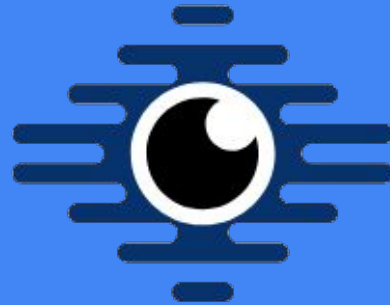



Nostroguard

Promouvoir la cybersécurité pour tous



NOSTROGUARD
SECURITY

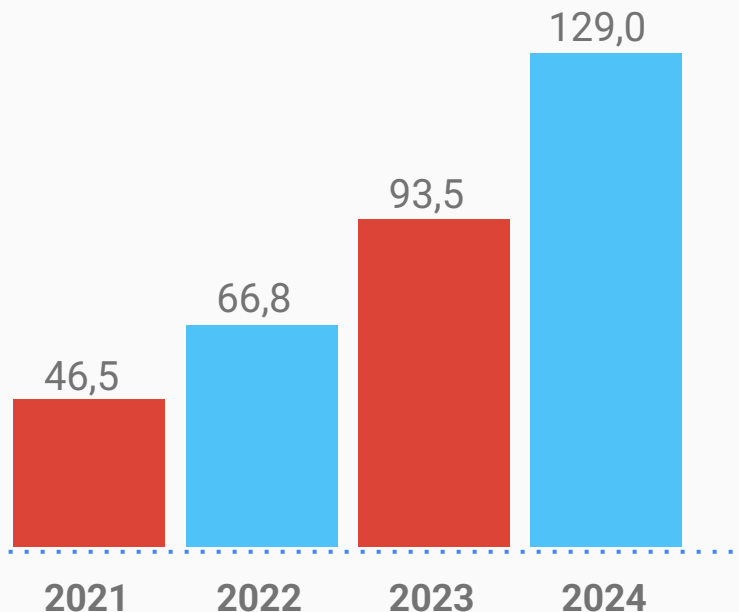
The background image shows a laptop screen with a dark overlay. On the screen, there is a line graph with a blue line showing an upward trend, and a pie chart with a blue and green segment. The text is overlaid in white, bold font.

Notre mission :
Sensibiliser aux attaques
cybercriminelles envers les
entreprises

Coûts en milliards en France

Les coûts incluent :

- Dommages de réputation
- Arrêt des activités
- Amendes et légalité
- Vols de propriété intellectuelle





Risques courants

Nous allons maintenant
présenter les vecteurs
d'attaque les plus utilisés
envers les entreprises.



