Info Délits Plus
Novembre 2015
Division prévention criminalité

L'ingénierie sociale, un risque pour les PME

Des entreprises locales basées dans le canton de Vaud sont régulièrement la cible d'arnaques et de tentatives de tromperie. Connues sous l'appellation « social engineering », ces escroqueries s'appuient sur une récolte d'informations sur les réseaux sociaux et les communications internes des entreprises visées. Elles permettent d'usurper l'identité de leurs dirigeants et de demander le transfert de sommes conséquentes auprès de collaborateurs de filiales basées en Suisse.

L'ingénierie sociale (ou social engineering en anglais) est une forme d'acquisition déloyale d'information et d'escroquerie utilisée pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la victime. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'escroc abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.

L'art d'extirper frauduleusement de l'information à l'insu de son interlocuteur en lui « tirant les vers du nez » désigne un processus d'approche relationnel frauduleux et définit plus globalement les méthodes mises en œuvre par certains malfaiteurs pour obtenir d'une personne manipulée, un accès direct à des informations clefs de l'entreprise.

Les méthodes d'ingénierie sociale reposent sur un principe simple. Les arnaqueurs cherchent tout d'abord à gagner la confiance de leurs victimes, avant de tenter de leur soutirer de l'argent. Les sociétés visées par ce type d'escroquerie sont de toutes tailles et branches d'activités. Pour parvenir à leurs fins, les escrocs récoltent un nombre conséquent de données sur les réseaux sociaux, ainsi que via les communications internes des entreprises telles que les newsletters. Ils acquièrent ainsi une connaissance très fine tant des personnes que des organisations visées.

Les demandes de transfert sont justifiées notamment par l'imminence de contrôles fiscaux ou le rachat d'entreprises et se déroulent généralement dans un climat de précipitation, par exemple un vendredi après-midi. Les escrocs vont jusqu'à imiter parfaitement la voix des personnes dont l'identité a été usurpée. Ils demandent à la cible de ne rien divulguer à ses supérieurs, insistant sur l'urgence de la situation et la discrétion de mise pour ce genre de transaction. Ils fournissent parfois un code d'identification chiffré qui devra être donné lors de chaque conversation ultérieure et exercent une forte pression sur leurs victimes, allant jusqu'à les appeler dix fois par jour.

Le « social engineering » est une technique ancienne et éprouvée. Ces dernières années, cet art de la supercherie, face à des victimes aussi formées ou préparées soient-elles, a trouvé un nouveau terrain de jeu avec Internet, et plus encore avec la montée en puissance des réseaux sociaux. Ces sites constituent en effet une mine de renseignements concernant l'entreprise et ses collaborateurs, et tout cela en libre accès ! Les escrocs s'en servent pour nuire aux intérêts des entreprises mêmes les mieux protégées. Posséder un arsenal technique capable d'arrêter le virus informatique le plus récent ou le plus agressif n'est d'aucune aide quand le point faible en matière de sécurité réside au cœur de l'organisation, incarnée par ses collaborateurs, par ses cadres et par ses directeurs.

Comment déceler une tentative d'arnaque ?

Les entreprises et les collaborateurs doivent rester particulièrement vigilants à la sensibilité des informations publiées sur les réseaux sociaux et respecter scrupuleusement les procédures internes avant de procéder à toute transaction. En cas de doute, il est indispensable d'en référer à la hiérarchie.

Généralement, l'escroc procède selon un schéma relativement précis:

- Une phase d'approche lui permet de mettre l'utilisateur en confiance. Il se fait passer pour une personne de sa hiérarchie, de l'entreprise, de son entourage ou pour un client, un fournisseur, etc.
- Une mise en alerte déstabilise la victime et s'assure de la rapidité de sa réaction. Il évoquera par exemple un souci de sécurité ou une situation exigeant une réaction immédiate.
- Une diversion permettra alors au malfaiteur de rassurer sa victime, l'encourageant à transmettre des données sensibles comme des codes d'accès.

Comment se protéger?

Le bon sens prévaut lorsqu'on fait face à une tentative de manipulation. Ainsi, pour ne pas divulguer à n'importe qui des informations pouvant nuire à la sécurité de l'entreprise, il est important de se renseigner sur l'identité de son interlocuteur en lui demandant des informations précises et de vérifier la pertinence des renseignements fournis.

Conseils !

Mettre en place des processus très précis concernant les transactions financières (compétences, contrôles, etc …).

Définir qui doit être informé lors de demandes inhabituelles de transferts d'argent, lorsque les responsables de l'entreprise ne sont pas atteignables (No de portable confidentiel, épouse du patron en son absence, …). L'employé susceptible de pouvoir virer de l'argent sur le compte d'un tiers doit pouvoir discuter d'une telle demande.

Informer et sensibiliser les employés potentiellement concernés, comme les RH et la comptabilité de l'entreprise.

3 règles à rappeler aux collaborateurs :

- **Aviser sans tarder la hiérarchie**, en cas de doute quant à la provenance d'un e-mail ou d'une demande inhabituelle de transfert d'argent. Si l'entreprise est très petite, définir à l'avance d'une procédure de partage d'information,
- **Ne pas se laisser mettre sous pression et ne jamais agir dans la soi-disant urgence,**
- **Ne pas contrevenir aux règles usuelles de sécurité interne à l'entreprise**, sous le prétexte de l'urgence et de la confidentialité.

Pour obtenir plus d'information ou des conseils, contactez les gérants de sécurité :

Arrdt Est vaudois : Adj Borloz Christian, 021 557 88 05
Arrdt La Côte : Adj Lambiel Christian, 021 557 44 66
Arrdt Nord vaudois Ouest : Adj Mermod Willy, 024 557 70 24
Arrdt Nord vaudois Est : Adj Perruchoud Gilles, 024 557 70 07
Arrdt Lausanne : Ipa Bourquenoud Christian, 021 644 82 77