La sécurité de la messagerie électronique

Définition de la sécurité de la messagerie :

La messagerie électronique ne constitue pas un moyen de communication sûr pour transmettre des données personnelles, sans mesure complémentaire. Une simple erreur de manipulation peut conduire à divulguer à des destinataires non habilités des données personnelles et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, toute entité ayant accès aux serveurs de messagerie concernés (notamment ceux des émetteurs et destinataires) peut avoir accès à leur contenu.

La sécurité des e-mails fait référence aux mesures collectives utilisées pour sécuriser l'accès et le contenu d'un compte ou d'un service de messagerie. Il permet à un individu ou à une organisation de protéger l'accès global à une ou plusieurs adresses e-mail / comptes.

La messagerie électronique est-elle sûre ?

Les emails ont été conçus pour être aussi ouverts et accessibles que possible. Il permet aux membres des organisations de communiquer entre eux et avec les membres d'autres organisations. Le problème est que le courrier électronique n'est pas sécurisé. Cela permet aux attaquants d'utiliser les emails comme un moyen de causer des problèmes pour tenter d'en tirer profit. Que ce soit par le biais de campagnes de spam, de malwares et d'attaques de phishing, d'attaques ciblées sophistiquées ou de compromission du courrier électronique professionnel (BEC), les attaquants tentent de profiter du manque de sécurité du courrier électronique pour mener à bien leurs actions. Étant donné que la plupart des organisations dépendent de la messagerie électronique pour faire des affaires, les attaquants exploitent le courrier électronique pour tenter de voler des informations sensibles.

Les risques/types d'attaque :

Les techniques d'attaque ne cessent d'évoluer, toutes ces techniques ciblent principalement les utilisateurs qui sont le maillon faible de chaque entreprise

Les méthodes les plus courantes utilisées par les pirates pour cibler les utilisateurs via la messagerie électronique sont les suivantes :

- Malware : logiciel malveillant qui infecte vos ordinateurs et serveurs. Il peut être acheminé sous la forme d'une pièce jointe, d'une URL malveillante ou d'un téléchargement effectué par un malware déjà installé sur les systèmes infectés.
    - Signes d'un malware :

L'adresse électronique de l'expéditeur ne semble pas être légitime ;
La réception d'une pièce jointe de la part d'un inconnu ;
Des e-mails qui incitent à cliquer sur un lien ;

    - Se protéger :

Installer un antivirus
Éviter d'ouvrir les messages électroniques d'origine douteuse sans avoir vérifié l'adresse mail de l'expéditeur au préalable ;
Ne pas cliquer sur des liens douteux,
Ne pas ouvrir les pièces jointes provenant d'expéditeur inconnus

- Phishing : emails malveillants qui consistent à récupérer des informations personnelles sur un Internaute tel que des identifiants de connexion ou des coordonnées bancaires.
- Business e-mail compromise (BEC)/ fraude par e-mail : type d'attaque de phishing visant à inciter les utilisateurs à transférer des fonds ou à divulguer des informations sensibles aux cybercriminels. La victime d'une attaque BEC reçoit un e-mail qui a l'air authentique et qui semble provenir d'une entreprise de confiance.

Ce genre de fraude s'appuie sur l'ingénierie sociale pour convaincre les victimes d'agir selon les désirs des cybercriminels. Ces attaques s'affichent généralement à l'utilisateur sous des noms trompeurs ou des domaines usurpés ou similaires pour amener les destinataires à faire confiance à l'expéditeur du message.

- Phishing interne : phishing qui exploite un compte de messagerie compromis pour cibler les utilisateurs sur le même nom de domaine, en général des collègues. Ce type de phishing est efficace, car la plupart des entreprises ne font pas attention aux menaces émanant de leur propre domaine. Les destinataires partent du principe que les emails envoyés par leurs collègues sont fiables.
    - Signes d'un BEC

Un cadre supérieur demandant des informations inhabituelles
Un message qui semble inhabituellement urgent ;
Une invitation à effectuer une action non conventionnelle.
Des demandes qui contournent les circuits habituels
Problèmes de langue et formats de date inahbituels
Adresses « Répondre à » ne correspondant pas à celles des expéditeurs Comment se protéger du BEC

- Phishing ciblant les messageries Web personnelles : attaques ciblant les utilisateurs par le biais de leurs comptes webmail personnels. De nombreux utilisateurs accèdent

à leur messagerie personnelle sur leur lieu de travail, ce qui expose leur entreprise aux menaces émanant de ce vecteur rarement protégé.

Les bonnes pratiques pour la sécurisation des messages :

Il existe des solutions pour protéger vos emails. Cela passe par l'adoption de plusieurs bonnes pratiques :

Pour les professionnels :

- **Vérifier les identités des destinateurs (émetteurs)**

Lire son adresse mail en détail, ne pas se fier à ce que l'outil de messagerie vous facilite la reconnaissance de vos interlocuteurs. Et si quelque chose vous paraît anormal, il ne faut pas hésiter à contacter directement l'émetteur du mail.

- **Chiffrer les emails**

Donc les en-têtes de vos messages ne pourront pas être chiffrés, pour permettre aux serveurs de lire les adresses. Une fois qu'on sait cela, on comprend qu'il est également important que le corps de votre message soit protégé. Donc on va pouvoir chiffrer le corps du message pour qu'il soit gardé privé ; par contre l'en-tête, qui permet de véhiculer les messages, va rester non chiffrée.

- **Mesurer les volumes de mails quotidiens, hebdomadaires...**

Le volume considérable d'emails peut affecter vos ressources informatiques ; utilisez les protections antivirus, antispam et antiphishing pour vos emails entrants : 90 % des mails entrants sont constitués de spams, supprimez les messages indésirables avant qu'ils ne se propagent sur votre réseau et libérez des ressources informatiques.

- **Filtrer les Spams**

Adopter des politiques via des règles, nettoyer régulièrement leurs boîtes de messagerie.

- **Etre attentifs aux pièces jointes**

Faire attention aux pièces jointes qui sont dans le corps du message, et à ne pas cliquer sur les liens URL, ce qui peut être très dangereux.

- **Comment se protéger des BEC**

Montrez-vous méfiant : prenez votre temps avant de répondre aux demandes inhabituelles, demandez des éclaircissements, appelez la personne concernée pour vérifier l'authenticité de l'e-mail.

Enfin, il faut désactiver l'ouverture automatique des documents en pièce jointe

Ne répondez jamais à une demande de codes confidentiels

Nul n'est en droit d'exiger de vous une telle information, cela ne pourra jamais être une demande qui viendrait d'une institution ou, en interne, de votre administrateur.

Pour les non professionnels:

- Choisir des mots de passe complexes avec des lettres minuscules, majuscules, des chiffres et des signes particuliers ;
- Changer régulièrement vos mots de passe ;
- Utiliser un système de tri sélectif de votre courrier électronique (élimination systématique des courriels signalés en tant que SPAMS) ;
- Eviter d'ouvrir les messages électroniques d'origine douteuse sans avoir vérifié l'adresse mail de l'expéditeur au préalable ;
- Ne jamais cliquer sur des liens inconnus (porte d'entrée de certains pirates informatique) ;
- Utiliser un système d'authentification à deux facteurs (un SMS est envoyé sur votre smartphone afin de pouvoir vous connecter et taper votre mot de passe) ;
- Utiliser un antivirus et un pare-feu sur chacun de vos appareils connectés.

Références :

Communigate Sytems

https://communigate.com/10-astuces-securiser-boite-mail/

proofpoint

https://www.proofpoint.com/fr/threat-reference/business-email-compromise