baloise

Guide Cybersécurité – PME

Nous vous montrons la voie dans la jungle numérique

À propos des Baloise Digital Scouts

L'équipe Digital Scouts de Baloise est composée de collaboratrices et collaborateurs motivés et enthousiastes. Ambassadeurs de la numérisation, ils vous offrent leur aide pour vous y retrouver dans la jungle numérique. L'organisation des Baloise Digital Scouts est une collaboration entre les domaines Group IT et Corporate Communications.

Les Baloise Digital Scouts apportent une contribution bénévole dans le cadre de la responsabilité sociale de l'entreprise Baloise, car les besoins de la société vont au-delà de l'achat de prestation de services de sécurité. Les collaborateurs de Baloise disposent d'un vaste savoir-faire qui est mis à la disposition de l'entreprise en plus des services liés à notre activité.

Une séance d'information sur la cybersécurité vous intéresse?

Contactez-nous par e-mail à l'adresse scouts@baloise.com

À propos de cette brochure

Cette brochure est destinée à aider les clients PME à informer leurs collaboratrices et collaborateurs des dangers et risques de l'utilisation quotidienne d'Internet sur le lieu de travail et à domicile. Elle a également pour vocation d'expliquer les bases de la cybersécurité et de montrer les directives préventives pour éviter les cyberincidents.

Les risques de cybersécurité existent sous de nombreuses formes et peuvent causer des dommages importants, voire désastreux. L'homme reste à l'origine de la plupart des incidents de sécurité dans une entreprise. Mais à travers une compréhension claire des risques et des conséquences de nos propres actions, ce risque peut toutefois être considérablement réduit.

Protection des informations en dehors des locaux professionnels

Ingénierie sociale
Pour de nombreuses entreprises, les déplacements professionnels font partie du quotidien, voire de l'objectif commercial. Aussi, il est important de préserver la sécurité de l'information et d'être conscient des dangers. Que ce soit dans un train, dans le hall d'un hôtel, dans un café ou dans la rue: partout, les murs ont des oreilles, ou des yeux indiscrets peuvent s'emparer d'informations, et à l'occasion, les utiliser à leur avantage. Les collaborateurs doivent donc être sensibilisés à la protection des informations, même en dehors des locaux de l'entreprise.

Télétravail
Les collaborateurs qui travaillent à domicile doivent être conscients qu'ils doivent protéger les données professionnelles aussi bien qu'au bureau. Il s'agit notamment de ne pas mélanger les données professionnelles et privées. Il vaut donc mieux utiliser des appareils différents. Toutefois, s'ils sont autorisés à utiliser leurs propres appareils (privés), il convient également de leur fournir les informations nécessaires à la protection des données. Réglez donc au moins les points suivants:

- Réalisation de mises à jour régulières
- Utilisation de pages HTTPS et VPN pour une connexion sécurisée
- Élimination sûre des informations écrites sensibles (pas dans les vieux papiers)
- Utilisation d'images d'arrière-plan et partage de contenu lors de vidéo-conférences
- Réalisation de sauvegardes
- Signalement d'anomalies inhabituelles

Dans les espaces publics
Dès que l'on travaille en public, que ce soit lors d'un repas d'affaires au restaurant ou en rentrant chez soi dans le train, les conversations peuvent être entendues. Il est donc important de choisir ses mots de manière à ce que les personnes qui écoutent ne puissent pas en déduire quelque chose. En outre, il est recommandé d'utiliser une protection contre les regards indiscrets lorsque des personnes étrangères peuvent regarder l'ordinateur portable ou le téléphone mobile. Certains entretiens ne devraient donc être menés que dans un espace protégé. Un appareil non surveillé même un court instant peut également être dérobé.

Conseils

- Sensibilisez vos collaborateurs afin qu'ils préservent la sécurité de l'information, même en voyage d'affaires ou à domicile.
- Rendez les conversations en public plus sûres, par exemple en ne citant que la première lettre des noms ou en disant «mon organisation» au lieu du nom de l'entreprise.
- Utilisez des écrans de confidentialité pour rendre plus difficile la lecture par des yeux indiscrets.