Phishing

Définition

L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

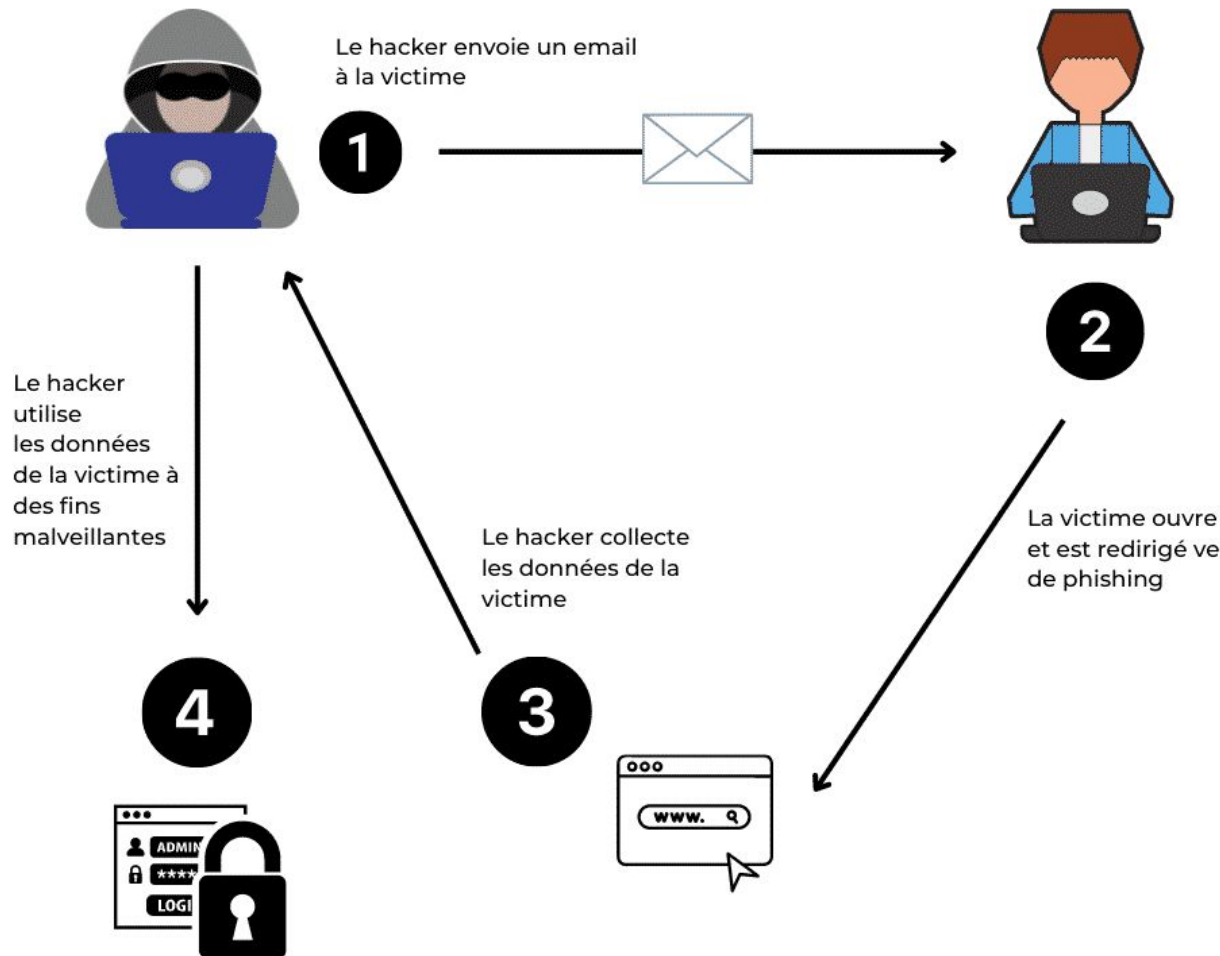
Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.).

CNIL

En pratique

Le phishing est le premier risque cyber dans les entreprises.

Une entreprise met en moyenne 50 jours à détecter des activités suspectes après l'attaque.



Phishing : les risques

Coûts : En moyenne 4.9M euros sont perdus par l'entreprise à chaque attaque réussie

Fréquence : Représente à peu près 40% des mails frauduleux

Utilisation : Méthode d'attaque principale dans les cyberattaques d'envergure

source : keepnetlabs



Fraude au président / FOVI

Définition

L'arnaque au président consiste pour le fraudeur à contacter une entreprise cible, en se faisant passer pour le président de la société mère ou du groupe. Le contact se fait par courriel ou par téléphone. Après quelques échanges destinés à instaurer la confiance, le fraudeur demande que soit réalisé un virement international non planifié, au caractère urgent et confidentiel. La société sollicitée s'exécute, après avoir reçu les références du compte étranger à créditer.

Fraude aux Faux Ordres de Virement #FOVI

1



L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)

2



Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétend exécuter une opération financière urgente et confidentielle

3



Sous la pression ou en confiance, l'entreprise exécute la transaction

4



L'escroc transfère l'argent vers des comptes basés à l'étranger

FOVI : les risques

Coûts : 312M d'euros en france en 2023

Fréquence : +18% d'augmentation des transactions frauduleuses.

