Baloise
DIGITALE
PFADFINDER

Cyber Security Guide – KMU

Wir zeigen Ihnen den Weg durch den digitalen Dschungel.

www.baloise.com/digitale-pfadfinder

Baloise
Group

Über die Baloise Digitale Pfadfinder

Der Digitale Pfadi-Corps der Baloise besteht aus motivierten und interessierten Mitarbeitenden. Als Botschafter der Digitalisierung wollen wir unseren Mitmenschen dabei helfen, den Weg durch den digitalen Dschungel zu finden. Die Organisation der Baloise Digitale Pfadfinder ist eine Zusammenarbeit aus den Bereichen Corporate IT und Corporate Communications.

Die Baloise Digitale Pfadfinder leisten im Rahmen der Corporate Social Responsibility der Baloise einen freiwilligen Beitrag, denn die Bedürfnisse der Gesellschaft gehen weiter als der Bezug von Sicherheitsleistungen. Baloise-Mitarbeitende verfügen über ein breites Know-how. Dieses wird über die geschäftsrelevanten Dienstleistungen hinaus der Gesellschaft zur Verfügung gestellt.

Sind Sie an einer Infoveranstaltung über Cyber Security interessiert? Kontaktieren Sie uns per E-Mail:
pfadfinder@baloise.com

Über diese Broschüre

Diese Broschüre soll KMUs dabei helfen, ihre Mitarbeitenden über die Gefahren und Risiken beim alltäglichen Gebrauch des Internets am Arbeitsplatz und zu Hause zu informieren. Weiter erklärt sie die Grundlagen der Cyber Security und zeigt präventive Richtlinien zur Verhinderung von Cyber-Vorfällen auf.

Cyber Security-Risiken existieren in vielen Formen und können unterschiedlich grossen und verheerenden Schaden anrichten. Die grösste Schwachstelle in der IT-Sicherheit eines Unternehmens ist und bleibt allerdings immer noch der Mensch. Durch klares Verständnis der Risiken und der Konsequenzen des eigenen Handelns kann diese Schwachstelle jedoch wesentlich reduziert werden.

Die wichtigsten Begriffe kurz erklärt

Social Engineering
Zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie beispielsweise aufgrund ihrer Gutgläubigkeit zur Preisgabe von vertraulichen Informationen zu bewegen. Auch durch das appellieren an die Hilfsbereitschaft ihres Opfers versuchen «Social Engineers» an sensible Daten zu kommen.

Malware
Oberbegriff für Programme, die unerwünschte und schädliche Funktionen ausführen. Malware verbreitet sich oft nicht selbst, sondern wirbt mit der Nützlichkeit eines Wirtsprogrammes für seine Installation durch den Benutzer. Zu den bekanntesten Malware-Programmen gehören Trojaner, Spyware und Ransomware.

Phishing
Versuche, über E-Mails, gefälschte Webseiten oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit den entsprechenden Personen zu schaden (z.B. Diebstahl von Daten oder Geldwerten). Es handelt sich dabei um eine Form des «Social Engineering».

Distributed Denial of Service (DDoS)
Eine durch eine Unmenge von Anfragen verursachte Blockade der dem Internet exponierten IT-Dienste, wie einer Webseite, einem e-Shop oder einem Forum. Durch diese Blockade wird die Verwendung des IT-Diensts verweigert. Dies kann durch unbeabsichtigte Überlastungen oder einen konzentrierten Angriff verursacht werden. Eine in Zeiten von digitalen Verkaufskanälen zunehmend beliebte Form der Erpressung.

Cyber Mobbing
Oberbegriff für Formen der Verleumdung und Belästigung anderer Menschen und Unternehmen über das Internet oder über Mobilgeräte. Dazu gehört auch der Diebstahl von Identitäten, um bspw. in fremdem Namen Geschäfte zu tätigen oder Aussagen zu machen. Es handelt sich ebenfalls um eine Form des «Social Engineering».

