Baloise
SCOUTS
DIGITAUX

Cyber Security Guide – PME

Nous vous montrons la voie dans la jungle numérique.

www.baloise.com/digitale-pfadfinder

Baloise
Group

À propos des Scouts Digitaux

La troupe des Baloise Scouts Digitaux réunit des collaborateurs motivés et impliqués. Ambas-sadeurs de la numérisation, ils vous offrent leur aide pour vous y retrouver dans la jungle numérique. L'organisation des Baloise Scouts Digitaux est une collaboration entre Corporate IT et Public Affairs.

Objet et but des Scouts Digitaux
Les Baloise Scouts Digitaux apportent une contribution volontaire dans le cadre de la respon-sabilité sociale de l'entreprise, car les besoins de la société vont au-delà des prestations de sécurité. Les collaborateurs de la Bâloise disposent d'un vaste savoir-faire qui est mis à la disposition de la société en plus des prestations de services liées à notre activité.

Une séance d'information sur la cybersécurité vous intéresse?
Contactez-nous par e-mail:
pfadfinder@baloise.com

Introduction

Cette brochure est destinée à aider les clients PME à informer leurs collaborateurs des dan-gers et risques de l'utilisation quotidienne d'Internet sur le lieu de travail et à domicile. Elle ex-plique ensuite les bases de la cybersécurité et fournit des lignes directrices de prévention permettant d'éviter les cyberincidents.

Les risques de cybersécurité existent sous de nombreuses formes et peuvent causer des dommages importants, voire désastreux. La plus grande faille dans la sécurité IT d'une entre-prise est, et demeure toutefois l'homme. Mais à travers une compréhension claire des risques et des conséquences de nos propres actions, cette faille peut toutefois être considérablement réduite.

Les principaux termes brièvement expliqués

Ingénierie sociale
Le mode opératoire consiste à manipuler des personnes afin de les inciter à adopter un cer-tain comportement – par exemple, abuser de leur crédulité pour les amener à révéler des informations confidentielles. En faisant aussi appel à la serviabilité de leurs victimes, les «social engineers» tentent de parvenir à des données sensibles.

Hameçonnage
Tentative d'accéder aux données personnelles d'un internaute au moyen d'e-mails, de pages web falsifiées ou de messages courts dans le but de lui nuire (p. ex. vol de données ou de valeurs pécuniaires). Il s'agit d'une forme d'ingénierie sociale.

Cyberharcèlement
Terme générique désignant les formes de calomnie et de harcèlement d'autres personnes et entreprises par le biais d'Internet ou d'appareils mobiles. Le vol d'identités afin par exemple de conclure des affaires ou de faire des affirmations au nom d'un tiers en fait aussi partie. Il s'agit là encore d'une forme d'ingénierie sociale.

Maliciels
Terme générique désignant les programmes qui accomplissent des fonctions indésirables et dommageables. Le maliciel ne se propage souvent pas de lui-même, mais sollicite l'utilisation d'un programme hôte afin de conduire l'utilisateur à l'installer. Les maliciels les plus connus sont les chevaux de Troie, les logiciels espions et les rançongiciels.

Rançongiciels
Aussi appelés ransomware ou Trojans encodeurs, ce sont des logiciels malveillants avec lesquels un intrus peut empêcher d'accéder à des données et de les utiliser, ou encore em-pêcher l'accès au système informatique tout entier. L'objectif est d'exiger une rançon pour obtenir le déchiffrage ou le déblocage. En 2017, «WannaCry» et «NotPetya» ont attiré l'attention aux quatre coins du monde en paralysant complètement des hôpitaux et entre-prises de logistique, entre autres.

Déni de service distribué (DDoS)
Blocage des services informatiques exposés à Internet (site web, boutique en ligne ou forum), provoqué par une énorme quantité de demandes. Ce blocage empêche l'utilisation du service informatique visé. Ce genre d'attaque peut être causé par des surcharges involontaires ou une attaque ciblée. Il s'agit d'une forme de chantage de plus en plus courante à l'ère du com-merce en ligne.

Sensibilisation
Gestion des mots de passe et sécurité

Les mots de passe ne devraient être ni inscrits, ni communiqués à un tiers. L'authentification à plusieurs facteurs est un moyen simple et efficace pour renforcer la sécurité d'un compte. Un SMS est par exemple envoyé au numéro de téléphone portable enregistré de l'utilisateur qui reçoit un code à chiffres pour continuer l'identification. Pour chaque compte, il faudrait utili-ser des mots de passe différents qui ne se ressemblent pas. Il faut partir du principe que l'on peut perdre les mots de passe, c'est pourquoi il faut les modifier régulièrement. À cet égard, il est important de ne pas remplacer uniquement un chiffre ou une lettre, et de choisir au con-traire un mot de passe entièrement nouveau.

