8 bonnes pratiques pour une cyber-résilience efficace

Passez avec assurance de la phase de planification à celle de l'exécution avant qu'une nouvelle attaque ne survienne.

Présentation

Même si vous disposez d'un plan de reprise après sinistre, la réponse à des cyberattaques destructrices nécessite une approche différente. La raison : Vous devez être en mesure de réagir rapidement, d'enquêter efficacement sur l'origine de l'attaque et de neutraliser les menaces afin d'assurer une reprise en toute sécurité.

Suivez ces 8 bonnes pratiques et vous serez sur la voie d'une véritable cyber-résilience.

1. Anticipez.

Votre première priorité consiste à mettre en place une équipe inter-fonctionnelle dédiée à la résilience face aux ransomwares, réunissant l'ensemble des parties prenantes. Les incidents liés aux ransomwares touchent l'ensemble de l'entreprise, il est donc essentiel que chacun connaisse précisément son rôle en cas de cyberattaque. Envisagez de réaliser un exercice de simulation réaliste avec l'ensemble des parties prenantes, d'élaborer une politique organisationnelle sur les ransomwares (et de la maintenir à jour), ainsi que de définir vos stratégies de sauvegarde cyber et de résilience opérationnelle.

2. Soyez proactif.

Renseignez-vous sur les opérateurs de ransomwares et leurs outils, techniques et procédures (TTP) en recueillant des informations issues de votre secteur d'activité ou de votre zone géographique. Documentez et conservez les coordonnées de tous les membres de votre équipe d'intervention, de préférence via un canal de communication hors bande. Mettez en place un canal dédié pour signaler tout comportement suspect s'apparentant à une attaque par ransomware. Constituez une équipe d'intervention à une crise cyber et, si nécessaire, faites appel aux services d'un prestataire spécialisé en réponse aux incidents.

3. Réduisez la surface d'attaque.

Identifiez et corrigez les vulnérabilités des actifs critiques. Renforcez la sécurité des systèmes, en donnant la priorité aux systèmes critiques et aux vecteurs d'attaque couramment exploités par les groupes de ransomwares. Veillez à ce que les identifiants et les droits d'accès sur l'ensemble des systèmes soient gérés selon le principe du moindre privilège. Mettez en place une segmentation du réseau afin de limiter la propagation des ransomwares et d'augmenter les chances de détecter les mouvements latéraux. Identifiez les référentiels de données mal sécurisés contenant des informations sensibles au sein de votre organisation.

4. Protégez vos sauvegardes.

Assurez-vous que les systèmes de sauvegarde sont suffisamment isolés (air-gapped), qu'ils respectent une séparation des responsabilités et qu'ils utilisent des stockages de données immuables, empêchant toute altération ou suppression par des acteurs malveillants. Utilisez l'authentification multifacteur (MFA) pour les comptes administrateurs des sauvegardes et mettez en œuvre un contrôle d'accès basé sur les rôles (RBAC). Créez et maintenez des images maîtres (« Golden Masters ») des systèmes critiques afin d'accélérer leur reconstruction en cas d'incident. Assurez-vous également que votre système de sauvegarde est capable de prendre en charge les fonctions de cybersécurité nécessaires pour répondre efficacement à un incident de type ransomware.

5. Renforcez votre protection contre les ransomwares.

Identifiez les lacunes dans la couverture actuelle de vos contrôles préventifs et de détection par rapport aux techniques ATT&CK utilisées par les groupes de ransomwares. Mettez en place des mécanismes de détection des anomalies sur les systèmes de fichiers des terminaux, correspondant à des attaques par ransomware ou wiper, telles que le chiffrement ou la suppression de fichiers. Mettez en place des filtres au niveau de la passerelle de messagerie afin de bloquer les e-mails contenant des indicateurs malveillants connus. Utilisez des applications permettant la gestion par liste d'autorisation (whitelisting) sur les actifs critiques, afin de garantir que seuls les logiciels autorisés puissent s'exécuter.

6. Renforcez la détection de vos ransomwares.

Effectuez de manière proactive des recherches dans les données historiques afin de détecter d'éventuelles compromissions. Mettez en place un mécanisme de détection des variations inhabituelles de l'utilisation du processeur (CPU) et du disque, indicatrices d'une activité potentiellement malveillante. Identifiez les protocoles réseau inhabituels, notamment I2P ou TOR, qui sont connus pour être utilisés par les groupes de ransomwares. Identifiez également les connexions réseau utilisant des ports ou des destinations connus pour être associés aux infrastructures de commande et de contrôle utilisées dans les attaques par ransomware ou wiper.

7. Réagissez à l'incident.

Identifiez et regroupez les alertes similaires liées aux actifs impactés. Élaborez une première estimation des pertes potentielles (périmètre d'impact) liées à l'incident. Identifiez les environnements de staging utilisés pour l'exfiltration de données et isolez les hôtes infectés à la fois des réseaux filaires et sans fil. Activez la salle blanche, restaurez la dernière sauvegarde des systèmes impactés et redéployez les outils de détection et de réponse de confiance sur les systèmes présents dans cet environnement sécurisé. Recherchez des preuves de mécanismes de persistance laissés par les attaquants et identifiez les vulnérabilités des systèmes qui ont été exploitées lors de l'attaque.

8. Communiquez.

Communiquez avec les parties prenantes internes, avec la presse afin de prévenir toute spéculation préjudiciable, avec les personnes concernées par les données compromises conformément aux obligations réglementaires et légales, ainsi qu'avec les autorités de régulation elles-mêmes. Informez votre compagnie d'assurance, les forces de l'ordre ainsi que le CERT national ou sectoriel compétent.

Pour plus de détails sur chacune de ces étapes, lisez le livre blanc.

COHESITY

cohesity.com/fr/

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

9100083-001-FR 4-2025