Journal du gestionnaire des incidents

Scénario 1

Une petite clinique américaine spécialisée dans les soins de santé primaires a été victime d'un incident de sécurité un mardi matin, vers 9 heures. Plusieurs employés ont signalé qu'ils n'arrivaient pas à accéder à des fichiers depuis leurs ordinateurs, notamment des dossiers médicaux. Les activités de l'entreprise ont été interrompues parce que les employés n'ont pas pu accéder aux fichiers et aux logiciels dont ils avaient besoin pour faire leur travail.

De plus, les employés ont également signalé qu'une demande de rançon s'était affichée sur leurs ordinateurs. La demande de rançon indique que tous les fichiers de l'entreprise ont été chiffrés par un groupe organisé de pirates informatiques sans scrupules, connus pour cibler les entreprises des secteurs de la santé et des transports. Pour rétablir l'accès aux fichiers chiffrés, la note de rançon exige une forte somme d'argent en échange de la clé de déchiffrement.

Les pirates ont pu accéder au réseau de l'entreprise en utilisant des e-mails d'hameçonnage ciblés, qui ont été envoyés à plusieurs employés de l'entreprise. Les e-mails d'hameçonnage contenaient une pièce jointe malveillante qui, une fois téléchargée, installait un logiciel malveillant sur l'ordinateur de l'employé.

Une fois l'accès obtenu, les pirates ont déployé leur rançongiciel, qui a chiffré les fichiers critiques. L'entreprise n'a pas pu accéder aux données critiques des patients, ce qui a entraîné des perturbations majeures dans ses activités. Elle a été contrainte de mettre ses systèmes informatiques hors service et de contacter plusieurs organismes pour signaler l'incident et recevoir une assistance technique.

Date : 15 juillet 2024	**Entrée :** #1
Description	L'incident de cybersécurité s'est produit lors de la phase de détection et d'analyse, ainsi que lors de la phase de confinement, d'éradication et de récupération.
Outil(s) utilisé(s)	Aucun
QQQOP	• **Qui a causé l'incident ?** Un groupe organisé de hackers. • **Qu'est-il arrivé ?** Rançongiciel. Les employés ne pouvaient plus utiliser leurs ordinateurs pour accéder à des fichiers tels que les dossiers médicaux, les opérations commerciales ont été interrompues, des notes de rançon ont été laissées. • **Quand l'incident s'est-il produit ?** Mardi matin, le 15 juillet 2024. • **Où l'incident a-t-il eu lieu ?** Dans une entreprise du secteur de la santé.

	• **Pourquoi l'incident s'est-il produit ?** L'incident a eu lieu lorsque les attaquants ont accédé au réseau de l'entreprise via des e-mails de phishing. Ces e-mails contenaient des pièces jointes malveillantes téléchargées par les employés. Peu de temps après leur téléchargement, le rançongiciel s'est déployé, cryptant les fichiers critiques et provoquant des perturbations majeures dans les opérations de l'entreprise. Ils exigent maintenant une rançon en échange de la clé de déchiffrement.
Autres remarques	• **Comment l'entreprise de santé pourrait-elle prévenir un tel incident à l'avenir ?** En renforçant la formation et la sensibilisation aux e-mails de phishing. • **L'entreprise doit-elle payer la rançon pour récupérer la clé de déchiffrement ?** Non, cela ne garantit pas la récupération des données et pourrait encourager d'autres activités criminelles.

Réflexions et notes :

- Le type d'incident de sécurité qui a affecté l'organisation est un rançongiciel via du phishing.
- La cause principale de l'incident est les e-mails de phishing. L'attaquant a utilisé les pièces jointes malveillantes par e-mail comme vecteur d'attaque. Une fois la pièce jointe cliquée par le destinataire, le rançongiciel se déployait.
- Offrir plus de formation et d'éducation pourrait résoudre ces problèmes. Sauvegarder les données de manière sécurisée pour les protéger contre le chiffrement par rançongiciel. Isoler les systèmes infectés du réseau pour empêcher la propagation du rançongiciel. Parfois, des entreprises de cybersécurité peuvent proposer des outils de déchiffrement pour des rançongiciels spécifiques. Communiquer avec les parties prenantes concernées. Si possible, signaler l'incident aux autorités.

Scénario 1 (suite)

Suite à l'incident de rançongiciel survenu le 15 juillet 2024, la petite clinique américaine spécialisée dans les soins de santé primaires a continué à rencontrer des défis liés à la cybersécurité. Après avoir isolé et récupéré certains systèmes, un nouvel outil d'analyse de trafic réseau a été mis en place pour surveiller toute activité suspecte et éviter une nouvelle attaque.

