Schutz vor Social Engineering

Faktor Mensch:
Die unterschätze Sicherheitslücke

Wie gut sind Ihre Mitarbeiter auf gezielte Cyberangriffe vorbereitet?

Schützen Sie Ihr Unternehmen vor Social Engineering: Prüfen Sie mit realistischen Angriffssimulationen, wie widerstandsfähig Ihr Unternehmen gegenüber manipulativen Hacker-Attacken ist.

Während IT-Systeme auf technischer Ebene immer aufwändiger gegen Eindringlinge geschützt werden, bleibt der Faktor Mensch in der Cybersecurity das größte Sicherheitsrisiko: Unachtsamkeit und fehlendes Risikobewusstsein sind nach wie vor die häufigsten Gründe für IT-Sicherheitspannen.

Genau hier setzt Kontron mit Social Engineering Tests an. Im Gegensatz zu klassischen Penetrationstests konzentrieren sich unsere Sicherheitsexperten nicht auf technische Schwachstellen, sondern auf menschliches Verhalten in der IT-Sicherheit. Mit gezielten Social Engineering Attacken testen und trainieren wir das Sicherheitsbewusstsein Ihrer Mitarbeiter gegenüber gängigen Manipulationsmethoden, stärken so gleichzeitig die Sensibilisierung für Bedrohungen und zeigen auf, wo Bedarf für Schulung und Übungen besteht.

Der Social Engineering Test von Kontron bietet:

- **Realistische Angriffssimulationen** zur Identifikation von Schwachstellen
- **Individuell angepasste Testszenarien** für Ihr Unternehmen
- **Übungen zur Etablierung** der richtigen Reaktion auf Angriffsszenarien
- **Auswertung und Analyse** der Angriffsergebnisse
- **Langfristige Sicherheitsstrategie** zur Stärkung der menschlichen Firewall

Echte Bedrohungen simulieren, um im Ernstfall sicher zu sein.

Kontakt

vertrieb@kontron-services.at
+43 732 7664 500
www.kontron-services.at

Jetzt kostenlos beraten lassen

Social Engineering

Menschliche Sicherheitslücken erkennen und schließen

Social Engineering nutzt psychologische Mechanismen, um Mitarbeiter zu manipulieren und Zugang zu vertraulichen Informationen oder Systemen zu erhalten. Angreifer nutzen diese Information dann zum Schaden der Betroffenen. Unsere Social Engineering Angriffsmethoden, wie z. B. Phishing oder Vishing, simulieren reale Bedrohungsszenarien und helfen dabei, Sicherheitslücken frühzeitig zu erkennen und zu schließen.

Der Kontron Social Engineering Test inkludiert:

Phase 1 – Planung & Strategie

- Analyse Ihrer Organisationsstruktur und Auswahl der passendsten Angriffsszenarien
- Definition der Angriffsszenarien basierend auf realistischen Bedrohungen
- Festlegung von Zielen und Erfolgsmetriken für die Testphase

Phase 2 – Durchführung

- Simulierte Social Engineering Angriffe, wie Phishing, Scam Calls und USB-Attacken
- Beobachtung und Analyse des Mitarbeiterverhaltens bei Sicherheitsvorfällen
- Dokumentation der Angriffe und Identifikation von Schwachstellen

Phase 3 – Analyse & Auswertung

- Erstellung eines detaillierten Berichts mit Ergebnissen und Handlungsempfehlungen für eine langfristige Sicherheitsstrategie, um zukünftige Risiken zu minimieren
- Präsentation der Ergebnisse und Diskussion mit dem Management

Phase 4 – Sensibilisierung & Schulung

- Schulungen für Mitarbeiter zum Erkennen von Social Engineering Angriffen
- Praxisnahe Übungen zur richtigen Reaktion auf Social Engineering Angriffe

Praxisnahe Angriffssimulationen als Verteidigung gegen zukünftige Angriffe

Gemeinsam gegen Social Engineering. Prävention statt Reaktion.

Der Social Engineering Test von Kontron hilft Ihnen, menschliche Sicherheitslücken frühzeitig zu erkennen und wirksame Maßnahmen zu ergreifen. Durch realistische Angriffssimulationen und darüberhinausgehende gezielte Sicherheitsschulungen sensibilisieren wir Ihre Mitarbeiter für die Risiken von Manipulationstechniken und stärken so Ihre gesamte Sicherheitsstrategie. Gemeinsam schützen wir Ihr Unternehmen gegen Social Engineering Angriffe.

Kontakt: vertrieb@kontron-services.at | +43 732 7664 500 | www.kontron-services.at