SOPHOS
Cybersecurity delivered.

Guide de Réponse aux incidents

Dix étapes pour un plan efficace de réponse aux incidents de cybersécurité

« Avant toute chose, la préparation est la clé du succès. »

Alexander Graham Bell

Comment éviter qu'une cyberattaque ne se transforme en une véritable violation de sécurité ? Il faut se préparer à l'avance.

Après avoir subi une violation, les organisations réalisent souvent qu'elles auraient pu s'éviter beaucoup de tracas, de dépenses et de temps d'arrêt si elles avaient eu en place un plan de réponse aux incidents efficace.

Ce guide est conçu pour vous aider à définir un cadre pour l'élaboration d'un plan de réponse aux incidents de cybersécurité, qui vous donne toutes les chances de contrecarrer les attaquants. Ces recommandations sont basées sur les expériences réelles des équipes Sophos Managed Detection and Response et Sophos Rapid Response, qui ont une grande expertise dans la gestion des cyberattaques.

Plan de réponse aux incidents de cybersécurité

Tout plan de réponse aux incidents efficace doit intégrer 10 étapes clés :

Planification de la réponse aux incidents

1. **Déterminez les principales parties prenantes**
2. **Identifiez les actifs critiques**
3. **Réalisez des exercices de simulation**
4. **Déployez des outils de protection**
5. **Assurez-vous d'avoir une visibilité maximale**
6. **Contrôlez les accès**
7. **Investissez dans des outils d'investigation**
8. **Établissez des actions de réponse**
9. **Organisez des formations de sensibilisation**
10. **Sollicitez un service de sécurité managé**

1. Déterminez les principales parties prenantes

Planifier en vue d'un incident potentiel n'est pas de la seule responsabilité de votre équipe de sécurité. Un incident aura probablement des répercussions sur presque tous les services de votre organisation, surtout s'il se transforme en une violation de grande ampleur. Pour coordonner correctement une réponse, vous devez d'abord déterminer qui doit être impliqué. Il s'agit souvent de représentants de la direction, de la sécurité, des technologies de l'information, du service juridique et des relations publiques.

Il convient de déterminer à l'avance toutes les parties prenantes de votre organisation qui participeront aux réunions de planification. De plus, pour assurer une réponse rapide vous devez établir au préalable une méthode de communication qui prenne en compte la possibilité que vos canaux de communication habituels (par exemple la messagerie de l'entreprise) soient affectés par l'incident.

2. Identifiez les actifs critiques

Pour déterminer la portée et l'impact d'une attaque, votre organisation doit d'abord identifier ses actifs les plus importants. La cartographie de vos actifs prioritaires vous aidera non seulement à déterminer votre stratégie de protection, mais facilitera également l'identification de l'ampleur et des conséquences d'une attaque. De plus, en les identifiant à l'avance, votre équipe de réponse aux incidents pourra se concentrer sur les actifs les plus critiques lors d'une attaque, ce qui limitera la perturbation de vos activités.

3. Réalisez des exercices de simulation

La réponse aux incidents est comme beaucoup d'autres disciplines, il faut de la pratique pour la maîtriser. Bien qu'il soit difficile de reproduire entièrement la pression intense que votre équipe subira lors d'une violation, les exercices de simulation garantissent une réponse plus étroitement coordonnée et plus efficace lorsqu'une situation réelle se produira. Il est important d'effectuer non seulement des exercices de simulation (souvent dans le cadre de tests Red Team), mais aussi des exercices plus larges qui incluent les différentes parties impliquées précédemment identifiées.

Les simulations devraient tester vos réponses organisationnelles à une variété de scénarios potentiels. Chacun de ces scénarios peut également inclure des parties prenantes autres que l'équipe technique immédiate. Votre organisation doit déterminer à l'avance qui doit être informé lorsqu'une attaque est détectée, même si la défense a été efficace.

Les scénarios de réponse aux incidents les plus courants comprennent :

- **Adversaire actif détecté sur votre réseau** : Dans ce scénario, il est essentiel que l'équipe de réponse détermine comment l'attaquant a pu s'infiltrer dans votre environnement, quels outils et techniques ont été utilisés, ce qui a été visé et si une persistance a été établie. Ces informations aideront à déterminer la ligne de conduite à adopter pour neutraliser l'attaque.

  Bien qu'il puisse sembler évident d'éjecter immédiatement l'attaquant de l'environnement, certaines équipes de sécurité choisissent d'attendre et d'observer son comportement pour obtenir des informations importantes pour déterminer ce qu'il tente de réaliser et les méthodes qu'il utilise pour y parvenir.

- **Violation des données réussi**e : Si une violation des données réussie est détectée, votre équipe devrait être en mesure de déterminer ce qui a été exfiltré et comment. Cela permettra ensuite d'apporter une réponse appropriée, y compris la possibilité de prendre en compte l'impact sur les politiques de conformité et de réglementation, si les clients doivent être contactés, et l'implication potentielle des services juridiques ou des forces de l'ordre.

