teleinformatik
IT & Communications Solutions since 1999

INTERNET SICHERHEIT

In Zeiten elektronischer Geschäftsprozesse und weltweiter Vernetzung ist die effiziente und effektive Nutzung moderner Informationstechnologie ein wichtiger Erfolgsfaktor eines Unternehmens. IT kann jedoch nur dann zum Erfolg beitragen, wenn sie verlässlich arbeitet und vor allem „sicher" ist.

Datenverluste und Sicherheitslücken in Technik oder Anwendungen, sowie Ausfälle und Nichtverfügbarkeit von Daten können erhebliche Folgen für die Geschäftstätigkeit, die Reputation und in Extremfällen sogar für das Überleben des Unternehmens haben.

FAKTEN

Neue Technologien verbreiten sich immer rasanter, die Digitalisierung schreitet immer schneller voran und beeinflusst markant die Unternehmensabläufe. Als vor nicht allzu langer Zeit Computer 14 lange Jahre gebraucht haben, um 50 Millionen Benutzer zu erreichen, hat es Facebook innert 3 Jahren, das Spiel Pokémon Go sogar innert 19 Tagen [1] erreicht.

Mit der Komplexität der IT und der zunehmenden Vernetzung der Geräte (im Jahr 2018 gab es bereits schätzungsweise 21 Milliarden vernetzte Geräte weltweit und im Jahr 2022 sollen es 50 Milliarden sein [2]) steigt auch die Gefahr, dass Firmen und Benutzer Opfer von Cyber-Angriffen werden. Gemäss einer Studie der gfs-Zürich [3] wurden schon 36% der Schweizer KMU von Malware wie Viren oder Trojanern befallen und sogar 4% Opfer von Erpressungen über das Netzwerk. Die Bundespolizei meldet, dass sich die Anzahl der Meldungen über Cyber-Attacken in der Schweiz in den letzten 5 Jahren verdreifacht haben.

KMU sind nicht zuletzt aufgrund mangelndem Know-how bezüglich Cyber Security ein beliebtes Ziel für Online-Kriminelle, Wirtschaftsspione und Produktpiraten, die sich die weitgehend elektronische Verarbeitung von Informationen und das Wissen über Geschäftsprozesse zunutze machen wollen. Ein hohes Niveau an IT-Sicherheit ist daher ein erheblicher Erfolgsfaktor.

Trotz steigendem Risiko ist die Sensibilisierung gegenüber Cyber-Attacken immer noch gering und adäquate Massnahmen werden nicht ausreichend umgesetzt. Die Teleinformatik Services AG ist Ihr Fachpartner in allen IT-Angelegenheiten und bietet ein breites Produktportfolio für den Schutz Ihres Unternehmens an, welches laufend erweitert und optimieret wird.

HABEN WIR IHR INTERESSE GEWECKT?

