infinigate
techservices

TechServices
Security Awareness

Serviceübersicht

Der Mensch ist das Einfallstor Nr. 1 – und zugleich die stärkste Verteidigungslinie

Security Awareness
powered by
keepnet

Security Awareness

Selbst die beste Technik schützt nie zu 100 %. Das wissen wir alle. Auch Angreifer gehen nicht vermehrt gegen die Technik vor, sondern wenden sich einem erfolgversprechenderen Ziel zu: dem Menschen.

Bei über 95 % aller Cyberattacken auf Firmen nimmt der Mitarbeiter eine zentrale Rolle ein und wird zum Einfallstor für einen Angreifer. Gleichzeitig sind Mitarbeiter aber auch der effektivste Schutz, den Sie in Ihrem Unternehmen haben. Wir von Infinigate wollen die IT-Welt jeden Tag etwas sicherer machen. Lassen Sie uns gemeinsam daran arbeiten. Wir haben uns intensiv mit dem Thema Security Awareness auseinandergesetzt, Seminare und Workshops entwickelt und kombinieren diese mit der Infinigate Awareness Plattform powered by Keepnet, um Sie umfassend zu unterstützen.

Denn Security Awareness ist ein Prozess, der – einmal gestartet – Ihrem Unternehmen eine neue Perspektive bietet, Ihre Mitarbeiter und Ihre Firma vor den ständig wachsenden Bedrohungen aus dem Cyber Space zu schützen.

Unser Fokus

Viele Hersteller bieten zahlreiche Lösungen rund um den Bereich Security Awareness an, jeweils mit verschiedenen Schwerpunkten und Stärken.

Unser Fokus hingegen liegt primär auf der Implementierung von Security Awareness als Prozess im Unternehmen. Wie man ein erfolgreiches und nachhaltiges, auf das jeweilige Unternehmen zugeschnittenes Konzept erstellt, ist der Schwerpunkt unserer zertifizierten Security Awareness Koordinatoren.

In einem individuellen Erstgespräch beraten wir Sie über eine möglichst passende Security Awareness Kampagne. Dabei können wir neben unserer Plattform (powered by Keepnet) auch Produkte unserer Hersteller sowie weitere, von uns erstellte Inhalte mit in das Konzept einbauen und Ihnen ein individuelles Angebot zukommen lassen.

infinigate

Infinigate Awareness Plattform - powered by Keepnet

Den digitalen Kern unseres Security-Awareness-Prozesses bildet die Infinigate Awareness Plattform (powered by Keepnet). Sie verbindet realistische Angriffssimulationen, ein umfangreiches Learning Management System und ein zentrales Risiko-Dashboard - als Self-Serviced-Modell oder als vollständig durch Infinigate betreuten Managed Awareness Service.

Multi-Channel-Simulation	Phishing über alle realen Kanäle: E-Mail-Phishing, Smishing (SMS), Vishing (Telefon), Quishing (QR-Code), MFA-Fatigue und Callback-Phishing.
LMS mit 7.000+ Materialien	Über 7.000 Trainingsmaterialien von 11 Content-Providern in mehreren Sprachen: Videos, interaktive Module, Quizze und Infografiken.
Phishing Reporter	Verdächtige E-Mails mit einem Klick direkt aus Outlook oder Gmail melden – Mitarbeitende werden zur aktiven Verteidigungslinie.
Human Risk Dashboard	Menschlicher Risikofaktor des Unternehmens auf einen Blick: Risikoscore pro Abteilung, Klickraten und Verbesserungstrends.
KI-adaptive Schulungen	Die Plattform analysiert das Verhalten und spielt automatisch passende Micro-Trainings aus, kein generisches Massentraining mehr.
Compliance-Reporting	Automatische Reports und lückenlose Audit-Trails für NIS2, DSGVO, ISO 27001 und DORA – Nachweise auf Knopfdruck.

Plattform-Partner:

keepnet Barracuda HORNETSECURITY BY proofpoint SOPHOS infinigate

Bestehende Produkte unserer Hersteller (z. B. Sophos, Hornetsecurity) lassen sich in jedes Projekt integrieren.

