Beste Abwehr gegen Cyberangriffe? Ein aufgeklärter Mensch.

#securityawareness

250.000
neue Schadprogramme werden durchschnittlich täglich gefunden

21.000
infizierte Systeme werden täglich erkannt

84%
aller betrügerischen E-Mails waren Phishing zur Erbeutung von Passwörtern

206
Milliarden Euro wirtschaftlicher Schaden

Quelle: Die Lage der IT-Sicherheit in Deutschland 2023 (BSI)

- Security Awareness Trainings: Der Schlüssel zu IT-Sicherheit sind die Menschen im Unternehmen. Denn die meisten Datenverluste durch Cyberangriffe ließen sich vermeiden, wenn die Menschen im Unternehmen besser informiert und aufgeklärt wären. Selbst die beste Technik ist wirkungslos, wenn die Mitarbeitenden die IT-Sicherheitsrisiken nicht kennen. Neben den nötigen technischen Lösungen bieten wir daher Security Awareness Trainings für Mitarbeitende an. Der Kunde wählt hierbei zwischen verschiedenen Maßnahmen-Paketen mit fortlaufenden Phishing-Simulationen, eLearnings und Social Engineering Sensibilisierungen aus. Unser Managed Service ist immer dabei. Alle genannten Maßnahmen sind auch einzeln verfügbar. Awareness-Materialien wie Webcam-Schutz oder Mousepads unterstützen die Wirkung als tägliche Erinnerung am Arbeitsplatz.

Anqa
IT–Security

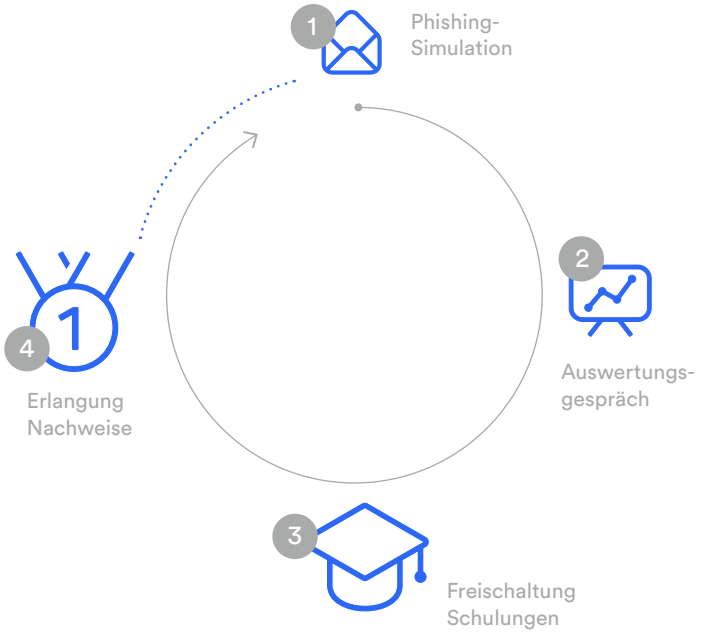
Unsere Grundsätze und Awareness-Philosophie

- 100% Managed Service: Was bringen die besten Tools, wenn es niemanden gibt, der sie einzusetzen weiß? Als Managed Security Service Provider liegt uns stets daran, Systemhäuser und IT-Verantwortliche zu entlasten. Nicht jedes Unternehmen hat die Kapazitäten, Awareness-Maßnahmen umfangreich zu konzeptionieren, durchzuführen und die Ergebnisse zu analysieren. Daher übernimmt unser Expertenteam in Köln nicht nur die Konzeptionierung, das Onboarding und die Durchführung der Maßnahmen, sondern auf Wunsch auch die komplette Kommunikation inkl. Auswertungsgespräche, das Monitoring der Schulungsfortschritte und die proaktive Planung weiterer Maßnahmen.
  Unser Ziel ist: Minimaler Aufwand für Sie, maximaler Schulungserfolg für das Kundenunternehmen.

