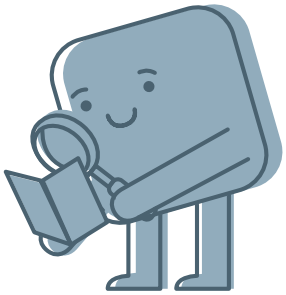
Informations-sicherheit



Informationssicherheit betrifft uns alle! Und überall!

Unter dem Begriff Informationssicherheit verstehen wir alle Maßnahmen, zum Schutz von Informationen und Daten, zu Abwehr von Gefahren und Bedrohungen, um wirtschaftlichen und persönlichen Schaden zu vermeiden.

Informationssicherheit umfasst 3 Säulen:

Menschen – Unser achtsamer Umgang mit Informationen und Daten.

Prozesse – Das Einhalten von Prozessen, die unsere Organisation vorgibt. Sie dienen der sicheren Handhabung von sich wiederholenden Vorgängen.

Technik – In der Organisation wird uns die Technik bereitgestellt und serviciert. Technik gewährleistet den sicheren Austausch und das Speichern von Daten und Informationen.

Informationssicherheit verfolgt die Ziele Vertraulichkeit, Integrität und Verfügbarkeit.

Nur wenn diese drei Ziele nachhaltig verfolgt werden, sind Informationen gut geschützt.

Vertraulichkeit: Nur die Personen, die auch berechtigt sind, Daten zu sehen/zu erhalten, haben auch Zugriff darauf. Diese Vertraulichkeit liegt zum Beispiel vor, wenn andere Personen Zugriff auf deine E-Mails, Benutzerkonten oder Bankdaten haben.

Integrität: Informationen liegen richtig und vollständig vor. Die Integrität ist verletzt, wenn zum Beispiel unbefugte Personen Daten manipulieren.

Verfügbarkeit: Bedeutet, dass wir Services und Dienstleistungen uneingeschränkt zur Verfügung haben. Im Falle eines Cyberangriffs, kann es zum Beispiel zu Serverausfällen kommen, wodurch wir keinen Zugriff mehr auf Daten und Informationen haben.

Was tun, bei verdächtigen Situationen?

Vertraue auf dein digitales Bauchgefühl! Wenn du bereits das Gefühl hast, dass die Situation verdächtig ist, ist das schon ein guter erster Schritt!

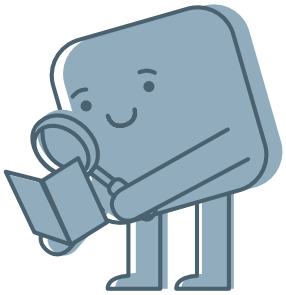
- Prüfe ob es sich um einen Angriff handelt bei Phishing E-Mails und SMS. Versuche Anrufer immer zu identifizieren!
- Bewahre Ruhe und lass dich nicht unter Druck setzen!
- Melde Vorgänge umgehend an die zuständige Stelle in deiner Organisation. Verdächtige Vorgänge in deinem privaten Umfeld, melde an die Polizei, allen voran Versuche von Erpressung und Manipulation.

Gemeinsam sind wir sicherer! Teile dein Wissen, mit Freunden und Familie, damit wir gemeinsam sicherer sind!

Verdächtige Vorfälle melde umgehend in deiner Organisation oder im privaten Umfeld an die Polizei!

DACHVERBAND
WIENER SOZIALEINRICHTUNGEN

Informations-sicherheit



Wichtige Begriffe der Informationssicherheit:

- Account: ist das Benutzerkonto auf einem Online-Service. Der Account ist mit Login-Daten geschützt.
- Browser: ist das Programm, mit dem du im Internet bist. Chrome, Firefox, Microsoft Edge und Safari fallen darunter.
- Cloud: ist ein virtueller Datenspeicher.
- Link: ist der Verweis, der durch Anklicken eine Internet-Adresse aufruft.
- Login bzw. Logindaten bezeichnet die Informationen, die du eingeben musst, um deinen Account "aufzusperren".Im Regelfall bestehen diese Daten aus deiner E-Mail-Adresse oder einem Benutzernamen sowie einem Passwort. Das Passwort solltest du unbedingt geheim halten!
- Phishing: Setzt sich aus Passwort und Fischen zusammen. Phishing ist der Betrug, um Benutzerdaten auszuspionieren.
- Spam kennzeichnet die unerwünschte Werbung und E-Mails mit verdächtigen Inhalten und Dateianhängen.
- Update: Updates sind Aktualisierungen. Hersteller von Software (Programmen, Apps) und Hardware (Speicher) bieten laufend Aktualisierungen. Diese sind wichtig, damit die Sicherheit gewährleistet wird.
- URL: „Uniform Resource Locator“. Sie setzt sich zusammen aus dem Protokoll (https://), der Domain (z.B. dachverband) und der Kennung, die meistens eine Abkürzung für Länder (zum Beispiel .at) oder für Organisationen (zum Beispiel .org). Übrigens .com steht für commercial (kommerziell). URLs sind einmalig weltweit.
- WLAN (Wireless Local Area Network) ermöglicht das Surfen im Internet ohne eine Kabelverbindung. Internet mit Kabelverbindung wird LAN genannt.

Verdächtige Vorfälle melde umgehend in deiner Organisation oder im privaten Umfeld an die Polizei!