

MENACES INTERNES

VOTRE PLUS GRAND RISQUE DE SÉCURITÉ VIENT DE L'INTÉRIEUR



Qu'est ce qu'une menace interne ?

Le risque de sécurité posé par les employés, associés, partenaires, sous-traitants et prestataires de services d'une entreprise ayant accès aux ressources et aux données de celle-ci est qualifié de menace interne. L'activité des collaborateurs est l'un des principaux problèmes de sécurité pour les données de l'entreprise, car les auteurs de ces actes ont déjà franchi la première ligne de défense.

34% DE TOUTES LES VIOLATIONS IMPLIQUENT DES ACTEURS INTERNES^[1]

Les profils des menaces internes



Les initiés négligents

compromettent la sécurité des entreprises en négligeant de suivre les stratégies de cybersécurité. Ils sont souvent la proie d'attaques d'ingénierie sociale.

UNE ARNAQUE PAR PHISHING A COÛTÉ À FACEBOOK ET GOOGLE **\$100 MILLION.**^[2]



Les initiés imprudents

sont des employés dont les comptes sont compromis par des acteurs externes. Ils sont des participants involontaires aux incidents de sécurité.

5.2 MILLION DE DOSSIERS CLIENTS DU MARRIOTT ONT ÉTÉ CONSULTÉS VIA DES COMPTES D'EMPLOYÉS COMPROMIS^[3]



Les initiés malveillants

utilisent délibérément leur accès légitime à des données essentielles pour les voler, supprimer, altérer ou divulguer à des fins de vengeance ou de gain personnel.

2.9 MILLIONS D'ENREGISTREMENTS DE PII ONT ÉTÉ DIVULGUÉS PAR UN EMPLOYÉ VINDICATIF DE DESJARDINS^[4]

Les motivations des menaces internes

Selon le

Data Breach Investigations Report,^[1]

les principales motivations du vol de données sont :



Le gain financier



L'espionnage



Autres
(La négligence, la vengeance, etc.)

L'impact des attaques internes

1

Des pertes monétaires considérables

Le coût par attaque interne se situe entre **\$100,000 ET \$2 MILLION.**^[5]



2

Des pertes de données critiques

En 2020, le nombre de données personnelles exposées a augmenté de **141%**^[6]



3

Des perturbations opérationnelles

Le coût des perturbations opérationnelles sur cinq ans pour une entreprise victime d'une violation de données s'élève à **\$1.2 BILLION.**^[7]



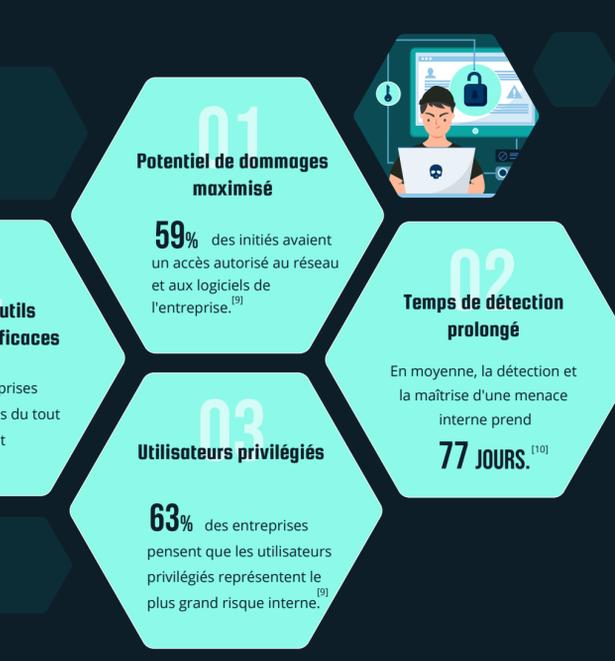
4

La perte de crédibilité

70% des consommateurs cesseraient de faire affaire avec une entreprise si celle-ci était victime d'une violation de données.^[8]



Pourquoi les attaques internes sont difficiles à combattre ?



Comment limiter les menaces internes ?

Regrouper les rapports d'activité des utilisateurs

Plus vous avez de visibilité dans votre environnement Active Directory, plus vous avez de chances de détecter les menaces internes.



Surveiller les utilisateurs privilégiés

Composante essentielle de la détection des menaces internes, la surveillance des utilisateurs privilégiés vous aidera à garder un œil sur les utilisateurs qui peuvent causer le plus de dommages.

Suivre l'utilisation et le déplacement de données :

Auditez tous les accès aux données, y compris les changements d'autorisation et les transferts de données vers des périphériques de stockage externes, afin de détecter rapidement les anomalies.

Automatiser les réponses aux incidents de sécurité

Appliquer des mesures telles que l'arrêt des machines et la déconnexion des sessions utilisateur pour limiter les violations de données.

Mettre en place une analyse du comportement des utilisateurs

Détectez, examinez et réduisez les menaces telles que les connexions malveillantes, les transferts de données, les abus de privilèges, les violations de données et les logiciels malveillants.

ManageEngine ADAudit Plus

Lutter contre les menaces internes avec ADAudit Plus

ManageEngine ADAudit Plus est un outil d'audit des changements piloté par UBA qui surveille en permanence l'activité des utilisateurs et fournit des rapports détaillés pour améliorer votre stratégie de détection des menaces internes.

Découvrez les capacités de détection des menaces internes d'ADAudit Plus grâce à un essai gratuit de 30 jours.

Écrivez-nous à commercial@pgsoftware.fr pour programmer une démonstration personnalisée.

Télécharger maintenant

PG Software

commercial@pgsoftware.fr
www.pgsoftware.fr

Data sourced from:

1. Data breach investigations report 2. CNBC 3. Marriott International 4. Secureworld 5. Bitglass - Insider threat report 6. Data Breach QuickView report 7. Beneath the surface of a cyberattack 8. Thales 9. Cybersecurity Insiders - Insider threat report 10. Cost of Insider threats