SOPHOS

Guide Sophos de planification de la réponse aux incidents

Sommaire

Introduction

Ce document est conçu pour fournir une vue d'ensemble des bonnes pratiques en matière de réponse aux incidents, en guidant l'examen des cybermenaces dans leurs aspects techniques et organisationnels. Ce guide a pour but d'aider les entreprises à mettre en place des processus efficaces de réponse aux incidents.

Destiné aux professionnels de la sécurité informatique exerçant des fonctions techniques ou organisationnelles, ainsi qu'aux débutants sans expérience en cybersécurité, ce guide sert d'introduction au processus de réponse aux incidents. Notez toutefois que vous n'y trouverez pas d'informations détaillées concernant le cadre juridique ou règlementaire de la gestion de la sécurité. Ce guide doit être utilisé comme un document complémentaire aux lignes directrices applicables à votre entreprise en matière de déclaration des incidents de sécurité et de réponse apportée. Notez par ailleurs que les recommandations suggérées dans ce guide pourraient différer des conditions spécifiées dans votre contrat de cyberassurance — veillez donc à vérifier soigneusement votre police d'assurance.

Une préparation efficace aux cyberincidents permet aux entreprises de s'appuyer sur des protocoles et des procédures établis pour réagir, assigner et contenir les risques plus rapidement. L'objectif de ce document est de vous aider à préparer votre stratégie de gestion des incidents pour vous permettre de neutraliser les menaces plus rapidement, et ainsi de réduire les répercussions financières et organisationnelles sur votre entreprise.

Nous encourageons les professionnels de la sécurité à intégrer ces concepts et méthodes d'investigation dans leurs propres stratégies et processus de réponse aux incidents. Ce guide peut être lu du début à la fin ou de manière sélective, en se concentrant sur le ou les chapitres les plus pertinents pour le lecteur. Plutôt que d'offrir un plan définitif, étape par étape, il est destiné à aider les équipes de sécurité à élaborer et à mettre en place leurs propres processus de réponse aux incidents.

Les phases de gestion des incidents définies dans ce guide se conforment au cadre de réponse aux incidents SANS (Systems Administration and Network Security), qui comporte six étapes distinctes. L'objectif du cadre SANS est de mettre l'accent sur chaque étape du cycle afin d'aider les professionnels de la sécurité à se préparer à répondre efficacement aux incidents. Toutefois, veuillez noter qu'il ne s'agit pas d'un manuel pratique. Bien que ces cadres vous permettront de mieux structurer votre stratégie de réponse aux incidents, rappelez-vous qu'étant donné le caractère dynamique des attaques de cybersécurité, ceux-ci ne remplaceront jamais l'expertise d'un professionnel ou l'évaluation d'une menace par le personnel chargé de la sécurité.

Préparation

La première étape du cycle de réponse aux incidents est la phase de préparation. Les actions entreprises durant cette phase influenceront considérablement l'efficacité des étapes suivantes. La phase de préparation est donc non seulement cruciale, mais elle doit également être revue et mise à jour régulièrement. Cette phase inclut des éléments non techniques (processus et procédures), ainsi que des éléments techniques (durcissement des systèmes, collecte de données télémétriques et formation). Une stratégie de réponse aux incidents robuste et pérenne se construit en accordant suffisamment de temps et de ressources à la phase de préparation.

Processus et procédures

L'efficacité de l'équipe de réponse aux incidents repose sur une documentation claire des processus et procédures. En formant le personnel chargé du traitement des incidents de manière adéquate, vous garantirez l'intégrité des informations et la cohérence des objectifs des collaborateurs. Des processus et procédures bien définis permettront à l'équipe de répondre de manière systématique, faciliteront la communication entre collaborateurs et contribueront à une réponse plus rationnelle et coordonnée.

Plan de traitement des incidents

Un plan de traitement des incidents efficace établit des procédures claires et fournit aux personnes concernées tous les conseils nécessaires à une bonne gestion de l'incident. Intégrez les éléments suivants à votre plan afin d'obtenir une approche complète de la réponse aux incidents :

- **Définition du rôle des collaborateurs :** Nommez tous ceux qui participeront au processus de traitement des incidents et attribuez-leur un rôle : responsable du dossier de l'incident, équipe IT supplémentaire, coordinateurs et directeurs, intervenants tiers (fournisseurs de services informatiques et juridiques, fournisseurs de services de réponse aux incidents), etc.
- **Classement des incidents par type et niveau de gravité :** Définissez des critères de classement basés sur des facteurs tels que l'impact potentiel, les systèmes affectés et le type de menace. Les niveaux de gravité ainsi définis permettront de prioriser et de guider la réponse aux incidents.
- **Procédures d'escalade :** Définissez des procédures d'escalade claires pour les incidents qui dépassent les capacités ou l'autorité des premiers intervenants, notamment en faisant appel à des niveaux de gestion plus élevés ou en faisant appel à des experts externes si nécessaire.
- **Plan de communication :** Pour assurer une communication efficace lors d'un incident, utilisez des modèles de communication prédéfinis destinés au personnel, aux clients et aux partenaires. Envisagez également d'intégrer des pratiques propres aux plans de reprise des activités afin de mettre en place des canaux de communication alternatifs pour les emails, la messagerie instantanée ou la visioconférence.
- **Inventaire des ressources :** Tenez à jour un inventaire des ressources matérielles et logicielles de l'entreprise pour assurer le suivi et une bonne gestion. Ce type d'information est déterminant pour évaluer l'étendue et l'impact d'une menace, et les mesures à prendre pour y répondre.
- **Chronologie de la réponse aux incidents :** Pour assurer une réponse rapide et organisée, créez un plan chronologique pour chaque phase du processus de réponse aux incidents, avec des délais limites pour les étapes clés.
- **Documentation et journalisation des incidents :** Standardisez la manière dont vous documentez tous les aspects d'un incident, comme les actions effectuées, les décisions prises et les résultats obtenus. Cette documentation s'avérera cruciale au moment de l'analyse post-incident ou en cas d'audit juridique ou règlementaire.
- **Analyses après action et amélioration continue des processus :** Instaurez un processus d'analyses après action (After-Action Reviews) afin d'évaluer l'efficacité de la réponse et d'identifier les points à améliorer. Utilisez ces informations pour mettre à jour et améliorer le plan de traitement des incidents si nécessaire.

En incorporant tous les éléments ci-dessus dans votre plan de traitement des incidents, vous serez mieux équipé pour gérer et répondre aux incidents de cybersécurité.

Documentation juridique

Au cours de la phase de préparation, les entreprises doivent se pencher sur les responsabilités juridiques liées à la déclaration des incidents, aux règlementations relatives au traitement des incidents et à d'autres aspects relatifs à la cybersécurité. Les sections suivantes illustrent certaines considérations juridiques courantes, mais chaque entreprise doit procéder à une analyse complète des exigences règlementaires propres à son secteur d'activité et à son lieu d'implantation. Identifiez les personnes responsables du rapport aux autorités et du respect de la législation au sein de l'entreprise et incluez-les en tant que parties prenantes dans le plan de réponse aux incidents, avec des rôles clairement définis.

- **Responsabilités légales et règlementaires en matière de déclaration :** Certaines entreprises peuvent être légalement tenues ou encouragées de notifier les incidents en fonction de leur secteur d'activité ou de leur statut.
  - Entreprises du secteur des infrastructures critiques
  - Agences gouvernementales
  - Entreprises cotées en bourse
- **Confidentialité des données :** Respectez les lois sur la protection des données qui imposent une déclaration transparente aux agences de la commission de l'information et aux clients ou individus concernés dont les droits en matière de données peuvent être compromis.
- **Conservation et destruction des données :** Établissez des politiques et des procédures pour la conservation, le stockage et la destruction sécurisée des données collectées lors des activités de réponse aux incidents, dans le respect des lois et règlements applicables.
- **Accords et contrats avec de tierces parties :** Examinez soigneusement les contrats et accords signés avec vos éditeurs de logiciels, fournisseurs et partenaires pour mieux comprendre leurs obligations en matière de réponse aux incidents et de déclaration en cas d'incidents de sécurité.
- **Protection de la propriété intellectuelle (PI) :** Penchez-vous sur les aspects juridiques de la protection de la propriété intellectuelle de l'entreprise : secrets commerciaux, brevets, copyright et marques déposées avant et après un incident de cybersécurité.
- **Transfert transfrontalier des données et journalisation :** Si votre entreprise opère à l'échelle internationale, tenez compte des implications juridiques et des exigences liées au transfert et à la déclaration des données dans différentes juridictions.
- **Droits et responsabilités des employés :** Décrivez les droits et responsabilités des employés en cas de cyber incidents, y compris leurs obligations de signaler les incidents et de protéger les informations sensibles.
- **Polices d'assurance :** Comprenez la procédure et les exigences relatives à une demande d'indemnisation au titre de la cyberassurance.
  - Lisez attentivement les conditions générales pour savoir ce qui est couvert et ce qui ne l'est pas.
  - Consultez les souscripteurs internes pour s'assurer de la bonne compréhension de la couverture.

