HERBST 2022

SPOTLIGHT

DAS ALLIANZ MAGAZIN

Das Leben kann kommen

Mutig: Wie eine Familie mit dem Velo die Welt umreist.

Mobil: Was Sie über Elektromobilität wissen sollten.

Engagiert: Wie wir uns für die Ukraine einsetzen.

Flexibel: Die neue Vorsorgelösung für alle Lebensphasen.

Schwachstelle Mensch: So funktioniert «Social Engineering»

— Text: Manuel Ott

Das Allianz Risk-Barometer weist Cyberkriminalität seit einigen Jahren als Top-Risiko für Unternehmen aus. Besonders perfide ist das sogenannte «Social Engineering», bei dem Angestellte mit psychologischen Tricks manipuliert werden. Welche Maschen es gibt und wie Sie sich dagegen schützen, lesen Sie hier.

Identitätsbetrug mit teuren Folgen
Beim «Social Engineering» nutzen Cyberkriminelle in der Regel eine falsche Identität, um sich zu bereichern. Zum Beispiel mit folgenden Tricks:

CEO Fraud: Cyberkriminelle geben sich per E-Mail oder am Telefon als Geschäftsführer aus und fordern Mitarbeitende auf, einen Geldbetrag auf ein unbekanntes Konto zu überweisen.

Fake Identity Fraud: Ein vermeintlich bekannter Geschäftspartner möchte Waren auf Rechnung beziehen. Die bestellte Ware wird wie vereinbart geliefert, auf die Zahlung wartet das Unternehmen vergeblich.

Payment Diversion Fraud: Mit einer gefälschten E-Mail wird dem Unternehmen vorgegaukelt, dass die Bezahlung für bezogene Dienstleistungen auf ein anderes Konto als üblich überwiesen werden soll.

So schützen Sie Ihr Unternehmen vor «Social Engineering»
«Social Engineering ist eine sehr erfolgreiche Methode, um die IT-Sicherheitsstandards eines Unternehmens auszuhebeln», sagt Gregor Huber, Leiter Unternehmensversicherungen der Allianz Suisse. «Denn gegen menschliche Schwäche hilft selbst die beste Firewall nichts.» Deshalb ist es besonders wichtig, die Angestellten für die Gefahren zu sensibilisieren. Zudem hilft die richtige Versicherung, um sich gegen die Folgen einer Cyber-Attacke abzusichern. So sind in unserer Cyber-Risk-Versicherung neben Haftpflichtschäden auch Betriebsunterbrüche und Eigenschäden durch Cyberkriminalität versichert. Und mit der Zusatzdeckung «Cyber Crime und Social Engineering» sind auch die oben genannten Betrugsschäden gedeckt.

→ allianz.ch/cyber-risk

4 Tipps gegen «Social Engineering»

1. Schulen Sie Ihre Angestellten regelmässig in Bezug auf Cyber-Risiken.
2. Investieren Sie in eine Cyberversicherung.
3. Verifizieren Sie verdächtige Mails, Anrufe und SMS durch einen Kontrollanruf auf eine bekannte Telefonnummer.
4. Geben Sie keine vertraulichen Informationen an unbekannte Personen weiter.