Unsere Security Awareness Koordinatoren

Armin Pfender
Awareness Koordinator

Oliver Listl
Awareness Koordinator

Unser Ziel ist die Schaffung, Erhaltung und nachhaltige Steigerung von Security Awareness bei jedem einzelnen Mitarbeiter im Unternehmen.

Sie interessieren sich für eine Security Awareness Schulung? Melden Sie sich bei uns. Wir helfen Ihnen, den Überblick im Produkt-Dschungel zu behalten und koordinieren sowie begleiten Ihre individuelle Security Awareness Kampagne.

Projektablauf - der Awareness-Baukasten

Wir legen in einem individuellen Kickoff-Workshop den genauen zeitlichen und organisatorischen Ablauf fest. Dabei gehen wir auf die speziellen Gegebenheiten Ihres Unternehmens ein. Aus den folgenden Bausteinen stellen wir Ihre Kampagne modular zusammen, durchgängig begleitet durch unsere zertifizierten Koordinatoren und gestützt auf die Infinigate Awareness Plattform:

Kickoff Workshop
Planung der Awareness-Kampagne, Definition des Teams

Projekt Koordination
Koordination, Reporting & Human Risk Dashboard

Live-Training
Awareness Basic

Live-Workshop
Awareness Management

Live-Training
Vertiefungsmodule (z. B. Mobiles Arbeiten, Social Engineering)

Self-Study Training
Diverse Module zum Selbststudium (LMS), inkl. Tests & Auswertungen

Live-Workshop
Awareness IT-Abteilung

Live Element
Awareness-Sprechstunde mit zertifizierten Koordinatoren

Simulation
Phishing-Angriff – erste & weitere Angriffswellen (powered by Keepnet)

KI-Awareness Training
Halbtages-Modul für Anwender & Fachbereiche

Self-Study-Trainings & LMS

Zur Steigerung der Nachhaltigkeit empfiehlt es sich, zusätzlich Inhalte zum Selbststudium über ein Learning Management System (LMS) bereitzustellen und in den Security Awareness Prozess zu integrieren.

Im Zentrum steht die Infinigate Awareness Plattform (powered by Keepnet) mit über 7.000 Trainingsmaterialien in mehreren Sprachen - Videos, interaktive Module, Quizze und Infografiken. Mitarbeitende lernen im eigenen Tempo, zu jeder Zeit und von jedem Gerät. Nachweisbare Lernfortschritte fließen direkt in die Compliance-Dokumentation ein.

Modulauswahl

01

- Vulnerability Management
- Access Control
- Authentication
- Security Monitoring
- System Security
- Network Security

02

- Secure Configuration
- Performance and Capacity Management
- Log Management
- ICS Security
- Harassment
- CEO Fraud

03

- Wi-Fi Security
- General
- Cloud Security
- Insider Threats
- Incident Response
- AI/ML Security

04

- Deepfake & Synthetic Media
- AI-Powered Threats
- Ransomware & Extortion
- Zero Trust Architecture
- Biometric Security
- Supply Chain Attacks

05

- Hospitality
- Secure Coding
- OT Security
- GDPR
- Social Engineering
- Removable Media

06

- Discrimination
- Diversity
- Equity & Inclusion
- Employment Law
- Information Security Governance
- Responsibilities and Compliance

07

- IoT Security
- Remote Working Security
- Travel Security
- Mobile Device Security
- Email Security
- Social Media Security

08

- Safe Online Shopping
- Malware
- Physical Security
- Cyber Spying
- Password Security

Live-Workshops

Security Awareness im Management

Dieser Workshop ist für die Managementebene des Unternehmens. Wie können Sie schnell und effektiv mehr für Ihre IT-Sicherheit sorgen? Wie erreichen Sie Akzeptanz und Verständnis? Wo lauern Stolperfallen, und warum sollten Sie Awareness auf gar keinen Fall auf die leichte Schulter nehmen?
Dauer: 4 Stunden Workshop

- Sicherheitskultur und Reifegrade - wo steht Ihr Unternehmen?
- Sicherheit ist Führungsaufgabe - Verantwortung übernehmen, unterstützen, planen, delegieren, kontrollieren, steuern
- Der Weg ist das Ziel - Sicherheit ist kein Projekt, sondern ein Prozess - Nachhaltigkeit mit Kampagnen
- Wie Mitarbeiter zur Gefahr werden - Fahrlässigkeit und Vorsatz - Konflikte managen
- Inklusive digital Footprinting light zur individuellen Vorbereitung des Workshops

Security Awareness in der IT-Abteilung

Dieser Workshop ist speziell für die IT-Abteilung entwickelt. Wir zeigen blinde Flecken in der Angriffsoberfläche eines Unternehmens und helfen diese Lücken zu schließen.

