UBS

Etes-vous en sécurité ?

A quels cyber-risques votre entreprise est-elle exposée et comment pouvez-vous vous en protéger ?

Depuis toujours les e-mails et Internet représentent le terrain de jeu favori des criminels. Ils utilisent le Web afin de se procurer des informations confidentielles qui leur servent à faire chanter les entreprises ou pour voler de l'argent sur des comptes qui ne leur appartiennent pas. Les moyens techniques sont une protection de base, les cybercriminels préfèrent donc utiliser la défaillance humaine afin de pénétrer dans les systèmes. Dans cet article, nous décrivons les cyberrisques actuels et vous indiquons comment y faire face.

Que dois-je savoir sur les cyber-risques, quels sont les dangers ?

Les cybercriminels n'ont souvent besoin que de quelques minutes afin de pénétrer dans un réseau, de provoquer des dommages et de disparaître à nouveau.

Les statistiques montrent que le nombre d'attaques réussies augmente sans cesse ; les entreprises de toutes tailles sont concernées. Les mesures techniques, comme les pare-feu, les logiciels antivirus, etc., qui sont mis à jour en permanence et à la pointe de la technique représentent la base de tout dispositif de protection contre les cyber-risques. Les cybercriminels accèdent toutefois de plus en plus souvent aux réseaux des entreprises en s'attaquant de manière ciblée à leurs collaborateurs et non en exploitant les failles techniques, le facteur humain devient le point faible décisif. Ils utilisent différentes méthodes dont voici les plus importantes :

- **ingénierie sociale :** les criminels s'efforcent de manipuler les collaborateurs afin qu'ils communiquent des informations confidentielles, le plus souvent par téléphone. Les attaquants utilisent des informations publiques (trouvées dans le profil Facebook de la personne appelée, par exemple) afin d'accéder à des informations confidentielles de l'entreprise ou à des données d'utilisateurs.

- **phishing :** les attaquants essaient de se procurer des informations confidentielles, comme des noms d'utilisateur ou des mots de passe, à l'aide de sites Web ou d'e-mails falsifiés. Les criminels manipulent les données ou effectuent des virements à l'aide des identités volées.

- **fraude au président :** un manager réel ou fictif demande aux collaborateurs d'une entreprise d'effectuer des virements. L'urgence et la discrétion représentent deux des aspects importants de la fraude au président. Les cybercriminels utilisent fréquemment des numéros de téléphone falsifiés afin d'éliminer tout doute.

- **programmes malveillants :** les attaquants poursuivent différents objectifs à l'aide des programmes malveillants. Les trois plus fréquents sont les suivants :
  - accéder à un système protégé (exemple : cheval de Troie, porte dérobée)
  - accéder à des informations confidentielles (enregistreur de frappe, logiciel espion)
  - supprimer ou chiffrer des données (virus, rançongiciel ou ransomware)

Depuis quelque temps, nous constatons que le nombre d'attaques à l'aide de rançongiciels (ou ransomware) augmentent : toutes les données de l'ordinateur concerné sont chiffrées et deviennent donc inutilisables. Les criminels exigent une rançon (ransom en anglais) pour les déchiffrer. Comme dans le cas d'un chantage normal, rien ne garantit qu'ils les déchiffreront après le paiement de cette dernière et qu'il sera à nouveau possible de les utiliser.

Les chevaux de Troie sont aussi fréquemment utilisés. Ce sont des programmes malveillants envoyés sous forme de pièces jointes d'un e-mail, souvent des fichiers Word ou Excel. Le programme malveillant s'installe sur l'ordinateur lorsque la pièce jointe est ouverte. Les attaquants peuvent ainsi accéder à distance à ce dernier afin de télécharger des données confidentielles ou d'effectuer des virements, par exemple.

Comment puis-je me protéger et protéger mon entreprise face aux cyberrisques ?

La vigilance reste la meilleure arme face à la cybercriminalité. Si vos collaborateurs et vous-même suivez les conseils ci-dessous, vous serez en mesure d'éviter bien des problèmes.

- Si vous ne connaissez pas l'expéditeur d'un e-mail ou si vous avez des doutes sur son identité, ne cliquez jamais sur un lien et n'ouvrez jamais de pièces jointes.
- Ne désactivez jamais les mécanismes de sécurité (par exemple un blocage des macros) lorsque cette action est exigée lors de l'ouverture d'un fichier. Informez immédiatement les responsables de la sécurité ou l'administrateur système de votre entreprise.
- Ne répondez jamais à des e-mails envoyés par des inconnus et/ou des expéditeurs inattendus. En répondant, vous signalez à un criminel potentiel que vous utilisez cette adresse e-mail ; il pourra alors y concentrer ses attaques.
- Ne réagissez pas aux e-mails vous promettant des avantages matériels (« Vous avez gagné ! »), vous poussant à des actions non réfléchies sous couvert d'urgence (« Agissez tout de suite ! ») ou jouant avec votre peur (« Votre compte va être bloqué ! »)
- Contrôlez les liens des e-mails avant de cliquer : en passant sur le lien avec votre souris, l'adresse cible apparaît dans la barre des tâches. Est-elle en adéquation avec le texte en question ? Faites très attention à l'orthographe ; pour les URL avec plusieurs mots séparés par des points, ce sont toujours les mots qui précèdent le suffixe qui importent (.ch, .com, .net).
- Vous faites sûrement l'objet d'une attaque si le contenu et le style de l'e-mail ne « collent » (vraisemblablement) pas avec l'expéditeur. Une entreprise sérieuse ne vous enverrait pas d'e-mails mal écrits avec des fautes d'orthographe.
- Faites preuve de circonspection avec vos informations personnelles sur les plateformes publiques telles que Facebook ou Twitter.

Vous avez reçu un e-mail qui vous semble suspect et impliquant UBS – par exemple en tant que soi-disant expéditeur ? Merci de soumettre l'email en question en utilisant ce formulaire. Veuillez-vous assu- rer que cet e-mail ne contient aucune donnée person- nelle telle que des informations sur votre compte.

Où trouver des informations complémentaires sur les cyberrisques actuels ?

Les organes étatiques publient régulièrement des informations sur leur site Internet et notamment sur la situation actuelle en matière de risques informatiques. Ils vous proposent également des guides pour vous protéger contre les cyberrisques les plus courants.

MELANI – est la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération. Vous trouverez sur le site Internet melani.admin.ch un aperçu des dangers actuels mais également des conseils de protection et des informations complémentaires. Ce dernier s'adresse aux PME et aux personnes privées Suisse.

Europol – ce site en anglais propose de nombreuses instructions utiles relatives à l'usurpation d'identité, les fraudes par carte, les logiciels espions et bien plus encore. europol.europa.eu > Media Corner > Crime Prevention

ENISA – Agence européenne chargée de la sécurité des réseaux et de l'information. Vous trouverez sur ce site en anglais une large sélection de contenus sur le thème des cyberrisques. enisa.europa.eu/topics