Comprendre ce qu'est l'Arnaque au Président

(Attaque via une adresse Mail frauduleuse.)

Le principe de ces attaques par e-mail repose sur une usurpation d'identité qui permet de tisser un lien de confiance et conduire un employé à faire une opération (au hasard : un virement) hors du cadre habituel.

Différentes formes d'attaques

L'Arnaque au Président classique

Une imposture par mail permet d'envoyer un message à un employé pour demander un virement de fond en lui laissant entendre que la requête est urgente et émane d'un cadre dirigeant de l'entreprise (voire du CEO lui-même). C'est justement parce que cette requête est urgente qu'elle outrepasse la procédure habituelle, cette méthode d'ingénierie sociale met la pression sur l'employé pour le contraindre à obtempérer.

Variante 1 : La fausse facture de fournisseur :

Ici, un tiers parvient à identifier une relation entre deux personnes : un fournisseur et son interlocuteur au sein de l'entreprise. Il peut ainsi adresser une facture à l'entreprise en se faisant passer pour ce fournisseur, mais en orientant le paiement vers son propre compte.

Variante 2 : L'imposture de l'avocat

Là encore, la pression est mise sur l'employé en insistant sur l'urgence d'un virement mais aussi sur son caractère confidentiel. L'employé ciblé est donc incité à s'exécuter sans prendre les avis de ses collègues ou supérieurs directs et menacé de mettre en grande difficulté son entreprise s'il ne s'exécute pas.

Mais ce n'est pas toujours une arnaque financières mais cela peut avoir comme objectif : Le vol de données

Jusqu'ici, nous avons évoqué des méthodes permettant à des tiers malveillants de réceptionner des transferts de fonds, mais l'objet de ces attaques peut être d'une autre nature. Une telle usurpation d'identité peut servir à récupérer des informations sensibles ou plus simplement des noms et des e-mails et surtout des identifiants bancaires qui pourront servir une arnaque encore plus élaborée.

Des attaques sophistiquées

L'arnaque au président repose donc sur un fondement essentiel : un lien de confiance établi avec le ou les employés ciblés par l'attaque. C'est la plupart du temps des directeurs adjoints, sous-directeurs ou adjoints au chef de service qui sont visés. Mais pratiquement jamais le directeur du service (vente, production, personnel, informatique etc..) qui est visé. Car les directeurs ont en général un accès privilégié au président ou au directeur général alors que les sous-directeurs, par principe, ne l'ont pas.

Choisir une cible adaptée : idéalement une grande entreprise avec une importante division des tâches. Il serait bien plus compliqué de monter une arnaque au président dans une PME dans laquelle le directeur travaille au quotidien avec ses employés et valide lui-même la plupart des paiements. Le nombre d'attaques s'accroît donc avec la taille de la structure, mais ce sont surtout les employés des entreprises ayant plus de 1000 employés qui sont les plus fréquemment confrontées à ce type d'e-mail frauduleux. Les très grandes entreprises sont aussi attaquées mais de manière moins intensive quand on rapporte ce nombre au volume des boites mails.

Procédure pour monter ce type arnaque :

Collecter des informations : les noms, les adresses e-mail, le rôle et les postes des personnes influentes de la société mais également la teneur de leurs échanges. Souvent ces informations sont fournies par une complicité interne (volontaire ou involontaire).

Mettre en œuvre l'usurpation d'identité : le mail doit sembler émaner d'un dirigeant ou d'un interlocuteur identifié, il faut donc pour l'attaquant parvenir à faire accepter un nouveau Mail comme étant celui du directeur ou comme le deuxième Mail du directeur.

Exemple 1
Remplacer : Jean.dupond@cabledelyon.fr par jeandupond@cablesdelyon.fr
(le «s » de cable et en plus)
Exemple 2
Remplacer : Jeandupond@RVI.fr par jeandupond@VOLVO-RVI.se
(Volvo étant la maison mère de RVI et, si VOLVO-RVI existe, créer VOLVO-RVI-France etc…)

Le pirate va donc construire (et publier) un site Web pirate qui va ressembler comme deux gouttes d'eau au site Web de l'entreprise et dont les liens retourneront sur le site officiel de l'entreprise.
Lors de la publication du site : exemple ; Volvo-RVI.se l'hébergeur du site offre, en général, une dizaine adresse Mail de type xxxx@Volvo-RVI.se. Il suffit alors d'en créer une au nom du PDG.
En premier il faut que la cible (exemple l'adjoint au chef comptable) reconnaisse le Mail reçu comme étant la deuxième adresse Mail du PDG.

Prenons un exemple :

> Pour (Volvo-RVI) la cible (sous-directeur) va recevoir un faux Mail du PDG qui lui rappellera que lors de sa dernière réunion au siège de Volvo en Suède il lui a été rappelé que dans tout le groupe Volvo l'égalité des chances homme/femme était une réalité etc… Et il va trouver en pièces jointe un document confidentiel qui est une copie d'un document officiel qu'il a déjà reçu de par son chef de service. Il va même remarquer que ce message a été envoyé à tous les directeurs et sous-directeur alors que en réalité il n'a été envoyé qu'a lui-même.

Le lien de confiance est établi et il est consolidé par d'autres Mail anodins échangés.

Un jour, (alors que de directeur du service est absent), le sous-directeur est mis sous pression par un MAIL du PDG de caractère urgent et confidentiel pour une opération exceptionnelle et il est invité à exécuter les consignes données.

On le voit : la dimension technique de ce type d'attaque est assez modeste et le principal levier qui permet à l'arnaque au président de fonctionner est la psychologie complexe d'employés tiraillés entre les impératifs de sécurité et la demande frauduleuse de pragmatisme qui leur est faite : faut-il obéir à des procédures strictes où à son supérieur ? L'employé se sent-il légitime pour rappeler ces règles à celui qu'il croit être une autorité ? On comprend aisément que la prévention est nécessaire pour se prémunir contre ce genre d'attaque mais qu'elle ne suffit pas. C'est justement le caractère "humain" des agents ciblés qui autorise quoi qu'il arrive des exceptions à toutes les règles, cette qualité qu'est le "bon sens " est transformée en vulnérabilité.

Stratégies préventives

Identifier une arnaque au président ou une attaque BEC

La confiance sur laquelle repose l'attaque est souvent liée au fait que peu de gens soupçonnent l'existence même de ces malversations. La première étape de la prévention est donc de communiquer en interne sur l'existence de ces menaces et encourager chacun des employés à se montrer extrêmement suspicieux à chaque demande sortant de l'ordinaire. Quelques éléments peuvent éveiller les soupçons :

Un caractère urgent qui ne va pas de soi.

Des destinations de paiements changés à la dernière minute.

Des communications par e-mails uniquement et jamais par téléphone ou en visio.

Des paiements exigés en avances quand ça n'était pas le cas jusqu'ici.

D’une manière générale, une situation exceptionnelle exigeant des mesures inhabituelles doivent encourager le destinataire à vérifier l’adresse de l’expéditeur, la comparer avec l’adresse de réponse, les destinations des éventuels liens présents dans le mail…

Mais un coup de téléphone de demande de confirmation à l’émetteur du Mail reste le meilleur moyen contrôler ce risque.