  Nachweislicher Lernerfolg durch Wiederholung: Mit unseren fortlaufenden Awareness-Paketen halten wir das Thema Awareness in den Köpfen der Mitarbeitenden präsent und bauen eine nachhaltige Lernkurve auf. Im Rahmen der DSGVO, NIS2, TISAX, DORA und diverser ISO-Zertifizierungen sind Unternehmen verpflichtet, ihre Mitarbeitenden für das Thema IT-Sicherheit fortlaufend zu sensibilisieren. Die Teilnahme an unseren eLearnings generiert personenbezogene und rechtskräftige Schulungsnachweise.

  Transparenz: Wir empfehlen die Awareness-Maßnahmen transparent im Kundenunternehmen zu kommunizieren. Dies erhöht die Akzeptanz der Mitarbeitenden für die Maßnahmen, und es werden deutlich bessere Ergebnisse erzielt. Selbstverständlich unterstützen wir den Kunden in der Gestaltung dieser Kommunikation durch diverse Textbausteine oder setzen gemeinsam ein Schreiben auf. Die Maßnahmen sollen sowohl im unternehmerischen als auch im privaten Kontext einen Mehrwert für die Mitarbeitenden bieten.

Beispielhafter Ablauf



Simulierte Phishing-Angriffe: Wie reagieren die Mitarbeitenden auf Phishing-E-Mails? Anhand einer Auswertung realitätsgetreu imitierter Phishing-E-Mails erhält der Kunde eine fundierte Aussage über den Umgang mit täglich vorkommenden Cyber-Angriffen in seinem Unternehmen.

Etablierung eines Lernkonzepts: Regelmäßige, gut platzierte und kurze Lerneinheiten führen nachweislich zum größten Lernerfolg. Das oftmals komplexe Thema der IT-Sicherheit kann man den Mitarbeitenden nicht aufzwingen – Daher ist es wichtig, einen für die Mitarbeitenden und das Unternehmen passenden Lernrhythmus zu etablieren, ohne die Mitarbeitenden zu überfordern.

Ganzheitliche Betreuung: Jedes Unternehmen ist anders. Im persönlichen Austausch mit den Kunden können zusätzliche Maßnahmen wie ein eLearning-Spezialkurs „Digitaler Ersthelfer“ oder eine Online-/Präsenzschulung durch einen TÜV-zertifizierten Cyber Security Awareness-Beauftragten besprochen werden.

Awareness ReTeach Pakete

	Basic	Plus	Premium
Phishing*			
Managed Service – Onboarding, Begleitung, technischer Support & Ergebnisanalyse	●	●	●
Anzahl Phishing Simulationen (Verteiler & personalisiert)	< ②	< ④	< ④
CEO-Fraud pro Simulation		●	●
CEO-Fraud+ (bestehenden E-Mailverlauf fälschen)			●
Erfassung von Dateneingabe auf Landingpages		●	●
Anonymisierte Auswertung	●	●	●
eLearning*			
Managed Service – Lernfortschrittsanalyse, Erinnerungen, Nutzeradministration & Kursfreischaltungen	●	●	●
Kontinuierliche Bereitstellung sämtlicher eLearnings	●	●	●
Abschluss-Quiz	●	●	●
Rechtsgültige Schulungszertifikate	●	●	●
Anzahl Zugänge zum Sonderkurs „Der Digitale Ersthelfer“			①
Phishing Sensibilisierung für „Top-Klicker“ der vorangegangenen Phishing Simulationen			●
Social Engineering Prävention*			
Managed Service – Durchführung & Begleitung			●
Zugang zu zweimal jährlich angebotenen Webcasts zu „Social Engineering &Voice Phishing“			●
Jährlicher „USB-Angriff“			●
Weitere Services*			
Browser Plug-In „AQ Detector“ zur Erkennung von Fake-Webseiten	●	●	●
Monatlicher Awareness-Newsletter		●	●
Monatliche Abrechnung pro Mitarbeiter	●	●	●
Monatlich kündbar	●	●	●

*Beinhaltet in 12 Monaten

Keine Macht den Phishern! Jetzt das Security Awareness Training beantragen und Ihr Unternehmen oder das Ihres Kunden langfristig schützen.

- Unser Awareness Team berät Sie gerne zu unseren Security Awareness Trainings +49 2203 290 63–63