Utilisation : Argent rendu intraçable après les transactions

source : banque de france

An aerial photograph of the New York City skyline at dusk. The sky is a mix of dark blue and orange, with scattered clouds. The city lights are visible, and the Empire State Building stands out prominently in the center. The title 'Violation des données Internes' is overlaid in white text.

Violation des données Internes

Définition

*Une violation de la sécurité se caractérise par la **destruction**, la **perte**, l'**altération**, la **divulgation** non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'**accès non autorisé** à de telles données, de manière accidentelle ou illicite.*

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles.

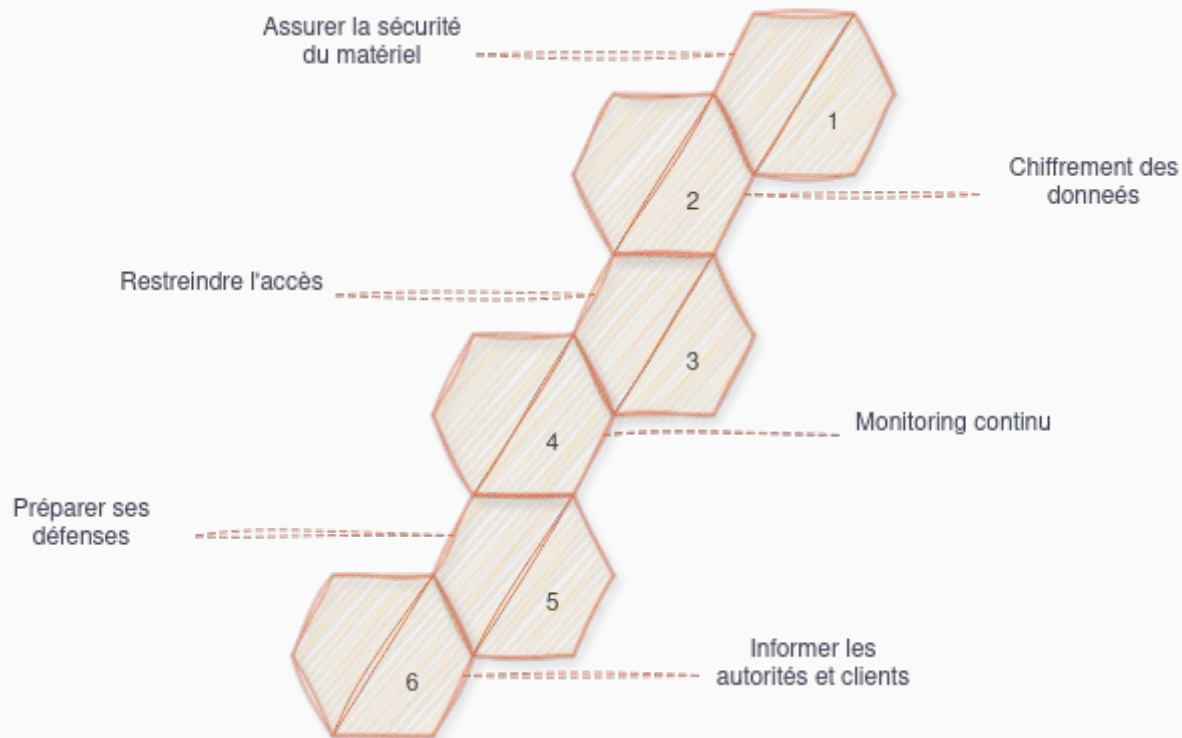
Prévention des violations

Dans la plupart des cas concrets :

Des services mal configurés peuvent exposer des données directement sur internet.

Une mauvaise sécurité permet à un utilisateur malintentionné d'accéder aux ressources

Les entreprises mettent en risque les utilisateurs en étouffant l'incident.



