Version 1.0

Einführung in die IT-Sicherheit

Mitarbeiterschulung

HISOLUTIONS

DATAKONTEXT

AGENDA

- Einführung
- Informationssicherheit – IT-Sicherheit – Datenschutz
- Vertraulichkeit, Integrität und Verfügbarkeit
- Security – Wie geht das?
- Relevante Bedrohungen
- Typische Angriffe
- Wichtige Maßnahmen
- Umgang mit IT-Sicherheitsvorfällen
- Quiz

EINFÜHRUNG

Informationssicherheit – Was ist das? Drei Beispiele

BEISPIEL 1: „SCHULTER-SURFEN“

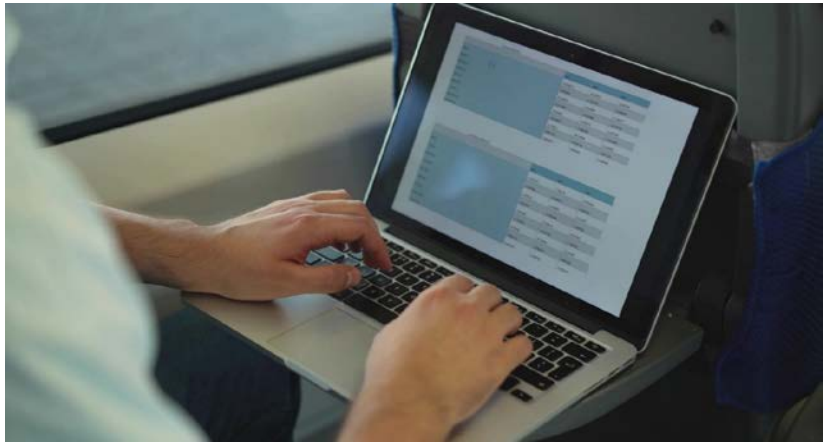
Sie sitzen in der Bahn.

Schnell noch ein Angebot fertig machen.

Zum Glück ist das durch UMTS-Mobilfunk-Karte im Laptop oder WLAN im Zug schnell erledigt: Eingeloggt ins CRM, und fertig.

Die Reise geht weiter.

Zwei Wochen später taucht bei einem Mitbewerber Ihrer Firma Ihre komplette Kundendatenbank auf.

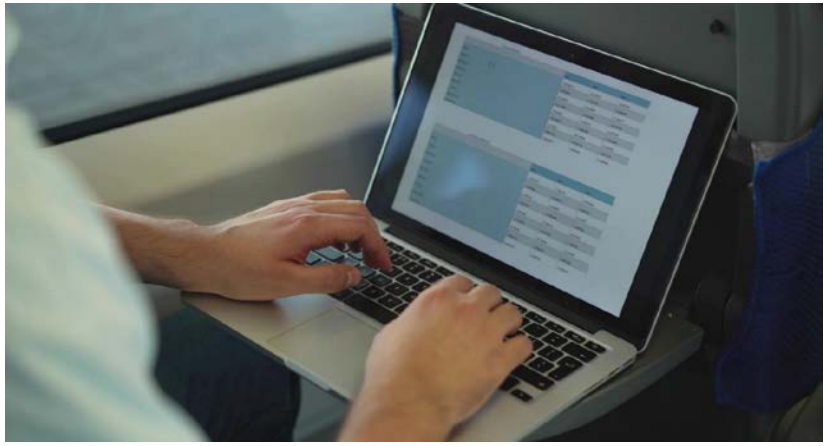


BEISPIEL 1: „SCHULTER-SURFEN“

Was ist passiert?

Klassisches „Schulter-Surfen“:

Jemand hat Sie bei der Eingabe Ihrer Zugangsdaten beobachtet und die Kundendaten danach heruntergeladen.



