terreActive
terreActive
terreActive
terreActive

Audit

Fact Sheet

Social Engineering: Sicherheit prüfen

Kontrollierte Angriffe sensibilisieren Mitarbeitende

Security Awareness gegen Cyberbedrohungen

Sensibilisierte Mitarbeitende mit einem geschärften Bewusstsein für Bedrohungen werden im Kampf gegen Cyberkriminelle wichtiger. Kontrollierte Phishing- und Social-Engineering-Attacken liefern Ihnen Antworten auf diese Fragen:

- Sind Sie in der Lage, Phishing-Attacken zu erkennen?
- Durch welche Art von Social Engineering ist Ihr Unternehmen verwundbar?
- Wie vorsichtig sind Ihre Mitarbeitenden im Umgang mit Phishing-Mails?
- Sind Sie gegenüber Ransomware-Angriffen genügend sensibilisiert?

Unser Vorgehen: Arbeitsschritte

- Gemeinsames Ausarbeiten von Phishing-Szenarios nach Ihren Bedürfnissen (z. B. das Fälschen der eigenen Webseite oder die Gestaltung einer branchenspezifischen Fake-Webseite)
- Definition einer oder mehrerer Zielgruppen (z. B. nur Geschäftsleitung, eine spezifische Abteilung oder gesamte Belegschaft)
- Kontrollierte Social-Engineering-Attacke auf ausgewähle Zielgruppen, Begleitung und Beratung

Im Anschluss an die Attacke:

- Awareness-Schulungen als Präventionsmassnahme gegen die identifizierten Schwachstellen
- Auswertung und Präsentation der Resultate für eine spezifische Zielgruppe (z. B. Phishing-Awareness-Workshop mit der HR-Abteilung)
- Auswertung von Attacken und Schulungen in Form eines schriftlichen Berichtes

Phishing bleibt gefährlich

Finger weg von Mails mit unbekanntem Absender, verdächtig wirkendem Betreff oder ungewöhnlichem Anhang. Phishing-Methoden sind heute zwar bekannt. Trotzdem ist es eine der verbreitetsten Angriffsmethoden.

Social-Engineering-Kampagnen vielseitig einsetzbar

- Als eigenständiges Projekt
- Im Rahmen eines breiteren Auditprojektes
- Als Durchlässigkeitsprüfung für Mailfilter, Firewall und Proxy
- Zur Überprüfung des Verhalten von Advance-Malware-Protection-Lösungen

Kontrollierte Phishing-Angriffe: Mittel individuell anpassbar

- Leicht bis schwer enttarnbaren Attacken
- Via E-Mail, SMS, USB-Token, CD u.a.
- Klonung bestehender Webseiten
- Neugestaltung von Phishing-Seiten
- Fälschung von E-Mails und Absendern
- Leicht skalierbar, bis zu mehreren hundert Empfängern

Audit

Fact Sheet

Was bringt eine Social-Engineering-Kampagne? Ihr Nutzen

Der beste Schutz sind geschulte Mitarbeitende, die die Bedrohungsszenarien kennen und die IT-Sicherheit in ihrer täglichen Arbeit berücksichtigen.

- Sie verhindern kostspielige Ransomware-Angriffe durch wachsame Kollegen in allen Abteilungen.
- Sie vermeiden Imageschäden für Ihr Unternehmen – etwa durch negative Zeitungsschlagzeilen über Cyberattacken.

Erfahrung bringt Effizienz

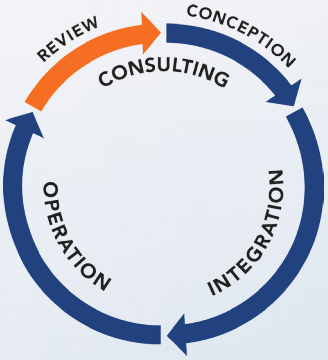
Reduzieren Sie Ihren eigenen Aufwand und gelangen Sie schneller zu Resultaten, indem Sie sich die Erfahrung von terreActive aus umfangreichen Social-Engineering-Projekten zu Nutze machen. Durch unser Security-Know-how können wir Ihre Wunschkampagne technisch professionell realisieren.

Mit einem ausführlichen Bericht inkl. Management Summary erhalten Sie eine nachvollziehbare Dokumentation für unterschiedliche Zielgruppen. Damit können Sie auch nach dem Social-Engineering-Projekt Ihre Schwachstellen bearbeiten und eliminieren.

Mehr zum Thema im Blog

www.securityMonitoring.ch/blog/phishing

- Was ist Phishing?
- Welche Arten von Phishing gibt es?
- Merkmale zur Erkennung einer Phishing-Attacke
- Einsatz von Social-Engineering-Frameworks



Ergänzende Themen

- Audit zur einmaligen Bestandesaufnahme
- Audit als fortlaufendes Abo
- Vulnerability Scan (as a Service)
- Security Monitoring
- Projektbegleitung aus Security-Sicht

Kontakt

terreActive AG
Kasinostrasse 30
5001 Aarau
Tel. +41 62 834 00 55
info@terreActive.ch
www.terreActive.ch

Wir sichern Ihren Erfolg.
www.terreActive.ch

terreActive
terreActive
terreActive
terreActive