Manuels de réponse aux incidents

L'élaboration de manuels de réponse aux incidents permet de mettre en place des actions précises à suivre en cas d'incident. Ces manuels devraient être élaborés sur la base d'une approche fondée sur les risques, en tenant compte de la probabilité et de l'impact potentiel de divers scénarios d'attaque. Prenez en compte les éléments suivants lors de l'élaboration de vos manuels de réponse aux incidents :

- **Contenu personnalisé :** Veillez à développer des manuels qui s'adaptent spécifiquement aux besoins, aux ressources et aux capacités de réponse de votre entreprise. Par exemple, prenez en compte la taille, le secteur d'activité et les risques propres à votre entreprise.
- **Menaces et scénarios spécifiques :** Pour les entreprises plus matures, il est recommandé d'élaborer des plans d'action pour des menaces spécifiques, telles que certains types de logiciels malveillants ou d'attaques ciblées. En revanche, si votre entreprise a des ressources plus limitées, développez un manuel plus général couvrant une multitude de cas de figure différents.
- **Instructions claires et concises :** Chaque étape du processus de réponse doit être décrite de manière claire et concise dans le manuel. Cela permettra au personnel de comprendre et d'exécuter rapidement les actions nécessaires lors d'un incident.
- **Rôles et responsabilités :** Définissez clairement les rôles et responsabilités de tous les membres impliqués dans le processus de réponse aux incidents. Cela permettra à chacun de savoir ce que l'on attend de lui et de collaborer efficacement.

- **Communication et escalade :** Prévoyez des lignes directrices pour la communication et les procédures d'escalade, par exemple pour savoir quand avertir la direction ou faire appel à une aide extérieure.
- **Intégration avec le plan de traitement des incidents :** Faites en sorte que vos manuels s'alignent sur votre plan de traitement des incidents et soutiennent sa mise en pratique. Cela vous permettra de maintenir l'homogénéité et la cohérence de vos efforts de réponse aux incidents.
- Actualisations et révisions régulières : Il convient de revoir et d'actualiser régulièrement les manuels afin de s'assurer qu'ils restent pertinents et efficaces face à l'évolution des menaces et des circonstances de l'entreprise.

En incorporant ces éléments dans vos manuels de réponse aux incidents, vous serez en mesure de répondre plus efficacement à une multitude d'incidents de cybersécurité et de réduire leur impact potentiel sur l'entreprise.

Sauvegardes

Un plan de sauvegarde efficace est essentiel à la continuité des activités de l'entreprise et permet de réduire l'impact d'une fuite de données accidentelle ou résultant d'une défaillance du système ou d'une attaque. La mise en œuvre d'une stratégie de sauvegarde solide implique la création et la validation de sauvegardes régulières, ainsi que le choix d'une variété d'options de stockage pour maximiser la disponibilité des données. Prenez en compte les éléments suivants lors de l'élaboration d'une stratégie de sauvegarde :

- **Fréquence de sauvegarde :** Déterminez la fréquence optimale de création des sauvegardes en considérant l'importance des données en question et le degré de risque acceptable. Des sauvegardes régulières vous permettront de réduire l'impact potentiel d'une fuite des données.
- **Types de sauvegarde :** Optimisez l'espace de stockage et facilitez la récupération des données en utilisant une combinaison de sauvegardes complètes, incrémentielles et différentielles.
- **Options de stockage :** Utilisez plusieurs types de stockage différents : local, Cloud et hors ligne. Cela vous permettra de garantir la disponibilité des données et d'éviter la perte de données due à l'utilisation d'un unique point de stockage.
- **Priorisation des données critiques :** Sauvegardez en priorité les données et les systèmes critiques qui sont essentiels au maintien des opérations et au soutien des processus clés de l'entreprise.
- **Chiffrement des sauvegardes :** Chiffrez les sauvegardes pour protéger les données sensibles et empêcher tout accès non autorisé durant leur transfert et leur stockage.
- **Validation des sauvegardes :** Validez régulièrement vos sauvegardes afin de vérifier leur fiabilité et de permettre la restauration des données en cas de besoin. Testez par exemple le processus de restauration et vérifiez l'intégrité des données sauvegardées.
- **Politiques de conservation des données :** Mettez en place des politiques de conservation des données qui permettent de gérer le stockage et la suppression des sauvegardes conformément aux exigences légales, règlementaires et commerciales.
- **Plan de reprise après sinistre :** Intégrez votre stratégie de sauvegarde au plan global de reprise après sinistre de votre entreprise pour garantir une réponse coordonnée et efficace en cas de perte de données.

En incorporant ces éléments à votre stratégie de sauvegarde, vous serez en mesure de vous remettre plus facilement après un incident.

Durcissement du système et du réseau

Le durcissement du système et du réseau consiste à réduire la surface d'attaque en limitant les fonctionnalités, les accès aux systèmes et les connexions au réseau. La mise en œuvre de pratiques de durcissement efficaces permettra à votre entreprise de réduire le risque de réussite d'une attaque. Prenez en compte les aspects suivants lors de l'élaboration d'une stratégie de durcissement du système et du réseau :

Correctifs

- **Programme de gestion des correctifs :** Élaborez un programme visant à assurer l'application régulière des correctifs sur les actifs de votre réseau, en utilisant une combinaison d'outils de correction automatisés ou semi-automatisés.
- **Documentation :** Tenez un registre des correctifs appliqués, ainsi que des exclusions effectuées.
- **Priorisation :** Planifiez les correctifs en fonction des risques, en corrigeant en priorité les vulnérabilités les plus dangereuses pour l'entreprise.

Configuration

- **Audit de conformité de la sécurité :** Réalisez fréquemment des audits internes et externes pour vérifier la configuration et les paramètres appropriés des outils de sécurité, en identifiant et en corrigeant toute configuration erronée ou toute exclusion.
- **Contrôle des applications :** Utilisez des listes d'autorisation et de blocage afin de limiter le nombre et les versions d'applications qui peuvent être exécutées sur les hôtes, afin de réduire le risque d'exploitation de logiciels non autorisés ou vulnérables.
- **Contrôle d'accès réseau :** Configurez les outils réseau pour restreindre l'accès aux adresses IP et aux ports aux seuls hôtes internes ou externes qui en ont besoin, afin de réduire les risques d'accès non autorisés et d'exfiltration des données.
- **Principe de moindre privilège :** Veillez à ce que vos utilisateurs aient uniquement accès aux outils nécessaires à l'exercice de leurs fonctions. Cela vous permettra de réduire les risques d'accès non autorisés et de compromission des données.

Sécurité du réseau

- **Segmentation du réseau :** Divisez votre réseau pour créer des segments isolés les uns des autres afin de limiter l'impact potentiel d'une violation de sécurité et d'empêcher l'attaquant de se déplacer latéralement sur le réseau.
- **Configuration du pare-feu :** Configurez les pare-feux de manière à bloquer tout trafic entrant ou sortant inutile. Révisez et mettez à jour régulièrement vos règles afin de maintenir une posture de sécurité optimale.
- **Systèmes de détection et de prévention des intrusions (IDPS) :** Déployez un système IDPS pour surveiller le trafic réseau afin de détecter les signes d'activité malveillante et de prendre les mesures appropriées.

Surveillance et télémétrie

La surveillance et la collecte de données télémétriques sont essentielles à l'élaboration d'une stratégie de réponse aux incidents efficace. Celles-ci offrent un aperçu précieux de l'environnement de l'entreprise et permettent une détection précoce des menaces. En apprenant à connaître votre environnement et en mettant en place des couches de détection et de défense appropriées, vous pouvez améliorer votre capacité à répondre aux incidents de manière efficace.

Votre environnement

Comprendre son environnement est la base d'une stratégie de surveillance et de télémétrie efficace. Cette approche comprend :

- Inventaire des ressources : Tenez un inventaire à jour de vos postes et de vos serveurs, ainsi que des plateformes de sécurité qui les protègent.
- Topologie du réseau : Apprenez à connaître votre réseau et notamment les points d'entrée et de sortie du trafic, la segmentation et les points de contrôle. Aidez-vous de préférence d'un diagramme pour plus de clarté.

Couches de détection et de défense

Une stratégie de sécurité complète se compose de plusieurs couches de détection et de défense. Considérez les sources télémétriques suivantes et veillez à ce qu'elles soient horodatées de façon cohérente, de préférence à la norme UTC :

- **Appareils de périphérie :** pare-feux, systèmes de prévention des intrusions (IPS), systèmes de détection des intrusions (IDS), VPN et proxys.
- **Protection Endpoint :** antivirus (AV), antivirus Next-Gen (NGAV), technologies Endpoint/Extended Detection and Response (E/XDR).
- **Journalisation centralisée :** outils de sécurité des informations et de gestion des évènements (SIEM), serveurs Syslog, stockage des données Cloud.
- **Authentification :** services d'authentification multifacteur (MFA) et services de gestion des accès (IAM).
- **Renseignements sur les menaces :** renseignements stratégiques (corrélation des informations et suivi de la marque) visant à surveiller l'exposition externe de l'entreprise.

