Inhouse Seminar (Online oder vor Ort bei Ihnen)

IT-Security Awareness I: Cybercrime – auch Sie sind ein potenzielles Opfer!

Bieten Sie den Angreifern Paroli! Wappnen Sie Ihre Mitarbeiter*innen gegen den Cyberwar, der täglich seine Opfer fordert. In diesem Seminar wird das nötige Rüstzeug vermittelt, mit dem Millionenschäden verhindert werden können. Öffentliche Institutionen, Finanzdienstleister und Industriebetriebe sind bevorzugte Angriffsziele. Geld auf direktem Wege oder Wettbewerbsvorteile über Werksspionage sind im Fokus findiger Krimineller.

„Wir haben nichts zu verbergen“, ist ein häufig gehörter Satz. Das Gegenteil ist der Fall. Jedes Unternehmen und erst recht jede Privatperson ist auch Geheimnisträger*in. Je sorgloser wir mit Informationen über uns, unser persönliches und berufliches Umfeld umgehen, umso mehr begünstigen wir den Missbrauch. Da geht es um Geld, das man erpressen kann, um die Befriedigung journalistischer Bedürfnisse, um die Veröffentlichung von internen Informationen oder privaten Details, die den Betroffenen schaden, um Mobbing, Rache, um Sabotage, um Werksspionage, Ideenklau usw. Die Liste von Cybercrime-Delikten ist lang. Wir alle fördern diese Entwicklungen durch Gutgläubigkeit und Fahrlässigkeit. In den allermeisten Fällen brauchen die Täter gar nicht persönlich in Erscheinung zu treten. Die Schäden, die sie verursachen, gehen aber in die Millionen. Virenschutz und Firewall helfen dagegen überhaupt nicht, nur ein höheres Sicherheitsbewusstsein verhindert Schlimmeres. Sicherheitsbewusstsein muss aber trainiert werden.

Zielgruppe: Alle Mitarbeiter*innen, keine Vorkenntnisse erforderlich. (Möglichkeit der Segmentierung mit bereichsspezifischer Schwerpunktsetzung)

Methode: Vortrag mit zahlreichen Praxisbeispielen und Diskussionsmöglichkeit (online oder vor Ort).

Inhalte (Auszug): **Modular flexibel an Ihre Bedürfnisse anpassbar**

- Nichts zu verbergen? Private und staatliche Überwachung vs. digitaler Wissens-Exhibitionismus
- Motive der Angreifer und unsere leichtsinnigen Handlungen, die Cybercrime begünstigen
- Der Zusammenhang zwischen Schwachstellen und Bedrohungen
- Wie können wir Cybercrime wirksam Paroli bieten?
- Was sind wirklich gute Passwörter und wie kann man sich diese ganz leicht merken?
- Social Engineering, ID-Klau und die bitteren Folgen (Datenverlust, Erpressungstrojaner)
- Wie gelangt ein Fremder leicht in Ihr Büro und wie spioniert er Sie dennoch aus, sollte es nicht klappen
- Notebook, Tablet, Smartphones – (zu) einfache Angriffsziele
- Datenschutz und E-Mails haben kaum Gemeinsamkeiten
- Warum 80% aller Menschen auf Spear-Phishing hereinfallen

Nutzen für das Unternehmen: Mitarbeiter*innen erkennen Angriffsmuster, können durch bewussteres Handeln Schaden vom Unternehmen und von sich selbst abwenden und sie werden auf Sicherheitsvorfälle richtig und schneller reagieren.

Nutzen für die Teilnehmer*innen: Deutliche Steigerung der Kompetenzen in Sachen Informationssicherheit.

Vortragender: Mag. Michael Gredler, IT-Security-Berater

Dauer: ca. 2 Std. inkl. einer Pause, keine Beschränkung hinsichtlich der Zahl der Teilnehmer*innen

Technische Voraussetzungen: Beamer & Flipchart bzw. Ihr gewohntes Onlinekonferenztool

Termine: nach Vereinbarung

CSD Unternehmensberatung GesmbH
A-6063 Rum, Kaplanstraße 2
Tel.:+43 / 512 / 585 181 (AB)
Fax:+43 / 512 / 585 181-4
gf@csd-ub.at
Firmenbuch-Nr.: FN 206359w
Landesgericht Innsbruck
UID-Nr. 51453207
www.csd-ub.at