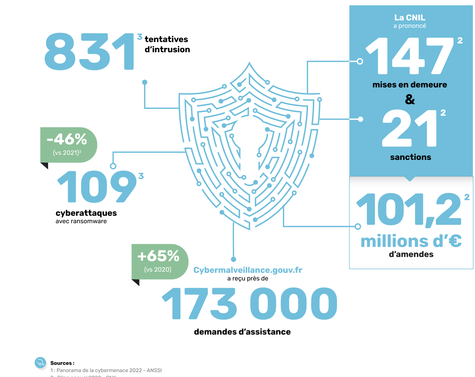
oodrive

Cybersécurité : quel bilan pour les entreprises ?

État des lieux de la cybersécurité :

Dans son dernier panorama[1] 2023 sur les risques cyber, l'**ANSSI** annonce un niveau encore élevé des menaces. Si les **opérateurs régulés** sont **épargnés**, les organismes moins sécurisés restent des cibles privilégiées. Les rançongiciels ont diminué pour laisser la place aux **menaces d'espionnage.**



831[3] **tentatives d'intrusion**

-46% (vs 2021)[3]

109[3] **cyberattaques** avec ransomware

+65% (vs 2020)

Cybermalveillance.gouv.fr a reçu près de

173 000 **demandes d'assistance**

La CNIL a prononcé

147[2] **mises en demeure**

&

21[2] **sanctions**

101,2[2] **millions d'€ d'amendes**

Sources :
1 : Panorama de la cybermenace 2022 - ANSSI
2 : Bilan annuel 2022 - CNIL
3 : Panorama de la menace informatique 2021 - CERT-FR

Quels sont les risques financiers[1] en cas de cyberattaque ?

Il est, aujourd'hui, presque impossible d'échapper aux risques cyber. Selon une étude menée par IBM, 83% des entreprises ont été victimes de plus d'une violation de données. **L'intrusion dans un système d'information entraine des coûts importants pour l'entreprise :**

4,09 millions d'€
Coût moyen d'une violation de données en 2022 en France

60%
des violations ont entrainé des hausses de prix répercutées sur les clients

19%
des intrusions se sont produites en raison d'un partenaire commercial compromis

277 jours en moyenne
pour identifier et neutraliser une cyberattaque, et plus le cycle de violation est long, plus le coût est élevé pour l'entreprise

En cas de piratage, la CNIL peut sanctionner l'entreprise victime, avec des amendes pouvant s'élever à

20 millions d'€

ou jusqu'à **4%** du CA annuel mondial

À noter que l'option Cloud sécurisé permet de réduire de **660 000 €** le coût moyen et de réduire le cycle de violation de **40j** en cas d'attaque.

Sources :
1 : Coût d'une violation de données en 2022 - IBM

Les 3 piliers pour bien protéger ses données

Les risques grandissants impliquent, pour les entreprises, **la mise en place de process et d'outils de protection, détection et de gestion des attaques.**

Protection

+139%[1]
pour le piratage de compte en 2021. L'humain est la première faiblesse d'un SI, il est donc indispensable de le former aux risques cyber.

L'ANSSI a mis en évidence une recrudescence des attaques sur les annuaires Active Directory, particulièrement mal protégés dans les entreprises. Elle met ainsi à disposition un recueil de points de contrôle, afin d'accompagner les chaines DSI et SSI dans le suivi du niveau de sécurité de ces annuaires.

Mettre en place un VPN ou un Proxy pour masquer son adresse IP et réduire les risques de ciblage des cyber criminels.

45%
des intrusions surviennent dans le Cloud.
Il est donc indispensable de choisir un Cloud sécurisé SecNumCloud.

Détection

Déployer un EDR (Endpoint Detection and Response), dispositif automatique détectant les comportements anormaux dans les systèmes d'information à l'aide de l'intelligence artificielle. Le programme évolue et s'enrichit également grâce au machine learning pour détecter de nouvelles menaces.

Le SOC (Security Operations Center), composé de spécialistes cyber et d'analystes des données, est un outil devenu indispensable. Qu'il soit interne, externe ou hybride, il renforce les capacités de détection d'une organisation tout en apportant une réponse rapide en cas d'attaque.

Gestion

Définir un protocole de gestion de crise clair et efficace grâce à des simulations régulières.

Souscrire à une cyber-assurance pour limiter les risques financiers.

En France,
2/3[2]
des entreprises ont déjà opté pour cette option.

Sources :
1 : Rapport d'activité 2021 - Cybermalveillance.gouv.fr
2 : Baromètre de la cybersécurité des entreprises 2023 - CESIN

www.oodrive.com