- **Attaque par ransomware réussie** : Si des données et des systèmes critiques sont chiffrés, votre équipe doit suivre un plan pour récupérer le plus rapidement possible ce qui a été perdu. Ce plan doit inclure un processus de restauration des systèmes à partir de sauvegardes. Pour s'assurer que l'attaque ne se répétera pas dès que vous serez de nouveau en ligne, l'équipe doit enquêter pour savoir si l'accès de l'adversaire a été coupé. De plus, votre organisation dans son ensemble doit déterminer si elle est prête à payer une rançon en cas de situation extrême et, si oui, combien elle est prête à dépenser.

- **Système de haute priorité compromis** : Lorsqu'un système critique est compromis, votre organisation peut ne pas être en mesure de mener ses activités normalement. Dans un tel scénario, en plus de toutes les mesures nécessaires à prévoir dans le plan de réponse aux incidents, votre organisation doit également envisager d'établir un plan de reprise des activités afin de garantir une perturbation minimale.

4. Déployez des outils de protection

La meilleure façon de faire face à un incident est de s'en protéger en premier lieu. Assurez-vous que votre organisation dispose d'une protection appropriée pour les systèmes endpoint, les réseaux, les serveurs, le Cloud, les mobiles et la messagerie.

5. Assurez-vous d'avoir une visibilité complète

Sans une bonne visibilité de ce qui se passe lors d'une attaque, votre organisation aura des difficultés à répondre de manière appropriée. Avant qu'une attaque ne se produise, les équipes informatiques et de sécurité doivent s'assurer qu'elles ont la capacité de comprendre la portée et l'impact d'une attaque, notamment en déterminant les points d'entrée et les points de persistance de l'attaquant. Une bonne visibilité comprend la collecte de données de logs, en se concentrant sur les données des systèmes endpoint et du réseau. Étant donné que de nombreuses attaques ne sont découvertes qu'après plusieurs jours ou semaines, il est important de pouvoir analyser des données historiques remontant à plusieurs jours ou semaines (voire plusieurs mois). De plus, assurez-vous que ces données sont sauvegardées de manière sécurisée afin de pouvoir y accéder pendant un incident actif.

6. Contrôlez les accès

Les attaquants peuvent exploiter les contrôles d'accès faibles pour infiltrer les défenses de votre organisation et élever leurs privilèges. Assurez-vous régulièrement que vous avez mis en place les contrôles appropriés pour établir un contrôle d'accès. Cela comprend, entre autres, déployer l'authentification multi-facteurs, limiter les privilèges admin au plus petit nombre de comptes possible (selon le principe du moindre privilège), modifier les mots de passe par défaut et réduire le nombre de points d'accès à surveiller.

7. Investissez dans des outils d'investigation

En plus de vous assurer d'avoir une visibilité adéquate, votre organisation doit investir dans des outils qui vous permettent de déterminer le contexte d'une attaque.

Les outils de réponse aux incidents les plus couramment utilisés sont l'EDR (Endpoint Detection and Response) ou le XDR (Extended Detection and Response), qui vous permettent de détecter les indicateurs de compromission (IOC) et les indicateurs d'attaque (IOA) sur l'ensemble de votre environnement. Les outils EDR aident les analystes à identifier les actifs compromis, ce qui permet de déterminer l'impact et la portée d'une attaque. Pendant votre investigation, plus vous recueillez de données plus vous aurez un aperçu clair du contexte de l'attaque. Une plus grande visibilité permettra à votre équipe de déterminer non seulement ce que les attaquants ont ciblé, mais aussi comment ils sont entrés dans l'environnement et s'ils ont encore la possibilité d'y accéder à nouveau.

En plus des outils EDR, les équipes de sécurité de haut niveau peuvent également déployer une solution SOAR (Security Orchestration, Automation and Response) qui facilite les processus de réponse.

8. Établissez des actions de réponse

Détecter une attaque n'est qu'une partie du processus. Afin de répondre de manière appropriée à une attaque, vos équipes informatiques et de sécurité doivent s'assurer qu'elles ont la capacité de mener un large éventail d'actions correctives pour intercepter et neutraliser les attaquants. Les actions de réponse comprennent, entre autres :

- Isoler les hôtes affectés
- Bloquer les fichiers, processus et programmes malveillants
- Bloquer les communications Command & Control (C2) et les sites Web malveillants
- Bloquer les comptes compromis et couper l'accès aux attaquants
- Nettoyer les artefacts et les outils des attaquants
- Fermer les points d'entrée et les zones de persistance exploitées par les attaquants (internes et tiers)
- Ajuster les configurations (politiques de sécurité, activer la sécurité Endpoint et EDR sur les appareils non protégés, ajuster les exclusions, etc.)
- Restaurer les ressources affectées grâce à des sauvegardes hors ligne

9. Organisez des formations de sensibilisation

Bien qu'aucun programme de formation ne soit efficace à 100 % contre un attaquant tenace, les programmes d'éducation (par exemple de sensibilisation au phishing) contribuent à réduire votre niveau de risque et à limiter le nombre d'alertes auxquelles votre équipe doit répondre. Des outils de simulation d'attaques de phishing mettent vos utilisateurs en condition réelle face à des emails de phishing pour les sensibiliser à la menace. Ceux qui échouent à reconnaitre le phishing peuvent être inscrits d'office à une formation et les utilisateurs identifiés comme les plus à risque peuvent bénéficier de formations approfondies.

