Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DES LANDES

Cybercriminalité : focus sur l'escroquerie au virement frauduleux

Cibles :

Les attaques portent principalement sur le **comptable** ou de manière plus large se concentreront sur la **direction financière de l'entreprise**.

Un travail préparatoire considérable :

Les cybercriminels recueillent d'abord le maximum d'informations sur l'organisation et le fonctionnement de l'entreprise par l'intermédiaire de virus informatiques permettant de récupérer des organigrammes, emplois du temps, signatures et autres documents comptables ainsi que par achat d'informations sur des sites de référencement comme infogreffe et societe.com.

Comment se déroule une attaque ?

Exemple 1 : le faux président.
Les attaques s'effectuent généralement soit au moyen d'une fausse facture (incitant l'entreprise à émettre un faux vrai ordre de virement), soit par **l'emprunt d'identité d'un dirigeant** (afin de leurrer l'établissement de crédit qui exécutera le faux ordre de virement).

Exemple 2 : l'escroquerie aux loyers.
L'escroc contacte le service comptabilité en stipulant que le loyer devra être viré (suite à changement de domiciliation bancaire) sur le compte d'une société **basée à l'étranger**. Il envoie ensuite les nouvelles coordonnées en utilisant le logo original et une adresse de courriel très proche du véritable bailleur.

Exemple 3 : l'escroquerie au virement SEPA (Single Euro Payments Area, ou espace unique de paiement en euros).
L'escroc prétexte une série de tests dans le cadre du passage à cette norme en fournissant des coordonnées bancaires **domiciliées à l'étranger** et en demandant le versement des montants correspondants aux virements tests.

Quand :

les attaques sont souvent lancées les veilles de week-end (vendredi après-midi) ou de périodes de vacances .

1) Les escrocs demandent l'exécution d'un virement d'une importante somme d'argent.
2) L'argent est viré vers un compte intra-européen (hébergé, par exemple, en Grèce, en Roumanie, à Chypre....), puis dans des délais très brefs, les fonds sont transférés vers un compte hors Union européenne (Singapour, Hong-Kong,...)

Comment réagir ?

Dans tous les cas, la victime doit déposer plainte auprès du commissariat ou de la brigade de gendarmerie la plus proche. Par ailleurs, dans ce type d'affaire, le recours à une assistance juridique est conseillé.

L'urgence est de bloquer l'argent sur le compte bancaire où il est détenu pour pouvoir ensuite le rapatrier. Ensuite, le temps de la procédure judiciaire permettra de rechercher les auteurs des faits.

1) Dans un délai de 24/48H, l'entreprise victime doit contacter directement sa banque afin de lui demander la rétro-action de l'opération de transfert. Pour ce faire, la banque française va informer la banque étrangère, où sont détenus les fonds, que l'opération de transfert fait l'objet d'une suspicion d'escroquerie. Dès lors, la banque étrangère est en principe tenue de bloquer les fonds dans l'attente de vérification de la régularité des opérations. Exemple: Les sommes transférées par faux ordre de virement un vendredi après-midi peuvent encore être gelées sur le compte destinataire ou tout simplement rapatriées le lundi suivant

2) Dans un délai de 5 jours maximum, l'entreprise doit s'assurer que les services de police/gendarmerie ou au procureur de la République ont mis en œuvre les moyens de coopération judiciaire ou policière (attaché de sécurité intérieure, magistrats de liaison, réseau CARIN) à même d'opérer le gel et la saisie des comptes destinataires. Exemple : à l'initiative de la direction de la coopération internationale (DCI), les attachés de sécurité intérieure (ASI) sont en mesure de faire le lien avec les autorités des pays à partir desquels certaines attaques sont émises. Par exemple, une entreprise victime d'une escroquerie financière par faux ordre de virement depuis la Chine peut mettre en oeuvre des actions juridiques directement sur place. Pour ce faire, en complément de la plainte déposée en France auprès des services de police ou de gendarmerie, ces derniers doivent informer directement l'ASI de l'Ambassade de France du pays concerné. En Chine, cette procédure se traduit la une demande d'entraide transmise au ministère de la sécurité publique chinois reprenant un exposé précis des faits constitutifs de l'infraction.

Les moyens de prévention :

1) Sensibiliser les directions et les personnels concernés (comptabilité, service financier).

2) Mettre en oeuvre une procédure de "redondance" (ordre confirmé et vérifié plusieurs fois) pour les opérations financières les plus importantes. Le but est de contrôler l'identité du

donneur d'ordre. Attention ! Dans certains cas les faussaires procèdent par "ingénierie sociale", leur permettant de connaître parfaitement l'organigramme de l'entreprise et les habitudes de ses dirigeants (maladie, voyage...).

3) Diffuser un guide de bonne pratique en interne et/ou faire appel à l'un des référents "Intelligence économique", "sûreté" ou "Nouvelle-technologie», de la Gendarmerie Nationale ou de la Police Nationale (contact : la brigade ou le commissariat le plus proche).

les 10 questions que les entreprises doivent se poser :

1- Quelles sont les informations stratégiques (brevets, recherches, fichiers, …) que vous ne souhaiteriez pas que votre concurrent connaisse ?

2- Ces informations sont-elles protégées matériellement (coffre pour les plans de brevets par exemple) ou virtuellement (cryptage ou protection informatique pour les fichiers) ?

3- Qui sont les personnes qui ont accès à ces informations ?

4- Ces personnes ont-elles été sensibilisées aux risques de « vol d'information » ou de piratage informatique ?

5- Vos employés/salariés/stagiaires sont-ils sensibilisés à la protection de leurs données personnelles (sur les réseaux sociaux notamment) ?

6- Votre comptable et/ou votre directeur financier sont-ils sensibilisés au risque d'escroquerie par faux ordre de virement ?

7- Les sous-traitants, fournisseurs, intervenants extérieurs, stagiaires, font-ils l'objet d'un contrôle particulier ?

8- Disposez-vous d'une procédure/protocole de gestion de crise en cas de perte d'informations stratégiques (qui contacter pour déposer plainte, quelle procédure juridique mettre en oeuvre, comment assurer la continuité de l'activité, …) ?

9- Disposez-vous d'un système de veille sur votre e-réputation ? Et sur celle de vos concurrents ?

10- Souhaitez-vous bénéficier de contacts auprès d'autres services publics, qui pourrez vous accompagner dans vos démarches de protection ou de développement économique ?

Retrouvez un diagnostic complet avec « DIESE » sur le portail de la délégation interministérielle à l'intelligence économique sur:

http://www.intelligence-economique.gouv.fr

Pour trouver le correspondant sûreté proche de votre entreprise :

http://www.landes.gouv.fr/vos-conseillers-a1557.html