VILDEUIL
PECOME
NAGOU

Dossier cybercriminalité

Le cybercriminel cherche à obtenir des informations personnelles afin de les exploiter ou de les revendre. Il va usurper l'identité de quelqu'un ou alors se faire passer pour un entrepeneur pour diffuser des messages frauduleux ou alors envoyer des liens piégés, des pièces jointes piégées etc...

Tableau des menaces

Nom de l'attaque	Objectif	Fonctionnement	Contre-mesure
Phishing (ameçonnage)	- Obtenir des informations personnelles	- L'expéditeur imite (ou usurpe) l'identité d'une personne digne de confiance que le destinataire connaît.	- Au moindre doute, contacter l'expéditeur par un autre biais - Ne jamais répondre à une demande personnelles
Ransomware (Attaque par rançon)	- Verrouille l'accès de l'ordinateur en échange d'une rançon	- Chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.	- J'effectue des sauvegardes régulièrement sur des périphériques externes. - Je mets à jour régulièrement tous les principaux logiciels .
Fraude au virement	- Identifier une transaction imminente ou récurrente entre le créancier et la victime. En usurpant l'identité du créancier.	- Détourner un virement.	- Contactez directement votre créancier pour toute demande de virement sur un nouveau RIB reçu par message.
Distributed Denial of Service (DDOS)	- Rendre le site/service indisponible	- Envoyer de multiple requête à la ressource WEB	- Mettre en place une infrastructure réseau robuste et extensible. - Utiliser un réseau de distribution de contenu
Fraude au faux	- Tromper la victime pour lui faire valider des opérations -	- En général, l'escroc appelle la victime ou l'incite à le contacter et se présente	Méfiez-vous des messages(mail ou SMS)

conseiller bancaire	- Frauduleuses sur ses comptes bancaires	- Comme conseiller ou agent du service anti-fraude de sa banque	qui vous amènent à communiquer des informations personnelles et/ou bancaires
Attaque par « défiguration de site Web »	- Modifier l'apparence ou le contenu d'un site, et donc altérer l'intégrité des pages.	- Le site n'est souvent plus utilisable, ce qui peut entraîner des pertes directes de revenus et de productivité	- J'utilise des mots de passe d'accès aux interfaces d'administration complexes et régulièrement renouvelés. - Je gère les droits d'accès pour chaque répertoire de votre site.
Violation de données	- Tout incident de sécurité, malveillant ou non, qui viole l'intégrité, des informations personnelles (d'une entreprise ou d'un particulier).	- Introduction malveillante dans une base de données et modification ou vol des données.	- Mettre en place un outil de surveillance permanente pour détecter et signaler les activités suspectes. - Former et sensibiliser les collaborateurs de l'entreprise afin de réduire les erreurs de sécurité informatique

Attaque XSS (Cross-site scripting)	- Enregistre les frappes de touches et des captures d'écran. Et collecte les informations réseau pour contrôler à distance l'ordinateur de la victime.	- Injecte un JavaScript malveillant dans la base de données d'un site Web. Lorsque la victime demande une page du site Web, le site Web transmet la page à son navigateur avec le script malveillant intégré au corps HTML.	- les développeurs peuvent assainir les données entrées par les utilisateurs dans leurs requêtes HTTP avant de les renvoyer. Il faut évidemment s'assurer que toutes les données soient valide avant de les renvoyer
Malware type Cheval de Troie	- Conçus pour espionner les victimes ou voler des données.	- Les chevaux de Troie se font passer pour des fichiers légitimes dans le but d'inciter les victimes à cliquer dessus, à les ouvrir ou à les installer. Ensuite, le cheval de Troie installe des malwares sur votre appareil, vous espionne ou provoque d'autres types de dommages.	- Installez toujours les mises à jour - Utilisez un antivirus - Utilisez des pare-feu - Créez des mots de passe forts - Effectuez des sauvegardes régulières - Soyez prudent lors de vos activités en ligne
DNS hijacking (aussi appelé redirection DNS)	- Obtenir des informations personnelles	- Rediriger les visiteurs du site Web d'une entreprise vers des sites contrefaits dans le but de dérober leurs identifiants et leurs données confidentielles	- Intégrer les pratiques de sécurisation des noms de domaine, du DNS et des certificats numériques dans votre stratégie de cybersécurité globale. - Appliquer une stratégie de Défense en profondeur pour sécuriser vos noms de domaine, votre infrastructure DNS et vos certificats numériques.

Piratage de compte	- Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).	- Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne	- Utilisez des mots de passe différents et complexes pour chaque site et application - Lorsque le site ou le service le permettent, activez la double authentification - Appliquez de manière régulière et systématique les mises à jour de sécurité

En quoi consiste ce nouveau règlement et comment les entreprises doivent s'y conformer.

- Le règlement général sur la protection des données (RGPD) encadre le traitement des données personnelles sur le territoire de l'Union Européenne. Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant.

- Toutes organisations publiques ou privées se situant sur le territoire de l'Union Européenne ou que son activité traite des données de résidents européens est concerné par le RGPD.

- La gestion des données personnelles doit être centralisée auprès d'une personne central

Quels nouveaux types de risque menacent les entreprises et leurs conséquences pour celles-ci

- Les entreprises risquent des amendes de la CNIL pour leur non conformité aux règles de la CNIL. Etant donné que le rgpd date de 2018, il y a pleins d'entreprises qui ne respectent pas le RGPD et les cyber attaquant traquent justement les entreprises qui ne sont pas en règle pour soit demander aux entreprises de les embaucher pour monter un fire-wall au niveau de la protection des données ou sinon pour les dénoncer à la CNIL et payer une amende.

Quels prévisions d'attaques pour 2023-2024

- On peut voir que ces dernières années les entreprises ont dû améliorer leur cybersécurité notamment avec le RGPD. On peut faire un top 10 des cyber malveillances les plus courantes en 2023 contre les entreprises.
    - Le phishing,
    - Le ransomware,
    - L'attaque en déni de service,
    - L'attaque de l'homme au milieu,
    - L'arnaque au président,
    - L'infection par un malware,
    - L'attaque par téléchargement furtif,

- L’attaque par mot de passe
- L’attaque par injection SQL.

La chaîne de blocs pourrait apporter aux entreprises si elle répond vraiment aux besoins exprimés. Préciser si cette technologie remplacera réellement les tiers de confiance ?

- La blockchain pourrait apporter confiance et transparence à l’entreprise de M.Latour tout en réduisant les risques impliqués dans les transactions; sans avoir besoin d'un tiers pour agir en tant qu'intermédiaire dans les transactions.
Ce qui va permettre d'avoir des transactions de se produire directement entre les personnes au lieu d'impliquer un tiers.