Net at Work
Building IT-Excellence.

Net at Work Attack Simulation Training

Sicherheitsrisiken minimieren: Mitarbeiterbewusstsein durch simulierte Cyberattacken schärfen

In den letzten Jahren hat die Zahl der E-Mail-Cyberangriffe kontinuierlich zugenommen. Dies unterstreicht die wachsende Dringlichkeit für Unternehmen, sich intensiv mit dem Thema zu befassen. Dazu gehört nicht nur der Erwerb geeigneter Technologie und Software, sondern auch die Sensibilisierung Ihrer Mitarbeitenden. Mit unserem Attack Simulation Training erhöhen Sie das Bewusstsein und schützen Ihr Unternehmen vor potenziellen Bedrohungen. Unser individuell anpassbares Sicherheitskonzept simuliert realistische Cyberangriffe, um die Aufmerksamkeit Ihrer Mitarbeitenden auf verschiedene Angriffsszenarien zu testen. Anschließend bieten wir gezielte Schulungen an, um etwaige Wissenslücken zu schließen.

Individuelle Simulationen

Wir gestalten Simulationen gemeinsam mit Ihnen nach Ihren Bedürfnissen

Geringe Aufwände

Erhalten Sie hochwertige Ergebnisse bei einer kosteneffizienten Gestaltung

Passgenaue Schulung

Basierend auf Ihren individuellen Unternehmensergebnissen bauen wir die Kompetenzen Ihrer Mitarbeitenden weiter aus

Entlastung Ihrer IT

Wir übernehmen die Planung, Durchführung und Nachbereitung der Kampagne, damit Sie sich Ihren Kernthemen widmen können

Leistungsumfang

Die Experten von Net at Work schaffen Bewusstsein für das Thema „Cybersecurity“ bei den Mitarbeitenden und testen die Bewusstseinslage mit simulierten Cyberattacken. Denn nur, wenn sich jeder einzelne Mitarbeitende seiner Verantwortung und der möglichen Auswirkungen bei Unwissenheit bewusst ist, können wir langfristig Personen und unternehmensbezogene Daten schützen. Dabei können sowohl Schweregrade der gefälschten E-Mails individuell festgelegt werden als auch der Empfängerkreis der Cyberattacke. Passgenaue Inhalte machen unsere Simulationen täuschend echt und führen den Mitarbeitenden die tatsächliche Bedrohungslage direkt vor Augen.

Die im Anschluss empfohlenen Schulungsmaßnahmen können optional an das Attack Simulation Training durchgeführt werden. Gerne entwickeln wir Ihnen hierzu das richtige Schulungskonzept und/ oder stellen Ihnen ein E-Learning für Ihre Cyber-Security Awareness Kampagne zur Verfügung. Dabei legen wir gemeinsam mit Ihnen individuell die Lerninhalte fest, deren Grundlage die Ergebnissen Ihres Attack Simulation Trainings sind.

Mögliche Inhalte für Ihre Cybersecurity Kampagne:

- Was sind Phishing Mails und wie erkenne ich solche?
- Welche Auswirkungen kann die Weitergabe von sensiblen Daten haben?
- Welche Rolle spiele ich bei der Sicherung von sensiblen Daten? (Social Engineering)
- Wie gehe ich richtig mit Passwörtern um?
- An welche Meldestelle wende ich mich, wenn ich Spam erhalte?

Systemanforderungen:

- Microsoft 365 E5 Lizenz (mindestens Defender for Office 365 Plan 2)
- Exchange Postfächer (der volle Funktionsumfang wird nur bei Exchange Online Postfächern angeboten)
- Einen Microsoft 365 Tenant, mit (synchronisierten) Benutzerkonten, die das Attack Simulation Training erhalten sollen
- Admin-Berechtigungen im Defender XDR Portal

Net at Work Attack Simulation Training

- Sensibilisierung aller Mitarbeitenden über die Eigenverantwortung im Umgang mit sensiblen Daten und verdächtig erscheinenden Inhalten
- Entwicklung von passgenauen Schulungsinhalten für die kontinuierliche Aufklärung über das Thema Cybersecurity – auch integrierbar in den HR Onboarding Prozess
- Kosteneffiziente Gestaltung der Simulationen
- Individualisierungsgrad der Cyberattacke: von offensichtlichen Fälschungen bis hin zu täuschend echt aussehenden E-Mails
- Entlastung Ihrer IT-Abteilung: Damit Sie sich um Ihr Kerngeschäft kümmern können