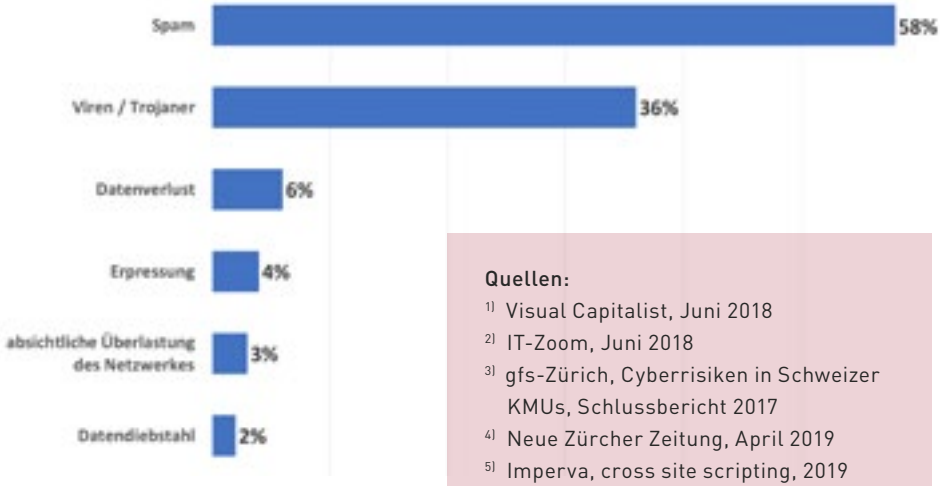
Telefon +41 44 315 15 15

WAS SIND CYBER-ANGRIFFE

Ein Cyber-Angriff ist eine gezielte Attacke von aussen auf eine IT-Infrastruktur, wobei eine Schwachstelle in der Infrastruktur des Angegriffenen ausgenutzt oder mittels Social Engineering der Mensch vor dem Computer missbraucht wird, um sich Zugang zu der Infrastruktur zu verschaffen.

Die Angriffe werden durch organisierte Kriminelle, Staaten, Unternehmensspione oder Hacker durchgeführt. Sie bezwecken hauptsächlich Gelderpressung oder -betrug, den Diebstahl von Unternehmensdaten oder das Anrichten von Schäden durch Sabotage. In letzter Zeit wurden die sogenannten Erpressertrojaner oft medialisiert. Dabei verschlüsselt der Trojaner die Daten auf dem Computer, wonach der Angreifer ein Lösegeld verlangt, da ansonsten die Daten nicht entschlüsselt werden. Weiter werden mittlerweile schätzungsweise bei 40% aller Unternehmen Ressourcen gestohlen, wobei viele dieser Fälle unbemerkt bleiben [4].

Gemäss einer Umfrage der gfs-Zürich bei Schweizer KMU [3] waren diese bereits wie folgt betroffen:

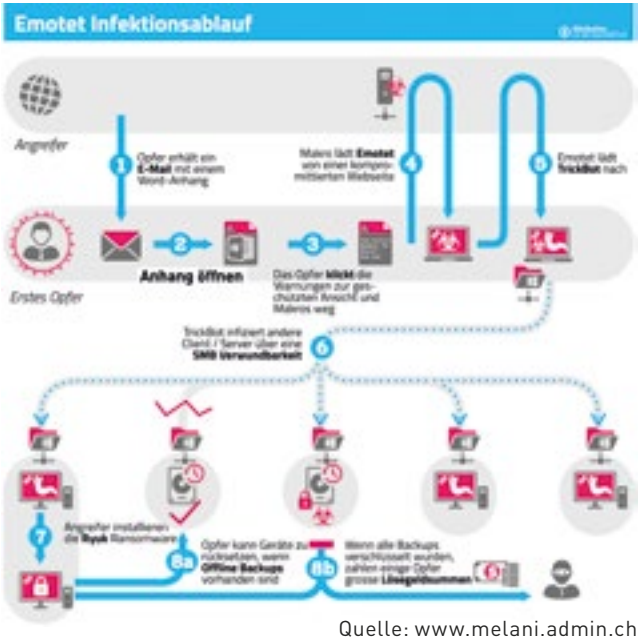


Quellen:

1) Visual Capitalist, Juni 2018
2) IT-Zoom, Juni 2018
3) gfs-Zürich, Cyberrisiken in Schweizer KMUs, Schlussbericht 2017
4) Neue Zürcher Zeitung, April 2019
5) Imperva, cross site scripting, 2019
6) Identity and access management, Hochschule für Technik Rapperswil, 2015

WIE GESCHIEHT EIN CYBER-ANGRIFF?

Der Angreifer braucht eine Eintrittstür und sucht dafür eine Schwachstelle im System. Gemäss dem «Internet Security Threat» Bericht 2019 von Symantec werden die meisten Attacken über E-Mails gestartet.



Quelle: www.melani.admin.ch

Nach wie vor stellt der Computer-Benutzer die grösste Schwachstelle in einem IT-System dar. Auch wenn die moderne Antivirus Software dank der Nutzung von künstlicher Intelligenz Erkennungsmodelle aufgrund bekannten Schadmustern dynamisch lernen, werden sie niemals entscheiden können, ob ein beliebiges Programm Schaden anrichtet oder nicht. Somit liegt die Entscheidung, ob ein Anhang oder der Link in einer Nachricht harmlos ist oder nicht, meistens beim Empfänger.

