

Retrouver les traces d'une attaque informatique peut s'avérer complexe et coûteuse





Le facteur temps : la clé de la réussite

Lorsqu'une faille est avérée, l'entreprise dépend des loc

En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.

Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.



Denis MCCORMY est Expert Informatique assumant spécialisé en cybersécurité et en protection des données personnelles.

- Expertises techniques (réseaux, systèmes, protocoles, firewalls, analyse forensique...) et juridiques (investigations MII/ANSSI, dossiers durs, emails, cookies, dédouanement de clientèle...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybersécurité ;
- Président de C.S.L. (Correspondants Informatique et Liberté) ;
- Ancien responsable de la sécurité des systèmes d'information de la Direction Générale de l'Armement (DGA) ;

Le Net Expert
INFORMATIQUE

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*