Wie machen wir es einem Angreifer möglichst schwer? Welche Technik brauche ich wirklich? Wie kommuniziere ich richtig mit meinen Mitarbeitenden in IT-Themen?
Dauer: 4 Stunden Workshop

- Angriffe rechtzeitig erkennen und richtig reagieren
- Miteinander reden - aber richtig
- Menschliche Fehler in der IT-Abteilung
- Wie Angreifer sich durch ein Unternehmen hacken
- Erkennung, Eindämmung, Abwehr
- Die Meldekette
- Know your assets - know your risks - plan your actions.
- Ein Notfall ohne Plan endet im Desaster
- Inklusive digital Footprinting light zur individuellen Vorbereitung des Workshops

Live-Trainings

Alle Trainings werden live von unseren erfahrenen Security Awareness Koordinatoren durchgeführt und können individuell an die Bedürfnisse und Anforderungen des jeweiligen Unternehmens angepasst werden; die hier vorgestellten Inhalte stellen unsere standardisierten Inhalte dar. Um eine möglichst große Nachhaltigkeit zu erzielen, empfehlen wir die Durchführung in Gruppen mit maximal zwanzig Teilnehmern.

Security Awareness Basic

In diesem Seminar für alle Mitarbeiter zeigen wir gängige Angriffstechniken und die grundlegende Verteidigung dagegen. Irgendwann trifft es jeden! Deshalb bereiten Sie sich besser darauf vor, dass auch Sie morgen schon Opfer von Cyberkriminellen werden können, als Einzelperson wie auch als Unternehmen.

Das Ziel unseres Security Awareness Basic Seminars ist es, eine gemeinsame Basis bzw. ein gemeinsames Verständnis von Security Awareness zu schaffen.
Basic kompakt: Dauer 90 Minuten
Basic: Dauer 4 Stunden

- Die aktuelle Bedrohungslage
- Fehlerkultur – Fehler passieren jedem. Entscheidend ist, wie man damit umgeht.
- Überblick über Techniken und Taktiken von Angreifern
- Social Engineering / Phishing
- Identitätsdiebstahl / Passwort / Authentifizierung
- Mobiles Arbeiten / Arbeiten im Homeoffice
- Internetnutzung und Surfverhalten
- Perimetersicherheit / Drop Device
- Der Tag X und seine Auswirkungen

Vertiefungs-Trainings

Um einzelne Themengebiete im späteren Projektverlauf dediziert und mit mehr Tiefgang zu transportieren, bieten wir entsprechende Trainings an.
Dauer: 90 Minuten je Modul

- Mobiles Arbeiten
- Passwörter & Identitäten
- Social Engineering
- Phishing erkennen
- u. v. m.

NEU: KI-Awareness Training

Künstliche Intelligenz verändert die Arbeitswelt rasant – mit enormen Chancen, aber auch neuen Risiken. Unser KI-Awareness Training macht Ihre Mitarbeitenden fit für den sicheren und verantwortungsvollen Einsatz von KI im Arbeitsalltag.

Dieses kompakte Halbtages-Modul ergänzt den Awareness-Baukasten und richtet sich an Anwender und Fachbereiche. Es vermittelt praxisnah die wichtigsten Grundlagen rund um KI: Wie lässt sich die Technologie sinnvoll nutzen, welche Potenziale ergeben sich, und worauf ist mit Blick auf Datenschutz, Compliance und verantwortungsvollen Einsatz zu achten?
Dauer: 4 Stunden

- Grundlagen: Was ist KI? Leicht verständlich erklärt
- Chancen & Grenzen
- Konkrete Potenziale für den Arbeitsalltag
- Hands-On-Tools: Text, Bild und Daten direkt ausprobieren
- Do's & Don'ts im Firmen-KI-Einsatz
- Risiken: Bias, Halluzinationen, Datenschutz, Abhängigkeiten
- Ethik: Fairness, Verantwortung, Transparenz
- Q&A & Diskussion: Praxisfälle der Teilnehmenden

Das KI-Awareness Training ist Teil eines breiteren KI-Trainingsportfolios der Infinigate Akademie - von KI-Kompetenz nach EU AI Act über Fachtrainings für Marketing, Vertrieb und Personal bis hin zu spezialisierten Formaten für Entwicklung, Management und Compliance.