WEB-ATTACKEN

Selbst eine moderne Antivirus Software ist nicht in der Lage, gängige Web Attacken abzuwehren. Im Gegensatz zu herkömmlicher Malware ist bei Web Attacken nicht der Computer, sondern der Server von Sicherheitslücken betroffen. So kann ein Angreifer auf einer Webseite (z.B. über ein normales Eingabefeld) Schadcode einfügen, welcher beim Aufruf durch einen anderen Computer ungefragt ausgeführt wird.

HABEN WIR IHR INTERESSE GEWECKT?

Telefon +41 44 315 15 15

Über eine infizierte Webseite können Passwörter von E-Mail-Accounts geändert werden, während im Hintergrund der Benutzer z. B. noch im Web-Mail eingeloggt ist. Als Benutzer hat man keine Chance, sich dagegen zu wehren. Daher empfiehlt es sich, sich stets aus dem Web-Mail auszuloggen, bevor weitere Internet-Seiten besucht werden.

Angreifer suchen Sicherheitslücken in Webseiten wie Blogs, sozialen Netzwerken oder Videotauschbörsen und fügen bösartigen Code in die ungeschützte Web Applikation ein. Jedes Mal, wenn die Webseite angeschaut wird, wird das bösartige Skript im Browser des Opfers ausgeführt. Somit kann der Angreifer z.B. Cookies von der Besuchersession stehlen. Dank diesen kann der Angreifer auf das Konto vom Benutzer zugreifen und Zugang zu seinen persönlichen Informationen wie auch z. B. Kreditkarten-Daten erlangen [5].

SOCIAL ENGINEERING

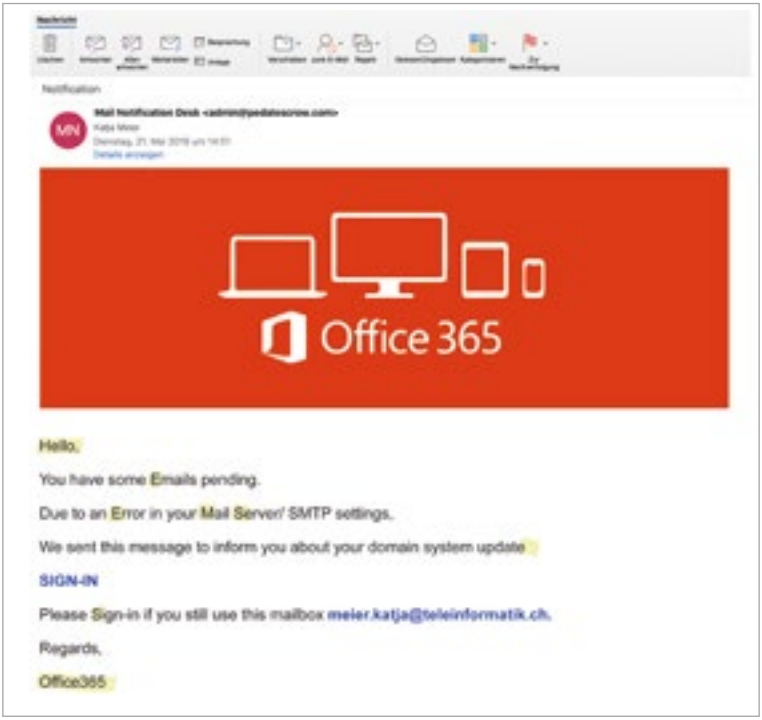
Dank einem adäquaten Schutz der IT-Infrastruktur können die Risiken minimiert, jedoch leider nie gänzlich eliminiert werden. Zudem ist der Mensch der erfolgversprechendste Angriffsvektor von Cyber-Attacken und deshalb beginnen die meisten Angriffe mit dem sogenannten «Social Engineering». Solche Angriffe sind zum Beispiel:

1. **Phishing:** Über E-Mails oder gefälschte Webseiten gelangen Angreifer an persönliche Daten eines Internet-Benutzers, Identitätsdiebstahl
2. **Hacking:** Illegales Eingreifen in computer- bzw. personenbezogene Systeme
3. **Malware:** Getarnte Schadfunktionen (z. B. Trojaner)
4. **Cyberbetrug:** Produktfälschungen, Vorschussleistungen, «Love Spam»
5. **DDoS** (Distributed Denial of Service): Konzentrierte Angriffe auf Server und Netzwerke. Durch die Überlastung an Anfragen wird das Netzwerk blockiert

Der Mitarbeiter wird u.a. durch Geldversprechen, Angstverbreiten (z.B. Drohung mit Strafe) oder Dringlichkeit manipuliert, sodass sich der Angreifer Zugang zum System verschaffen kann. Über E-Mails werden Anhänge (z.B. PDF oder Office-Dateien) sowie Links zu gefährlichen Webseiten verschickt (Phishing). Die Gefahr hinter Links und PDF-Anhängen (auch mit Formular-Funktionen) ist für Virenscanner und für den Menschen mit geringen Informatikkenntnissen schwieriger zu entdecken. Viele PDF-Reader-Applikationen, auch solche, die in Webbrowser integriert sind, haben Sicherheitslücken.

TÄUSCHEND ECHT

Die E-Mails sehen oft echt aus und sind mit denjenigen von bekannten Firmen wie zum Beispiel Banken oder Telefonanbietern leicht zu verwechseln. Mitarbeiter von kleinen Firmen sind meist häufiger betroffen als von grossen Unternehmen. Im Jahr 2018 hat die Melde- und Analysestelle Informationssicherung MELANI vom Bund 5'756 Phishing-Seiten bestätigt.



Hinweis:

Bei Spam Mails niemals auf den Link «unsubscribe» oder «vom Newsletter abmelden» klicken, sofern der Link eine undefinierbare URL enthält.

Beispiel 1, Office 365

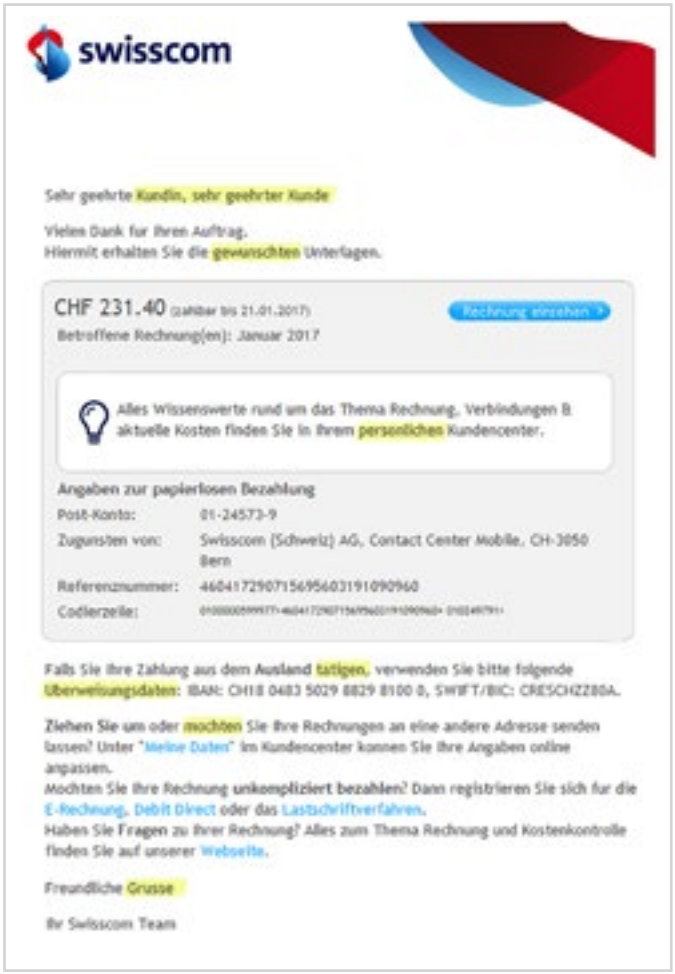
PHISHING

Im Beispiel 1 kann man eine Phishing-Nachricht aufgrund folgender Faktoren einfach erkennen oder vermuten:

1. Der Empfänger wird mit «Hello» und nicht namentlich angeschrieben
2. Das Layout ist eher einfach anstatt professionell
3. Die Sprache ist nicht einwandfrei
4. Die Nachricht wird mit «Office365» unterschrieben

Beim Beispiel 2 ist die bösartige Absicht schwieriger zu erkennen. Die **unpersönliche Anrede sowie die fehlenden Umlaute im Text** deuten auf eine Phishing E-Mail hin. Genaueres erkennt man, wenn mit der Maus über die Schaltfläche gefahren wird (nicht drauf klicken!) und die Zieladresse des Links ersichtlich wird, welche nicht zum Absender passt.

Cyber-Betrüger nehmen auch persönlich Kontakt mit ihrem Opfer auf, wie das Beispiel der Microsoft-Anrufe kürzlich gezeigt hat. Der Betrüger ruft Privatpersonen oder Unternehmen an und gibt sich als Mitarbeiter der Microsoft aus. Er behauptet, dass er auf dem Computer der angerufenen Person schwerwiegende Sicherheitsprobleme festgestellt hat, welche unbedingt und dringend behoben werden müssen. Folglich verschafft er sich einen Fernzugriff zum Computer, spioniert alle Daten aus und versucht dem Opfer eine Softwarelizenz oder weitere «Supportdienstleistungen» zu verkaufen.



swisscom

Sehr geehrte Kundin, sehr geehrter Kunde

Vielen Dank für Ihren Auftrag.
Hiermit erhalten Sie die gewünschten Unterlagen.

CHF 231.40 (zahlbar bis 21.01.2017) Rechnung einsehen >
Betroffene Rechnung(en): Januar 2017

Alles Wissenswerte rund um das Thema Rechnung. Verbindungen & aktuelle Kosten finden Sie in Ihrem persönlichen Kundencenter.

Angaben zur papierlosen Bezahlung

Post-Konto:	01-24573-9
Zugunsten von:	Swisscom (Schweiz) AG, Contact Center Mobile, CH-3050 Bern
Referenznummer:	460417290715695603191092960
Codierzeile:	

Falls Sie Ihre Zahlung aus dem Ausland tätigen, verwenden Sie bitte folgende Überweisungsdaten: IBAN: CH18 0483 5029 8829 8100 0, SWIFT/BIC: CRESCHZZ80A.

Ziehen Sie um oder möchten Sie Ihre Rechnungen an eine andere Adresse senden lassen? Unter "Meine Daten" im Kundencenter können Sie Ihre Angaben online anpassen.
Möchten Sie Ihre Rechnung unkompliziert bezahlen? Dann registrieren Sie sich für die E-Rechnung, Debit Direct oder das Lastschriftverfahren.
Haben Sie Fragen zu Ihrer Rechnung? Alles zum Thema Rechnung und Kostenkontrolle finden Sie auf unserer Webseite.

Freundliche Grüsse

Ihr Swisscom Team

Beispiel 2, Swisscom

Tipp:
Hier kann man seine Fähigkeiten testen, Phishing-Nachrichten zu erkennen: www.teleinformatik.ch/security-info

WIE SCHÜTZT MAN SICH GEGEN ATTACKEN

Ein möglichst guter Schutz gegen Cyber-Attacken ist mehrschichtig: Prozess – Technologie – Mensch.

PROZESS

Unternehmensintern sollen Richtlinien für den Umgang mit dem Internet und der IT im Allgemeinen definiert und gelebt werden, wobei die Verantwortlichkeiten auf strategischer und operativer Ebene klar sein müssen. Die Geschäftsleitung definiert die zu schützenden Daten und Infrastrukturen, den Zugriff und die Berechtigungen auf die Systeme. Bei Bedarf beauftragt die Geschäftsleitung anhand einer Risikobewertung die IT-Abteilung mit der Definition und Umsetzung der Schutz- und Datenaufbewahrungsmassnahmen. Diese müssen in regelmässigen Abschnitten, mindestens 1 Mal im Jahr, auf ihre Aktualität und deren Umfang überprüft werden.