Ransomware (vom Englischen «ransom» für «Lösegeld»)
Das sind Schadprogramme, auch Erpressungs- oder Krypto-Trojaner genannt, mit deren Hilfe ein Eindringling den Zugriff auf Daten, deren Nutzung oder den Zugriff auf das ganze Computersystem verhindern kann. Ziel ist es, für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern. Im Jahr 2017 erlangten «WannaCry» und «NotPetya» weltweite Aufmerksamkeit, indem sie u.a. Spitäler und Logistikunternehmen komplett lahmlegten.

Sensibilisierung
Umgang mit Passwörtern und deren Sicherheit

Passwörter sollten nicht aufgeschrieben und mit niemandem geteilt werden. Multi-Faktor-Authentisierung ist eine gute und einfache Art, die Sicherheit eines Accounts zu steigern. Dabei wird beispielsweise beim Login eine SMS an die registrierte Handynummer des Benutzers gesendet, die einen Zahlencode für den weiteren Login enthält. Es sollten für jeden Account verschiedene Passwörter verwendet werden, die sich auch nicht zu sehr ähneln. Es muss davon ausgegangen werden, dass Passwörter verloren gehen können, weshalb sie regelmässig geändert werden müssen. Dabei ist es wichtig, nicht nur eine Zahl oder einen Buchstaben zu ändern, sondern sich ein komplett neues Passwort auszudenken.

Sollte Verdacht auf Missbrauch eines Accounts bestehen, ist es wichtig, das dazugehörige Passwort sofort zu ändern.

Password-Vaults

Da man idealerweise für jeden Dienst einen eigenen Account mit verschiedenen Passwörtern verwenden sollte, und damit Ausdenken und Merken von neuen und bestehenden Passwörtern zu vereinfachen, gibt es sogenannte Password-Vaults. Dies sind Applikationen, die es ermöglichen, ein sicheres Passwort zu generieren und dieses in Verbindung mit einem Account abzuspeichern. Die Applikation selbst wird durch ein komplexes Master-Passwort oder auf dem Smartphone auch durch Fingerprint- oder Face-ID geschützt. So muss sich der Mitarbeitende nur noch das Master-Passwort merken und kann alle anderen Passwörter einfach nachschauen. Gute Beispiele für Password-Vaults sind: SecureSafe, 1Password und Keeper Security.

Checkliste Passwortsicherheit

- ☐ Mind. 8 Zeichen lang
- ☐ Klein- und Grossbuchstaben
- ☐ Zahlen und Sonderzeichen
- ☐ Keine im Wörterbuch aufgelisteten Buchstabenfolgen
- ☐ Noch nie zuvor verwendet

Tipp

Verwenden Sie keinen Password-Vault, helfen Eselsbrücken und Passwortsätze dabei, neue Passwörter zu erstellen und sich diese einfacher zu merken. Dabei handelt es sich um einfache Sätze, wobei man den Anfangsbuchstaben jedes Wortes nimmt. Aneinandergereiht ergeben diese Buchstaben ein Passwort.

Beispiel:

→ Passwortsatz: Mein Sohn ist im Februar 1994 geboren. Er ist dieses Jahr 24 geworden.

→ Alle Anfangsbuchstaben in ihrer Reihenfolge und Gross- bzw. Kleinschreibung und Zahlen ergeben das neue Passwort. Zusätzlich noch die Satzzeichen mit einem Sonderzeichen austauschen und ein sicheres und leicht zu merkendes Passwort ist erstellt:

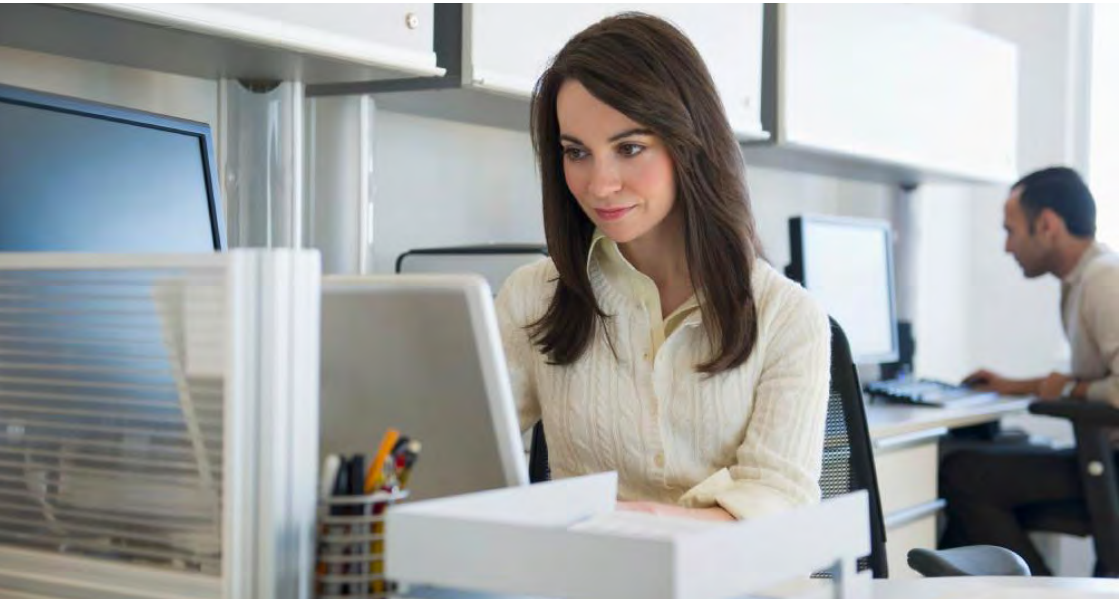
Mein Sohn ist im Februar 1994 geboren. Er ist dieses Jahr 24 geworden.
→ Passwort: **MSiiF94g$EidJ24g**

Social Engineering
Szenarien und Umgang

Social Engineering Angriffe nutzen grundsätzlich die menschlichen Emotionen aus. Die Angreifer können die Gier oder Neugierde ihrer Opfer gegen sie verwenden, um sie in ihre Falle zu locken. Auch können sie ihren Opfern durch Drohungen oder der vermeintlichen Dringlichkeit ihres Anliegens Angst einflössen und so manipulieren. Sehr oft missbrauchen die Angreifer aber auch einfach das menschliche Vertrauen ihrer Opfer, um beispielsweise an vertrauliche Daten zu gelangen.

Social Engineering kann im direkten Gespräch, wie auch online und am Telefon gegen Sie praktiziert werden. Folgende Beispielszenarien sollen Ihnen helfen, auf gewisse Muster aufmerksam zu werden:

- → Der Gesprächspartner fragt beiläufig nach vertraulichen Informationen
- → Die Gesprächspartnerin gibt sich als Mitarbeiterin aus und fordert Zugang zu einem geschützten Bereich



→ Der Gesprächspartner besteht auf die hohe Dringlichkeit des Anliegens und verwendet Drohungen. Der Gesprächspartner fordert Sie auf, Regelungen ausnahmsweise zu umgehen.

Falls Sie Opfer eines solchen Angriffs werden oder vermuten, gerade Opfer eines Angriffs zu werden, empfehlen wir folgendes Vorgehen:

→ Bleiben Sie ruhig.

→ Geben Sie keine Informationen weiter, sofern Sie sich nicht sicher sind, mit wem Sie sich unterhalten und welche Informationen diese Person über Ihr Unternehmen wissen darf.

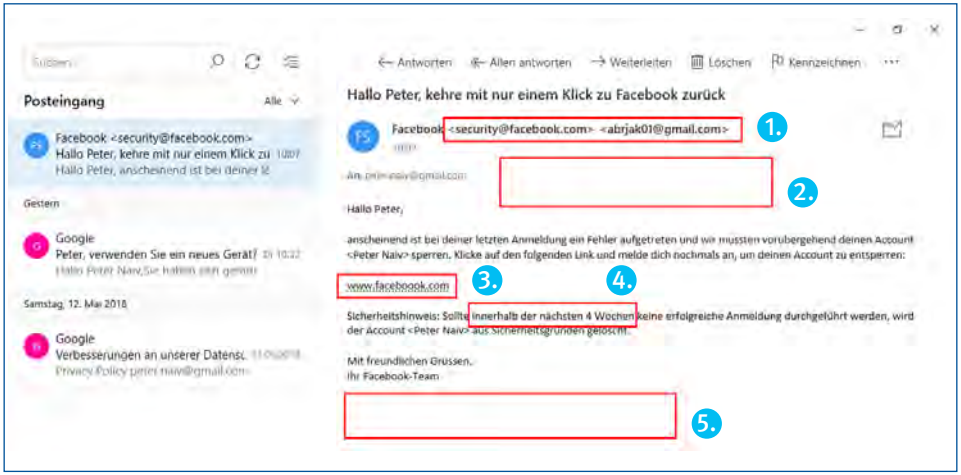
→ Verlangen Sie bei Anfragen den Mitarbeiter- oder Besucherausweis und lassen Sie niemals eine unbekannte Person in einen geschützten Bereich.

