DATA SHEET

SERVICES DE CONSULTING SÉCURITÉ

Réponse à incident et analyse forensique

Incidents de sécurité : êtes-vous prêts ?

Les menaces ont atteint un tel niveau de complexité que plus aucune entreprise n'est à l'abri d'une cyberattaque ou d'une compromission de sa sécurité. Aujourd'hui, les capacités de réponse à incident ont un impact direct sur la réputation, la capitalisation boursière et la croissance des entreprises. C'est pourquoi la préparation est une thématique de plus en plus présente dans les stratégies d'entreprise.

Élaborer un plan de réponse à incident n'est pas juste une question de bon sens, mais aussi une exigence du RGPD (Règlement Général européen sur la Protection des Données) et des directives NIS (Network and Information Systems Regulations). Pour se conformer à ces réglementations, les entreprises ont l'obligation de 1) maintenir un niveau élevé de sécurité de l'information, 2) signaler toute compromission dans les plus brefs délais et 3) détailler les mesures prises pour prévenir de futures attaques.

Alors que les incidents deviennent de plus en plus fréquents, les entreprises consacrent automatiquement plus de temps et de moyens à leur résolution. Mais la maturité des dispositifs de réponse à incident varie considérablement d'une entreprise à l'autre. Pour les plus avancées, la gestion des incidents fait partie intégrante de leur plan de continuité d'activité (PCA).

Tous les incidents ne se ressemblent pas

Pouvez-vous gérer n'importe quel incident ? Pour répondre à cette question, vous devez d'abord disposer d'une visibilité complète et en temps réel de votre activité réseau. C'est là le seul moyen de savoir si vous êtes ou non l'objet d'une attaque. Vous pourrez ainsi élaborer un plan de remédiation clair et adapté à votre entreprise. Tous les incidents ne se ressemblent pas, d'où l'importance de les classer par niveau d'impact. Vous aurez alors toutes les cartes en main pour y apporter une réponse appropriée, y consacrer les ressources nécessaires pour limiter les dommages et les perturbations et reprendre rapidement le cours normal de vos activités.

Une bonne réponse à incident commence donc par une bonne analyse du risque et une parfaite connaissance de vos ressources informatiques. Mais cela ne se traduit pas forcément par de nouveaux investissements technologiques.

Les entreprises manquent parfois de clarté sur les processus, les compétences internes nécessaires et les personnes à contacter en cas de compromission. Par ailleurs, rares sont celles qui disposent d'équipes d'astreinte, mobilisables en cas d'incident. C'est pourquoi elles se tournent généralement vers un partenaire de confiance pour les situations d'urgence.

Maîtriser les enjeux de la conformité

Il est vital de bien comprendre vos obligations réglementaires et de définir leur place dans vos processus de réponse, notamment en matière de signalement d'un incident.

NTT accompagne ses clients dans la mise en place de ces processus afin qu'ils sachent quand et comment notifier les autorités judiciaires et organismes de tutelle.

Avantages de nos analyses forensiques et plans de réponse à incident

Intervention immédiate – La détection d'incidents permet de déployer une équipe d'intervention

Réduction de l'impact d'un incident – Une détection rapide des incidents permet d'en réduire considérablement l'impact

Baisse des coûts – Un contrat prénégocié est synonyme de réduction du coût de gestion d'un incident

Conservation des preuves – Les preuves forensiques sont essentielles aux investigations numériques des autorités judiciaires et à l'engagement d'éventuelles poursuites

Protection de la marque – Une gestion compétente d'un incident réduit fortement les dommages sur la marque

Atteinte des objectifs de conformité et de réduction des risques – L'application des procédures assure votre conformité aux exigences de reporting

Cette démarche comprend la mise en place de protocoles en concertation avec les pôles de l'entreprise susceptibles d'être impactés par un incident. Avec l'entrée en vigueur du RGPD et des directives NIS, les entreprises doivent désormais signaler une compromission de données aussitôt qu'elle

est détectée, détailler les mesures prises pour gérer l'incident en cours et prévenir de futures attaques.