Gestion des mots de passe et leur sécurité

Les mots de passe ne devraient être écrits nulle part, ni communiqués à un tiers. L'authentification à plusieurs facteurs est un moyen simple et efficace visant à renforcer la sécurité d'un compte. Par exemple, lors de la connexion, après avoir saisi le nom d'utilisateur et le mot de passe, un autre code est demandé à partir d'une application d'authentification que vous avez installée sur votre appareil mobile. Il est important pour chaque compte, d'utiliser des mots de passe différents qui ne se ressemblent pas. Si l'on soupçonne qu'un mot de passe a été perdu ou compromis par un autre incident, il faut le changer immédiatement. À cet égard, il est important de ne pas remplacer uniquement un chiffre ou une lettre, et de choisir au contraire un mot de passe entièrement nouveau.

Gestionnaire de mots de passe
Pour chaque service, il convient d'utiliser un compte distinct avec des mots de passe différents. Les gestionnaires de mots de passe simplifient la création et la mémorisation de mots de passe nouveaux ou existants. Ces applications permettent de générer un mot de passe sûr et de le sauvegarder en le reliant à un compte. L'application est elle-même protégée par un mot de passe principal complexe, ou sur un smartphone, par la reconnaissance faciale ou une empreinte digitale. 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.

Check-list pour la sécurité des mots de passe

- Au moins 12 caractères (plus c'est long, plus c'est sûr)
- Minuscules et majuscules
- Chiffres et caractères spéciaux tels que: !, &, %, ç, +
- Pas de mots figurant dans un dictionnaire
- Pas de séquences de lettres comme «abcdefgh»
- Mot de passe jamais utilisé auparavant
- Idéal: un mot de passe à partir d'une phrase de passe

Comment créer une phrase de passe

1. Choisissez une phrase qui vous vient facilement à l'esprit.
2. Utilisez toutes les premières lettres dans le bon ordre et faites attention aux majuscules et aux chiffres. Cette séquence de caractères constitue le nouveau mot de passe.
3. Enfin, remplacez les signes de ponctuation par des caractères spéciaux et voilà qu'un mot de passe sûr et facile à retenir est constitué.

Exemple:
Mon fils est né en février 1998.
Cette année, il a eu 26 ans!
Phrase mot de passe: Mfenef98.Ca%iae26a!

Conseils

- Utilisez également l'authentification à plusieurs facteurs pour votre gestionnaire de mots de passe et préférez les applications d'authentification aux codes SMS.
- Ne communiquez en aucun cas votre mot de passe.
- Vérifiez sur des sites comme ibarry.ch si vos données d'accès ne sont pas déjà apparues dans un recueil de données. Si oui, changez impérativement votre mot de passe.

Ingénierie sociale

Les attaques par ingénierie sociale exploitent essentiellement les émotions humaines. Les attaquants peuvent piéger leurs victimes en faisant appel à leur serviabilité 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 toutefois simplement de la confiance des victimes pour accéder à des données confidentielles, 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 prendre conscience de certains schémas:

Votre interlocuteur

- vous demande de manière désinvolte des informations confidentielles;
- se fait passer pour un collaborateur et demande à accéder à une zone protégée;
- insiste sur le caractère urgent de la demande et use de menaces;
- vous invite à déroger exceptionnellement aux règles.

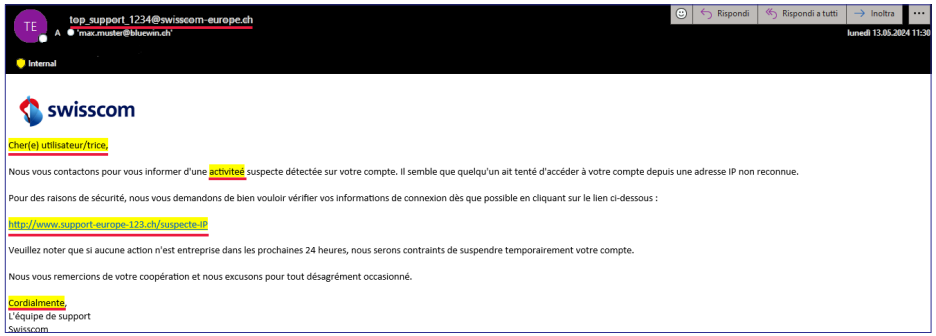
Si vous êtes ou pensez être victime d'une telle attaque, nous recommandons la procédure suivante:

- Restez calme.
- Ne transmettez pas d'informations dans la mesure où vous n'avez pas la certitude de savoir avec qui vous discutez et quelles informations la personne est autorisée à connaître à propos de vous et 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 (par exemple sur l'identification) et répétez-les si nécessaire. Cela 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 rappeler (les appels de ce genre sont souvent passés avec un numéro masqué ou anonyme) ou mettez fin à la conversation sans donner d'informations.
- Gardez à l'esprit que vous ne voulez pas chasser immédiatement l'«ingénieur social», mais l'identifier. Vous pourrez ainsi le dissuader d'éventuelles futures tentatives d'attaques contre vous et vos collaborateurs.