Mon rôle a été de mener une analyse approfondie du réseau pour identifier la source de l'attaque, enquêter sur d'éventuelles communications malveillantes encore actives et vérifier que le réseau est désormais sécurisé. Pour ce faire, j'ai utilisé **Wireshark** pour analyser un fichier de capture de paquets.

Date: 20 août 2024	Entrée: #2
Description	Enquêter sur d’éventuelles communications malveillantes encore actives et vérifier que le réseau est désormais sécurisé
Outil(s) utilisé(s)	**Wireshark**, un analyseur de protocoles réseau, pour surveiller et analyser le trafic réseau de la clinique. Cet outil permet d'examiner les paquets échangés au sein du réseau et d'identifier les anomalies
QQQOP	● **Qui :** Un groupe organisé de hackers, les mêmes que dans l'incident initial. ● **Quoi :** Le réseau de la clinique a continué à montrer des signes de tentatives de connexion suspectes, probablement liées à l'attaque précédente. ● **Où :** Le réseau interne de la clinique, où l'analyse des paquets a été réalisée. ● **Quand :** 20 août 2024, soit un mois après la première attaque. ● **Pourquoi :** Le premier incident de rançongiciel a souligné la vulnérabilité de la clinique face aux attaques par phishing et à la compromission du réseau. Wireshark a été utilisé pour analyser les paquets réseau et identifier toute activité malveillante résiduelle ou toute nouvelle tentative d'intrusion.
Résolution de l'incident	● **Analyse du fichier de capture avec Wireshark :** Après avoir importé les fichiers de capture dans Wireshark, j'ai commencé par filtrer le trafic réseau pour isoler les connexions suspectes, en ciblant principalement les communications en provenance ou à destination d’adresses IP inconnues ou suspectes. J'ai également recherché des paquets contenant des logiciels malveillants potentiels ou des tentatives de communication avec les serveurs de commande et de contrôle (C&C). ● **Identification des tentatives d'accès malveillantes :** Durant l’analyse, j'ai identifié plusieurs tentatives de connexion provenant de serveurs externes non reconnus. Ces tentatives semblaient être liées aux pirates responsables de la première attaque, qui tentaient de rétablir leur accès au réseau de la clinique. Heureusement, l'analyse des paquets a révélé que ces tentatives échouaient, car les systèmes avaient été mis hors ligne et renforcés après l'attaque initiale.

	• **Blocage des adresses IP suspectes :** Après avoir identifié les adresses IP des serveurs malveillants, j'ai pris des mesures immédiates en bloquant toutes les connexions réseau à ces adresses via le pare-feu de l'entreprise. Cela a permis de sécuriser davantage le réseau et de prévenir toute future communication avec les pirates.
Autres remarques	• **Prévention pour l'avenir :** J'ai également recommandé l'intégration de mesures de sécurité supplémentaires, comme la mise en place d'une segmentation réseau plus stricte et l'utilisation d'une solution de détection des intrusions (IDS) pour surveiller activement le trafic réseau et identifier toute activité suspecte en temps réel. • **Formation du personnel :** L'incident initial avait montré un manque de sensibilisation du personnel aux risques liés aux e-mails de phishing. Pour cette raison, j'ai proposé des séances de formation régulières sur la détection des tentatives de phishing et sur la gestion des cybermenaces. Cette formation devrait également inclure des exercices simulant des attaques de phishing pour renforcer la vigilance des employés. • **Conclusion :** L'utilisation de Wireshark pour analyser les paquets réseau a permis de détecter des tentatives de communication malveillantes toujours actives après l'attaque initiale. En bloquant les adresses IP suspectes et en renforçant la sécurité du réseau, la clinique a pu sécuriser ses systèmes et prévenir une nouvelle intrusion. L'intégration de mesures de formation pour le personnel et de solutions de surveillance réseau en temps réel garantira une meilleure protection à l'avenir. Grâce à cette analyse, la clinique a pu reprendre ses activités sans payer la rançon et avec des systèmes plus sécurisés.

Réflexions et notes :

- **Combien d'entrées y a-t-il jusqu'à présent ?** Il y a 2 entrées à ce jour.
- **Le type d'incident de sécurité** : L'organisation a été victime d'un rançongiciel distribué via des e-mails de phishing. Ce deuxième scénario concerne l'analyse du trafic réseau

pour détecter d'éventuelles tentatives d'intrusion résiduelles.