→ Stellen Sie selbst Fragen (z.B. zur Identifikation) und wiederholen Sie diese nötigenfalls. Dies blockt einerseits die konstante Befragung des Gegenübers ab, andererseits hilft es Ihnen, die Situation zu verstehen.

→ Erfolgt der Angriff per Telefon, fragen Sie nach einer konkreten Nummer, um zurückzurufen (Anrufe dieser Art erfolgen oft mittels unterdrückter bzw. anonymer Nummer). Oder legen Sie kommentarlos auf.

→ Behalten Sie jedoch im Hinterkopf, dass Sie den «Social Engineer» nicht verscheuchen, sondern identifizieren und so von möglichen zukünftigen Angriffsversuchen auf Sie und Ihre Mitarbeitenden abhalten wollen. Denken Sie auch daran, dass der Angreifer oder die Angreiferin höchstwahrscheinlich nicht allein arbeitet.

Phishing
Szenario und Umgang



Anhand der oben abgebildeten Mail wird erklärt, woran man eine Phishing-Mail erkennen kann und wie man mit dieser umgeht.

Erkennungsmerkmale (rote Boxen) von oben nach unten:

1. Der angegebene Absender hat zwei E-Mail-Adressen, wobei die zweite überhaupt nicht nach einem Facebook-Mitarbeitenden aussieht.
2. Das Logo von Facebook fehlt. Die gesamte Mail ist nicht in dem gewöhnlichen Facebook-Look formatiert.
3. Der angegebene Link zu Facebook hat ein «o» zu viel. Auch zeigt der Link keinerlei Anzeichen dafür, den User auf eine Login- oder Entsperrungsseite weiterzuleiten.

4. Eine gewisse Dringlichkeit wird angedeutet. Im gleichen Satz wird auch eine Drohung in Form der Account-Löschung ausgesprochen.

5. Typische Disclaimer und Datenschutzbemerkungen am Ende der Mail fehlen. Auch mögliche Wege der Kontaktaufnahme mit dem Support von Facebook werden nicht aufgelistet. Sollte der Account wirklich nächstens gelöscht werden, wären hier definitiv Kontaktangaben zu finden.

Weitere typische Merkmale von Phishing-Mails können sein:
- → unpersönliche Ansprache
- → fehlerhafte Rechtschreibung und Probleme mit Umlauten
- → landesunübliche Sprache (beispielsweise Englisch, obwohl der Service auf Deutsch verwendet wird)
- → unterschiedliche Formatierungen in der Mail.

Zahlen und Fakten:
45% aller Internetnutzer klicken auf Links in E-Mails von unbekannten Absendern.

92 % aller Cyber-Angriffe beginnen mit einer Phishing-Mail.

Wie umgehen mit Phishing-Mails?
Nicht alle Phishing-Mails sind eindeutig identifizierbar. Sollte jedoch der Verdacht bestehen, dass es sich bei einer empfangenen Mail um eine Phishing-Mail handelt, kann Folgendes unternommen werden:
- → E-Mail löschen; sollte es sich wirklich um eine wichtige Mail handeln, wird sich ein echter Onlinedienst nochmals melden.
- → Manuell (nicht über den Link in der E-Mail) den Status des Profils oder Services überprüfen.
- → Kundensupport des Absenders anrufen und nach Informationen fragen. Die Nummer des Kundensupports eines Serviceanbieters findet man meistens sehr schnell über Google.

