

Ransomware

Ransomware-Angriffe können nicht nur technische Schwachstellen ausnutzen, sondern auch bei Mitarbeitenden ansetzen. Das E-Learning vermittelt, wie ein solcher Angriff abläuft, welche Rolle Mitarbeitende dabei einnehmen und welche Reaktion im Ernstfall wichtig ist, um eine starke Sicherheitskultur und ein klares Risikobewusstsein im Unternehmen zu fördern.



Quick Facts

-  **Fokus:**
Erkennung von Ransomware und Verhalten im Ernstfall
-  **Zielgruppe:**
Alle Mitarbeitenden im Unternehmen
-  **Dauer:**
durchschnittlich 20 Minuten
-  **Zertifikat:**
Personalisiertes Abschlusszertifikat
-  **Flexibel:**
Verfügbar über Ihr LMS oder unsere Online-Plattform
-  **Adaptives Lernen:**
Inhalte passen sich dem individuellen Wissensstand an. Alternativ steht eine Basisversion mit festen Inhalten für alle zur Verfügung.

Wichtige Lerninhalte für Ihre Mitarbeitenden

Ransomware verstehen:

Was Ransomware ist, wie sie funktioniert und in welchen Phasen ein Angriff abläuft.

Die eigene Rolle erkennen:

Welche Rolle Mitarbeitende beim Schutz des Unternehmens einnehmen.

Erkennen und vorbeugen:

Woran verdächtige Nachrichten erkannt werden können und konkrete Schutzmaßnahmen im Arbeitsalltag.

Richtig reagieren:

Wie im Fall eines tatsächlichen Angriffs schnell und korrekt gehandelt wird.

Effektives Lernen durch moderne Methoden

Storytelling

Risiken werden durch nachvollziehbare Geschichten greifbar.

Spielerisches Lernen

Interaktive Elemente fördern aktive Anwendung.

Praxisbeispiele

Reale Situationen zeigen die Übertragung in den Alltag.

Abschlussquiz

Das Verständnis wird direkt während der Schulung überprüft.

Expertenwissen aus der Praxis

Die Schulung wurde gemeinsam mit Dr. Jan Scharfenberg, Rechtsanwalt und Experte aus dem IT- und Datenschutzrecht, entwickelt, um fundierte Fachkenntnisse mit praxisnahen Handlungsschritten für Mitarbeitende zu verbinden.

Dr. Jan Scharfenberg, Rechtsanwalt, Partner, Counsel



Sicherheitskultur beginnt mit dem Bewusstsein Ihrer Mitarbeitenden. Jetzt unverbindlich testen!

[Demo starten](#)