Si l'on soupçonne une utilisation abusive d'un compte, il est important de changer immédiate-ment le mot de passe s'y rapportant.

Gestionnaires de mots de passe (password-vaults)

Étant donné que chacun devrait, idéalement, utiliser son propre compte et différents mots de passe pour chaque service, il existe des gestionnaires de mots de passe (password-vaults) qui simplifient la création et la mémorisation des mots de passe nouveaux et existants. Ces applications permettent de générer un mot de passe sûr et de le stocker en le reliant à un compte. L'application est elle-même protégée par un mot de passe principal complexe ou par la reconnaissance faciale ou d'empreinte sur un smartphone. Ainsi, le collaborateur n'a que le mot de passe principal à mémoriser et il peut consulter de façon très simple tous les autres mots de passe. Voici quelques bons exemples de gestionnaires de mots de passe: Se-cure-Safe, 1Password et Keeper Security.

Check-list pour la sécurité des mots de passe

- ☐ Au moins 8 caractères
- ☐ Minuscules et majuscules
- ☐ Chiffres et caractères spéciaux
- ☐ Pas de suites de lettres figurant dans un dictionnaire
- ☐ Jamais utilisé auparavant

Conseil

Si vous n'utilisez pas de gestionnaire de mots de passe, les moyens mnémotechniques ou les phrases mots de passe peuvent vous aider à créer des mots de passe ou à les mémoriser plus facilement. Il s'agit en l'occurrence de phrases simples dans lesquelles on utilise l'initiale de chaque mot pour former un mot de passe.

Exemples:

→ Phrase mot de passe : Mon fil est né en février 1994, il va avoir 26 ans cette année.

→ Chaque première lettre ou chiffre dans l'ordre en respectant les minuscules et majuscules:

Mon fil est né en février 1994, il va avoir 26 ans cette année.
→ Mot de passe: **Mfenef94$iv**

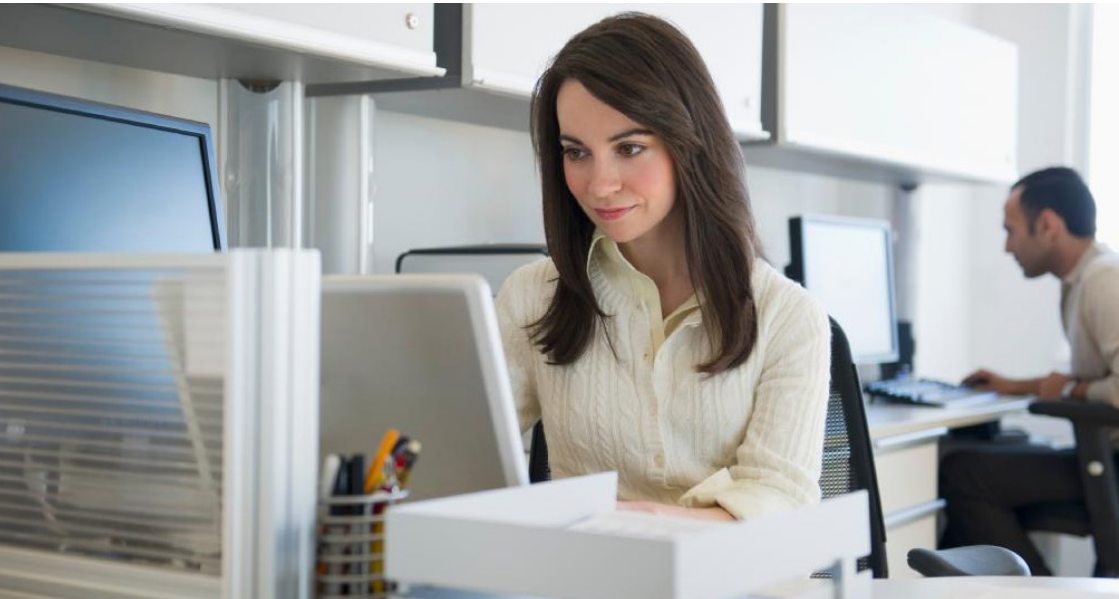
Ingénierie sociale
Scénarios et conduite à tenir

L'ingénierie sociale exploite essentiellement les émotions humaines. Les attaquants peuvent piéger leurs victimes en faisant appel à leur cupidité ou à leur curiosité. Ils peuvent également effrayer leurs victimes par des menaces ou par la prétendue urgence de leurs demandes, puis les manipuler. Très souvent, les attaquants abusent également de la confiance des vic-times pour accéder à leurs données personnelles, par exemple.