Outils et techniques de surveillance

Une stratégie de détection et de réponse aux incidents efficace repose sur le choix de bons outils et techniques de surveillance. Considérez les approches suivantes :

- **Surveillance continue :** Déployez des tactiques de surveillance à la fois continues et périodiques pour obtenir une vision claire de l'environnement.
- **Détection des anomalies :** Utilisez des techniques d'analyse avancées et des algorithmes de Machine Learning pour identifier les comportements et modèles anormaux susceptibles d'indiquer la présence d'une menace potentielle.

- **Corrélation des journaux :** Agrégez et corrélez les données de log provenant de différentes sources afin d'identifier les modèles et tendances susceptibles d'indiquer la présence d'une attaque.
- **Priorisation des alertes :** Développez un processus permettant de prioriser les alertes en fonction de facteurs tels que la gravité de l'incident, son impact potentiel et le niveau de menace.

En apprenant à connaître votre environnement, en mettant en place des couches de détection et de défense robustes et en déployant des outils et techniques de surveillance adéquats, vous renforcerez considérablement votre capacité à répondre rapidement et efficacement aux incidents de sécurité.

Communication

Il est essentiel que le processus de réponse aux incidents soit accompagné d'une stratégie de communication bien définie afin d'assurer la bonne coordination des opérations et une collaboration efficace au sein de l'équipe. Cette section décrit les éléments clés à prendre en compte en matière de communication interne et externe, en tenant compte des exigences règlementaires.

Communication interne

- **Plan de communication :** Élaborez un plan de communication détaillé qui couvre les méthodes d'escalade des problèmes, les canaux de communication autorisés et les points de contact principaux. Ce plan doit être revu et mis à jour périodiquement afin de garantir son efficacité en cas d'incident.
- **Équipe de réponse aux incidents :** Constituez une équipe de réponse aux incidents (IRT) et nommez un chef d'équipe chargé de coordonner les opérations. Assurez-vous que tous les membres de l'équipe comprennent leurs rôles et responsabilités et sont capables de communiquer efficacement tout au long de l'incident.
- **Canaux sécurisés :** Utilisez des canaux de communication sécurisés et fiables afin d'éviter que des personnes non autorisées n'accèdent à vos données sensibles. Envisagez l'utilisation d'applications de chiffrement des messages, de solutions de protection de la messagerie ou de plateformes de communication dédiées.
- **Modèles de réponse :** Créez une bibliothèque de modèles de réponse prédéfinis adaptés à différents types de scénarios. Cela permettra d'accélérer et de standardiser le processus de communication. Ces modèles devraient être facilement accessibles, personnalisables et alignés sur les directives de communication de l'entreprise.
- **Information des parties prenantes :** Informez régulièrement les parties prenantes tout au long du processus de gestion de l'incident, en incluant des rapports de situation, les mesures prises et les résultats escomptés. Ce niveau de transparence montrera que l'entreprise prend le traitement des incidents au sérieux.

Communication externe

- **Stratégie de déclaration :** Développez des stratégies de déclaration personnalisées visant à informer les clients, fournisseurs, partenaires et organismes d'application de la loi des violations ou autres incidents les concernant. Décrivez dans cette stratégie les critères de déclaration, les canaux appropriés et les membres en charge de la communication.
- **Conformité juridique et règlementaire :** Veillez à ce que vos communications externes respectent les lois et règlementations en vigueur (protection des données, divulgation responsable, etc.), ainsi que des lois concernant votre propre secteur industriel. Demandez à un conseiller juridique de confirmer que vos communications respectent toutes les directives appropriées.
- **Désignation d'un porte-parole :** Désignez un porte-parole ou une équipe de relations publiques chargés de répondre aux médias et de faire des déclarations publiques. Cela assurera la cohérence du message de l'entreprise. Attribuez ce rôle à un individu ou une équipe se spécialisant dans les communications de crise et les relations avec les médias.
- **Préparation aux communications externes :** Préparez un modèle adapté à chaque type d'incident pour veiller à la clarté de vos communiqués externes. Adaptez ces modèles au type de destinataire auxquels ils s'adressent : clients, partenaires et régulateurs.
- **Collaboration entre différents services de l'entreprise :** Travaillez étroitement avec le service juridique, le service de relations publiques et tout autre service concerné afin que vos communications externes soient conformes aux règlementations, protègent la réputation de l'entreprise et soient effectuées en toute transparence.

Ces stratégies de communication permettront à votre entreprise de répondre de manière efficace et coordonnée aux incidents de cybersécurité, et de démontrer sa capacité à traiter ce type d'incident avec sérieux.

Sensibilisation et formation à la sécurité

La sensibilisation des employés aux menaces et aux bonnes pratiques de cybersécurité est cruciale pour la posture de sécurité globale de l'entreprise. Dans cette section, nous nous penchons sur les éléments clés que doit contenir un programme de sensibilisation et de formation à la sécurité, notamment les initiatives de sensibilisation à adopter, le contenu et la fréquence des formations, les simulations d'incident et les exercices.

Programmes de sensibilisation à la sécurité

- **Objectifs du programme :** Fixez clairement les objectifs de votre programme de sensibilisation. Ceux-ci seront basés sur les connaissances et comportements que vous souhaitez faire adopter à vos employés afin de protéger les ressources et les données de l'entreprise.
- **Formation ciblée :** Concevez des supports de formation destinés à chaque service de l'entreprise, en tenant compte de leur accès aux données sensibles et des responsabilités de chacun.
- **Actualisation continue :** Revisitez régulièrement votre programme de sensibilisation à la sécurité en y incorporant les tendances et les bonnes pratiques les plus récentes afin qu'il reflète le contexte du moment.
- **Statistiques et évaluation :** Mesurez l'efficacité du programme de sensibilisation à la sécurité à l'aide d'indicateurs clés de performance (KPI), tels que l'engagement des employés, le taux de formations terminées et l'amélioration des comportements envers la sécurité.

Contenu et fréquence des formations

- **Conception du contenu :** Créez des contenus engageants et éducatifs qui couvrent un large éventail de sujets, comme la gestion des mots de passe, la sensibilisation au phishing, l'ingénierie sociale ou encore comment naviguez sur le net en toute sécurité.
- **Formation :** Proposez plusieurs formats de formation : en ligne, en personne, ou sous forme de webinaire interactif. Cela permettra de satisfaire les préférences et les emplois du temps de chacun.
- **Fréquence :** Répartissez les sessions de formation sur l'ensemble de l'année en prévoyant au minimum une session par trimestre. Organisez des sessions supplémentaires pour répondre à des incidents spécifiques ou à des menaces émergentes.
- **Formation continue :** Favorisez une culture de formation continue en mettant des ressources supplémentaires à la disposition des employés, comme des articles, des vidéos ou des podcasts. Cela renforcera leurs connaissances en matière de cybersécurité.

Simulation d'incidents et exercices

- **Scénarios réalistes :** Créez des simulations d'incidents et des exercices basés sur des situations que les employés sont susceptibles de rencontrer un jour. Ces scénarios réalistes les aideront à mieux comprendre l'impact potentiel d'une violation de sécurité et à s'exercer à y répondre.
- **Collaboration entre services :** Impliquez plusieurs services dans ces simulations pour encourager la collaboration et la communication entre des équipes ayant des spécialités différentes.
- **Évaluation et feedback :** Évaluez en détail les performances des employés durant les simulations et les exercices, afin de leur faire part de vos commentaires et des points à améliorer.
- **Assimilation des enseignements :** Communiquez les enseignements tirés des simulations à l'ensemble de l'entreprise pour renforcer les concepts clés et les bonnes pratiques.

Un programme robuste de sensibilisation et de formation à la sécurité vous permettra de transmettre à vos employés les connaissances et les compétences nécessaires pour détecter et répondre aux menaces de cybersécurité. Au final, vous réduirez le risque d'attaques graves.

Équipe de réponse aux incidents

Il est essentiel de nommer une équipe de réponse aux incidents pour gérer les menaces de cybersécurité rapidement et efficacement. Dans cette section, nous nous penchons sur les rôles et responsabilités des membres, la composition de l'équipe et l'importance du support et de l'expertise en matière de réponse aux incidents apportés par des intervenants externes.

Rôles et responsabilités

- **Responsable de la gestion des incidents :** Cette personne supervise le processus de réponse aux incidents, coordonne les activités de l'équipe, veille à l'efficacité de la communication entre les membres de l'équipe interne, ainsi qu'avec les collaborateurs externes.
- **Analystes de la sécurité :** Cette équipe recherche et analyse les incidents de sécurité, dispose des compétences nécessaires pour identifier la cause racine, l'étendue et l'impact de l'incident.
- **Analystes forensiques :** Cette équipe effectue des recherches digitales forensiques, notamment par la collecte, l'analyse et l'enregistrement des preuves qui permettront de soutenir les investigations et les recours juridiques.
- **Opérations informatiques :** Cette équipe soutient les efforts de confinement, d'éradication et de reprise en gérant l'infrastructure du système et en implémentant les changements nécessaires permettant de bloquer les attaques futures.
- **Juridique et conformité :** Cette équipe fixe le cadre juridique et règlementaire de la réponse aux incidents, en veillant à ce que les informations soient correctement divulguées et rapportées.
- **Relations publiques et communication :** Cette équipe gère les communications internes et externes, compose les messages destinés aux employés, aux clients, aux partenaires et aux régulateurs.

