MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Gendarmerie nationale

LA LETTRE CYBER *en région Grand Est*

Septembre 2023

La thématique du mois
MOYEN DE COMMUNICATION:LE MAIL

? LE MAIL , UN RISQUE CYBER ?

Environ 90 % des attaques, quel que soit leur type, impliquent à un moment ou un autre l'utilisation du mail. La façon dont un utilisateur utilise ce moyen de communication va donc augmenter ou diminuer le risque de se faire attaquer un jour. Certaines sécurités matérielles ou logicielles sont certes mises en place comme des anti-spam par exemple : CELA NE SUFFIT PAS.

• Quels sont les objectifs des attaquants ?

L'objectif d'un attaquant, hacker, délinquant, peu importe comment on l'appelle, est dans la majorité des cas de « gagner » de l'argent. La manière de récupérer l'argent importe peu. Le mail est donc un vecteur d'attaque très important car il est devenu le moyen de communication principal dans le cadre professionnel.
L'objectif principal va être de collecter des données quelles qu'elles soient. Ces dernières pourront être exploitées ou vendues. La sensibilité de la donnée fera varier le prix de vente mais restera intéressante. Un login et un mot de passe seront par exemple moins chers qu'un numéro de carte bancaire.
Les escrocs évoluent et font évoluer leurs techniques d'approche pour nous inciter à leur donner de la donnée. C'est pourquoi les méthodes de Phishing (lettre de mars 2022) ou de Spoofing (avril 2023) pour ne citer que ces exemples continueront d'exister.

Les escrocs peuvent ainsi chercher par tous les moyens à nous inciter à rentrer nos logins et mots de passe et/ou n° de carte bleue sur un faux site sur lequel ils nous auront dirigés via un lien glissé subtilement dans leur mail.

Plus élaboré, les escrocs peuvent aussi "écouter" nos conversations et apprendre notre manière de communiquer avec nos partenaires. Ainsi ils usurpent l'identité d'une personne de confiance et nous envoient un document que nous pensons légitime comme une facture par exemple. Cependant l'escroc y aura introduit au préalable un ransomware, qui aura pour effet de chiffrer tout le réseau de l'entreprise ou de la collectivité...

Les exemples cités ci-dessus, montrent à quel point l'utilisateur est une cible, peu importe les moyens mis en place par le service informatique.

Mais cela veut dire que je dois vérifier TOUS les mails ?

La réponse est **OUI**, des réflexes sont à adopter afin que cela ne soit plus une contrainte.

Les réflexes à adopter.

- **Avoir un mot de passe fort** (15 caractères contenant des chiffres, majuscules, minuscules, et caractères spéciaux) selon les recommandations de l'Agence Nationale de Sécurité des Systèmes d'Informations. Le changement de mot de passe régulier est également recommandé.

- **Privilégiez la double authentification :** si un mot de passe fort est recommandé, cela ne veut pas dire qu'il ne peut pas être découvert, c'est pourquoi le mot de passe ne doit pas être utilisé plusieurs fois sur des sites ou applications différentes. Avoir le même mot de passe pour sa boîte mail ET pour accéder à une session administrateur de votre réseau ouvre clairement la porte aux attaquants.

- **Ne pas cliquer sur un lien ou une pièce jointe** sans avoir au préalable vérifié la source (prise de contact téléphonique par exemple)

-**Ne jamais communiquer d'information personnelle / sensible** à une source, ou sur un lien qui vous a été transmis.

- **Toujours cacher les destinataires d'une liste de diffusion** afin de na pas offrir une liste d'adresses complètes et liées entre elles aux escrocs.

- **Ne pas se connecter à sa boîte mail sur un wi-fi public** qui par définition n'est pas sécurisé.

- **Ne pas utiliser son adresse mail professionnelle à des fins personnelles** pour quelque raison que ce soit, c'est notamment de cette manière que les spams, publicités, mails de phishing arrivent…

- **Respecter la charte informatique mise en place par votre service ou prestataire informatique** et savoir comment les alerter au plus vite en cas de problème ou attaque.

CONCLUSION

Une expression très répandue et souvent reprise dans le monde de l'informatique dit que **"Le problème se trouve souvent entre la chaise et le clavier"**
La majorité des attaques commencent par un clic sur un lien, une pièce jointe ou encore la fourniture de données confidentielles ou sensibles.
En résumé il ne faut jamais avoir une confiance aveugle lors de la réception d'un mail.