La menace du phishing plane sur les PME : trois étapes pour éviter le pire

La menace du phishing plane sur les PME : trois étapes pour éviter le pire

Les attaques informatiques ciblant de grands groupes, comme TV5monde, font régulièrement la une des journaux. Selon le rapport 2014 PwC sur la sécurité de l'information, 117 339 attaques se produisent chaque jour au niveau mondial.

Depuis 2009, les incidents détectés ont progressé de 66%.
Cependant, ce type d'attaques, très répandue, cible en grande partie les PME. Selon un rapport de l'ANSSI, 77% des cyber-attaques ciblent des petites entreprises.
Les conséquences peuvent être désastreuses pour ces structures à taille humaine, n'ayant pas forcément la trésorerie suffisante pour assurer leur activité en attendant le remboursement de leur assurance. Le coût d'une attaque peut s'avérer très élevé et la crédibilité de l'entreprise visée peut également en pâtir.
Suite à une attaque informatique du type « fraude au président », la PME française BRM Mobilier a ainsi perdu cet été 1,6 M€ et se trouve aujourd'hui en redressement judiciaire.
En mai dernier, le PMU a effectué un test grandeur nature en envoyant un faux email, proposant de gagner un cadeau, avec une pièce jointe piégée. Résultat : 22% des salariés ont téléchargé la pièce jointe et 6% ont cliqué sur le lien contenu dans l'email et renseigné leurs données personnelles.

Comment éviter que ce type de scénario ne vire à la catastrophe ?
1 – Connaitre le déroulé d'une attaque Le phishing, également appelé hameçonnage, est une technique employée par les hackers pour obtenir des données personnelles, comme des identifiants ou des données bancaires.
Le déroulement est simple : le hacker envoie un email en usurpant l'identité d'un tiers de confiance, comme un partenaire, un organisme bancaire, un réseau social ou encore un site reconnu.
L'email contient une pièce jointe piégée ou un lien vers une fausse interface web, voire les deux.
Si le subterfuge fonctionne, la victime se connecte via le lien, et toutes les informations renseignées via la fausse interface web sont transmises directement au cybercriminel.
Autre possibilité : la pièce jointe est téléchargée et permet ainsi à un malware d'infester le réseau de l'entreprise.

2 – Comprendre la dangerosité d'une attaque pour l'entreprise
Pour les entreprises, le phishing peut s'avérer très coûteux. Il est bien évidemment possible que le hacker récupère les données bancaires pour effectuer des virements frauduleux.
Puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites, les informations recueillies sont parfois réutilisées pour pirater d'autres comptes, comme une messagerie, un site bancaire, ou autre.Mais – puisque nous sommes nombreux à utiliser les mêmes mots de passe sur plusieurs sites – il est aussi possible que le hacker réutilise les informations recueillies pour pirater une boite mail, ou un compte cloud.
Le cybercriminel peut ainsi consulter l'ensemble de la boîte mail, ou des comptes de sauvegarde cloud, et mettre la main sur des documents confidentiels, comme des plans ou des brevets, pouvant nuire à l'entreprise.
Enfin, les hackers profitent du piratage des boîtes mails pour envoyer à tous les contacts un nouvel email de phishing. La crédibilité de l'entreprise peut ainsi être touchée et ses clients pourraient subir à leur tour des pertes.

3 – Se préparer et éduquer avant qu'il ne soit trop tard
Les emails de phishing ont bien souvent une notion « d'urgence », qu'il s'agisse d'une demande pressante de la part d'un organisme ou d'un partenaire, ou d'une participation à un jeu concours « express ». Le but étant bien évidemment de ne pas laisser le temps à la victime de prendre du recul.
Comprendre le procédé d'une attaque est la première étape pour organiser sa défense. Il faut donc éduquer les salariés et leur donner quelques astuces pour ne pas tomber dans le piège :
• faire attention aux fautes d'orthographe : bien que les emails de phishing soient de mieux en mieux conçus, on y retrouve régulièrement des erreurs de syntaxe ou d'orthographe.
• regarder l'adresse mail ou le lien URL : même lorsqu'un email ou une interface web est une parfaite copie de l'original, l'adresse de l'expéditeur ou l'URL n'est pas la bonne puisqu'elle ne provient pas du même nom de domaine.
Des salariés éduqués et conscients du danger sont le meilleur atout contre les cyber-attaques, en particulier contre le phishing.
Mais, cela n'est pas suffisant, notamment sur les terminaux mobiles où nous avons tous tendance à être plus spontanés et donc, à adopter des comportement à risques.
Il est donc important de mettre en place un filtre anti-phishing aussi bien sur les postes fixes que sur les terminaux mobiles. Ces filtres scannent automatiquement les expéditeurs et les contenus afin de bloquer les emails suspects.
Pour les PME, il est donc important d'éduquer l'ensemble du personnel, mais aussi de mettre en place des solutions de filtrage email et de sécurité complètes. Par ailleurs, garder une proximité avec son équipe informatique, ou ses fournisseurs de services, peut également jouer un rôle primordial pour limiter les dommages si un employé est tombé dans le piège.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-menace-du-phishing-plane-sur,20151123,57740.htm