Composition de l'équipe de réponse aux incidents

- **Représentation transversale :** Formez une équipe diverse composée de représentants de plusieurs services différents, tels que les services IT, sécurité, juridique, RH, communication, afin de répondre au caractère multidisciplinaire de la réponse aux incidents.
- **Compétences et expertise :** Veillez à ce que les membres de l'équipe possèdent les compétences et l'expertise nécessaires à l'exercice de leurs fonctions, et fournissez-leur suffisamment d'opportunités de développement et de formation.
- **Disponibilité et rotation :** Assurez-vous que l'équipe soit disponible 24 h/24 et 7 j/7 en mettant en place des rotations de garde ou des équipes dédiées pour assurer une couverture continue.

Support et expertise externes

- **Éditeurs tiers :** Employez des experts externes (conseillers en cybersécurité, fournisseurs de services managés, etc.) pour supplémenter vos ressources internes et bénéficier de connaissances spécialisées sur des sujets tels que l'investigation numérique et les renseignements sur les menaces.
- **Conseillers juridiques :** Dotez-vous du soutien de conseillers juridiques externes experts en cybersécurité et en confidentialité des données. Ceux-ci pourront vous aiguiller sur la conformité et la déclaration des incidents et vous représenter en cas de procédure liée à un incident de sécurité.
- **Organismes chargés de l'application de la loi et de la règlementation :** Formez des liens privilégiés avec les organismes chargés de l'application de la loi et de la règlementation concernés, afin de faciliter la coopération et le partage d'informations lors des investigations sur les incidents.
- **Collaboration sectorielle :** Participez à des forums de cybersécurité spécifiques à votre secteur industriel et rejoignez des groupes de partage d'informations. Cela vous permettra d'échanger des renseignements sur les menaces et les bonnes pratiques à adopter afin de mieux lutter contre les menaces et les tendances émergentes.

En formant une équipe de réponse aux incidents bien structurée et en faisant appel à la bonne expertise externe, vous serez mieux équipé pour gérer les incidents de cybersécurité et réduire leur impact potentiel sur votre entreprise.

Identification

La phase d'identification est cruciale pour détecter une menace sur le réseau ou le système. Il est essentiel de surveiller en continu la télémétrie du réseau afin de réduire le temps entre l'intrusion et l'identification. Plus vite vous réagirez, plus vous limiterez l'impact de l'attaque sur la confidentialité, l'intégrité et la disponibilité des données, des systèmes et des réseaux. Les solutions MDR (Managed Detection and Response) peuvent accompagner ces efforts en vous fournissant des capacités de détection et de réponse managées avancées.

Composants clés de l'identification

- **Télémétrie du réseau et des appareils :** Afin de détecter et de répondre aux menaces en temps réel, il est essentiel de surveiller en continu plusieurs sources différentes, comme mentionné dans la section Télémétrie. Ce processus sera renforcé par la mise en place d'une solution MDR.
- **Notifications externes :** En collaborant avec les forces de l'ordre et d'autres sources externes afin de collecter et d'analyser les renseignements sur les menaces, vous identifierez plus rapidement les intrusions potentielles.
- **Renseignements sur les menaces :** La surveillance du Dark Web et des sites clandestins, pour identifier la vente de compromissions potentielles d'entreprises, améliore encore les capacités de détection.
- **Signalisation par les utilisateurs :** Encouragez les utilisateurs à signaler les emails ou liens suspects et à répondre rapidement aux menaces potentielles. Cela permettra à l'équipe de réponse aux incidents de prendre connaissance de toute situation critique dans les meilleurs délais.

Mettez en place des processus clairs de catégorisation des incidents basés sur le niveau de risque. Basez-vous sur les critères suivants :

- **Fiabilité :** Concerne la fiabilité de la source (par ex. IPS, FW, AV, XDR).
- **Criticité :** Prend en compte l'importance du système infecté au sein de l'environnement.
- **Malveillance :** Évalue les comportements suspects susceptibles d'indiquer la présence d'une violation jusqu'alors inconnue.
- **Type d'incident :** Classifiez les incidents en vous appuyant sur des cadres de référence tels que le Cyber Kill Chain et MITRE ATT&CK.
- **Horodatage :** Assurez la cohérence de l'horodatage en utilisant des normes communes, telles que UTC et NTP.

Types d'incidents

L'Institut national des normes et de la technologie américain, ou NIST, reconnait deux types d'incidents :

- **Incident précurseur :** Détectez les signes de reconnaissance, tels que les analyses lancées par le hacker pour identifier les ports ouverts et les failles logicielles. Les solutions MDR peuvent être particulièrement utiles dans ce contexte. Identifiez la présence d'exploits de vulnérabilités de code à distance connus dans l'infrastructure de l'entreprise.
- **Incident indicateur :** Identifiez les différents types d'incidents indicateurs, tels que les alertes de malwares, les modifications de fichiers ou d'Active Directory, les comportements utilisateur suspects (connexions via RDP à des heures inhabituelles, etc.), et lancez la réponse appropriée. Une solution MDR peut vous aider à détecter et à répondre à ce type d'incidents.

En mettant en œuvre une stratégie de surveillance complète, en exploitant les notifications externes et les renseignements sur les menaces, en encourageant les utilisateurs à signaler les problèmes et en utilisant des critères bien définis pour la catégorisation des incidents, les entreprises peuvent améliorer leur posture globale de sécurité. L'utilisation d'une solution MDR augmentera vos chances de détecter et de répondre efficacement aux incidents. La phase d'identification réduit non seulement l'impact des incidents de sécurité, mais favorise également une attitude proactive envers la sécurité. Vous préservez la continuité de vos activités et protégez vos ressources importantes.

Fichiers, annuaires, processus et mécanismes de persistance suspects

En comprenant et en identifiant les fichiers, annuaires, processus et mécanismes de persistance suspects, vous serez en mesure de détecter les incidents avant qu'ils ne puissent nuire.

- **Fichiers et annuaires :** Les fichiers et annuaires inhabituels ou situés dans des endroits inattendus pourraient être indicateurs d'un incident de sécurité. Par exemple :

- Les fichiers portant des extensions ou des noms inhabituels
- Les fichiers situés dans des endroits inattendus
- Les annuaires contenant des données sensibles qui, en temps normal, ne seraient pas accessibles

- **Processus :** Les processus suspects peuvent être indicateurs d'une activité malveillante sur le système. Par exemple :
  - Les processus avec une consommation élevée de la mémoire ou du processeur
  - Les processus s'exécutant depuis des emplacements inattendus
  - Les processus tentant d'accéder aux données ou aux ressources sensibles sur le réseau
- **Persistance :** Les attaquants mettent souvent en place des mécanismes servant à maintenir l'accès à un système compromis. Ces techniques peuvent inclure :
  - Des tâches programmées ou des tâches cron exécutant des scripts malveillants
  - Des malwares qui se réinstallent après leur suppression ou au redémarrage de l'appareil
  - Des clés de registre ou des éléments de démarrage qui lancent des processus malveillants
- **Accès aux identifiants :** L'accès non autorisé aux identifiants peut davantage compromettre les systèmes et les données sensibles. Par exemple :
  - Les attaques par force brute ciblant les comptes utilisateur
  - Les campagnes de phishing visant la collecte d'identifiants utilisateur
  - Le dumping des données d'identification provenant de systèmes compromis
- **Autres lieux d'implantation et sources d'accès :** Les attaquants tentent parfois de s'implanter dans plusieurs endroits différents de manière à étendre leur accès et leur contrôle de l'environnement. Par exemple :
  - En exploitant des comptes utilisateur compromis dotés de privilèges élevés
  - En exploitant des failles non corrigées dans les systèmes ou applications
  - En se déplaçant latéralement sur le réseau pour obtenir un accès à d'autres ressources

En reconnaissant ces types d'incidents et leurs exemples, les entreprises peuvent identifier plus efficacement les menaces potentielles et répondre en conséquence. C'est essentiel pour détecter et résoudre rapidement les incidents de sécurité.

