder au serveur utilisé pour accepter les paiements des produits sur Internet. Les acteurs de la friandise ont exploité un compte d'utilisateur et un mot de passe faible pour accéder à la base de données des clients. Toutes les informations sur le client étaient présentées dans un fichier facile à lire. Le fichier a été chargé sur un serveur utilisé par des hackers et les informations ont été vendues à d'autres hackers.

Étape 1: Analysez l'attaque

Lisez la description de l'incident et répertoriez les étapes de l'attaque.

- Les pirates sont entré via la connexion réseau du fournisseur d'équipement, qui était mal protégé.
- Ensuite ils ont repéré où se trouvait le serveur de paiement sur le réseau.
- Ils ont trouvé un compte utilisateur avec un mot de passe trop simple et s'en sont servi pour accéder à la base.
- Ils ont copié le fichier contenant les infos clients, qui n'était même pas chiffré.
- Puis ils ont envoyé ce fichier sur leur serveur pour le revendre.

Étape 2: Recommander des mesures d'atténuation

Pour chaque événement qui s'est produit au cours de cet incident, recommander des mesures qui pourraient atténuer l'événement.

- Sécuriser les tiers : Exiger que les fournisseur aient une sécurité correcte (VPN, double auth) avant d'accéder au réseau.
- Isolation des machines : La machine pour l'outil de bois doit pas être sur le même réseau que le serveur de paiement.
- Politique de mot de passe : Obliger des mots de passe complexes et un changement régulier pour limiter le bruteforce.
- Chiffrement : Les infos clients doivent jamais être stockées en clair, il faut tout chiffrer.

Remarques générales

1. Quelles ressources spécifiques avez-vous trouvées sur le web qui vous ont aidé à recommander des mesures d'atténuation ?

J'ai regardé le site de l'ANSSI et aussi quelques blogs de cybersécurité comme ZDNet pour trouver des solutions standard.

Top 5 des menaces de cybersécurité (PME & grandes entreprises)
Sources : Kaspersky / ANSSI

- Ransomware
- Phishing
- Mots de passe faibles
- DDoS
- Intrusion par un tiers

2. Recherchez sur le web les 5 principales menaces de cybersécurité auxquelles sont confrontées les petites et moyennes entreprises (PME) et les grandes entreprises (PME). Répertoriez les menaces dans le tableau et suggérez des techniques d'atténuation pour les contrer. Les réponses varient, les sites web répertoriant les différentes menaces. Ce n'est pas un problème. Assurez-vous simplement que les informations sont récentes et recherchez brièvement leur source pour vérifier leur qualité.

a. Où avez-vous trouvé vos informations ? Copiez et collez l'URL ci-dessous.

J'ai principalement consulté le site de l'ANSSI (l'agence nationale de la sécu) ainsi que Cybermalveillance.gouv.fr, car ils proposent des fiches pratiques pour pas mal d'attaques différentes. J'ai aussi jeté un œil aux docs techniques de Cisco vu que ça correspond au contenu du cours.

https://www.cert.ssi.gouv.fr/cti/
Cybermalveillance.gouv.fr

b. Quel est le nom de l'entreprise qui a fourni les informations ?

ANSSI (Agence nationale de la sécurité des systèmes d'information)

c. Quelle est la nature de l'entreprise ?

C'est un organisme public français qui dépend du Secrétariat général de la défense et de la sécurité nationale (SGDSN).

d. Complétez le tableau ci-dessous.

Menace	Recommandation d'atténuation
Ransomware	Faire des sauvegardes régulières hors-ligne et avoir un antivirus fiable.
Phishing	Sensibiliser les employés pour qu'ils ne cliquent pas sur des liens suspects dans les emails.
Utilisation de mots de passe trop faibles	Mettre en place l’authentification à deux facteurs (MFA/2FA) pour sécuriser les comptes.
Attaques par déni de service distribué	Utiliser des services de protection DDoS (genre Cloudflare) afin de filtrer le trafic malveillant.
Compromission via un fournisseur ou un tiers	Réduire les accès des fournisseur au strict minimum, selon le principe du moindre privilège.

VALIDATION :