Culture et collaboration

En cas de violation de sécurité, chacun a tendance à se renvoyer la responsabilité. Bien que les exercices de simulation soient monnaie courante, les entreprises n'ont pas toujours conscience de la valeur de ces « grandes manœuvres », sortes d'exercices d'urgence grandeur nature qui permettent à chacun de bien cerner son rôle et de prendre ses repères.

D'après notre expérience, ces exercices renforcent le sentiment de partage de responsabilité pour une résolution efficace des problèmes.

Création d'un modèle adapté de réponse à incident

Toutes les entreprises n'ont pas la même maturité en matière de planification et de réponse à incident. C'est pourquoi nous travaillons au contact étroit de nos clients pour concevoir un plan structuré qui articule clairement l'approche, les avantages et les mesures de réduction du risque applicatif. Mais notre travail ne s'arrête pas là. L'étendue de notre expertise nous permet aussi d'assurer le déploiement de ce plan – et de vous en confier les rênes une fois que tous les tests se sont avérés concluants.

- Pour les entreprises sensibles à l'importance d'une réponse rapide et efficace, le plan pourra prévoir le recours à une équipe spécialisée dans la réponse à incident. Dotée d'une parfaite connaissance de votre entreprise et de votre infrastructure technologique, cette équipe attitrée interviendra à plusieurs niveaux :
- Établissement d'une présence sur votre lieu d'activité
- Enquête forensique sur le réseau et les hôtes après incident
- Mise à disposition de compétences en gestion d'incident
- Rédaction de synthèses et de recommandations post-incidents

Actions en cas d'incident

Détection des menaces, analytique avancée, Cyber Threat Intelligence : vous bénéficiez de toute la palette des services de cybersécurité assurée par un seul et même fournisseur mondial. La création du rapport d'incident marque le point de départ de l'intervention.

NTT Incident Response peut être combiné à nos prestations de conseil (NTT Consulting Services) et fourni dans le cadre de notre offre mondiale de services de sécurité managés. À l'heure où de nombreuses entreprises peinent à gérer tous les enjeux de la cybersécurité en interne, choisir les services de NTT, c'est opter pour des experts en sécurité et une structure d'envergure mondiale.

Nos services de sécurité managés assurent la gestion des équipements de sécurité qu'ils mettent régulièrement à jour pour neutraliser les attaques. Par ailleurs, notre service EDR (Endpoint Detection and Response) procède à une mise en quarantaine des terminaux touchés pour empêcher toute propagation de malware.

Lorsqu'un incident est validé, les clients de nos services de sécurité managés peuvent demander aux analystes du SOC de NTT de prendre le relais. Ces derniers auront alors pour responsabilité de neutraliser toute menace sur le réseau. Concrètement, l'équipe du SOC se chargera d'identifier les menaces, de les confiner et de prendre les mesures nécessaires pour empêcher toute propagation de l'attaque.

De leur côté, les services de conseil de NTT accompagnent nos clients dans la gestion des incidents critiques et la sortie de crise pour reprendre rapidement le cours normal de leurs activités. Ces services prévoient l'intervention d'architectes et d'analystes forensiques sur site ou à distance.

Graphique 1 : NTT Incident Response vous permet de minimiser l'impact et le coût d'un incident, tout en protégeant vos données critiques et en adoptant des mesures efficaces de prévention de nouveaux incidents.

A propos de NTT

NTT est un leader mondial des services technologiques. Convaincus qu'ensemble nous accomplissons de grandes choses, nous avons conjugué les capacités de 28 entreprises remarquables afin de créer un leader des services technologiques. En partenariat avec vous, nous mettons notre gamme complète de capacités hors pair au service de vos collaborateurs, stratégies, opérations et technologies. Ensemble nous préparons le futur connecté.

Vous souhaitez en savoir plus sur nos services de consulting sécurité ?

Rendez-vous sur **hello.global.ntt**