Denken Sie daran, dass seriöse Firmen wie Bank- und Versicherungsinstitute ihre Kunden niemals auffordern würden, auf eine wichtige Mitteilung per Link in einer E-Mail zu reagieren. Im Normalfall werden Sie als Kunde immer auch telefonisch informiert.

Falls Sie doch eine (angebliche) E-Mail von Ihrer Bank oder Ihrer Versicherung mit der Aufforderung, sich über einen vorgegebenen Link anzumelden, erhalten, könnte dies tatsächlich eine Phishing-Mail sein. Falls Sie unsicher sind, können Sie Ihren Browser starten und sich direkt im Anmelde-Portal der Bank oder der Versicherung anmelden. Falls das Finanzinstitut eine Reaktion von Ihnen erwartet, werden Sie es dort erkennen können. Als weitere Alternative können Sie sich auch bei Ihrer Bank oder Versicherung telefonisch erkundigen.

Phishing-SMS

Phishing-Angriffe können auch via SMS auf das Mobiltelefon versendet werden. Prüfen Sie SMS-Nachrichten mit enthaltenen Links, damit Sie Phishing-Versuche leichter erkennen können:

- → Name und Nummer des Absenders (Kontakt-Details) prüfen
- → Rechtschreibung prüfen
- → Links anschauen (z. B. Firmenname des Absenders korrekt geschrieben?)
- → Im Zweifelsfall das Kundencenter des Absenders telefonisch oder per E-Mail kontaktieren.

Schutz vor Ransomware
und Reaktion bei einem Vorfall

Ransomware kann über verschiedene Wege auf Ihr System gelangen und Ihnen durch die Verschlüsselung Ihrer Daten Schaden zufügen. Denken Sie an folgende Massnahmen, um diese Art der Erpressung zu vermeiden:

- Vorsicht bei E-Mails, insbesondere beim Öffnen von Anhängen. Ransomware wird hauptsächlich per E-Mail verteilt und verbreitet sich durch das Anklicken von Links und Herunterladen von Anhängen auf Ihrem System. Lassen Sie Anhänge von unbekannten Absendern unbedingt von Ihrem Virenschutz überprüfen.

- Vorsicht bei Speichermedien wie USB-Sticks und portablen Festplatten. Vor allem, wenn Sie den vorherigen Benutzer des Speichermediums nicht kennen und sich nicht eindeutig sicher sind, was sich auf dem Medium befindet, sollten Sie dieses nicht mit Ihrem System verbinden.

- Halten Sie Ihre Systeme immer aktuell. Neue Betriebssoftwareversionen bringen oft Verbesserungen bezüglich der Informationssicherheit mit sich. Auch Aktualisierungen von Ihrem Antivirus-Programm enthalten Verbesserungen in der Virenerkennung und -bekämpfung und sollten immer durchgeführt werden.
  Verwenden Sie ausserdem eine Backup-Lösung und erstellen Sie regelmässig Sicherheitskopien Ihrer Daten.

Was tun bei einem Vorfall?

- Zahlen Sie den verlangten Betrag nicht! Oft wird anschliessend nur noch mehr verlangt, ohne Ihre Daten zu entschlüsseln.

- Ziehen Sie einen Spezialisten bei und versuchen Sie, ein Backup Ihres Systems von vor dem Vorfall wiederherzustellen.

Weitere wichtige präventive Richtlinien

Verantwortlichkeiten zuteilen
Informationssicherheit ist die Aufgabe und Herausforderung eines jeden Mitarbeitenden. Dennoch sollten Sie eine für die Informationssicherheit Ihrer Firma verantwortliche Person sowie eine Stellvertretung bestimmen. Die verantwortliche Person soll sich der Sicherheitsaufgaben annehmen und Sie und Ihre Mitarbeitenden regelmässig über den Stand der Informationssicherheit in Ihrem Unternehmen informieren. Auch soll Sie als Anlaufstelle für Fragen, bei Unsicherheiten und bei Vorfällen wirken.