TECHNOLOGIE

Bei der technischen Umsetzung sind Firewalls und eine moderne Antivirus-Lösung für Computer und Server unabdingbar. Es muss zudem sichergestellt werden, dass die Sicherheitsupdates der Clientgeräte und Server immer auf dem aktuellsten Stand sind. Die Daten müssen neben der produktiven Anlage auch auf einem anderen System gesichert werden (Backup). Für die Unternehmenskerndaten empfiehlt es sich, ein zweites Backup an einem externen Standort einzurichten (offsite Backup). Die Wiederherstellung der gesicherten Umgebung sollte mindestens 1 Mal pro Jahr geprüft werden (Restore). Es wird noch allzu oft davon ausgegangen, dass die Sicherung der Daten an sich genügt, aber nicht selten können die Backups aus unterschiedlichen Gründen nicht mehr zurückgespielt werden und somit gehen viele Daten dennoch verloren.

MENSCH

Die technischen Schutzmassnahmen sind eine Grundvoraussetzung für eine gut geschützte Infrastruktur. Sie nützen jedoch wenig, wenn die Mitarbeiter im sicheren Umgang mit ihren IT-Systemen nicht geschult sind. Neben der vorsichtigen Vorgehensweise mit E-Mails ist die Wahl von möglichst sicheren Passwörtern eine massgebende Voraussetzung.

PASSWÖRTER

Aus heutiger Sicht wäre ein sicheres Passwort eine zufällige Zeichenverkettung von etwa 22 Stellen. Ein Passwort mit einer Kombination von 8 Zeichen aus Klein- und Grossbuchstaben und Zahlen kann in lediglich 2 Minuten geknackt werden [6]. Ein vertretbarer Kompromiss ist eine Kombination mit mindestens 10 Zeichen aus Klein-/Grossbuchstaben, Zahlen und Sonderzeichen. Um ein solches Passwort zu knacken würde es fast ein Jahr (347 Tage) dauern; der zeitliche und finanzielle Aufwand für den Angreifer wäre somit beachtlich.

Das Passwort sollte:

- Mindestens alle 6 Monate gewechselt werden
- Kein Wort einer bekannten Sprache enthalten
- Keine Tastaturfolge wie z. B. 1234 oder qwert beinhalten
- Nicht überall wie auch nicht mit anderen Personen gemeinsam genutzt werden (z. B. Web-Accounts im Unternehmen)
- Nie unverschlüsselt gespeichert werden oder in Word Files aufgeschrieben werden
- Auf keinem Fall auf einem Post-It auf dem Monitor oder unter der Tastatur kleben

Tipp: Einen Satz nehmen, den man sich gut merken kann und die ersten Zeichen für das Passwort nutzen:

Ich esse jeden Tag um 1:15 Uhr! >> IejTu1:15U!

Mit Hilfe von Passwort-Manager-Lösungen können lange und komplexe Passwörter definiert werden, die zentral verschlüsselt verwaltet werden.

Eine 2 Faktor-Authentifizierung erhöht die Zugriffssicherheit, wobei z. B. das Login mittels eines Passwortes mit einem Zusatzcode bestätigt werden muss, welches von einer App auf dem Smartphone generiert oder per SMS gesendet wird. Biometrische Zugangsmethoden wie zum Beispiel Fingerabdruck- oder Gesichtserkennung bieten ein hohes Sicherheitsniveau.