Conseils

- Faites attention à ce que vous révélez à votre propos sur les médias sociaux. Vos amis et connaissances ne sont pas les seules personnes à pouvoir lire ces informations.
- L'intelligence artificielle est aujourd'hui utilisée pour vous tromper encore mieux via différents canaux.
- En cas d'incertitude, contactez la personne présumée sur un autre canal que vous possédez déjà.

Phishing, ou hameçonnage



Le phishing est une forme d'ingénierie sociale. Il s'agit de tenter de gagner la confiance du destinataire, de lui soutirer des informations confidentielles ou de l'inciter à agir dans le but de nuire à l'entreprise. Le phishing est l'une des plus grandes portes d'entrée pour les cyberattaques.

À l'aide de l'e-mail ci-dessus, nous expliquons comment reconnaître un e-mail de phishing et comment le traiter.

Caractéristiques distinctives (parties marquées en rouge) de haut en bas:

1. L'expéditeur indiqué n'a pas de véritable adresse Swisscom.
2. Approche impersonnelle sans nom. En général, quand on est connu comme client, on s'adresse à nous personnellement.
3. L'orthographe ne respecte pas les règles habituelles.
4. Le lien, tout comme l'adresse e-mail, n'a aucun lien avec Swisscom.

D'autres caractéristiques typiques des e-mails de phishing peuvent être:

- l'utilisation d'une langue inhabituelle pour le pays (p. ex. l'anglais alors que le service est utilisé en français);
- des mises en forme ou des logos différents dans l'e-mail;
- des e-mails envoyés à l'adresse professionnelle, bien que l'expéditeur ne soit utilisé que dans le cadre privé.

Comment procéder avec des e-mails de phishing?

Les e-mails de phishing ne sont pas toujours faciles à identifier. Si l'on soupçonne qu'un e-mail reçu est un courriel d'hameçonnage, il ne faut ni ouvrir les pièces jointes ni cliquer sur les liens contenus dedans.

Il ne faut pas non plus répondre directement à l'e-mail via «Répondre». Si l'e-mail a été envoyé depuis une adresse d'entreprise impersonnelle, par exemple le support ou le service clientèle, contactez l'entreprise via un canal vérifié de manière indépendante. Par exemple, allez directement sur le site de l'entreprise via votre navigateur Internet et recherchez les possibilités de contact.

Si vous disposez d'un service informatique, contactez vos collègues de l'IT pour leur signaler l'e-mail et, le cas échéant, faire en sorte que d'autres collaborateurs soient avertis.

Comment se protéger?

Utilisez un mot de passe différent pour chaque compte. Si cela est possible, activez l'authentification à plusieurs facteurs. Celle-ci offre une protection supplémentaire et réduit le risque d'abus. Aucune banque ne vous demandera jamais par e-mail de modifier un mot de passe ou de vérifier les données de votre carte de crédit.

Conseils

- Le phishing ou hameçonnage n'existe pas seulement par e-mail, mais aussi par SMS (smishing), par appel téléphonique (vishing) et par code QR (quishing).
- En cas de doute, contactez le centre clientèle de l'expéditeur par téléphone ou par e-mail.
- Et demandez-vous si vous vous attendiez à recevoir ce message.

Ransomware (rançongiciel)

Ce terme est composé de l'anglais «ransom» pour rançon et «malware» pour maliciel. Il s'agit là de programmes malveillants, également appelés chevaux de Troie de chantage ou crypto. L'objectif des criminels est d'extorquer une rançon. Pour ce faire, les données sont soit cryptées sur le réseau, soit volées avant d'être cryptées, en envoyant les données vers un serveur externe aux criminels. Une rançon est ensuite extorquée, soit pour le décryptage des données, soit pour la non-publication des données.

Comment fonctionne une attaque de rançongiciel?
Il existe différentes portes d'entrée pour une attaque de rançongiciel. Le moyen le plus répandu est encore la voie classique via un e-mail de phishing ou hameçonnage. Sensibilisez vos collaborateurs aux risques et veillez en particulier, lors de l'utilisation de courriels, à ne pas cliquer inconsidérément sur des liens ou à ne pas ouvrir de pièces jointes. Le risque est de permettre au rançongiciel de pénétrer dans le réseau de l'entreprise, de s'y propager et de causer un maximum de dommages.