Analyse forensique

L'analyse forensique est un aspect crucial du processus de réponse aux incidents, car elle aide les entreprises à identifier la cause première d'un incident, à comprendre son impact et à collecter des preuves pour étayer les investigations ultérieures ou les actions en justice. Voici quelques éléments clés de l'analyse forensique :

Outils et techniques d'analyse forensique

Il existe une multitude d'outils et de techniques d'analyse forensique qui facilitent l'analyse approfondie des systèmes tout au long du processus de réponse aux incidents. Ces outils sont utiles pour la collecte, l'analyse et la conservation des données. Vous trouverez ci-dessous plusieurs exemples d'outils et de techniques d'analyse forensique :

- Les outils d'image disque et de clonage permettent de conserver l'état d'un système compromis
- Les outils d'analyse de la mémoire permettent d'analyser les données volatiles et d'identifier les processus malveillants
- Les outils d'analyse du trafic réseau permettent d'examiner l'activité sur le réseau et d'identifier d'éventuels indicateurs de compromission
- Les outils d'analyse des journaux permettent de détecter les signes d'activité suspecte en analysant les logs d'activité des systèmes et des applications

Collecte et conservation des preuves

En matière d'analyse forensique, il est important d'utiliser des méthodes adéquates de collecte et de conservation des preuves afin d'assurer l'intégrité des données et leur recevabilité comme preuve en cas d'actions légales. Vous trouverez ci-dessous plusieurs exemples des bonnes pratiques à adopter en matière de collecte et de conservation des preuves :

- Documentez chaque étape du processus de collecte des preuves, notamment les outils et méthodes utilisés.
- Créez une chronologie détaillée des évènements liés à l'incident.
- Utilisez des bloqueurs d'écriture et autres outils d'analyse forensique pour éviter l'altération des preuves au cours du processus de collecte.
- Conservez les données recueillies dans des conteneurs inviolables ou des dispositifs de stockage chiffrés.
- Veillez à ce que les données soient stockées dans un emplacement contrôlé et sécurisé.

Chaîne de contrôle

Il est important de veiller à la fiabilité de la chaîne de contrôle afin d'assurer l'intégrité des données et leur recevabilité comme preuve en cas d'actions légales. Le terme « chaîne de contrôle » (chain of custody) se rapporte aux documents et au suivi du traitement, au stockage et au transfert de preuves tout au long de l'investigation. Afin de garantir la fiabilité de la chaîne de contrôle :

- Enregistrez les informations de chaque personne impliquée dans le traitement des preuves : nom, rôle et coordonnées.
- Enregistrez la date, l'heure et l'emplacement de chaque transfert de données ou de traitement des preuves.
- Enregistrez toutes les actions effectuées : copie, analyse, stockage, etc.
- Veillez à ce que le stockage et le transfert des preuves soient toujours effectués en toute sécurité, sous scellé ou en utilisant une méthode de chiffrement.

L'analyse forensique vous permettra d'obtenir des informations importantes sur la nature et l'étendue des incidents de sécurité, de recueillir des preuves cruciales et de dégager toutes les informations nécessaires à vos recherches et actions juridiques. Pour utiliser les différents outils, techniques et pratiques d'analyse forensique à bon escient, il est essentiel de bien les comprendre.

Exfiltration de données

Le terme « exfiltration des données » se rapporte à tout transfert non autorisé d'informations ou de données sensibles depuis le réseau ou les systèmes de l'entreprise vers un emplacement externe, généralement contrôlé par l'attaquant. La détection et la prévention d'un incident d'exfiltration de données sont cruciales pour limiter l'impact d'une violation de sécurité et pour préserver l'intégrité des ressources précieuses. Tenez compte des aspects suivants pour vous protéger efficacement contre l'exfiltration de données :

- **Surveillance et alertes :** Mettez en place un système complet de surveillance capable de détecter les transferts de données ou les modèles de trafic réseau suspects, comme le transfert de fichiers volumineux, les communications avec des adresses IP suspectes ou les tentatives multiples de connexion échouées. Mettez en place des mécanismes d'alerte fiables pour permettre à l'équipe de réponse aux incidents de prendre rapidement connaissance de toute exfiltration de données potentielle.
- **Solutions de prévention des fuites de données (DLP) :** Déployez des solutions DLP afin d'identifier et d'empêcher le transfert de données sensibles vers l'extérieur du réseau de l'entreprise. Les solutions DLP détectent et bloquent les transferts non autorisés d'informations sensibles en fonction de politiques de sécurité et de règles prédéfinies.
- **Chiffrement :** Chiffrez les données sensibles inactives et en transit pour réduire la valeur des données aux yeux de l'attaquant une fois exfiltrées.
- **Sensibilisation et formation des employés :** Informez les employés du risque d'exfiltration des données et formez-les sur l'importance de respecter les politiques de sécurité en place. Apprenez-leur par exemple à ne pas partager de données au travers de voies non sécurisées ou avec des individus qui ne sont pas autorisés à y accéder.

Validation et priorisation

Une fois qu'un incident de sécurité potentiel a été identifié, il est important de le valider et de prioriser votre réponse en fonction de sa gravité et de son impact potentiel sur l'entreprise. La validation et la priorisation comprennent les étapes suivantes :

- **Validation de l'incident :** Vérifiez qu'il s'agit bien d'un véritable évènement de sécurité et non d'un faux positif. Pour valider l'incident, analysez les données disponibles, comparez-les aux renseignements sur les menaces connues dont vous disposez et examinez le contexte de l'évènement.
- **Priorisation de l'incident :** Évaluez l'impact potentiel de l'incident sur les ressources, les opérations et la réputation de l'entreprise. Tenez compte de facteurs tels que la nature des données ou des systèmes concernés, l'étendue de la violation et les conséquences potentielles de l'incident.
- **Niveaux de gravité :** Attribuez un niveau de gravité à l'incident en fonction de votre évaluation de sa priorité. Le niveau de gravité peut être défini en fonction d'un barème prédéfini (par ex. faible, moyen, élevé, critique) et sert de guide à l'équipe de réponse aux incidents pour déterminer les ressources à déployer et le degré d'urgence de la réponse.
- **Plan de réponse :** En fonction du niveau de gravité et de la nature de l'incident, sélectionnez le plan de réponse le plus approprié dans le manuel de réponse aux incidents de l'entreprise. Ce plan doit présenter les mesures à mettre en place pour confiner, investiguer et remédier à l'incident, indiquer les procédures de communication à adopter et le type de rapport à générer.

En identifiant, validant et priorisant efficacement les incidents de sécurité, vous serez en mesure de distribuer efficacement vos ressources et de concentrer vos efforts sur les incidents les plus critiques. Cela limitera l'impact général de l'incident sur l'entreprise.

Confinement

L'objectif principal du confinement est d'empêcher tout dommage supplémentaire en isolant les systèmes identifiés comme étant compromis ou qui sont soupçonnés de l'être. Cette mesure permet d'éviter la propagation des incidents (malwares, exfiltration de données, etc.) et de préserver l'état du système afin d'en extraire les preuves nécessaires. Élaborez des stratégies de confinement pertinentes pour l'investigation, telle que la collecte d'indicateurs de compromission (IOC) qui seront documentés et utilisés ultérieurement.

Confinement à court terme

Le confinement à court terme regroupe toutes les actions prises dans le but de limiter l'impact immédiat de l'incident. Celles-ci sont généralement effectuées pour contenir la menace dès l'identification de la machine compromise. Exemples de mesures de confinement à court terme :

- **Isoler l'hôte :** Utilisez les fonctionnalités offertes par les plateformes de sécurité, telles que Sophos Intercept X Advanced, pour isoler les hôtes compromis tout en maintenant une connexion active pour des recherches ultérieures.
- **Bloquer les hachages SHA256 :** Utilisez Sophos Intercept X Advanced pour éviter l'exécution des fichiers malveillants en bloquant leurs hachages SHA256.
- **Isoler le réseau :** Modifiez les politiques de routage du commutateur, du routeur ou du pare-feu pour empêcher le segment du réseau contenant la machine infectée de communiquer avec d'autres machines.
- **Isoler manuellement :** Déconnectez le câble Ethernet du réseau ou désactivez la carte réseau (Wi-Fi) de la machine infectée.
- **Réinitialiser le compte :** Réinitialisez tous les comptes utilisateur que vous suspectez d'être compromis.

Confinement à long terme

Le confinement à long terme permet d'éviter que la même menace ne se propage sur d'autres machines et d'autres ressources du réseau après la phase d'investigation initiale. Exemples de mesures de confinement à long terme :

- Bloquer les connexions réseau vers les URL compromises et les serveurs de command-and-control (C2) identifiés durant l'investigation.
- Suspendre les comptes de domaine compromis, réinitialiser/suspendre les mots de passe du compte administrateur local/de domaine, réinitialiser tous les mots de passe du domaine si l'ampleur de l'incident ne peut pas être déterminée.
- Isoler automatiquement l'appareil en fonction de son état de sécurité.
- Installer des agents de sécurité sur les machines non protégées ou celles ayant été nettoyées afin d'apporter plus de visibilité et une meilleure protection.

Bonnes pratiques

Adoptez les bonnes pratiques suivantes pour optimiser le confinement :

À faire

- Isolez la machine à l'aide de l'une des options proposées ci-dessus.
- Documentez toutes les étapes du processus de confinement : l'heure, l'action et par qui celle-ci a été prise.
- Suivez vos plans de réponse aux incidents et votre stratégie de confinement, surtout en cas de litige. Évaluez les avantages de prendre des images forensiques et d'impliquer votre cyberassurance.
- Catégorisez la menace selon son niveau de gravité et notifiez l'équipe de direction si elle représente un risque élevé.
- Déterminez les indicateurs de compromission (IOC) pour faciliter l'investigation et recueillez des preuves.
- Communiquez avec tous les collaborateurs concernés (direction, service juridique, service de relations publiques, etc.) en fonction du niveau de gravité et de l'impact potentiel de l'incident.

