Frage des Monats September 2022

Cyberrisiko: Ist eine Mitarbeiterschulung sinnvoll?

Die Antwort der Merki-Experten

Mit der rasch voranschreitenden Digitalisierung ist und bleibt für die Mehrheit der Unternehmen die Cybersicherheit eine der grössten Herausforderungen. Nach wie vor wird das Risiko eines IT-Angriffs massiv unterschätzt, obwohl schon viele Schweizer Unternehmen Opfer einer Attacke wurden. Obwohl oftmals bereits viel in ein IT-Sicherheitskonzept investiert wurde, beschränkt sich diese lediglich auf technische Massnahmen wie beispielsweise der Einsatz von Firewalls. Es besteht ein hoher Nachholbedarf bei den organisatorischen Massnahmen wie u.a. regelmässige Mitarbeiterschulungen. Denn der Mensch ist häufig das schwächste Glied im Kampf gegen Cyberangriffe. Der Grossteil aller Sicherheitsvorfälle sind auf menschliche Fehler zurückzuführen. So werden beispielsweise Links angeklickt, die zu Phishing-Seiten führen, oder bösartige Webseiten aufgerufen.
Deshalb ist es so wichtig, dass Mitarbeitende für solche Risiken sensibilisiert werden. Mitarbeitende müssen Gefahren erkennen und angemessen reagieren können. Geschulte Mitarbeiter haben wesentlich bessere Voraussetzungen, Angriffen richtig zu begegnen und Gefahren abzuwenden.
Eine Mitarbeiterschuldung könnte folgende Inhalte umfassen:
a. Gefahr durch Phishing und Ablauf einer Phishing-Attacke
b. Umgang mit mobilen Datenspeichern
c. Risiken und Gefahren bei der Verwendung mobiler Geräte
d. Sicherer und verantwortungsvoller Umgang mit Passwörtern
e. Richtiges Verhalten bei sicherheitsrelevanten Ereignissen
f. Gefahren und Gegenmassnahmen am Arbeitsplatz

Empfehlung für die Praxis
Wir empfehlen, solche Schulungen regelmässig durchzuführen, um das Bewusstsein für Cybersicherheit auch langfristig zu stärken. Denkbar und sinnvoll wäre zudem eine Simulation einer Cyberattacke, bei welcher realistische Angriffsszenarien durchgespielt werden. Damit werden die Mitarbeitenden auf die Probe gestellt und allfällige Lücken aufgedeckt.
Ein KMU kann das Thema selber intern angehen oder dafür externe Anbieter beauftragen, die solche Trainings inklusive Phishing-Simulationen virtuell durchführen.