10. Sollicitez un service de sécurité managé

De nombreuses organisations ne sont pas équipées pour gérer les incidents par elles-mêmes. Une réponse rapide et efficace nécessite des opérateurs de sécurité expérimentés. Pour vous assurer que vous pouvez répondre de manière appropriée, envisagez de travailler avec un prestataire externe tel qu'un fournisseur de services MDR (Managed Detection and Response).

Les fournisseurs de services MDR proposent la chasse aux menaces, l'investigation et la réponse aux incidents 24 h/24, 7 j/7, sous la forme d'un service managé. Les services MDR aident non seulement votre organisation à répondre aux incidents avant qu'ils ne se transforment en violation, mais aussi à réduire la probabilité qu'un incident ne se déclare en premier lieu. Les services MDR sont aujourd'hui très populaires : selon Gartner*, d'ici 2025, 50 % des organisations utiliseront des services MDR (contre moins de 5 % en 2019).

Les services DFIR (Data Forensic Incident Response) permettent de conserver des données après un incident afin d'obtenir des preuves pour appuyer une demande en justice ou une réclamation auprès d'une assurance.

Résumé

Lorsqu'un incident de cybersécurité survient, le temps est un facteur critique. Un plan de réponse bien préparé et bien compris, que toutes les parties clés peuvent immédiatement mettre en œuvre, réduira considérablement l'impact d'une attaque sur votre organisation.

Comment Sophos peut vous aider

Service Sophos MDR (Managed Detection and Response)

Sophos MDR (Managed Detection and Response) est une offre de services de chasse aux menaces, de détection et de réponse, entièrement managés par une équipe d'experts, 24 h/24 et 7 j/7. L'équipe Sophos MDR ne se contente pas de vous notifier lorsqu'une attaque ou un comportement suspect sont identifiés, mais elle intervient à votre place pour neutraliser les menaces les plus sophistiquées et les plus complexes à l'aide d'actions ciblées.

L'équipe Sophos MDR, composée d'experts de haut niveau spécialisés dans la chasse aux menaces et la réponse, vont :

- Chasser de manière proactive et confirmer les menaces et incidents potentiels
- Utiliser toutes les informations disponibles pour déterminer l'ampleur et la criticité des menaces
- Prendre en compte le contexte professionnel approprié pour valider les menaces
- Lancer des actions pour intercepter, contenir et neutraliser les menaces
- Fournir des conseils pratiques pour remédier aux causes profondes des incidents récurrents

Consultez www.sophos.fr/mdr pour en savoir plus.

Service Sophos Rapid Response

Piloté par une équipe d'experts en réponse aux incidents, le service Sophos Rapid Response identifie et neutralise de manière ultra-rapide les menaces actives ciblant les organisations. La prise en charge (onboarding) s'effectue en quelques heures et la majorité des clients font l'objet d'une priorisation (triage) sous 48 h. Le service est disponible à la fois pour les clients Sophos actuels, mais aussi pour les non-clients Sophos.

L'équipe Sophos Rapid Response, composée d'experts en réponse aux incidents, d'analystes et de chasseurs de menaces, peut :

- Prendre rapidement des mesures pour prioriser, contenir et neutraliser les menaces actives
- Expulser les attaquants de votre parc informatique pour empêcher d'autres dommages
- Surveiller et répondre aux menaces 24h/24 et 7j/7 pour renforcer votre protection
- Recommander en temps réel des mesures de prévention pour résoudre les causes profondes
- Fournir un compte-rendu post-incident de la menace détaillant l'investigation

Consultez www.sophos.fr/rapidresponse pour en savoir plus.

Sophos XDR

Sophos XDR est la seule solution XDR du secteur qui synchronise les protections natives des postes de travail, des serveurs, du pare-feu, de la messagerie, du Cloud et de M365. Obtenez une vue globale de l'environnement de votre organisation avec le plus riche ensemble de données et une analyse approfondie pour la détection, l'investigation et la réponse aux menaces, tant pour les équipes SOC dédiées que pour les administrateurs informatiques.

Consultez www.sophos.fr/xdr pour en savoir plus et commencer un essai gratuit.

* Gartner, Market Guide for Managed Detection and Response Services, 26 août 2020, Analystes : Toby Bussa, Kelly Kavanagh, Pete Shoard, John Collins, Craig Lawson, Mitchell Schneiderd

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

22-08-08 WPFR (PC)

SOPHOS