Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

Spear-phishing

Aujourd'hui, la sécurité cybernétique est plus importante que jamais. Quotidiennement, de nouvelles attaques sont signalées sur les messageries numériques, en conséquence la cybersécurité est devenue une priorité pour de nombreuses entreprises.

DE QUOI PARLE T-ON ?

Technique de piratage ciblée la plus répandue, elle est utilisée par les cybercriminels qui ciblent principalement les entreprises. Variante puissante du phishing, c'est une technique malveillante qui utilise les courriels, les médias sociaux, la messagerie instantanée et d'autres plateformes pour amener les utilisateurs à divulguer des informations personnelles ou à effectuer des actions compromettant le réseau et générant la perte des données.

Les courriels utilisés pour une campagne de harponnage semblent provenir d'une source fiable. L'expéditeur est en général une grande entreprise ou une plateforme Internet importante et bien connue avec un grand nombre de membres comme par exemple Paypal ou eBay. La technique du spear-phishing est peut-être le moyen le plus perfide d'accéder à des ordinateurs étrangers.

Le cybercriminel connaît non seulement l'adresse e-mail personnelle de la victime, mais également les détails de l'environnement privé et professionnel. Il pirate l'identité d'un ami ou d'un collègue, de façon à ce que le courriel semble complètement inoffensif. Cela semble presque impossible de détecter l'attaque. C'est la forme d'acquisitions d'informations confidentielles la plus réussie sur Internet puisqu'elle représente 91 % des attaques.

Les attaques de spear-phishing ciblent une victime choisie et les messages sont modifiés pour s'adresser spécifiquement à cette victime, provenant prétendument d'une entité avec laquelle elle est familière et qui contient des informations personnelles. La technique du spear-phishing nécessite plus de réflexion et de temps pour les cybercriminels que le phishing.

QUE FAIRE ?

Le courrier électronique étant le point d'entrée le plus commun de ces attaques ciblées, il est important de protéger cette zone contre les probables attaques d'harponnage. Voici des conseils pour éviter ces attaques.

1. La sensibilisation :
Les employés doivent être formés afin de pouvoir repérer les fautes d'orthographe, le vocabulaire étrange ainsi que d'autres indicateurs de mails suspects qui pourraient empêcher la réussite d'une attaque d' harponnage. La sensibilisation des utilisateurs est la base de la sécurité de votre système d'information.

2. Mettre fréquemment à jour votre logiciel :
Si votre fournisseur de logiciels vous informe qu'il y a une nouvelle mise à jour, faites-le tout de suite. La majorité des systèmes logiciels incluent des mises à jour logicielles de sécurité qui devraient vous aider à vous protéger des attaques courantes. Les systèmes d'exploitation, les pilotes de logiciels et applications tierces doivent également être mis à jour régulièrement.

3. Utiliser des mots de passe puissants :
N'utilisez pas un seul mot de passe ou des variantes de mots de passe pour chaque compte que vous possédez. Réutiliser les mots de passe ou les variations de mot de passe signifie que si un attaquant a accès à l'un de vos mots de passe, il aura accès à tous vos comptes.

4. Protéger sa messagerie électronique :
Il est également indispensable d'utiliser une solution de protection efficace contre le spear-phishing. Des logiciels proposent aux entreprises, sa solution de sécurisation des emails qui protège l'ensemble des boites aux lettres des escroqueries par hameçonnage.

5. En cas d'attaque, déposer plainte auprès des services de police ou de gendarmerie.

Ne pas déposer plainte (même pour une simple tentative), permet aux escrocs de poursuivre leurs activités délictuelles en toute impunité