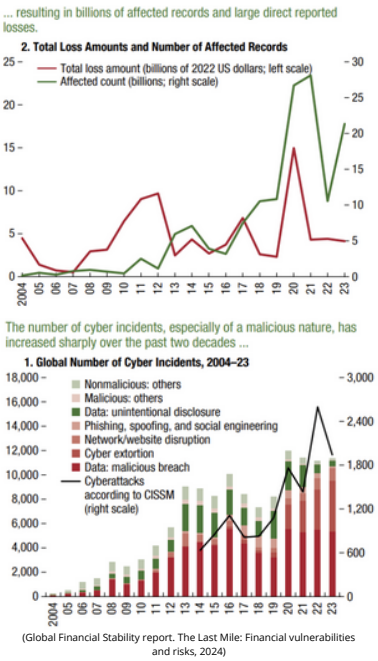
La sécurité proactive des données: votre meilleure défense

Les cyberattaques sont en forte augmentation : Depuis la pandémie de COVID-19, leur nombre a presque doublé.

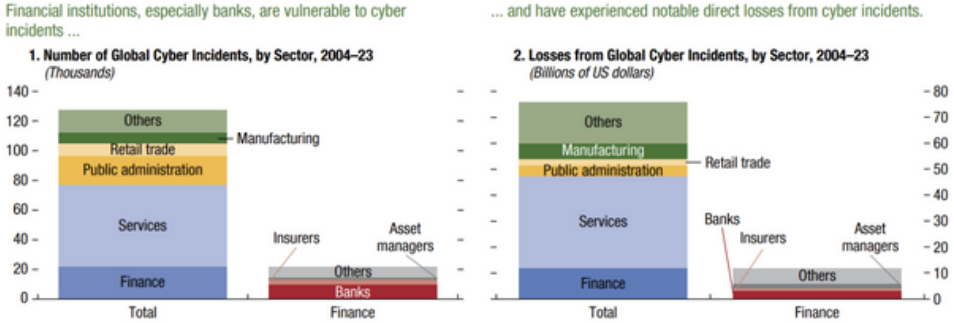
- Pertes directes signalées généralement faibles (~0,5 million $), mais le risque de pertes extrêmes (>2,5 milliards $) est en hausse.
- Le secteur financier est particulièrement vulnérable, avec 20 % des incidents le touchant.

*Depuis 2020, les pertes directes agrégées signalées à la suite d'incidents cyber atteignent près de **28 milliards de dollars**, avec **des milliards de données volées ou compromises**.*



(Global Financial Stability report. The Last Mile: Financial vulnerabilities and risks, 2024)

Pourquoi la sécurité des données n'est pas qu'une question informatique : Dans le secteur financier, la sécurité des données dépasse largement l'informatique. C'est un pilier essentiel de la gestion des risques, de la confiance des clients et de la conformité réglementaire. Une violation de données peut déstabiliser l'ensemble de votre organisation.



(Global Financial Stability report. The Last Mile: Financial vulnerabilities and risks, 2024)

Sécurité des données & Gestion des risques :

Des pratiques solides en sécurité des données sont essentielles pour gérer efficacement les risques.

- 60 % des entreprises victimes d'une cyberattaque ferment en six mois [Cybersecurity Ventures].
- Le coût moyen des interruptions pour les entreprises financières est de 700 000 $ par heure [ITIC].
- Une violation de données entraîne en moyenne une perte de 3,9 % de la valeur boursière [Comparitech].

L'importance d'une approche globale :

La sécurité des données nécessite l'implication de toutes les parties prenantes.

- 95 % des violations de sécurité sont dues à une erreur humaine [World Economic Forum].

Sécurité des données & Confiance des clients :

Les clients confient leurs informations financières les plus sensibles.

- 80 % des consommateurs changeraient d'entreprise après une violation de données personnelles [ForgeRock].
- 69 % des consommateurs perdent confiance après une telle violation [PwC].

Sécurité des données & Conformité réglementaire :

- DORA, NIS2 et FINMA imposent des exigences strictes sur la gestion des données financières. Le non-respect des règles FINMA peut entraîner des amendes importantes, des restrictions ou la révocation de licence.