Daten sichern – Backups erstellen
Nicht nur im Falle eines Cyber-Angriffs können sensible Daten wie Kundeninformationen oder Transaktionen verloren gehen. Auch andere, äussere Einflüsse wie Feuer oder Wasserschäden können zu Datenverlust führen. Erstellen Sie deshalb regelmässig Sicherheitskopien – sogenannte **«Backups»** – von Ihren Daten. Auch dafür werden bessere und schlechtere, teurere und günstigere Programme angeboten. Wichtig ist, dass Sie auch regelmässig testen, ob sich die gesicherten Daten wiederherstellen lassen und dass die Backups an einem anderen Ort als der originale Datenträger aufbewahrt werden. Weiter empfehlen wir den Einsatz einer Firewall, die Sie gegen Angriffe von aussen schützt, sowie eines Virenschutzes, der Ihr System und die darauf liegenden Dateien regelmässig auf Schädlinge prüft.

Die meisten Antivirus-, Firewall- und Backup-Programme bieten eine Testversion an oder sind von Grund auf kostenlos erhältlich. Nehmen Sie sich daher Zeit, einige Programme auszutesten und entscheiden Sie sich für eine Lösung, die preislich und leistungsmässig zu Ihrem Unternehmen passt. Backup-Lösungen in einer Cloud sind mittlerweile ebenfalls gängig. Seien Sie sich allerdings bewusst, dass für Ihre Daten das Datenschutzgesetz von dem Land gilt, in welchem der Server der Cloud steht. Zusätzlich sollten sie trotzdem weiterhin auch physische Backups von Ihren Daten machen.

Betriebssystem und Programme aktuell halten
Installieren Sie zeitnah die regelmässigen Service- und Sicherheitsupdates für Ihr Betriebssystem und Ihre Programme. Mit diesen «Patches» werden bekannte Fehler und Lücken geschlossen und somit die Sicherheit bei allen Funktionen erhöht. Sämtliche Betriebssysteme und Programme für Computer oder Smartphones sind nicht fehlerfrei. Die Autoren von Schadsoftware nutzen sehr oft diese Lücken, um in den Computer oder das Smartphone einzudringen.

Gesunder Menschenverstand
Lassen Sie beim Surfen und bei sensitiven Internetgeschäften immer den gesunden Menschenverstand walten. Weitere präventive Guidelines, Informationen über Cyber Security und interessante Live-Hacks können Sie bei Infoveranstaltungen und Vorträgen der Baloise Digitale Pfadfinder erhalten.

Hacken ist strafbar
Jegliche Art von Cyber-Angriffen ist per Gesetz verboten.

Staatliche Unterstützung
Der Bundesrat hat am 18. April 2018 die neu erarbeitete Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018–2022 verabschiedet. Die Strategie baut auf der ersten NCS (2012–2017) auf und zeigt Massnahmen der Minderung von Cyber-Risiken auf, welche der heutigen Bedrohungslage entsprechen.
Weitere Infos zu der NCS finden Sie unter **www.isb.admin.ch**.

Ausserdem bietet der Staat seit 2010 die Melde- und Analysestelle Informationssicherung (MELANI) auf **www.melani.admin.ch** an. Dort erhalten Sie Informationen über aktuelle Gefahren und Massnahmen, wie auch ein Meldeformular bei Vorfällen für Privatpersonen sowie KMUs.

Have I Been pwned?
Der Webservice «Have I Been pwned» (HIBP) sammelt und analysiert sogenannte «Data Dumps», welche von Hackern nach Data Breaches (engl. Datenleck) ins Internet gestellt werden. HIBP bietet dem User die Möglichkeit, in diesen Unmengen an offen liegenden und dadurch gefährdeten Userdaten durch die Eingabe einer E-Mail-Adresse oder eines Usernamen nach ihren eigenen zu suchen. Zusätzlich kann man auch einen Service einrichten, welcher per Mail informiert, sollten eigene Userdaten in einem Data Breach offengelegt werden. Auch kann man nach bereits veröffentlichten Passwörtern suchen. Deshalb ist es wichtig, mehrere Passwörter zu verwenden, da Passwörter, welche in einem Data Breach offengelegt wurden, im Internet verkauft werden und daher nicht mehr verwendet werden sollten.
https://haveibeenpwned.com

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

www.baloise.com

000.1038 d 1.20 200