LE CORONAVIRUS SEDUIT LES FRAUDEURS

AVRIL 2020

Les fraudeurs et les criminels semblent bien décidés à tirer parti du contexte de crise actuel pour profiter des employés les moins méfiants. Les grandes catastrophes sont systématiquement exploitées par les cybercriminels à des fins pécuniaires ou d'espionnage.

Alors que de plus en plus d'entreprises adoptent des politiques en faveur du travail à domicile comme mesure préventive, les fraudeurs profitent de l'occasion pour lancer davantage d'attaques.

QUELLE SONT LES ATTAQUES LES PLUS COURANTES ?

- **Se faire passer pour un fournisseur :** une entreprise de la région de Rouen vient de subir une arnaque à 6,6 millions d'euros en passant une commande de masques de protection et de gels à une entreprise qui s'est révélée être une société fantôme. Les escrocs se sont fait passer pour les fournisseurs habituels de l'entreprise, dont ils ont usurpé l'identité, et ont offert de livrer rapidement une grande quantité du matériel voulu. Ils ont ensuite disparu et l'argent est, lui, arrivé à Singapour.
- **Envoyer des mails de phishing pour inciter des employés à cliquer sur un lien malveillant ou à ouvrir une pièce jointe** (faux mails d'autorité de santé, attestation de sortie sur des sites non officiels...). De cette façon, le fraudeur va pouvoir espionner la manière dont l'entreprise fonctionne, comment se donnent les ordres, et pouvoir réaliser une usurpation d'identité et/ou voler les identifiants et mots de passe et tromper l'interlocuteur sur de faux ordres de virements.
- **Fraude à l'expédition vers de faux lieux de livraison** : les fraudeurs tentent de faire expédier des marchandises vers d'autres lieux de livraison invoquant des modifications d'organisation du fait du Coronavirus. Ils jouent sur l'urgence afin d'accélérer les expéditions dans le contexte actuel (et restreindre ainsi les vérifications).
- **Attaques de type ransomware ou cyber extorsion** : ce sont des logiciels malveillants (souvent une pièce jointe au mail) qui chiffrent les données présentes sur les espaces mémoires. Les fraudeurs exigent le paiement d'une rançon en échange d'une clé permettant de les déchiffrer.

QUELLE SONT LES BONNES PRATIQUES POUR VOUS PREMUNIR ?

- **Mettre en place un protocole de vérification dans le traitement des emails**. Il faut être vigilant dans le traitement de ses mails (souvent utilisés par les pirates pour infecter une machine). Ne jamais ouvrir des mails dont la provenance ou la forme est suspecte (expéditeur inconnu…). Lorsqu'un « fournisseur » soumet un nouveau numéro IBAN pour un virement, il convient de déclencher un protocole rigoureux de vérification au-delà d'un simple échange de mail (procédure de contre appel auprès de ses contacts habituels).

- **Appliquer les mises à jour de sécurité sans délai.** Procéder aux mises à jour des logiciels et des systèmes d'exploitation dès lors qu'elles sont proposées. Celles-ci n'apportent pas seulement de nouvelles fonctionnalités, elles corrigent les vulnérabilités.

- **Sauvegarder régulièrement sur des supports non connectés aux machines** (disque dur externe, clé usb).

- **Protéger les accès et mot de passe**. Les mots de passe doivent être robustes et personnels. Il faut aussi restreindre les accès, gérer les droits, cloisonner les usages.

- **Ne pas réduire la sécurité.** Protéger les accès en utilisant une connexion VPN (réseau internet sécurisé) ou explorer l'approche dite « zerotrust », une alternative au VPN. Généraliser la double authentification.

- **Ne pas utiliser ses outils informatiques personnels.** Utiliser les moyens professionnels sécurisés fournis par son entreprise (téléphone, ordinateur, VPN, etc.). Ne pas les contourner, par l'usage de moyens personnels (ex. : messagerie personnelle).

EN SAVOIR PLUS

RDV sur votre site Mon espace EH
pour découvrir nos solutions Fraude

Si vous souhaitez vous assurer contre les risques de Fraude et Cyberfraude,
parlez-en à votre courtier ou mandataire.

Euler Hermes France -Succursale française d'Euler Hermes SA -RCS Nanterre B 799 339 312
Adresse postale : 1, place des Saisons -92048 Paris La Défense Cedex -Tél. + 33 1 84 11 50 50 -www.eulerhermes.fr

Euler Hermes SA -Entreprise d'assurance belge agréée sous le code 418
Siège social : avenue des Arts 56 -1000 Bruxelles, Belgique -Immatriculée au RPM Bruxelles sous le n°0403 248 596