- **Cause principale de l'incident :** Le premier incident a été provoqué par des e-mails de phishing contenant des pièces jointes malveillantes, tandis que ce deuxième incident montre que des tentatives de connexion malveillantes persistaient, probablement en lien avec le groupe de hackers responsable.
- **Analyse réseau :** L'utilisation de Wireshark a été essentielle pour identifier les communications suspectes. Bien que l'outil ait été complexe à utiliser au départ, il s'est avéré très efficace pour surveiller et analyser le trafic réseau.
- **Résolution :** Le blocage des adresses IP malveillantes et le renforcement des pare-feu ont aidé à protéger le réseau de la clinique. Une segmentation réseau stricte et une surveillance active du réseau aideront à prévenir de futurs incidents similaires.
- **Mesures préventives :** Une formation plus poussée des employés concernant les attaques de phishing, la sensibilisation aux cybermenaces et l'adoption de pratiques de sécurité robustes comme les sauvegardes régulières et les solutions de détection d'intrusions sont des priorités.
- **Réflexion personnelle :** Cette expérience m'a permis de comprendre l'importance de combiner la technologie et l'éducation des employés pour renforcer la sécurité organisationnelle. Wireshark, bien que complexe, s'est révélé être un outil très puissant, et cette première utilisation m'a donné envie de continuer à me perfectionner dans l'analyse du trafic réseau

Scénario 2

L'entreprise fictive **LèdighTech Solutions**, spécialisée dans la gestion des dossiers médicaux électroniques, a rencontré des ralentissements sur son réseau interne. L'équipe de sécurité a suspecté une attaque externe ou une fuite de données. J'ai été chargé de capturer et d'analyser le trafic réseau à l'aide de **tcpdump** pour identifier la source de ces perturbations.

Date: 26 juillet 2024	Entrée: #1
Description:	Découvrir la cause des ralentissements et de vérifier s'il y avait des tentatives d'exfiltration de données vers des adresses IP externes
Outil(s) utilisé(s)	**Tcpdump**, un puissant outil d'analyse de paquets en ligne de commande, utilisé pour capturer le trafic réseau, examiner les paquets circulant sur le réseau et diagnostiquer les problèmes de sécurité.
QQQOP	• **Qui :** Les utilisateurs internes et systèmes de LèdighTech Solutions. • **Quoi :** Capture et analyse de paquets réseau pour identifier d'éventuelles fuites de données ou activités malveillantes. • **Où :** Réseau interne de LèdighTech

	Solutions. ● **Quand :** 26 juillet 2024. ● **Pourquoi :** Des ralentissements inhabituels du réseau ont été signalés, soulevant des soupçons d'attaques externes ou de fuites de données.

Résolution de l'incident	● **Capture du trafic réseau avec tcpdump :** J'ai commencé par capturer l'ensemble du trafic réseau sur l'interface principale (`eth0`) des serveurs de MediTech Solutions à l'aide de la commande suivante :
	`sudo tcpdump -i eth0`
	Cela a permis de visualiser le trafic réseau en temps réel, révélant un nombre important de connexions vers une adresse IP externe inconnue, ce qui suggérait une possible fuite de données.
	● **Filtrage des paquets liés à l'adresse IP suspecte :** Pour isoler les communications suspectes vers cette adresse IP externe, j'ai utilisé la commande suivante pour filtrer spécifiquement le trafic vers et depuis l'IP suspecte :
	`sudo tcpdump -i eth0 host 203.0.113.50`
	Cela a confirmé que de nombreuses requêtes et réponses réseau étaient envoyées à cette adresse, ce qui était inhabituel pour le fonctionnement normal de l'entreprise.
	● **Exportation des paquets pour analyse détaillée :** Pour une analyse plus approfondie des paquets, j'ai capturé les données dans un fichier `.pcap` afin de pouvoir les analyser plus tard :
	`sudo tcpdump -i eth0 host 203.0.113.50 -w suspect_traffic.pcap`
	● **Analyse manuelle des paquets capturés :** J'ai ensuite ouvert ce fichier de capture pour analyser les paquets en utilisant une commande `tcpdump` supplémentaire :

	`sudo tcpdump -r suspect_traffic.pcap`
	J'ai pu identifier des données chiffrées qui semblaient correspondre à des dossiers médicaux en cours d'exfiltration, indiquant une tentative de fuite de données.
	● **Blocage de l'adresse IP malveillante :** Après avoir confirmé que l'adresse IP 203.0.113.50 était malveillante, j'ai immédiatement bloqué cette adresse dans le pare-feu de MediTech Solutions à l'aide de la commande suivante pour empêcher toute communication supplémentaire :
	`sudo ufw deny from 203.0.113.50`
	● **Isolation des systèmes compromis :** Les serveurs qui avaient été utilisés pour exfiltrer des données ont été mis en quarantaine pour éviter toute propagation ou exploitation ultérieure. J'ai recommandé de les analyser plus en profondeur pour détecter la faille de sécurité exploitée par les attaquants.

