Les grandes tendances de la cybersécurité 2021

En plus de fragiliser considérablement les systèmes informatiques des entreprises, la crise du Covid-19 a transformé le terrain de jeu des cybercriminels et remodelé les cyber menaces. Selon L'ANSSI, le niveau d'alerte des cyberattaques atteint des sommets si bien que fin 2020; le nombre de victimes des cyberattaques aurait quadruplé en l'espace d'un an en France. Focus sur l'état de la cybersécurité en 2021 !

Les cyberattaques en entreprise

Alors que le coût moyen d'une cyberattaque atteignait l'année dernière **3,86 millions de dollars**, ce dernier est estimé cette année à pas moins de **4,24 millions**. **Cette augmentation conséquente de 10%** résulte des multiples changements opérationnels et des vulnérabilités associées apparues pendant la crise sanitaire mondiale du Covid-19.

LE COÛT MOYEN D'UNE CYBERATTAQUE EN ENTREPRISE EN 2021
(Rapport IBM Security 2021)

+10%

LE COÛT MOYEN D'UNE CYBERATTAQUE REPRESENTE +10% PAR RAPPORT À 2020
(Rapport IBM Security 2021)

Entre le premier semestre 2020 et le premier semestre 2021, **l'ANSSI évalue l'augmentation du nombre d'attaques à :**

+60%

Le délai moyen écoulé entre une **intrusion** et sa **détection** est aujourd'hui de :

212 jours

Il faut ensuite pas moins de **75 jours en moyenne** pour **sécuriser une intrusion**

75 jours

> «Les cybercriminels ont mis en place un modèle économique du « ransomware as a service » (RaaS) qui est redoutablement efficace. Avec le RaaS, n'importe quel escroc sans compétence informatique peut devenir un cybercriminel. Les logiciels de rançon sont commercialisés clé en main sur le darkweb. »
>
> Guillaume Poupard
> Directeur de l'ANSSI

Selon des estimations Gartner, les dépenses mondiales en **technologies et services de sécurité informatique et de gestion des risques** devraient augmenter **de 12,4 %** atteignant ainsi **150,4 milliards de dollars en 2021.**
Cela représente une augmentation près de **deux fois supérieurs à 2020.**
(Rapport Gartner 2021)

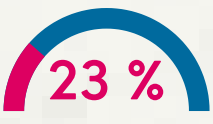
Les principaux secteurs et types d'attaques

> Les violations de données dans **le secteur de la santé** sont celles qui ont été les plus coûteuses : "en moyenne elles ont coûté 9,23 millions de dollars, suivies par les services financiers (5,72 millions de dollars) et les produits pharmaceutiques (5,04 millions de dollars)".
> *(Rapport IBM Security 2021)*

A l'échelle mondiale, les secteurs les plus touchés par les attaques informatiques sont **les secteurs de la santé et les services financiers.**

En France en revanche, ce sont les services financiers mais aussi **le secteur pharmaceutique ainsi que celui des technologies** qui enregistrent les plus grosses compromission de données.
(Rapport IBM Security 2021)

En 2020, les hôpitaux français auraient subi pas moins de 27 cyber-attaques majeures.
(Rapport IBM Security 2021)



La recrudescence des Rançongiciels

les attaques par rançongiciels représentent ainsi **23%** de toutes les attaques observées en 2020.
(Rapport IBM Security X-Force)

Le facteur humain : nouvelle faille de l'ingénierie sociale et du phishing

85 %

85% des compromissions de sécurité informatique engagent **le facteur humain**
(Rapport Verizon 2021)

Le phishing se retrouve dans **36 % des compromissions observées en 2021** (25 % en 2020).
La compromission d'adresses e-mail professionnelles devient la 2e forme la plus commune d'ingénierie sociale. Ceci illustre bien l'augmentation conséquente des usurpations et violations d'identité, 15 fois plus nombreuses qu'en 2020.
(Rapport Verizon 2021)

HUMAN FIRST.
DIGITAL EXPLORERS.

mc2i