- Surveillez tout signe de représailles ou d'intensification des actions de l'attaquant pendant le processus de confinement. S'il s'aperçoit que ses activités ont été découvertes, celui-ci pourrait tenter de faire plus de dégâts.
- Veillez à ce que vos mesures de confinement soient réversibles en cas de besoin, dans le cas de faux positifs ou de conséquences inattendues.
- Effectuez une analyse approfondie de l'incident afin d'identifier les causes premières et tirez les leçons de l'expérience pour améliorer votre posture de sécurité et votre processus de réponse aux incidents.

À ne pas faire

- N'éteignez pas ou ne redémarrez pas la machine compromise.
- Ne prenez aucune action sans avoir consulté le responsable de l'équipe de réponse aux incidents conformément à votre plan de réponse aux incidents.
- N'installez pas immédiatement un système de sauvegarde sans avoir terminé la collecte et les investigations initiales des IOC.
- Ne médiatisez pas l'incident et ne partagez pas d'informations confidentielles en dehors de l'équipe : cela pourrait alerter l'attaquant et potentiellement compromettre le processus de confinement.
- N'effectuez pas le confinement en vous appuyant uniquement sur des outils et des processus automatisés. L'expertise et le jugement humain sont essentiels à la prise de décisions informées.
- N'oubliez pas de prendre en considération l'impact commercial potentiel des mesures de confinement (comme les interruptions de service ou la perte de fonctionnalité), et de mettre ces facteurs en balance avec les risques encourus si aucune action n'est prise.
- Pour mieux vous préparer aux incidents futurs, ne négligez pas l'importance de mettre à jour votre plan de réponse aux incidents et vos procédures en fonction des enseignements tirés du processus de confinement.

N'oubliez pas qu'une approche unique ne convient pas toujours ; le choix des actions à effectuer s'adaptera au type d'incident, à l'environnement du réseau et à son accessibilité. Si le confinement bloque la menace immédiatement et laisse une marge de manœuvre pour d'autres actions, ce n'est souvent pas l'étape ultime de la gestion d'un incident. Restez toujours vigilants. Un incident de cybersécurité pose un risque persistant, car le criminel est susceptible d'intensifier son attaque s'il se rend compte qu'il a été découvert.

Éradication

L'éradication consiste à éliminer complètement la menace ou l'attaquant de l'environnement. C'est un processus dont les étapes visent à identifier, documenter et éradiquer toutes les activités, modifications du système, malwares et exécutions effectuées par l'attaquant sur le réseau et les machines. La plupart des cyberattaques étant pilotées manuellement et coordonnées sur plusieurs fronts, il est essentiel de pouvoir identifier tout comportement anormal qui passerait au travers des contrôles automatisés. Lorsque vous éradiquez une menace, il est essentiel de prendre en compte tous les effets potentiels qui en découlent.

Il existe deux stratégies principales d'éradication : reconstruire ou réimager les machines et procéder à une suppression ciblée. Chacune présente des avantages et des inconvénients, et les deux méthodes sont souvent combinées pour un maximum d'efficacité

Reconstruire ou réimager des machines

La meilleure façon d'éradiquer les ressources compromises est de reconstruire ou de réimager les hôtes, afin de les restaurer vers leur état antérieur à l'attaque. Ce processus est plus simple si les entreprises déploient des images logicielles standard sur les hôtes et ont accès à l'image principale pour la récupération. L'image maitre doit être créée avant d'être déployée en production afin de garantir son intégrité.

Il est rare de restaurer les serveurs critiques, tels que les systèmes ERP, les serveurs de messagerie et les serveurs de fichiers à partir d'une image maitre en raison du risque de perte des données et des coûts associés. Vous pouvez à la place restaurer les données à partir d'un fichier de sauvegarde sain (par ex. serveur de sauvegarde, bande magnétique, Cloud ou autre média). Ce processus nécessite de vérifier la disponibilité et l'intégrité des fichiers de sauvegarde et de restaurer les données vers un état qui n'est pas infecté. Pour garantir la stratégie de reconstruction et de réimage la plus efficace, les entreprises doivent étudier les IOC et les Tactiques, Techniques et Procédures (TTP) sur l'ensemble du réseau, en se concentrant particulièrement sur les machines vulnérables.

Procéder à une suppression ciblée

La suppression ciblée est une stratégie visant à identifier tous les malwares et artefacts présents sur le système, à identifier les modifications les plus importantes effectuées par l'adversaire, et à les supprimer ou d'en renverser les effets. Cette approche est particulièrement utile dans le cas de machines opérant des systèmes de production, de systèmes de contrôle industriels ou d'autres fonctions critiques dont l'interruption pourrait avoir des conséquences importantes.

La suppression ciblée est souvent déployée en combinant des outils et des compétences techniques d'experts en réponse aux incidents qui chassent les menaces sur la base des IOC observés, des renseignements sur les menaces associés et de leur expérience face aux TTP des adversaires. Les entreprises peuvent avoir recours à la suppression ciblée pour mieux comprendre l'attaque et en tirer des enseignements afin de mettre en œuvre des améliorations à long terme et de réduire le risque de cyberattaques futures.

Par exemple, si l'attaquant s'est infiltré sur une machine en exploitant une vulnérabilité, une erreur de configuration ou un malware dormant, le processus d'éradication devra corriger ou nettoyer la faille en question afin d'éviter que l'hôte ne devienne une source de réinfection ou le point de départ d'une nouvelle attaque. Une analyse détaillée de l'attaque (RCA) vous permettra de comprendre les étapes prises par l'attaquant avant que l'attaque n'ait été découverte, et d'identifier le « patient-zéro » pour éviter de futures attaques.

Nous vous conseillons de continuer à documenter vos découvertes et d'utiliser des cadres, tels que MITRE ATT&CK, pour conceptualiser la structure de l'attaque. Cette approche structurée permet d'identifier la cause première de l'incident et de permettre aux entreprises d'améliorer leur posture de sécurité globale.

Rétablissement

Le but de la phase de rétablissement est de progressivement restaurer les machines et les systèmes touchés par l'attaque et de permettre à l'entreprise de reprendre des activités normales. La stratégie de rétablissement dépend de l'incident, car certains incidents peuvent conduire à l'isolement de quelques machines avec un impact opérationnel minimal, tandis que des attaques plus importantes, comme les ransomwares, peuvent cibler plusieurs machines, entraînant un impact opérationnel significatif et une interruption des activités. Il est donc nécessaire d'adapter le plan de rétablissement à l'attaque en question.

- Un seul hôte affecté par un email de phishing dont la charge virale a été détectée et nettoyée par l'agent de protection Endpoint peut justifier l'isolement de la machine pendant qu'un analyste de sécurité procède à l'investigation et au nettoyage, avec un impact opérationnel global minimal.
- La détection précoce d'un botnet dans le réseau affectant deux machines avec des mécanismes de persistance installés peut conduire à l'isolement immédiat et à la reconstruction des machines de ces utilisateurs, ce qui entraîne un temps d'arrêt pour les employés, mais un impact opérationnel minimal sur l'entreprise.
- Une attaque de ransomware sur l'ensemble du réseau avec une durée de plusieurs semaines et une cause première identifiée conduira à l'isolement non seulement des postes et des serveurs, mais aussi de la messagerie, des VPN, des comptes Active Directory et d'autres services. Dans ce cas, les mesures de confinement devront rester en place jusqu'à ce que l'incident ait été maitrisé en identifiant les points d'implantation, en appliquant des correctifs et en réimaginant les machines. La stratégie de rétablissement consistera à créer un réseau « sain » alternatif, à le reconstruire tout d'abord sans les machines infectées, puis en réintégrant les machines de manière progressive. Les machines seront réintégrées en fonction de leur niveau de risque de réinfection. L'approche et la chronologie de l'opération seront déterminées après consultation entre l'équipe de réponse aux incidents et l'équipe de direction.

Une approche prudente

Le rétablissement est un processus qui exige de la concentration et une attention toute particulière aux détails critiques du système. Mais attention : un excès de confiance ou de fatigue peut être préjudiciable. Restez donc vigilant et portez attention aux éléments suivants :

- Évaluez l'état de sécurité général de la machine infectée. Celle-ci sera réintégrée sur le réseau en testant l'intégrité des données et la stabilité du système.
- Corrigez les failles de sécurité, surtout si vous restaurez la machine à partir d'une version précédente susceptible d'être réinfectée.
- Vérifiez que les politiques et les contrôles de sécurité sont appliqués sur chaque machine.
  - Déployez l'agent de sécurité sur toutes les machines réintégrées.
  - La liste des exclusions lors du contrôle doit être minimale. Configurez les exclusions et les applications spécifiques en fonction de l'élément exclu, de la machine exclue et du groupe d'utilisateurs concerné.
- Analysez et recherchez la présence d'IOC identifiés lors de l'attaque et les points d'implantation que l'attaquant aurait pu laisser derrière lui.

