protiviti®
Global Business Consulting

SOCIAL ENGINEERING | HUMAN RISK NACHHALTIG REDUZIEREN

AWARENESS-PLATTFORMEN SIND BEI IHNEN SCHON IM EINSATZ? GLÜCKWUNSCH, DAS FUNDAMENT STEHT.

Foto: Getty Images

Security Awareness braucht mehr als nur Standard-Phishing-Training.

Ihre Mitarbeitenden lernen kontinuierlich, Social Engineering-Angriffe zu erkennen. Awareness-Trainingslösungen und automatisierte Phishing-Tests leisten hier wertvolle Arbeit und schaffen eine solide Sensibilisierungsgrundlage.

Zeit für den Praxis-Check!

Haben Sie schon einmal getestet, wie Ihre Teams auf maßgeschneiderte Angriffe reagieren, die gezielt interne Informationen oder aktuelle Unternehmensereignisse nutzen? Hier stoßen standardisierte Tests an ihre Grenzen.

Echte Angreifer kombinieren E-Mails mit Anrufen, SMS, und Sie können ihnen sogar persönlich begegnen. Standardisierte Tests können diese individuellen Angriffsvektoren nicht abbilden. Social Engineering ist weit mehr als nur Phishing. Die Frage ist: Wie verlässlich ist Ihre „Human Firewall“ im Ernstfall? Wir helfen Ihnen dabei, dies herauszufinden und Ihre menschliche Verteidigungslinie nachhaltig zu stärken.

DIE STÄRKEN VON PROTIVITI

HOHE WIRKSAMKEIT

- Realitätsnahe Social Engineering-Szenarien statt Standard-Phishing
- Anwendung von Multi-Stage-Angriffen (Phishing, Vishing, Smishing) für erhöhte Aussagekraft
- Einsatz unterschiedlicher Szenarien basierend auf dem Risikoprofil der Mitarbeitenden
- Quantifizierung von Schwachstellen und Angriffserfolgsraten mit konkreten Handlungsempfehlungen
- Ergänzung bestehender Programme durch realitätsnahe Benchmarks
- Messung der Widerstandsfähigkeit Ihrer Teams gegen individualisierte Angriffe

98 %

- 98 % aller Cyberangriffe basieren zumindest teilweise auf Social Engineering.
- Der Mensch ist - und bleibt - das größte Einfallstor in der Cybersecurity.

Quelle: Splunk

70 %

70 % weniger erfolgreiche Social Engineering Angriffe lassen sich durch **nachhaltige,** regelmäßige Social-Engineering-Kampagnen erreichen.

Quelle: Ponemon Institute

Warum Social Engineering Angriffssimulationen unabdinglich sind

Cyberangriffe sind heute allgegenwärtig und fast immer steckt Social Engineering dahinter. Mit 98 % aller Angriffe, die zumindest teilweise auf menschliche Schwachstellen abzielen, wird klar: Ein System ist nur so sicher wie seine Nutzerinnen und Nutzer. Selbst modernste Technik allein kann diese Lücke nicht vollständig schließen. Genau hier setzt das Human Risk Assessment an.

Kurz gesagt: Wer bewährte Awareness-Schulungen durch realitätsnahe Social Engineering-Szenarien ergänzt, macht das größte Einfallstor - den Menschen - deutlich sicherer. Standardlösungen schaffen eine wichtige Sensibilisierungsgrundlage, doch erst gezielte Belastungstests zeigen, wie sich Ihre Human Firewall unter Extrembedingungen verhält. Nur durch praxisnahe „Penetrationstests“ der menschlichen Verteidigungslinie lassen sich kritische Schwachstellen identifizieren und gezielt beheben. Social Engineering-Simulationen sind daher kein Nice-to-have, sondern ein unverzichtbarer Bestandteil jeder modernen Human Risk Assessment Strategie.

Unsere Services im Kontext von Social Engineering

Human Risk Profiling

Mit gezielter Open Source Intelligence (OSINT) identifizieren wir **kritische Risikogruppen**, aktuelle Unternehmensereignisse und potenzielle Angriffsvektoren. Auf Basis öffentlich verfügbarer Informationen erstellen wir abteilungsspezifische Gefährdungsprofile und entwickeln maßgeschneiderte Assessment-Szenarien. HR reagiert anders als Finance, IT anders als Sales. Daher passen wir die Szenarien sowohl an die spezifischen Risiken als auch an die jeweilige Sicherheitsreife der Abteilungen an.

Human Risk Assessment

Aktive Social Engineering Angriffssimulationen testen die Widerstandsfähigkeit Ihrer Human Firewall unter realen Bedingungen. Mit personalisierten **Multi-Channel-Kampagnen** über E-Mail, Telefon, SMS und physische Angriffe messen wir konkrete Schwächen im Sicherheitsbewusstsein und quantifizieren das tatsächliche Sicherheitsrisiko Ihrer Teams.

Human Firewall Optimization

Nachhaltige Stärkung Ihrer **menschlichen Firewall** durch gezielte Empfehlungen und strategische Verbesserung. Wir entwickeln **langfristige Sensibilisierungsstrategien**, die über Einmalschulungen hinausgehen und eine kontinuierliche Steigerung der Resilienz sicherstellen.

Executive & High-value Target Assessment

Führungskräfte und kritische Mitarbeitende stehen im Fokus gezielter Angriffe. Durch umfassende OSINT-Analysen decken wir spezifische Bedrohungen für Ihre Schlüsselpersonen auf und entwickeln **maßgeschneiderte Schutzstrategien** für besonders exponierte Ziele.

Evaluierung & Report

Klickraten, Dateiausführungen und Informationspreisgabe am Telefon. Wir quantifizieren alle Schwachstellen und identifizieren kritische Verhaltensmuster für gezielte Nachschulungen.

Ansprechpartner

DR. MICHAEL RIEKER
Director
+49 173 575 40 29
michael.riecker@protiviti.de

SAED ALAVI
Senior Manager
+49 175 715 09 60
saed.alavi@protiviti.de

KONTAKTIEREN SIE UNS!
+49 69 963 768 100
contact@protiviti.de
www.protiviti.de

protiviti®
Global Business Consulting

90	25	11.000
Standorte	Länder	Mitarbeitende

Protiviti berät Unternehmen praxisorientiert und auf Augenhöhe in den Bereichen Strategie, Organisationstransformation und -optimierung, ESG, Digitale Transformation, Risikomanagement, Interne Revision und Kontrollsysteme, Compliance sowie IT. Gemeinsam finden wir individuelle Lösungsansätze, um Ihr Unternehmen zukunftssicher aufzustellen.

We Care. We Collaborate. We Deliver.