Phishing-Simulationen

93 % aller Datenpannen gehen von Phishing aus.

In den letzten Jahren haben Phishing-Angriffe drastisch zugenommen, da Angreifer ihre Strategien immer weiter ausfeilen und erfolgreiche Angriffstypen untereinander austauschen. Insbesondere Malware-as-a-Service-Angebote im Dark Web werden vermehrt genutzt, um Effizienz und Volumen von Angriffen zu steigern.

Gemeinsam mit Ihnen definieren wir eine individuell auf Ihren Endkunden zugeschnittene Phishing-Kampagne, führen diese über die Infinigate Awareness Plattform (powered by Keepnet) durch und stellen das aktuelle Sicherheitsbewusstsein transparent dar - vom einfachen Massenmail bis zum auf den einzelnen Benutzer zugeschnittenen Targeted Attack.

Auswertungen, Nachbearbeitung und die Ableitung von Folgeaktionen zur Anpassung der Awareness-Kampagne gehören selbstverständlich ebenfalls zum Leistungsumfang. Auch hier können wir Produkte unserer Hersteller (Barracuda, Hornetsecurity, Sophos) ergänzend einbinden.

Weitere Bausteine

Darüber hinaus bieten wir Ihnen weitere individuelle Möglichkeiten der Messung und Verbesserung der Security Awareness. Unter anderem decken wir folgende Themenbereiche ab:

- Awareness-Sprechstunde – regelmäßiger Austausch der Benutzer mit unseren zertifizierten Koordinatoren
- Smishing: Benutzer dazu bringen, auf einen Link in einer SMS zu klicken
- Vishing: Benutzer dazu bringen, auf einen Anruf oder eine Voicemail zu reagieren
- Quishing: Phishing über manipulierte QR-Codes, die klassische E-Mail-Filter umgeht
- USB: Benutzer dazu bringen, einen manipulierten USB-Stick anzustecken

Die Bedrohungslage 2026

Angreifer setzen zunehmend auf neue Vektoren, die klassische technische Schutzmaßnahmen umgehen:

- Quishing (QR-Code-Phishing) – rasant wachsend, umgeht E-Mail-Filter
- KI-generiertes Spear-Phishing – täuschend echte, personalisierte Angriffe in Sekunden
- Deepfake-Vishing – KI-generierte Stimmen imitieren Vorgesetzte oder Kollegen
- MFA-Fatigue – Nutzer werden mit Anfragen überflutet, bis sie aus Erschöpfung bestätigen
- Callback-Phishing – E-Mail verweist auf eine Telefonnummer statt auf einen Link und umgeht URL-Filter

NIS2 & Compliance: Seit Dezember 2025 fallen über 30.000 Unternehmen in Deutschland unter die erweiterten NIS2-Pflichten – die Geschäftsleitung haftet persönlich. Der globale Security-Awareness-Markt wächst auf rund 6,74 Mrd. USD (2026). Der durchschnittliche Schaden eines Sicherheitsvorfalls im KMU liegt bei rund 1,2 Mio. Euro. Nachweisbare Schulungen, dokumentierte Awareness-Maßnahmen und regelmäßige Phishing-Simulationen sind damit Pflicht - genau das liefert unser Security-Awareness-Prozess powered by Keepnet.

Kontakt

Sie interessieren sich für unsere Security Awareness Services powered by Keepnet?

Sprechen Sie uns an.
Wir beraten Sie individuell und erstellen Ihnen ein passendes Angebot.

Security Awareness
powered by
keepnet

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8,
85540 Haar/München

+49 89 89048-403
techservices@infinigate.de
www.infinigate.com/de

infinigate
spark your growth