Le mail, porte d'entrée préférée des hackers

Plus de 3 millions de mails sont envoyés chaque seconde à travers la planète, ce qui en fait le deuxième service le plus utilisé après la consultation de sites internet. Simple, facile d'accès, universel, l'email a su se rendre incontournable aussi bien pour les entreprises que pour le grand public. Oui mais voilà, ce succès n'est pas sans contrepartie et l'email est aussi devenu de fait, la porte d'entrée préférée des hackers sur les réseaux d'entreprise ou vers les données personnelles et sensibles des particuliers.

Peut-on encore avoir confiance en l'e-mail ?

Techniquement, l'échange d'emails se traduit par le besoin d'ouvrir un port (le 25), afin de permettre la communication entre les différents serveurs de messagerie. En imageant, l'ouverture d'un port revient à ouvrir une porte sur le réseau et c'est pour cela que seuls les ports indispensables doivent être ouverts.

Le protocole permettant d'acheminer les mails est le protocole SMTP, qui a été normalisé pour la première fois en 1981 (par une RFC - Request for Comments), et dont la dernière mise à jour date de 2008. La sécurité n'étant évidemment pas une priorité aux prémices de l'Internet, aucune protection, ou chiffrement, n'a été prévue au moment de la création de l'email.

Il a été construit sur un principe de base très simple: permettre l'envoi d'un texte d'un émetteur à un destinataire. Pour ce faire, uniquement trois champs sont indispensables au bon acheminement de l'email : De, A et objet, signifiant respectivement : qui envoie le message ? A qui est-il destiné ? Quel est son contenu ? Une fois ceci assimilé, il devient très simple de comprendre la dangerosité du mail sans l'ajout de protection supplémentaire.

En d'autres termes, le mail passera par défaut en clair sur le réseau et par conséquent, toute personne écoutant celui-ci pourra lire son contenu. L'usurpation de l'identité d'une personne est également extrêmement facile, le hacker peut indiquer au serveur que le mail provient de n'importe qui puisqu'aucune vérification n'est faite. Plusieurs autres sécurités ont donc dû être mises en place afin de palier aux faiblesses du protocole.

Une mauvaise configuration ou une négligence de la sécurité des serveurs mail peut entrainer des

dégâts conséquents, voire même désastreux pour n'importe quelle entité. L'arrêt du service email peut aller jusqu'à entraîner une paralysie complète de l'entreprise. Récemment, des banques (aux US, on estime que quelques cent banques se sont fait dérober pour près de 300 millions de dollars) ou encore des médias bien connus (TV5 Monde, Le Monde) en ont fait les frais. Des mails bien préparés permettant de voler des mots de passe ou amenant à installer des malwares, ont probablement été à l'origine de ces attaques

De l'hameçonnage au harponnage

Deux grandes méthodes de phishing (hameçonnage) se distinguent. Le « phishing de masse » consiste à envoyer le plus grand nombre d'emails tout en espérant amener un maximum de personnes à fournir des informations sensibles, ou à cliquer sur des documents/liens permettant d'infecter leur poste. Cette attaque fait généralement suite au vol d'une base de donnée, qui est ensuite rachetée par le hacker sur le « Black Market ». Ceci lui permet de forger des mails plus crédibles avec par exemple nom, adresse, numéro de téléphone de la victime.

La seconde méthode est bien plus ciblée (harponnage ou spear phishing), le pirate va procéder à une grande récolte d'informations sur la victime et son entourage via les réseaux sociaux ou les blogs. Pour un pirate tout est intéressant: profession, employeur, adresse IP, loisir, etc. Plus il a de connaissances sur la cible, plus ses chances de réussite sont grandes. Imaginons par exemple, une RH recevant un mail d'un candidat parfait avec un CV en pièce jointe, ou encore un employé recevant un mail de son responsable hiérarchique lui indiquant de changer d'urgence son mot de passe sur le réseau d'entreprise avec un lien pour le faire le piège est parfait !

Comment améliorer la sécurité des mails ?

Pour renforcer la sécurité de leurs échanges et de leur réseau, chaque entreprise se doit d'avoir une maîtrise totale et une gestion stricte, de la chaine permettant d'acheminer les emails de ses utilisateurs.

Or les principales lacunes de l'email sont le chiffrement et l'authentification. Concernant la première, il est possible de configurer des connexions sécurisées avec TLS (Transport Layer Security) permettant de préserver la confidentialité des messages.

L'authentification étant plus compliquée, car tout le monde peut envoyer des emails et de nouvelles adresses sont créées chaque jour, des solutions ont été trouvées au niveau du DNS (Système de noms de domaines) pour protéger des domaines. En effet, la seule information fiable reste l'adresse IP du serveur émetteur, il suffit donc de publier un enregistrement, appelé SPF, permettant de spécifier les adresses autorisées à envoyer des mails pour ce domaine.

Le DKMI (DomainKeys Identified Mail) offre également la possibilité d'ajouter une signature numérique permettant de vérifier à la fois l'authenticité du domaine expéditeur et l'intégrité du message.

D'autres outils peuvent être utilisés afin d'apporter des protections d'authentification et de chiffrement.

Dernier point, afin de protéger les serveurs mails, il est possible de mettre en place des proxys permettant d'assurer une première couche de sécurité. Ils auront comme missions principales de filtrer et de les décharger. Un filtre Antispoofing permet par exemple de placer directement en quarantaine les mails arrivant d'Internet avec votre domaine.

Comment repérer un mail pirate ?

Contrairement au mail d'hameçonnage diffusé à plus large échelle et qui est donc plus facilement identifiable, la méthode ciblée est difficilement décelable si les protections que nous venons de voir ne sont pas mises en place, et quand bien même elles le sont, un moment d'inadvertance ou de fatigue peut nous amener à tomber dans le piège. Cette méthode nécessitant du temps de préparation, ces mails seront surtout destinés aux personnes importantes dans la société pour le hacker (PDG, DRH, etc.). Mais chaque employé peut ouvrir la première porte au réseau interne d'une entreprise.

Chaque mail reçu mérite donc une attention particulière :

Regarder l'expéditeur, il est essentiel de se poser les bonnes questions, le connaissez-vous ? Le domaine est-il cohérant avec le contenu du mail ? L'adresse de l'envoyeur et celle de l'enveloppe sont-elles identiques ?

Prêter attention au corps même du message. Si le message vous incite à réagir rapidement, redoublez d'attention. De plus, de nombreuses fautes d'orthographe doivent éveiller votre vigilance.

Par la suite, et ce avant de cliquer, regardez vers quel site/domaine redirige le lien hypertexte lui même et non le texte qui permet la redirection, son orthographe doit être exactement identique (même commentaire que pour le header vs enveloppe).

Les images mais aussi les fichiers PDF, Word ou Excel, doivent également susciter une méfiance. Leur simple chargement peut entraîner une action sur un site selon la requête qui se cache derrière.

Dernier point crucial, la pièce jointe. Il est actuellement impossible d'être certain qu'un fichier est sain malgré les antivirus. En cas de doute, n'ouvrez tout simplement pas la pièce jointe

Malgré les solutions mises en place (pare-feu de nouvelle génération, WAF, Proxy,) pour protéger un système d'information, le comportement humain (fatigue, spontanéité, excès de confiance) est critique. Quelques soient les connaissances de chacun, tout le monde peut être victime un jour ou l'autre d'un email provenant d'un hacker. Prudence et sensibilisation sont les maîtres mots face aux conséquences qu'aurait l'ouverture d'un seul et unique email malicieux.