Les systèmes présentant des points faibles, c'est-à-dire ne disposant pas de mises à jour de sécurité, par exemple les systèmes d'exploitation ou les navigateurs Web, constituent une autre porte d'entrée.

La troisième voie la plus répandue est celle des accès exposés de maintenance à distance, directement accessibles via Internet

Comment puis-je me protéger et protéger mon entreprise?
Des mesures préventives permettent de réduire considérablement les risques:

- Installez les mises à jour de sécurité rapidement après leur développement.
- N'utilisez que des logiciels qui sont encore pris en charge par le fournisseur.
- Faites des sauvegardes régulières, si possible automatisées, et stockez-les en dehors de votre réseau.
- Testez régulièrement si les sauvegardes sont fonctionnelles et effectuez des tests de restauration.
- Lors du choix de la sauvegarde, tenez compte du temps nécessaire à la restauration complète ainsi que du niveau de perte de données acceptable pour votre entreprise.
- Sensibilisez vos collaboratrices et collaborateurs à la procédure à suivre en cas d'incident et à la manière de signaler les e-mails suspects ou les événements inhabituels.

Que faire en cas d'incident?
Garder son calme. Il est généralement utile de faire appel à des spécialistes externes qui ont de l'expérience avec les cyberattaques. Ils peuvent vous conseiller et vous aider à identifier comment l'incident s'est produit et quelles sont les étapes utiles pour pouvoir reprendre le travail le plus rapidement possible.

Contactez l'Office fédéral de la cybersécurité (OFCS). Les spécialistes de l'OFCS apportent leur soutien en fournissant des informations utiles concernant l'analyse et la procédure.

Conseils

- N'utilisez que des logiciels qui sont encore pris en charge par le fournisseur.
- Élaborez un plan en cas de cyberattaque.
- Installez un logiciel de protection des terminaux (endpoint protection software) sur tous les appareils afin de détecter les attaques à un stade précoce.

Autres directives de prévention importantes

Prendre les dispositions
La sécurité de l'information est un défi pour chaque entreprise. Préparez-vous à l'avance à une cyberattaque. Établissez un plan et entraînez-vous à réagir en cas d'incident. Quand une cyberattaque a lieu, il est trop tard pour se pencher sur la question.

Sauvegarder les données – créer des sauvegardes et les tester régulièrement
Ce n'est pas seulement en cas de cyberattaque que des données sensibles telles que des informations sur les clients ou des données peuvent être perdues. D'autres événements, tels qu'un incendie ou des dégâts d'eau, peuvent entraîner une perte de données. Créez donc régulièrement des copies de sécurité de vos données, les dénommés «back-ups». Il est également important de tester régulièrement si les données sauvegardées peuvent être restaurées. Stockez les sauvegardes séparément des données d'origine afin qu'elles soient également disponibles en cas d'incident. Lors de la création de la sauvegarde, réfléchissez au préalable à quelle quantité de données vous pouvez accepter de perdre. En fonction de cela, vous devriez planifier les cycles de sauvegarde.

Mises à jour
Installez les mises à jour de sécurité disponibles dans les meilleurs délais pour vos systèmes d'exploitation et vos programmes. Veillez à ce que le logiciel utilisé soit encore pris en charge par le fournisseur.

Faire preuve de bon sens
Lorsque vous surfez et effectuez des opérations sensibles sur Internet, faites toujours preuve de bon sens. Ne vous laissez pas mettre sous pression par un e-mail ou un appel téléphonique. Il y a toujours du temps pour réfléchir.

Soutien de l'État
L'Office fédéral de la cybersécurité (OFCS) propose des informations et une aide sur les dangers actuels et les mesures à prendre, ainsi qu'un formulaire d'annonce d'incidents pour les entreprises et les particuliers.

Comment puis-je vérifier si mes données ou moi-même sommes concerné·es?
iBarry est la plateforme suisse pour la sécurité sur Internet. Ce site propose des informations et des outils utiles à chaque entreprise pour sensibiliser ses propres collaborateurs.

iBarry met également à disposition un contrôle de sécurité qui permet de vérifier si ses données d'accès à des services web ont été volées.

Conseils
- **Soutien de l'État auprès de l'Office fédéral de la cybersécurité (https://www.ncsc.admin.ch/)**
- **iBarry – Plateforme pour la sécurité sur Internet (https://www.iBarry.ch)**

Baloise Group
Aeschengraben 21
CH-4002 Basel
baloise.com
www.baloise.com/digital-scouts

000.1038f 5.24 pdf