Nous vous conseillons vivement de continuer à contrôler l'environnement à la recherche d'autres activités malveillantes, et notamment de chercher activement les activités usuelles afin d'identifier et de répondre aux menaces à mesure qu'elles apparaissent.

La phase de rétablissement ne doit pas nécessairement suivre la phase d'éradication complète, mais doit être menée de manière interchangeable, car les machines restaurées vers un état sain peuvent être réintégrées dans l'environnement de production.

Bilan post-incident et enseignements tirés

Une fois l'incident de cybersécurité résolu, il est crucial d'en tirer des enseignements pertinents en effectuant un bilan post-incident. Ce processus vous aidera à analyser l'efficacité de votre réponse, et à identifier et à implémenter les améliorations à apporter à votre plan de réponse aux incidents. Vous renforcerez ainsi vos défenses et réduirez le risque que le même type d'incident ne se reproduise plus à l'avenir.

Bilan post-incident

Analyser l'efficacité de la réponse aux incidents

Afin d'évaluer l'efficacité de votre réponse à l'incident, passez en revue les actions entreprises par l'équipe de réponse aux incidents et mesurez leurs résultats. Considérez les aspects suivants :

- Le temps nécessaire pour détecter, contenir et remédier à l'incident
- L'efficacité de la communication et de la coordination entre les membres de l'équipe et avec les collaborateurs externes (autorités, fournisseurs, etc.)
- La pertinence des stratégies de confinement, d'éradication et de rétablissement
- L'exactitude et l'utilité des informations fournies par les outils de surveillance et de détection

Déterminer les points à améliorer

Une fois l'efficacité de votre réponse analysée, identifiez quels processus et procédures peuvent être améliorés. Il pourrait s'agir par exemple des domaines suivants :

- La sensibilisation et la formation du personnel
- Les capacités de détection et de surveillance des incidents
- La mise à jour du plan de réponse aux incidents
- Les contrôles techniques et mesures de sécurité
- Les rôles et responsabilités de l'équipe de réponse aux incidents
- La communication externe et la collaboration avec les parties concernées

Modifier et mettre à jour le plan de réponse aux incidents

Après avoir identifié les points à améliorer, effectuez toutes les modifications nécessaires au niveau du plan de réponse aux incidents. Assurez-vous de :

- Mettre à jour les procédures, directives ou mesures techniques si nécessaire.
- Communiquer les changements à toutes les personnes concernées : personnel, direction et collaborateurs externes.
- Organiser régulièrement des formations et des exercices pour s'assurer que le plan actualisé est assimilé et peut être exécuté efficacement.
- Contrôler et évaluer l'efficacité des changements au fil du temps et apporter plus de modifications au plan si nécessaire.

Un bilan post-incident complet vous permettra de tirer des enseignements importants de l'attaque, d'améliorer votre posture de cybersécurité et de mieux préparer vos défenses pour l'avenir. N'oubliez pas que la réponse aux incidents est un processus continu. C'est pourquoi il est important de passer en revue et de mettre à jour votre plan de réponse aux incidents régulièrement afin de rester résilient face aux cybermenaces émergentes.

Enseignements tirés

Les enseignements tirés dépendent du type d'incident et du processus de traitement de l'incident. Ils correspondent aux domaines à améliorer. Cette phase, pourtant critique, est souvent négligée une fois l'état d'alerte passé, que l'équipe de direction se désengage de l'incident et que les activités reprennent leur cours normal. Il est donc d'autant plus important que la phase d'assimilation des enseignements tirés intervienne immédiatement après la phase de rétablissement et qu'elle se déroule en présence de l'équipe de direction pour comprendre les détails de l'incident et convenir des améliorations à apporter pour atténuer les risques futurs.

En général, ce processus prend la forme d'un rapport d'incident écrit comprenant un résumé pouvant être partagé et compris par les parties prenantes non techniques au sein de l'entreprise. Ce rapport doit être collaboratif en vue de recueillir les commentaires d'un large éventail de collaborateurs. Il doit se conclure par un consensus sur les détails techniques et les enseignements tirés de l'expérience.

Vous trouverez ci-dessous une liste non exhaustive des éléments susceptibles d'être améliorés durant cette phase.

Bonnes pratiques de sécurité recommandées :

- Décommissionnez les logiciels, les applications et le matériel obsolètes au sein de l'entreprise afin de minimiser le risque d'exploitation.
- Mettez en place un processus solide de gestion des correctifs pour les logiciels et le matériel qui s'aligne sur les besoins de l'entreprise et assure la mise à jour régulière des correctifs.
- Installez des agents de protection Endpoint basés dans le Cloud sur tous les ordinateurs de l'entreprise afin de détecter et de neutraliser les menaces malveillantes.
- Implémentez l'authentification multifacteur (MFA) pour le VPN, le RDP et tous les autres services nécessitant une protection renforcée.
- Sécurisez l'infrastructure en implémentant des mécanismes de contrôle de sécurité de base et en protégeant les services connectés à Internet contre les accès non autorisés.
- Renforcez la gestion des identifiants en exigeant des critères de complexité, en utilisant des gestionnaires de mots de passe et en changeant régulièrement les identifiants.
- Implémentez des protocoles d'authentification tels que DMART, DKIM et SPF afin de protéger contre les emails de phishing et l'usurpation.

Configuration du réseau :

- Implémentez le contrôle d'accès réseau (NAC) pour ajouter une couche de sécurité supplémentaire et vous défendre contre les appareils indésirables et les menaces.
- Isolez les réseaux VLAN afin de protéger les systèmes critiques et les données sensibles. Isolez les plateformes et les services à l'intérieur d'une DMZ.

Durcissement :

- Implémentez le géoblocage des adresses IP au niveau des pare-feux afin de bloquer le trafic réseau indésirable en fonction de son origine géographique.
- Déployez des solutions de contrôle des applications, telles qu'AppLocker, afin d'éviter l'installation et l'exécution d'applications indésirables au sein du réseau de l'entreprise.
- Durcissez les contrôleurs de domaine en revoyant et en supprimant les services non essentiels, les logiciels non supportés et les protocoles hérités qui pourraient constituer des risques de sécurité.

Gestion proactive et précautions de sécurité :

- **Vérification de l'infrastructure :** Vérifiez régulièrement la configuration des ports de tous les appareils connectés à Internet. Assurez-vous que seuls les services de protocole nécessaires sont autorisés, et que les ports de flux réseau sont configurés de manière adéquate.
  - Par exemple, eth0 est connecté à Internet et eth1 est uniquement accessible de l'intérieur.
- **Vérification des contrôles Web :** Vérifiez régulièrement la configuration du trafic Web sur les serveurs proxys et les plateformes de flux de trafic Web. Renforcez les contrôles de sécurité dans tous les cas possibles, en respectant le principe du moindre privilège. Implémentez une stratégie de blocage par défaut. Par exemple :
  - Bloquez les types de fichiers qui posent des risques inutiles à l'entreprise.
  - Vérifiez vos politiques de catégorisation par défaut pour les URL et les domaines non classés.
  - Exportez les données statistiques pour identifier les anomalies, les modèles ou les évènements suspects ou malveillants récurrents.
  - Assurez-vous que les groupes et stratégies de sécurité soient mis à jour conformément au principe de RBAC (contrôle d'accès basé sur les rôles).
- **Vérification des comptes :** Effectuez des audits réguliers des comptes administrateur local ou équivalents non standard et non approuvés au sein de l'entreprise, afin de supprimer ces comptes.
- **Logs d'évènement Windows :** Configurez les logs d'évènement Windows pour conserver les données. Vous pouvez par exemple agrandir la capacité des journaux ou créer de nouveaux journaux d'évènements lorsque les anciens ont atteint leur limite. Les logs d'évènement Windows offrent des informations forensiques très utiles.
- **Plan de réponse aux incidents :** Développez, implémentez, testez et maintenez un plan de réponse aux incidents de cybersécurité. Examinez et testez régulièrement ce plan, en mettant à jour et en affinant son contenu si nécessaire.

- **Gestion des ressources matérielles et logicielles :** Implémentez un plan de gestion des ressources logicielles et matérielles pour l'ensemble de l'entreprise. Incorporez un système de priorisation dans votre solution de gestion des ressources afin d'identifier rapidement les actifs les plus importants. Tenez un inventaire à jour des ressources matérielles et logicielles. Celui-ci vous aidera à identifier les risques potentiels et vous permettra de formuler des stratégies visant à les limiter.
- **Topologie du réseau :** Maintenez à jour un schéma détaillé de la topologie du réseau. Celui-ci constituera une base de référence claire des configurations et des types d'infrastructure existant dans l'entreprise, pour vous aider à formuler et implémenter des stratégies de modification du réseau. Lors d'une attaque, ce schéma vous permettra de comprendre la structure organisationnelle du réseau et d'exécuter plus précisément et plus rapidement les actions de réponse.

