FÉVRIER 2022

La réelle pandémie de 2022

Décryptage des cyberattaques et mesures de protection face au risque

CABINET PREVIAVIE

LES TROIS TYPES DE CYBERATTAQUES LES PLUS COURANTES

L'**hameçonnage** aussi appelé **phishing**, reste l'une des principales formes de la cybercriminalité. Il s'agit d'une technique de fraude qui vise à duper le destinataire d'un courriel en apparence légtime afin de l' inciter à transmettre ses données personnelles ou bancaires en se faisant passer pour un tiers de confiance (banques, administrations, sites de commerce en ligne, fournisseurs d'énergie, ...).

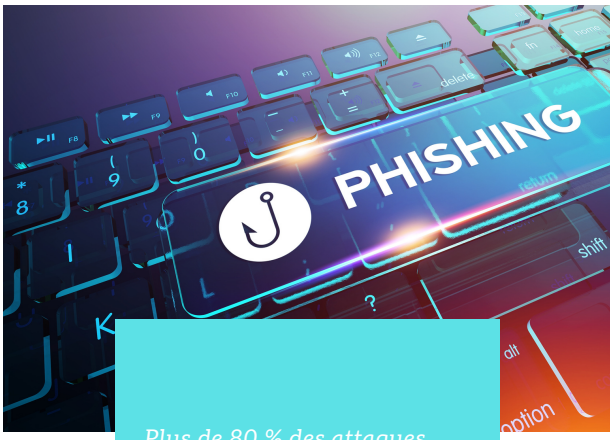
Les cybercriminels utilisent divers types de messages (mail, SMS, appel téléphonique) pour duper leur victime et leur extorquer des informations confidentielles ou en mettant à leur portée des codes malveillants en attendant qu'elle les active à leur insu soit en ouvrant une pièce jointe soit en cliquant sur un lien hypertexte.

Ces codes lorsqu'ils sont activés permettent aux cybercriminels de pirater le compte de la victime en pénétrant le système d'information et ainsi d'en faire un usage frauduleux.

L'hameçonnage peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès.

Les vecteurs d'**attaque par phishing s'élèvent à environ 80 %.** (1)

Google a découvert plus **de 2.1 millions de sites de phishing** en janvier 2021.(2)



Plus de 80 % des attaques informatiques serai des attaques par phishing

Néanmoins ce type d'attaque informatique dépend en majeur partie de l'éducation informatique des collaborateurs d'une entreprise.

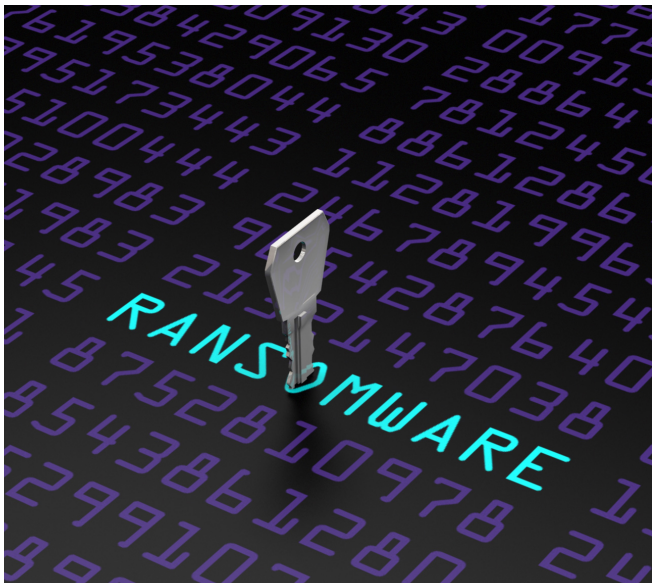
Ainsi, la quasi-totalité des attaques par hameçonnage sont dues à une erreur humaine, car ce sont les utilisateurs qui ouvrent une porte dans l'entreprise en donnant malencontreusement leurs codes d'accès.

On estime qu' **un dirigeant sur dix seulement, sensibilise** régulièrement **ses employés sur cette menace cyber**.

(1) : Rapport d'information du Sénat relatif à la cybersécurité des entreprises -2020-2021

(2) : https://www.groupe-delta.com/communication/cybersecurite-10-statistiques-choc-a-retenir-en-2021/

Un **ransomware,** en français **rançongiciel**, est un type de programme malveillant conçu pour pirater les ordinateurs et contraindre les victimes à payer une rançon pour que leurs fichiers soient déchiffrés. Les pirates informatiques infectent votre ordinateur en vous demandant de télécharger la pièce jointe malveillante attachée à un e-mail ou de vous rendre sur un site contenant un code, qui chiffre par la suite vos fichiers critiques ou vous refuse l'accès à votre ordinateur.