CLOUD UND WEB-APPLIKATIONEN

Aus technischer Sicht beeinflusst der Standort der Systeme und Daten die Sicherheit nicht. Bei Cloud-Diensten verändern sich hauptsächlich Verantwortlichkeiten der IT Security, denn je nach Cloud Servicemodell behält der Kunde eine gewisse Verantwortung über die Sicherheit. Daher empfiehlt es sich, dies genauer abzuklären. Bedeutender ist jedoch, dass die meisten Applikationen heute im Browser ausgeführt werden und somit fast immer via Internet zugänglich sind. Als Kunde oder Benutzer einer Webapplikation ist man also darauf angewiesen, dass diese Applikation «sicher» programmiert wurde, was in sehr vielen Fällen nicht immer der Fall ist.

Sogenannte **Web Application Firewalls** (WAF) oder Reverse Proxys schützen Webserver vor Angriffen, indem sie vorgängig Attacken-Anfragen an den Server analysieren. Somit kann man in Bezug auf Sicherheit ungenügend sicher programmierte Software schützen, wobei dies jedoch nur für die eigenen Business Applikationen und nicht für öffentliche Web Applikationen wie z.B. Facebook oder Twitter gilt. Als Benutzer sollte man sich vor dem Verlassen einer Web Applikation immer abmelden und wenn möglich nicht gleichzeitig in einer Web-App angemeldet sein und weitersurfen.

UNSER ANGEBOT

teleinformatik
IT & Communications Solutions since 1999

Für die gesamte Sicherheitskette

CONSULTING

Von der Definition der Massnahmen bis zu regelmässigen Sicherheits-checks, Definition des Sicherheits-levels in Ihrem Unternehmen und interner IT-Richtlinien

PROTECTION

Aktueller Schutz dank Managed Services (Firewall und Endpoint Security), tägliche Datensicherung dank Onsite und Offsite Backup-Lösungen, Backup-Wiederherstellungstests im Labor, Aktualisierung der Sicherheitsupdates auf Computer und Server dank Maintenance Checks, Verschlüsselungs-Software für sicheren Versand vertraulicher E-Mails

Tipp:
Aktuelle Infos finden Sie unter
teleinformatik.ch/security-info

AUDIT

Sicherheitsaudits zeigen den Gap zwischen aktuellem und Ziel-Zustand Ihrer IT-Infrastruktur

2-FAKTOR-AUTHENTIFIZIERUNG

Zusätzliche Authentifizierung bei Zugriff auf Ihre Daten mit 2 Bestätigungsvarianten der Identität

MITARBEITER/PASSWÖRTER

Mitarbeiterschulung im Umgang mit Internet/IT-Infrastruktur, einfache Anwendung komplexer Passwörter dank Passwort-Manager-Lösung

Ihr Ansprechpartner:

Pascal Péquignot +41 44 315 15 15

www.teleinformatik.ch
TELEINFORMATIK SERVICES AG
SCHULSTRASSE 37, 8050 ZÜRICH

DO'S

Login:
- Wählen Sie komplexe Passwörter
- Aktivieren Sie die 2-Faktor Authentifizierung

E-Mails:
- Aktivieren Sie den Spamfilter
- Achten Sie auf verdächtige E-Mails (Phishing)
- Verschlüsseln Sie sensible E-Mails

Updates:
- Führen Sie alle Sicherheitsupdates von Software, Betriebssystemen & Firmware durch

Backup:
- Automatisieren Sie Backups Onsite und Offsite
- Überprüfen Sie laufend den Daten-Restore

Schutz:
- Installieren Sie eine Firewall
- Installieren Sie Antivirus, Client Management (Endpoint Security)

DONT'S

NO POST-IT

Passwörter niemals auf einem Post-It aufschreiben und beim Arbeitsplatz aufkleben

NO EASY PASSWORD

Niemals einfache Passwörter wählen, keine Tastaturfolge wie z. B. 1234

NO FORWARD

Niemals Passwörter weitergeben, auch nicht dem IT-Verantwortlichen oder gemeinsam im Team nutzen

DO NOT OPEN IF UNSURE

Anhänge und Links nicht öffnen, bevor die Quelle sicher identifiziert wurde, im Zweifelsfall seinen IT-Verantwortlichen fragen

Diese Seite können Sie heraustrennen und als praktischen Ratgeber aufhängen oder aufbewahren.