Intégrité des données

Sauvegardes :

- Protégez les données de sauvegarde en implémentant différentes solutions de sauvegarde, en stockant les données dans des emplacements réseau/types de supports complètement séparés et indépendants du reste de l'environnement, et en gérant l'accès à l'aide de contrôles de sécurité robustes.
  - Commencez à formuler des solutions de redondance des sauvegardes en vous référant à la règle des 3-2-1 et en chiffrant les données de sauvegarde inactives : créez 3 copies des données, stockez les données sur 2 types de supports différents, stockez au moins 1 copie hors site.

Chiffrement :

- Appliquez le chiffrement intégral du disque (FDE) sur les ordinateurs, appareils mobiles et clés USB afin de protéger les données contre tout accès non autorisé en cas de perte ou de vol de l'appareil.
- Chiffrez les données inactives (Data At Rest Encryption ou DARE) en priorisant les données hautement sensibles. Pour ce qui est des données réseau en transit, mettez en place des mécanismes de chiffrement stricts. Installez par exemple la version du protocole TLS (Transport Layer Security) la plus récente pour protéger les communications chiffrées impliquant une certification numérique, et empêchez les serveurs de rétrograder les suites de codage pour accommoder les navigateurs non pris en charge.

Investissements de sécurité

Servez-vous des enseignements tirés d'incidents de sécurité passés pour solliciter un financement et un budget accrus aux fins d'amélioration de la posture de sécurité de l'entreprise.

- Investissez dans la sensibilisation et la formation du personnel. L'humain étant souvent le premier vecteur d'attaque, il convient d'investir dans :
  - Un programme de sensibilisation et de formation au phishing qui forme et teste les utilisateurs à reconnaitre les techniques usuelles de phishing. Intégrez cette formation aux activités quotidiennes de l'entreprise par le biais d'exercices planifiés et de simulations d'attaques automatisées. Fournissez les rapports obtenus à l'équipe IT qui pourra identifier les utilisateurs les plus susceptibles de se faire avoir et pourra prodiguer des conseils.
  - La formation continue du personnel en matière de cybersécurité, et plus particulièrement en matière de contrôle de la sécurité, de chasse aux menaces et de réponse aux incidents.

Services managés de cybersécurité

- Employez des professionnels de la cybersécurité spécialisés dans des domaines tels que le contrôle de la sécurité, la chasse aux menaces, l'ingénierie des fonctions de détection des outils de sécurité, etc. Mettez en place un centre d'opérations de cybersécurité (SOC) vous permettant de surveiller et de répondre aux menaces 24/7.
- Investissez dans une solution de cybersécurité managée telle que Sophos Managed Detection and Response (MDR). Les services MDR sont des opérations de sécurité externalisées, assurées par une équipe d'experts qui agissent comme une extension de l'équipe de sécurité de leur client.

Investir dans des outils

- Sophos XDR (Extended Detection and Response) est une solution qui stocke et permet d'interroger les informations critiques provenant des postes, des serveurs, des pare-feux, de la messagerie et d'autres produits compatibles XDR, optimisant ainsi les workflows de détection et de réponse aux menaces.

- La technologie de gestion des informations et des évènements de sécurité (SIEM) offre des capacités de détection des menaces, de conformité et de gestion des incidents en collectant des évènements et des informations à partir de diverses sources de données dans un référentiel centralisé de données sur les menaces.
- Des investissements supplémentaires peuvent être envisagés sur la base des enseignements tirés. Vous devriez par exemple améliorer votre posture de sécurité en comblant les failles dans la protection/filtrage, la détection et la surveillance à l'aide de solutions antivirus, de systèmes de prévention et de détection des intrusions (IPS/IDS), des pare-feux, etc.

Votre entreprise améliorera ainsi considérablement sa posture de cybersécurité et sera plus à même de se protéger contre de futures attaques. N'oubliez pas que l'assimilation des enseignements tirés est un processus continu. C'est pourquoi il est important de passer en revue et de mettre à jour vos pratiques de sécurité régulièrement pour maintenir des défenses solides face aux cybermenaces émergentes.

Rapports d'incident

Après la résolution d'un incident de cybersécurité, il est essentiel de communiquer les détails, les découvertes et les mesures de remédiation prises aux différentes parties prenantes. Pour maintenir la transparence, garantir la conformité et soutenir les investigations, il est essentiel de signaler l'incident par la production de rapports qui seront remis en interne, aux autorités de régulation et aux autorités judiciaires.

Rapports internes

Pour favoriser une culture d'apprentissage et d'amélioration continue, établissez un processus clair pour l'établissement de rapports internes. Dans ce rapport, il est important de :

- Documenter l'incident, notamment la chronologie de l'évènement, les systèmes affectés et la nature de l'attaque.
- Résumer l'impact de l'incident sur les opérations, les finances et la réputation de l'entreprise.
- Décrire les mesures prises pour contenir l'incident, l'éradiquer et se rétablir.
- Identifier les enseignements tirés et les recommandations pour améliorer la posture de sécurité de l'entreprise.
- Communiquer le rapport d'incident aux parties prenantes concernées : la direction, les équipes IT et les employés ou services affectés.

Rapports aux autorités de régulation

Certains incidents de cybersécurité devront être communiqués aux autorités de régulation en fonction de la juridiction concernée et de votre secteur d'activité. Le respect de ces exigences est essentiel pour éviter une amende, une pénalité ou une atteinte à la réputation de votre entreprise. Lorsqu'elles font rapport aux autorités de régulation, les entreprises doivent :

- Déterminer l'autorité ou les autorités compétentes à notifier, en fonction de la nature de l'incident, du secteur d'activité et du lieu d'implantation de l'entreprise.
- Identifier les éléments à inclure dans le rapport, y compris les informations nécessaires et le délai d'établissement du rapport.
- Préparer un rapport détaillé, en respectant le format et le contenu spécifiés par l'autorité de régulation.
- Soumettre le rapport dans les délais impartis et maintenir une communication ouverte avec l'autorité de régulation tout au long du processus d'investigation et de résolution.

Rapports aux autorités judiciaires

En cas d'activité criminelle ou de cyberattaque importante, les entreprises sont encouragées à signaler l'incident aux autorités judiciaires. Cela aidera les autorités à enquêter sur l'incident et pourra potentiellement mener à l'arrestation des attaquants. Lorsqu'elles font rapport aux autorités judiciaires, les entreprises doivent :

- Identifier les organismes d'application de la loi auxquels signaler l'incident : police locale, unités nationales de lutte contre la cybercriminalité ou les agences spécialisées (Police judiciaire, etc.).
- Recueillir les preuves nécessaires : journaux, images du système, captures du trafic réseau, tout en préservant la chaîne de contrôle et en respectant les lois en vigueur.
- Préparer un rapport détaillant l'incident : la nature de l'attaque, les systèmes et données touchés, la chronologie des évènements et les informations que vous connaissez concernant l'attaquant.
- Coopérer avec les forces de l'ordre tout au long de l'enquête afin de leur fournir les renseignements supplémentaires dont elles pourraient avoir besoin.

Ces conseils pour la déclaration des incidents vous permettront d'agir en toute transparence et dans le respect de la règlementation en vigueur, mais aussi, de manière plus générale, à contribuer à la lutte contre le cybercrime.

Conclusion

Pour conclure, ce guide de planification de la réponse aux incidents fournit un cadre complet permettant aux entreprises de se préparer efficacement aux incidents de cybersécurité, de les gérer et de s'en remettre. Les entreprises peuvent améliorer de manière significative leur résistance aux cybermenaces en mettant en œuvre une gestion proactive et des mesures de sécurité, en garantissant l'intégrité des données, en investissant dans la formation du personnel et dans des outils de sécurité, et en établissant des protocoles de déclaration clairs.

Un plan de réponse aux incidents efficace vous permettra non seulement de réduire les dégâts causés par les cyberattaques, mais aussi de favoriser une culture d'amélioration et d'apprentissage continus dans l'entreprise. Comme le paysage des cybermenaces évolue sans cesse, les entreprises doivent régulièrement revoir et mettre à jour leurs plans de réponse aux incidents afin de garder une longueur d'avance sur les nouvelles menaces et vulnérabilités.

Les recommandations fournies dans ce guide vous permettront de mieux détecter, contenir et remédier aux incidents de sécurité, de protéger vos données et vos ressources sensibles, de rester conforme aux règlementations en vigueur et de préserver votre réputation dans un monde de plus en plus interconnecté.

Pour en savoir plus sur le Service Sophos de réponse aux incidents, cliquez ici

En proie à une attaque active ?

Appelez le numéro ci-dessous correspondant à votre pays pour être mis en relation avec l'un de nos conseillers.

Australie : +61 272 084 454

Autriche : +43 7 3265575520

Canada : +1 778 589 7255

France : +33 1 86 53 98 80

Allemagne : +49 611 711 86 766

Italie : +39 0294752897

Pays-Bas : +31 16 270 8600

Suède : +46 858 400 610

Suisse : +41 44 515 2286

Royaume-Uni : +44 1235 635 329

États-Unis : +1 408 746 1064

Email : RapidResponse@Sophos.com

Nos conseillers vous répondront le plus rapidement possible.

2023-07-03 (IRG-MP)

SOPHOS