Autres remarques	L'utilisation de **tcpdump** a été essentielle pour identifier les paquets malveillants en temps réel et permettre de réagir rapidement à une tentative de fuite de données. Cet outil, bien que puissant, nécessite une bonne maîtrise des filtres pour isoler les paquets pertinents, surtout lorsque le trafic est volumineux.

Réflexions et notes :

- **Défis rencontrés :** La capture de trafic réseau en temps réel avec tcpdump peut générer une grande quantité de données. Le filtrage adéquat et l'utilisation de commandes spécifiques sont essentiels pour éviter de se noyer dans des informations inutiles.
- **Importance de la vigilance continue :** Ce scénario montre l'importance d'une surveillance réseau proactive dans un environnement où des données sensibles sont en jeu, comme dans une entreprise de santé. L'utilisation de tcpdump pour détecter des anomalies m'a permis de découvrir la tentative d'exfiltration avant qu'elle ne cause des dommages irréversibles.
- **Apprentissages :** Cette activité a renforcé mes compétences en analyse réseau, en particulier dans l'utilisation d'outils de ligne de commande tels que tcpdump. Cela a également mis en évidence l'importance de la segmentation réseau et des pare-feu pour prévenir les fuites de données.

Scénario 3

En tant qu'analyste SOC de niveau 1, j'ai reçu une alerte du système de détection d'intrusion (IDS) à 13 h 20 concernant un fichier suspect détecté sur l'ordinateur d'un employé dans une société de services financiers. Le fichier provenait d'une pièce jointe malveillante dans un e-mail, et son hachage SHA-256 (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) avait été signalé par les systèmes de sécurité. Ma tâche consistait à utiliser VirusTotal pour vérifier si ce fichier représentait une menace réelle et à coordonner les actions nécessaires pour protéger le réseau.

Date: 30 août 2024	Entrée: #1
Description	Enquêter sur un hachage de fichier suspect.
Outil(s) utilisé(s)	**VirusTotal**, un service en ligne d'analyse de fichiers et d'URL qui permet de vérifier rapidement si un indicateur de compromission (fichier ou URL) a été signalé comme malveillant.
QQQOP	• **Qui** : un acteur malveillant inconnu • **Quoi** : un courrier électronique envoyé à un employé contenait une pièce jointe malveillante dont le code SHA-256 est 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. • **Où** : l'ordinateur d'un employé d'une société de services financiers • **Quand** : à 13 h 20, une alerte a été envoyée au SOC de l'entreprise après que le système de détection d'intrusion a détecté le fichier • **Pourquoi** : un employé a pu télécharger et exécuter une pièce jointe malveillante par courrier électronique.
Résolution de l'incident	• **Analyse du hachage avec VirusTotal :** J'ai copié le hachage SHA-256 du fichier suspect et l'ai recherché sur **VirusTotal**. Ce dernier a comparé le hachage avec sa base de données et m'a fourni un rapport détaillé indiquant que le fichier avait été signalé comme un cheval de Troie par plusieurs moteurs antivirus. • **Validation des résultats :** VirusTotal a confirmé que la pièce jointe malveillante détectée correspondait à une menace bien connue, utilisée pour exfiltrer des données financières sensibles. Le fichier était marqué

	comme dangereux par une majorité de moteurs de sécurité. ● **Isolement de l'ordinateur :** Après avoir confirmé la nature malveillante du fichier, l'ordinateur de l'employé a été immédiatement isolé du réseau pour prévenir toute propagation de la menace. Une procédure de nettoyage complet a été lancée. ● **Blocage et alerte :** Le hachage du fichier a été ajouté à la liste de menaces bloquées de l'entreprise. De plus, j'ai mis en place une règle de sécurité pour empêcher l'exécution de tout fichier contenant ce hachage et notifié les équipes techniques pour surveiller toute activité suspecte liée à ce fichier.
Autres remarques	Pour éviter que ce type d'incident ne se reproduise, il est crucial de renforcer la **formation à la sécurité des employés**, en particulier sur la reconnaissance des e-mails de phishing. L'organisation devrait envisager d'implémenter des simulations régulières de phishing pour éduquer le personnel sur les risques potentiels et les mesures à prendre.

Réflexions et notes :

- **Importance de l'outil VirusTotal :** L'utilisation de VirusTotal a permis une détection rapide de la menace, offrant un moyen fiable de confirmer la gravité de l'incident.
- **Formation continue des employés :** Ce type d'incident met en lumière la nécessité de **former les employés** à reconnaître les signes d'un e-mail de phishing. Une meilleure sensibilisation pourrait empêcher de futurs incidents.
- **Réactivité et protection :** En isolant rapidement l'ordinateur et en bloquant la menace au niveau du réseau, nous avons pu éviter des dommages plus importants et protéger les données sensibles de l'entreprise.