Vous saurez immédiatement si un ransomware est présent dans votre appareil car il bloque l'accès et chiffre généralement vos fichiers. Dans les deux cas, vous ne pouvez plus ouvrir et travailler avec des données cruciales : documents de travail, photos ou vidéos personnelles. Les cybercriminels à l'origine de l'attaque vous contacteront pour vous faire part de leurs exigences, en vous promettant de déverrouiller votre ordinateur ou de déchiffrer vos fichiers une fois que vous aurez payé une rançon (généralement en Bitcoin).

Parmi les voies d'infection les plus courantes des ransomwares, citons la visite de sites Web malveillants, le téléchargement d'une pièce jointe malveillante ou l'utilisation de modules complémentaires indésirables lors des téléchargements. Il suffit d'un seul moment d'inattention pour être victime d'une attaque par ransomware.

Le fait de disposer **d'un personnel informatique formé et capable d'arrêter les attaques est la principale raison pour laquelle certaines entreprises sont convaincues qu'elles ne seront pas touchées par un ransomware à l'avenir**. Et pourtant en France (3) :

- **30 % des entreprises** déclarent avoir été touchées par **un ransomware en 2020**
- le **montant moyen des rançons** versées est de **128 000 euros**.

Cependant, en moyenne, **seulement 65 % des données chiffrées** ont été restaurées après le paiement de la rançon.

- **le coût moyen de remédiation d'une attaque de ransomware**, qui incluent les temps d'arrêts, les commandes perdues, les coûts opérationnels et de nombreux autres paramètres, **sont passés de 390 000 euros en 2020 à 921 000 euros en 2021**.

Ainsi, **le coût moyen de reprise d'activité après une attaque par ransomware** est désormais presque **10 fois plus important** que **le montant moyen des rançons versées.**

ATTAQUE PAR DOS (DÉNI DE SERVICE) OU DDOS (DÉNI DE SERVICE DISTRIBUÉ)

Les attaques par DoS (Déni de service en anglais Denial of service) visent à saturer un ordinateur ou un système en réseau sur internet en dirigeant vers lui un volume considérable de requêtes le rendant ainsi inaccessible. On parle également d'attaques par DDoS (Déni de service distribué en anglais Distributed denial of service) pour des attaques visant elles aussi les ressources d'un système mais lancées à partir d'un grand nombre d'autres machines hôtes infectées par un logiciel malveillant contrôlé par l'attaquant.

Qu'il s'agisse d'une attaque DoS ou DDoS, le cybercriminel agit souvent pour extorquer une rançon, mettre une entreprise hors service pour des concurrents malveillants ou encore exprimer le mécontentement de certains employés actuels ou anciens.

Les **attaques DDoS** ont **augmenté de 151%** au cours du **premier semestre 2020 et** constituent **aujourd'hui un** enjeu bien réel pour les entreprises. **(4)**

En 2020, les rançons par DDos **demandées à des entreprises européennes** atteignaient **10 bitcoins**, **soit 90 000 €. Aujourd'hui,** ce montant **se rapprocherait des 330 000 €. (5)**

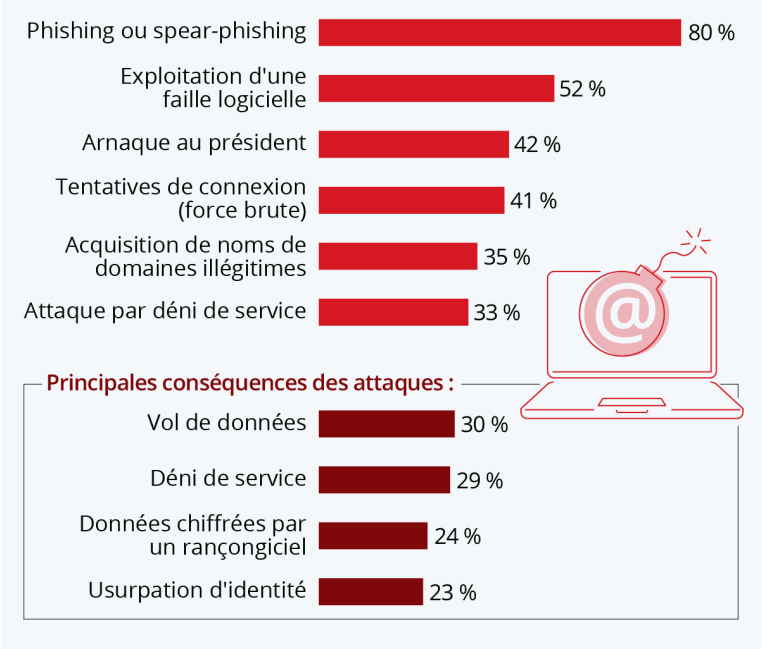
(3) : https://news.sophos.com/wp-content/uploads/2021/05/sophos-state-of-ransomware-2021-wpfr.pdf
(4) : Rapport de Neustar Inc. sur les menaces et les tendances en matière de cybercriminalité, 2020
(5) : « Le retour de la rançon par DDoS »-Journal du Net 2021

