Phishing 1x1

Gefahren & Statistiken für KMU in D-A-CH

Phishing ist eine Methode, bei der Cyberkriminelle versuchen, durch gefälschte E-Mails, Websites oder Nachrichten an vertrauliche Informationen wie Passwörter, Bankdaten oder Unternehmenszugänge zu gelangen. Besonders kleine und mittlere Unternehmen (KMU) sind häufig Ziel solcher Angriffe.

Gefahren ⚠

- **Finanzielle Verluste**: Betrugsüberweisungen, Erpressung durch Ransomware.
- **Datenverlust**: Kunden- und Unternehmensdaten können gestohlen oder veröffentlicht werden.
- **Betriebsunterbrechung**: Systemausfälle und Produktionsstillstände durch Schadsoftware.
- **Reputationsschaden**: Vertrauensverlust bei Kunden und Partnern.
- **Folgeangriffe**: Ein erfolgreicher Angriff öffnet Tür und Tor für weitere Attacken.

Warum ist Phishing-Training notwendig?

- **Häufigkeit**: 87 % der österreichischen Unternehmen wurden in den letzten 12 Monaten Opfer von Phishing-Attacken.
- **DACH-Region betroffen**: 55 % der Unternehmen in Deutschland, Österreich und der Schweiz wurden innerhalb eines Jahres mit Spear-Phishing angegriffen.
- **Menschliche Fehler als Hauptursache**: 74 % der Sicherheitsvorfälle sind auf menschliches Versagen zurückzuführen.
- **Erfolgreiche Angriffe haben drastische Folgen**: 24 % der Unternehmen hatten mindestens ein kompromittiertes E-Mail-Konto, von dem im Schnitt 370 bösartige Mails versendet wurden.

SPIDER

Wichtige Trainingsinhalte

» **Erkennen von Phishing-Mails**: Verdächtige Absender, gefälschte Links, ungewöhnliche Anfragen.

» **Sicherer Umgang mit E-Mails**: Keine Anhänge oder Links von unbekannten Quellen öffnen.

» **Meldung verdächtiger Mails**: Klare Prozesse für die interne IT-Sicherheit.

» **Regelmäßige Tests**: Simulierte Phishing-Angriffe, um das Erlernte zu festigen.

Vorteile eines geschulten Teams

» Reduzierung von Sicherheitsvorfällen durch frühzeitige Erkennung.

» Erhöhung der Unternehmenssicherheit durch wachsames Verhalten.

» Schutz vor finanziellen Schäden durch Prävention statt Schadensbegrenzung.

» Einhaltung gesetzlicher Vorgaben (DSGVO, NIS2, ISO 27001).

» Wettbewerbsvorteil durch Vertrauen von Kunden und Partnern.

> **“Phishing-Training ist eine Investition in die Sicherheit und Zukunft des Unternehmens.”**

SPIDER

Bestens vorbereitet durch unser Phishing-Training

» **User-Sicherheitsmaßnahmen**: Phishing-Awareness wird durch simulierte Angriffe und Fallbeispiele vermittelt. Diese Maßnahmen werden jährlich wiederholt, um neue Mitarbeiter einzubeziehen und das Wissen regelmäßig aufzufrischen. Ein Turnus von zwei bis drei Monaten pro Jahr ist empfehlenswert.

» **Technische Sicherheitsmaßnahmen**: Wichtige Maßnahmen sind die Einschränkung von Benutzerrechten, die Aktivierung von Zwei-Faktor-Authentifizierung (2FA) und das Melden verdächtiger Absender an die IT. Zudem sollte Mail Protection durch Filtermechanismen wie SPF und DKIM gewährleistet sein. Ergänzend sind Offsite-Backups sowie ein Wartungsplan für die IT-Infrastruktur essenziell.

» **Vorbereitung der Mitarbeiter auf den Ernstfall**: Schnelles Handeln ist notwendig. Informieren der Vorgesetzten und SPIDER.

» **Optionale Empfehlung**: systematische Schwachstellenanalyse von Clients, Server und Netzwerk.

Interessiert? Melde dich jetzt!

+43 5572 386 122 info@spidernet.at www.spidernet.at

SPIDER

SPIDER Netzwerk Consulting GmbH
Riedgasse 50, 6850 Dornbirn, Österreich
+43 5572 386 122, info@spidernet.at, www.spidernet.at