Vous pouvez être victime d'ingénierie sociale au cours d'un entretien direct, en ligne ou au téléphone. Les exemples de scénarios suivants devraient vous aider à être attentif à certains schémas:

- L'interlocuteur demande de manière fortuite des informations confidentielles.

- L'interlocutrice se fait passer pour une collaboratrice et demande à accéder à une zone pro-tégée.



→ L'interlocuteur insiste sur le caractère urgent de la demande et use de menaces.

→ L'interlocutrice vous invite à contourner exceptionnellement les règles.

Si vous êtes victime d'une telle attaque ou supposez être victime d'une attaque, nous recom-mandons d'adopter le comportement suivant:

→ Restez calme.

→ Ne transmettez pas d'informations dans la mesure où vous n'êtes pas certain de savoir avec qui vous discutez et quelles informations la personne est autorisée à connaître à propos de votre entreprise.

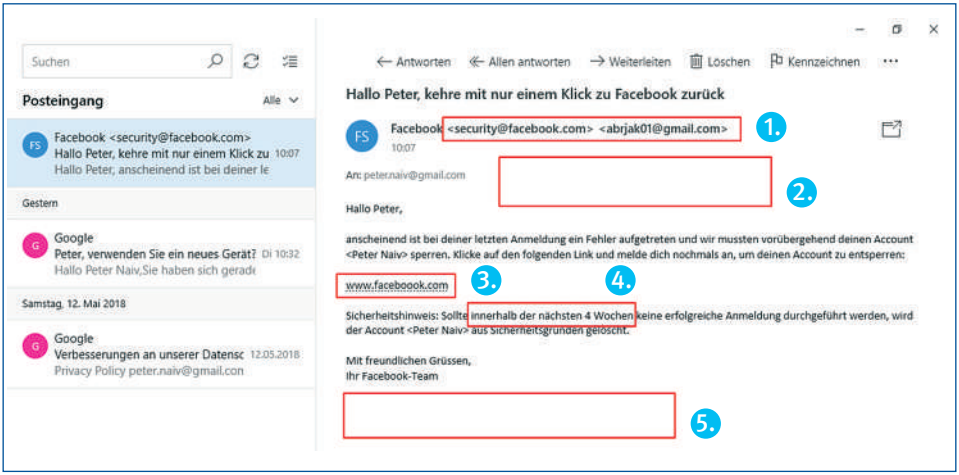
→ En cas de demande, exigez le badge visiteur ou collaborateur et ne laissez jamais entrer dans une zone protégée une personne que vous ne connaissez pas.

→ Posez vous-même des questions (p. ex. pour identifier la personne) et répétez si besoin. Ce-la bloque d'une part l'interrogation constante de l'interlocuteur, et vous aide d'autre part à comprendre la situation.

→ Si l'attaque se produit au téléphone, demandez un numéro de téléphone concret afin de rap-peler (les appels de ce genre sont souvent passés avec des numéros masqués ou ano-nymes). Ou bien raccrochez sans commentaire.

→ Gardez cependant à l'esprit que votre objectif n'est pas de faire fuir le «social engineer», mais de l'identifier et ainsi de protéger vos collaborateurs et vous-même contre d'éventuelles tenta-tives d'attaques à l'avenir. Pensez aussi que l'assaillant ou l'assaillante n'agit très vraisembla-blement pas seul(e).

Hameçonnage
Scénario et conduite à tenir



L'e-mail sur la page de droite explique à quoi l'on peut reconnaître un e-mail de hameçonnage et comment se comporter dans une telle situation.

Caractéristiques distinctives (boîtes rouges) de haut en bas:

1. L'expéditeur indiqué a deux adresses e-mails et la seconde ne ressemble vraiment pas à celle d'un collaborateur Facebook.
2. Il manque le logo Facebook. L'ensemble de l'e-mail n'a pas le formatage habituel de Face-book.
3. Le lien mentionné vers Facebook contient un «o» de trop. De plus, le lien ne montre aucun signe pour rediriger l'utilisateur vers une ouverture de session ou une page de déverrouillage.