Solutions Fortinet : Sécuriser les données des institutions financières

L'expertise de keyIT en solutions Fortinet : **keyIT**, partenaire de confiance en cybersécurité, est spécialisé dans les solutions Fortinet pour le secteur financier. Au-delà de simples outils standards, nous configurons des politiques de sécurité sur-mesure et déployons des solutions avancées, adaptées à vos besoins et à votre profil de risque. Forts de notre expérience en sécurité réseau et cloud, keyIT propose une protection complète et efficace.

find us www.keyit.ch | mail us sales@keyit.ch | call us +41 58 450 20 50

Solutions clés : keyIT déploie une large gamme de solutions Fortinet

FortiGate SD-WAN	FortiAnalyzer Analytics	FortiGate Firewall	FortiGate VM Virtual Firewall

Protection des données sensibles :

- Surveillance et blocage des menaces : FortiGate prévient les cyberattaques (piratage, malwares).
- Contrôle des accès : Gestion des applications autorisées et blocage des accès non autorisés.
- Filtres web : Blocage des sites dangereux et prévention des téléchargements malveillants.
- Analyse du trafic : Détection et suppression des malwares dans le trafic réseau.
- Isolation des menaces : FortiGate identifie et bloque les fichiers suspects.

Respect des exigences de conformité :

- Audit et conformité : Fortinet génère des rapports prouvant l'alignement avec DORA, NIS2, et FINMA.
- Normes de sécurité : Mesures conformes aux meilleures pratiques du secteur.

Sécurisation de l'accès à distance et des succursales :

- Tunnels chiffrés : Confidentialité garantie pour toutes les connexions, même à distance.
- Authentification renforcée : FortiGate vérifie utilisateurs et appareils avant l'accès.

Amélioration des performances réseau :

- Optimisation : FortiGate et SD-WAN assurent des performances fluides pour les applications critiques.
- Gestion de la bande passante : Évite les ralentissements.

Renforcement de la confiance :

- Stratégie de sécurité solide : keyIT et Fortinet protègent les données des clients, renforçant la confiance.

Réduction des coûts :

- Consolidation des outils : Fortinet réduit le besoin de plusieurs fournisseurs, simplifiant la gestion.

Études de cas réelles

Étude de cas 1 : Protéger un héritage familial - Un petit family office

Défi : Un family office multi-générationnel devait protéger ses données financières sensibles, accessibles par des membres et conseillers depuis différents lieux et appareils.

Solutions :

- **Passerelle sécurisée :** FortiGate Firewall pour protéger et surveiller toutes les connexions réseau.
- **Gestion centralisée :** Centralisation et chiffrement des données, permettant un accès sécurisé en tout lieu.
- **Accès à distance sécurisé :** Connexion sécurisée pour les membres de la famille et les conseillers.
- **Sécurité multicouche :** Protection avancée contre les menaces et prévention des pertes de données.

Résultats :

- **Tranquillité d'esprit :** Protection totale contre les accès non autorisés et les violations de données.
- **Opérations simplifiées :** Gestion centralisée améliorant la collaboration.
- **Conformité :** Conformité réglementaire facilement démontrée.

Étude de cas 2 : Protéger la confiance des clients - Une société EAM

Défi : Cette société en pleine croissance devait sécuriser l'expansion de son infrastructure tout en maintenant une connectivité fluide et une sécurité cohérente entre plusieurs bureaux.

Solutions :

- **Expansion sécurisée :** Extension transparente du réseau pour garantir un accès sécurisé entre bureaux.
- **Sécurité cohérente :** Politiques de sécurité appliquées uniformément sur tous les sites.
- **Intégration rapide :** Mise en place technique de nouveaux bureaux, facilitant une croissance évolutive.
- **Protection proactive :** Détection et blocage des cyberattaques avec des mesures de sécurité avancées.

Résultats :

- **Tranquillité d'esprit :** Protection totale contre les accès non autorisés et les violations de données.
- **Opérations simplifiées :** Gestion centralisée améliorant la collaboration.
- **Conformité :** Conformité réglementaire facilement démontrée.

Contactez keyIT dès aujourd'hui. Discutons ensemble de la manière dont nous pouvons bâtir une posture de sécurité robuste qui vous permettra de naviguer dans le paysage numérique en toute confiance.

find us
www.keyit.ch
mail us
sales@keyit.ch
call us
+41 58 450 20 50