USB Drop

An aerial photograph of the New York City skyline at dusk. The sky is a mix of dark purple, blue, and orange. The city is densely packed with skyscrapers, many of which are illuminated with their lights. The Empire State Building is prominent in the center, with its top lit in red and green. The Hudson River is visible on the right side of the image. The text "USB Drop" is overlaid in a large, white, sans-serif font on the left side of the image.

Définition

*Une attaque par **USB Drop**, où des attaquants laissent des clés USB pour que des victimes non méfiantes les trouvent et les connectent à leurs ordinateurs, est une menace cybernétique importante souvent sous-estimée.*

*Bien que les **clés USB** soient très utiles pour stocker et transférer des données, elles servent également de puissants vecteurs pour des cyberattaques.*

De nombreux utilisateurs ignorent les risques de sécurité liés à ces petits appareils portables.

En détails

Attaque très simple à réaliser

50% des clés trouvées sont branchées

Très peu de prévention par rapport à d'autres attaques

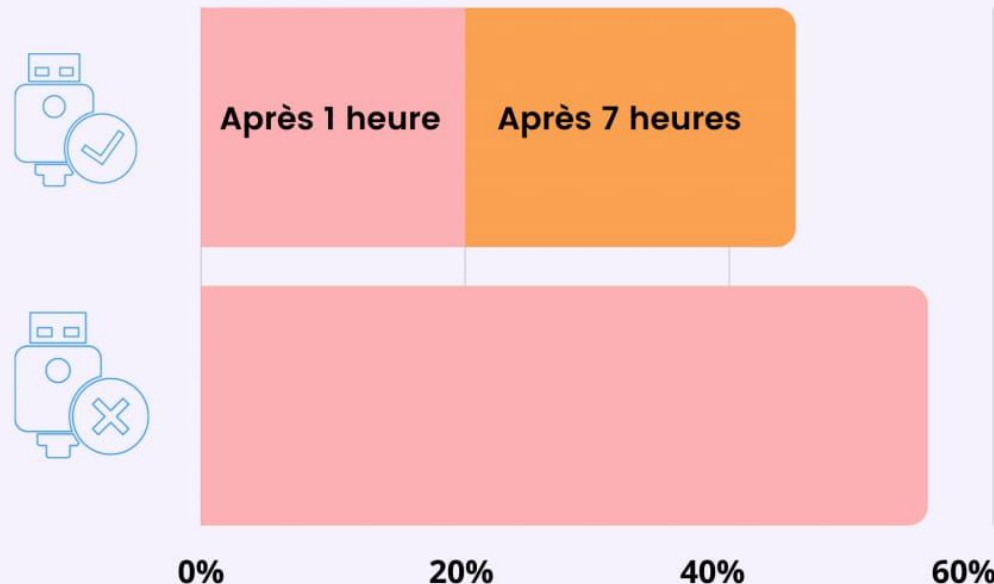
La plupart des attaques par USB contiennent des script de "rebond/pivot".

Le script télécharge le véritable malware depuis un serveur distant sur l'ordinateur de la victime.

Cela permet à l'attaquant de passer outre les limitations du support USB

TAUX DE CLÉS BRANCHÉES

Taux de connexion des clés USB dans l'étude de l'université de l'illinois

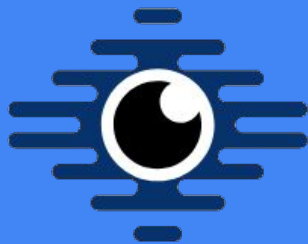




En résumé

Chaque année, les entreprises subissent d'énormes pertes économiques et morales dues à de nombreuses failles de sécurité que les attaquants déploient via un arsenal très varié d'outils.

Vous pouvez prendre un rendez-vous avec nos experts pour demander les derniers conseils et protéger vos systèmes informatiques.



NOSTROGUARD
SECURITY

Demander un audit sur notre site [web](#)