UNE RECRUDESCENCE DES CYBERATTAQUES

Les menaces informatiques sont **variées et redoutables de sophistication**. Toutes les études arrivent à la même conclusion : les **entreprises sont de plus en plus victimes de piratage informatique.**

Selon les chiffres de l'ANSSI, **les cyberattaques ont explosé en 2020, soit une hausse de 255% en un an.** De plus, les attaques par **hameçonnage** (phishing) ont **augmenté de 22% sur le premier semestre 2021, par rapport à 2020.** Selon le baromètre établi par le FIC (Forum International de la Cybersécurité), **les entreprises publiques et privées ont été largement ciblées par les organisations pirates, engendrant des violations de données en hausse de 20% en 2020.** (5)
Selon le rapport 2021 VmWare sur l'état des menaces en France, **74 % des RSSI français interrogés craignent que leur entreprise subisse une violation significative au cours de l'année à venir.**

Répartition des cyberattaques visant les entreprises depuis 2020



(5) : « Le retour de la rançon par DDoS »-Journal du Net 2021

L'OR Numérique

> *L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique.*
>
> *Albert Einstein*

La data est omniprésente, la protection des données personnelles est un enjeu de taille.
En effet, bien que nous « consentions » à la collecte et à l'utilisation de nos informations personnelles sur le web, en cochant la fameuse case « J'accepte » sans aucune contrepartie hormis l'accès gratuit au service, rien ne nous garantit la protection de celles-ci, ni qu'elles ne seront pas utilisées à des fins de revente.

COMMENT S'EN PROTÉGER ?

LA CYBERSÉCURITÉ ET SES BOUCLIERS

Se couvrir des risques Cyber c'est possible !

Dans un monde de plus en plus digitalisé, les «risques numériques » ou «risques cyber» évoluent très rapidement car ils capitalisent sur les technologies émergentes (comme le big data, l'intelligence artificielle...), profitent du développement du cloud et de l'accélération du télétravail.

Ces nouveaux risques représentent une réelle menace pour les entreprises quels que soient leur taille et leur secteur d'activité. La **cyber assurance** est désormais **indispensable** pour **protéger** le **patrimoine, l'activité de l'entreprise** et lui permettre de **faire face à une cyber attaque**.

Avec une **cyberattaque toutes les 39 secondes dans le monde, aucune solution de protection de données peut être efficace à 100% :** ni authentification à deux facteurs ni autres mesures de ce type, même **si elles sont fortement conseillées**.

En général, **nos entreprises sont couvertes contre les dommages tels que les dégâts des eaux, incendies, vol de matériel etc... et non contre le risque cyber dont elles sous-estiment le danger.**

Les victimes de cyberattaques pensent souvent que leurs assurances traditionnelles les couvrent contre les risques cyber, mais c'est FAUX!

Un chiffre qui illustre à lui seul **le danger invisible mais réel des cyberattaques : 60% des entreprises touchées par des cyberattaques déposent le bilan (6) !**

Les **entreprises** commencent **à prendre conscience de l'intérêt de souscrire à une assurance cyber** pour se protéger des **terribles conséquences financières** et de **réputation** liées aux cyberattaques dont elles pourraient être victimes.

(6) : Rapport d'information du Sénat relatif à la cybersécurité des entreprises -2020-2021

Previavie

VOTRE CYBER PROTECTION

POURQUOI NOUS CONTACTER ?

La cybersécurité au coeur des enjeux économiques de votre entreprise

Previavie

Qui sommes nous ?

Des experts en assurance :

- **Cyber**
- **Fraude**
- **RGPD**

Nous travaillons avec plusieurs entreprises que nous assurons contre le risque cyber. Elles sont plus sereines pour la pérennité de leurs activités car protégées contre cette menace invisible mais réelle.

L'équipe Previavie vous apporte conseils, expertise et savoir-faire pour que l'accès à la cyber assurance ne soit plus un frein à la cyber protection.

Si vous souhaitez protéger votre entreprises de ces risques, je vous invite à nous contacter ou scanner le code QR et remplissez le formulaire pour une demande d'entretien.

Dans un monde interconnecté où la collecte d'informations et les échanges numériques explosent, l'exposition aux cyberattaques ne cesse d'augmenter.

Ce risque est aussi réel que celui d'avoir un accident de voiture ou de faire une chute dans l'escalier !

La cybersécurité n'est plus une option !

01 82 83 01 50

www.cyber.previavie.com