Que faire en priorité en cas d’attaque informatique

Que faire en priorité en cas d’attaque informatique

Quelles sont les premières mesures à prendre lorsque l’on suspecte d’avoir été la victime d’un incident de sécurité informatique ?

A un moment ou l’autre, votre entreprise devra faire face à un incident de cybersécurité. Mais sous la pression, l’effet du stress, on fait des erreurs. Trop reporter la prise de décisions critiques peut renforcer l’impact de l’incident, mais inversement, prendre des décisions trop hâtives peut causer d’autres dommages à l’entreprise ou entraver une réponse complète.
Il existe de nombreuses façons de soupçonner qu’un incident de sécurité s’est produit, de la détection d’activités inhabituelles par le suivi proactif des systèmes critiques jusqu’aux audits, en passant par la notification externe par les forces de l’ordre ou la découverte de données compromises perdues dans la nature.
Toutefois, des indicateurs tels que la consommation inhabituelle de ressources CPU ou réseau sur un serveur peut avoir plusieurs origines différentes, dont beaucoup n’ont rien à voir avec des incidents de sécurité. Il est là essentiel d’enquêter davantage avant de tirer des conclusions.
Disposez-vous des d’indices cohérents ? Par exemple, si l’IDS détecte une attaque de force brute contre le site Web, les journaux Web le confirment-ils ? Ou, si un utilisateur signale une attaque suspectée de hameçonnage, d’autres utilisateurs ont-ils été visé ? Et quelqu’un a-t-il cliqué sur des liens ou des documents joints ?
Vous devez également réfléchir à des questions relatives à la nature de l’incident. S’agit-il d’une infection par un logiciel malveillant générique ou un piratage de système ciblé ? Y’a-t-il une attaque intentionnelle en déni de service (DoS) en cours ?…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Que faire en premier en cas d’attaque informatique*