4. L'e-mail semble urgent. Une menace sous forme d'une suppression de compte est aussi ex-primée dans la même phrase.

5. Les typiques disclaimer et remarques sur la protection des données à la fin de l'e-mail sont absents. Les moyens possibles pour prendre contact avec l'assistance de Facebook ne sont pas indiqués. Si le compte doit vraiment être supprimé dans les plus brefs délais, c'est là que vous trouveriez les données de contact.

D'autres caractéristiques typiques des e-mails de hameçonnage peuvent être:
- → une formulation impersonnelle;
- → une orthographe incorrecte et des problèmes d'accentuation;
- → l'utilisation d'une langue inhabituelle pour le pays (p. ex. l'anglais alors que le service est utili-sé en français);
- → une mise en page non homogène dans l'e-mail.

Faits et chiffres:
45% des internautes cliquent sur les liens dans les e-mails d'expéditeurs inconnus.

92 % des cyberattaques commencent par un e-mail de hameçonnage.

Comment procéder avec des e-mails de hameçonnage?
Les e-mails de hameçonnage ne sont pas toujours clairement identifiables. Si l'on soupçonne toutefois qu'un e-mail reçu est un e-mail de hameçonnage, il est possible de procéder comme suit:
- → Supprimer l'e-mail; s'il s'agit effectivement d'un message important, un véritable service en ligne se manifestera de nouveau.
- → Vérifier manuellement (sans passer par le lien indiqué dans l'e-mail) le statut du profil ou du service.
- → Appeler l'assistance clientèle de l'expéditeur et demander des informations. Le numéro de l'assistance clientèle d'un prestataire de services se trouve la plupart du temps très rapidement sur Google.

Notez que des entreprises sérieuses, telles que des établissements bancaires et d'assurance, ne demanderaient jamais à leurs clients de réagir à une communication impor-tante en cliquant sur un lien

dans un e-mail. Normalement, les clients sont toujours informés par téléphone. Si vous recevez un (prétendu) e-mail de votre banque ou de votre assureur vous demandant de vous inscrire via le lien indiqué dans le message, il peut s'agir en réalité d'un e-mail d'hameçonnage. En cas de doute, vous pouvez ouvrir votre navigateur et vous connecter directement sur le portail d'accès de votre banque ou de votre assureur. Une fois sur le por-tail, vous saurez immédiatement si l'établissement financier attend une réaction de votre part. Une autre solution consiste à contacter également votre banque ou votre assureur par téléphone.

Hameçonnage SMS

L'hameçonnage peut également se produire via un SMS sur votre téléphone mobile. Vérifiez lors de la réception d'un SMS avec un lien, à reconnaitre une tentative d'hameçonnage:

- → Vérifier nom et numéro de l'expéditeur
- → Vérifier l'orthographe du message
- → Regarder le lien (par ex. nom de l'entreprise correctement orthographiée)
- → En ca de doute contacter le service client de l'entreprise par téléphone ou par mail.

Protection contre les rançongiciels
et réaction en cas d'incident

Un rançongiciel peut parvenir sur votre système par divers moyens et vous causer des dommages en cryptant vos données. Pensez aux mesures suivantes pour éviter cette forme de chantage:

→ Prudence avec les e-mails, en particulier en ouvrant des pièces jointes. Le rançongiciel est principalement diffusé par e-mail et se propage lorsque vous cliquez sur des liens et que vous téléchargez des pièces jointes sur votre système. Confiez impérativement à votre protection antivirus le soin d'examiner les pièces jointes provenant d'expéditeurs inconnus.

→ Prudence avec les supports de stockage tels que les clés USB et les disques durs nomades. En particulier si vous ne connaissez pas le précédent utilisateur du support de stockage et que vous n'êtes pas sûr de savoir ce qui se trouve dessus, vous ne devriez pas le connecter à votre système.

→ Maintenez toujours vos systèmes à jour. Les nouvelles versions des logiciels d'exploitation apportent souvent des améliorations portant sur la sécurité de l'information. Les mises à jour de votre programme antivirus aussi contiennent des améliorations dans la détection et la lutte contre les virus. Elles devraient toujours être effectuées.
Utilisez en plus une solution de sauvegarde et créez régulièrement des copies de sécurité de vos données.

En cas d'incident

→ Ne payez pas la somme exigée! Souvent, la somme augmente par la suite, sans pour autant que vos données soient décryptées.

→ Tournez-vous vers un spécialiste et essayez de restaurer votre système avec une sauve-garde ayant été faite avant l'incident.

