

THE TECHNOLOGY PROVIDER

SECURITY AWARENESS

Best Practice

Unser Best Practice geht über traditionelle Schulungsansätze hinaus und konzentriert sich darauf, eine Umgebung zu schaffen, die nicht nur Wissen vermittelt, sondern auch zur Reflexion und Veränderung anregt. Denn wahre Awareness geht über das bloße Verstehen hinaus; sie erfordert eine aktive Beteiligung, persönliche Auseinandersetzung und die Bereitschaft, Verhalten zu ändern.

Bestandteile der Lösung

- Security Escape Room
- Live Hacking Area
- Simulated Phishing Plattform
- Security Awareness Schulung
- Workshop



Security Awareness - Phase 1

1. Initial Event: Security Escape Room / Live Hacking Area
Startpunkt des Programms ist das initiale Event mit dem Security Escape Room oder der Live Hacking Area.
Dabei werden die Teilnehmer*innen mit realen Sicherheitsszenarien konfrontiert. Hier lernen sie auf spielerische Weise, wie wichtig Sicherheitsbewusstsein im Umgang mit digitalen Bedrohungen ist.

2. Start der ersten Phishing Kampagne
Nach dem initialen Event startet eine dreimonatige Phishing-Kampagne, um die Reaktionen der Teilnehmer*innen auf realistische Cyberangriffe zu testen. Die Kampagne simuliert verschiedene Phishing-Szenarien, um das Bewusstsein für diese häufigen Bedrohungen zu schärfen. Empfehlung: Es sollte im Vorfeld ein Abgleich der aktuellen Datenschutzbestimmungen durchgeführt und etwaige Interessensvertretungen involviert werden.

3. Auswertung der ersten Kampagne & Awareness Schulung
Nach Abschluss der Phishing-Kampagne folgt eine gezielte Awareness-Schulung. Die Auswertung der Kampagnenergebnisse wird genutzt, um die Schulungsinhalte an die spezifischen Bedürfnisse der Mitarbeiter*innen anzupassen.

4. Implementierung
Es werden Awareness-Tools implementiert, um zukünftige Phishing E-Mails melden zu können.

Initial Event
Security Escape Room / Live Hacking Area

↓

Für 3 Monate
Phishing Kampagne

↓

Anschließend
Awareness Schulung & Auswertung

↓

Implementierung
Installation von Awareness Tools



Security Awareness - Phase 2

5. Start der zweiten Phishing Kampagne
Diese Phishing-Kampagne Phase erstreckt sich über fünf Monate und testet die Auswirkungen der implementierten Awareness-Tools. Dies dient dazu, die Effektivität der Tools zu bewerten und die kontinuierliche Aufmerksamkeit der Mitarbeiter*innen aufrechtzuerhalten.

Für 5 Monate
Erweiterte Phishing Kampagne

6. Auswertung der zweiten Kampagne & Awareness Schulung
Nach Abschluss der erweiterten Phishing-Kampagne erfolgt eine erneute Awareness-Schulung. Die Auswertung konzentriert sich auf die Fortschritte der Mitarbeiter*innen im Vergleich zur vorherigen Schulung und identifiziert mögliche Verbesserungsbereiche.

Anschließend
Awareness Schulung

7. Analyse der gesamten Kampagne
Eine umfassende Analyse der gesamten Kampagne wird durchgeführt, um Trends, Erfolge und Herausforderungen zu identifizieren. Diese Analyse dient als Grundlage für zukünftige Sicherheitsstrategien und Schulungsmaßnahmen.

Recap
Analyse der gesamten Kampagne

8. Einführung einer permanenten Phishing Plattform
Basierend auf den gesammelten Erkenntnissen wird eine permanente Lösung eingeführt, die Sicherheitsbewusstsein zu einer dauerhaften Priorität im Unternehmen macht. Dies kann regelmäßige Schulungen, kontinuierliche Überwachung, und fortgeschrittene Sicherheitstools umfassen, um die Cyberresilienz des Unternehmens zu stärken.

Einführung
Permanente Lösung

Dieses ganzheitliche Programm kombiniert erlebnisorientierte Schulung, gezielte Phishing-Tests, kontinuierliche Trainings und fortlaufende Anpassungen, um eine nachhaltige Sicherheitskultur im Unternehmen zu etablieren.

Kontaktieren Sie uns

+49 2921 99 2333

presales@also.com