BEISPIEL 2: „ANRUF VOM CHEF“

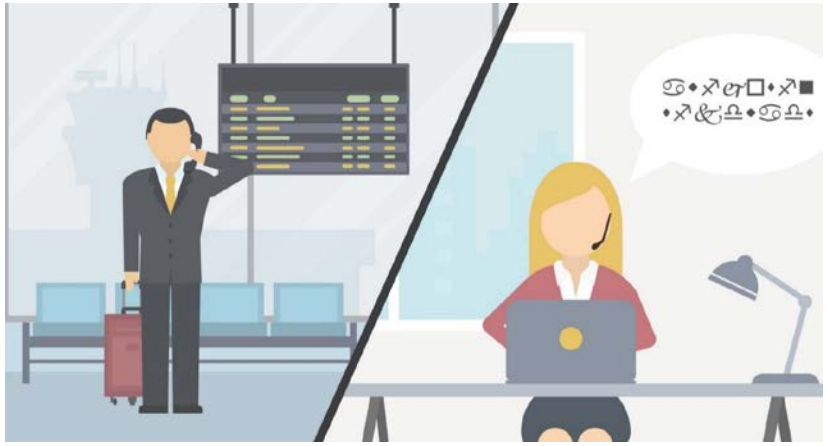
Der Chef ruft an. Vielleicht auch der CFO, auf jeden Fall ist es dringend. Die Verbindung ist schlecht, klar, er ist im Ausland unterwegs.

Und muss dringend sofort eine Überweisung anstoßen, sonst ist der Auftrag verloren.

In Ihnen weckt sich Zweifel. Das ist doch nicht im Rahmen der Prozesse?

Aber der Chef hat ja am Morgen schon eine E-Mail geschrieben, also wird das schon seine Richtigkeit haben?

Mit leichten Bauchschmerzen weisen Sie den Transfer an. Das Geld ist weg.

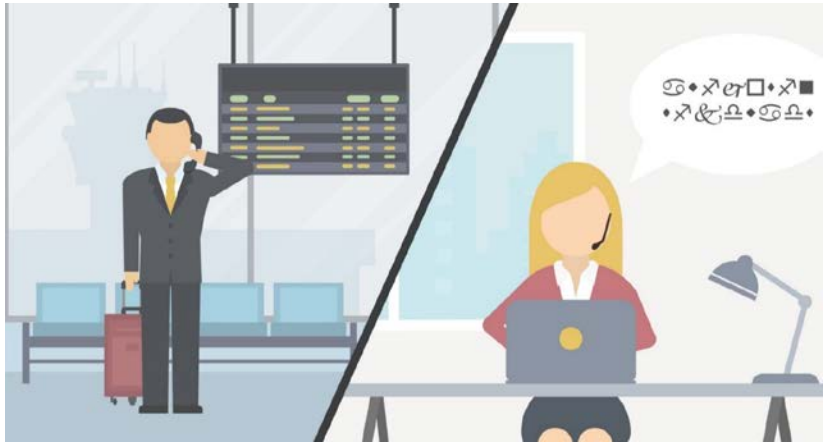


BEISPIEL 2: „ANRUF VOM CHEF“

Was ist passiert?

Sie sind dem sogenannten „CEO Fraud“, auch „Business Email Compromise“ (BEC) genannt, aufgesessen.

E-Mail wie Anruf waren gefälscht, der Chef hatte nichts damit zu tun.



BEISPIEL 3: „DAS BEWERBUNGSSCHREIBEN“

Eine E-Mail trifft ein.

Endlich der erhoffte Bewerber!
Im Anhang sein Lebenslauf.

Das Virenschutzprogramm hat sich nicht beschwert, also schnell doppelgeklickt.

Schade, die Qualifikationen passen nicht ganz. Aber was ist das?

Auf dem Netzlaufwerk nur noch unlesbare Dateien, die Nachbarabteilung kann auch schon nicht mehr arbeiten! Hoffentlich sind die Backups nicht betroffen …

BEISPIEL 3: „DAS BEWERBUNGSSCHREIBEN“

Was ist passiert?

Die E-Mail enthielt sogenannte „Ransomware“, eine bösartige Form von Schadprogramm, die Dateien verschlüsselt und verspricht, diese angeblich gegen ein „Lösegeld“ wieder lesbar zu machen.

DREI GESCHICHTEN, ZWEI GEMEINSAMKEITEN

1. Ob gestohlene Informationen, manipulierte Prozesse oder nicht verfügbare Daten: Am Ende stand immer ein Schaden für das Unternehmen – und dieser hatte mit IT zu tun.
2. Der Schweregrad reicht dabei von kleinen Unbequemlichkeiten bis zu ausgewachsenen Katastrophen, die die Existenz einer Organisation zerstören können.

IT-SICHERHEIT

IT-Sicherheit ist der Versuch, Unternehmen und Behörden, aber auch Privatpersonen vor derartigen Schäden, die mit Informationstechnik und ihrer Nutzung zusammenhängen, zu schützen.

GRUNDBEGRIFFE

Informationssicherheit – IT-Sicherheit – Datenschutz