Autres lignes directrices de prévention importantes

Attribuer les responsabilités
La sécurité de l'information est la mission et le défi de chaque collaborateur. Néanmoins, vous devriez désigner une personne responsable de la sécurité de l'information au sein de votre entreprise, ainsi qu'un suppléant. La personne responsable doit prendre en charge les tâches de sécurité et informer régulièrement vos collaborateurs et vous-même sur l'état de la sécuri-té de l'information dans votre entreprise. Elle doit également être la personne à contacter en cas de questions, d'incertitudes et d'incidents.

Sécuriser les données – faire des back-up
Les données sensibles telles que les informations des clients ou les transactions peuvent se perdre indépendamment d'une cyberattaque. D'autres facteurs externes, tels qu'un incendie ou des dégâts d'eau, peuvent également entraîner une perte de données.
Créez donc régulièrement des copies de sécurité de vos données, les dénommés «back-up». Pour ceci, des programmes plus ou moins bons, et plus ou moins chers sont proposés. Il est important, aussi, de tester régulièrement s'il est possible de restaurer les données sécurisées et de veiller à ce que les back-up ne soient pas conservés au même endroit que le support de données d'origine.

Nous recommandons en outre l'installation d'un pare-feu qui vous protège des attaques exté-rieures, et d'un antivirus qui contrôle régulièrement votre système et les données qu'il con-tient.
La plupart des antivirus, pare-feu et programmes de back-up offrent une version d'essai ou sont pour certains disponibles gratuitement. Prenez par conséquent le temps de tester quelques programmes et choisissez une solution qui convienne à votre entreprise, tant au niveau du prix que des prestations.
Les solutions de sauvegarde dans un cloud sont maintenant courantes. Soyez toutefois conscients que vos données seront soumises à la loi sur la protection des données du pays où le serveur du cloud est installé. Même si vous optez pour cette solution, vous devez également effectuer des sauvegardes physiques de vos données.

Mise à jour du système d'exploitation et des programmes
Installez rapidement les mises à jour d'exploitation et de sécurité régulières pour votre sys-tème d'exploitation et

vos programmes. Ces «correctifs» permettent de rectifier des failles de sécurité connues, ce qui améliore la sécurité de toutes les fonctions.

Tous les systèmes d'exploitation et programmes pour ordinateur et smartphone ne sont pas sans faille. Les concepteurs des maliciels tirent souvent parti de ces failles pour accéder à l'ordinateur ou au smartphone.

Faire preuve de bon sens
Lorsque vous surfez et effectuez des opérations sensibles sur Internet, faites toujours preuve de bon sens.

Pour d'autres lignes directrices de prévention, des informations sur la cybersécurité ou en-core d'intéressants piratages en direct, participez aux séances d'information et aux présenta-tions des Baloise Scouts Digitaux

Le piratage est répréhensible
Toutes les sortes de cyberattaques sont interdites par la loi.

Soutien de l'État
Le Conseil fédéral a adopté la nouvelle Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022 le 18 avril 2018. La stratégie repose sur la première SNPC (2012-2017) et met en évidence des mesures de réduction des cyber-risques correspondant au niveau de menace actuel. Vous trouverez plus d'informations concernant la SNPC sur **www.isb.admin.ch**.

De plus, l'État met à disposition depuis 2010 la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) sur **www.melani.admin.ch**. Vous y trouverez des informa-tions sur les risques et mesures actuels, ainsi qu'un formulaire de déclaration d'incident pour les particuliers et pour les PME.

Have I Been pwned?
Le site Internet «Have I Been pwned» (HIBP) réunit et analyse des «data dumps», autrement dit des vidages de mémoires qui, suite à des violations de données, ont été mis en ligne par des pirates informatiques. HIBP offre à l'utilisateur la possibilité de vérifier si dans cette multi-tude de données utilisateurs divulguées et par conséquent menacées, se trouve sa propre adresse e-mail ou son nom d'utilisateur. Il est également possible d'intégrer une fonction qui informe l'utilisateur par e-mail si ses propres données ont été divulguées dans une violation de données. Ou encore de chercher des mots de passe déjà publiés. C'est pourquoi il est important d'utiliser plusieurs mots de passe car les mots de passe ayant été divulgués dans une violation de données sont vendus sur Internet et ne devraient par conséquent plus être utili-sés.
https://haveibeenpwned.com

Baloise Group
Aeschengraben 21
CH-4002 Basel
pfadfinder@baloise.com

www.baloise.com

000.1038 f 2.20 150