

AUDIT DE SÉCURITÉ

CONNAISSEZ-VOUS LES FAILLES DE SÉCURITÉ DE VOTRE INFRASTRUCTURE INFORMATIQUE?

À CETTE QUESTION, PEU DE GESTIONNAIRES D'ENTREPRISE PEUVENT Y RÉPONDRE. ET POUR CAUSE, SEULE 1 COMPAGNIE SUR 4 AU QUÉBEC DISPOSE DES OUTILS INFORMATIQUES NÉCESSAIRES POUR RÉALISER UN AUDIT DE SÉCURITÉ EXHAUSTIF.

UN AUDIT DE SÉCURITÉ, C'EST QUOI?

++

Un audit de sécurité peut être défini par une suite logique de tests permettant d'éprouver la sécurité d'une infrastructure informatique. Ces tests impactent aussi bien l'aspect réseautique que le côté matériel. Il est possible de procéder à un audit de sécurité de manière semi-automatisée. Le « monitoring », ou supervision, s'en trouve ainsi considérablement facilité.

Par exemple, il vous est possible de configurer un répertoire confidentiel (rapports de comptabilité, historique des paies...) afin de savoir qui a tenté d'y avoir accès, qui a tenté d'en modifier le contenu...

++

Audit de sécurité, quels tests?

- Le monitoring de l'observateur d'évènements
- Le test d'intrusion fondement
- Le test d'intrusion réseau
- Le test d'intrusion applicatif
- Le test d'intrusion web
- Le test de la propagation
- Le test de détection de clef wi-fi en mode SSID invisible
- Le test des ports ouverts (de 1 à 65 536)
- Le test de charge sur chaque port (de 1 à 65 536)
- Le test d'exfiltration des données

À chaque test correspond une analyse permettant de dégager une politique stricte de sécurité informatique.

Vous souhaitez vous aussi bénéficier de l'expertise de nos équipes certifiées en sécurité informatique? Contactez notre département d'Audit de sécurité.