Leistungsbestimmungen

Awareness Academy Leistungsbestimmungen

Im Folgenden finden Sie eine detaillierte Beschreibung der Leistungen, die im Rahmen der IT-Seal Awareness Academy eingesetzt werden können. Die Leistungsmodule, die nur in ausgewählten Pakten enthalten sind, sind mit entsprechenden Badges markiert. Zusätzlich buchbare Module sind mit „optional“ gekennzeichnet.

Lite | Basic | Professional | Premium

Detaillierte Beschreibung der Leistungsmodule

IT-Seal Awareness Engine

Basic | Professional | Premium

Die IT-Seal Awareness Engine bildet das technologische Herzstück für Ihre Awareness Academy im Auto-Piloten. Sie wertet regelmäßig das Sicherheitsverhalten Ihrer Teilnehmer:innen aus und entscheidet auf dieser Basis, welche Teilnehmergruppen wie weiter trainiert werden. Jede:r Teilnehmer:in erhält dadurch genau so viel Training wie nötig und gleichzeitig so wenig wie möglich.

Als Awareness-Kennzahl dient hierbei der „Employee Security Index“ (ESI®). Zu Beginn der Awareness Academy wird ein angestrebtes Sicherheitsniveau festgelegt (Ziel-ESI®). Basierend darauf entscheidet die IT-Seal Awareness Engine im jeweils dreimonatigen Zyklus bedarfsgerecht, welche Teilnehmergruppen welche weiteren Trainings-maßnahmen erhalten, bzw. welche Teilnehmergruppen pausieren können. Mögliche Trainingsmaßnahmen werden im weiteren Verlauf beschrieben und umfassen unter anderem Spear-Phishing-Simulationen, E-Training-Module, Kurz-videos, Awareness-Materialien, Präsenzschulungen und Online-Seminare.

Die IT-Seal Awareness Engine stellt darüber hinaus sicher, dass alle Teilnehmer:innen bedarfsgerecht trainiert werden. So bauen beispielsweise Spear-Phishing-E-Mails der IT-Seal Spear-Phishing-Engine in ihrem Schwierig-keitsgrad aufeinander auf. Sie werden von der IT-Seal Awareness Engine für jeden Teilnehmer:in, basierend auf seinem aktuellen Lernstand, individuell ausgewählt.

Der Ziel-ESI® unterscheidet sich je nach gebuchtem Paket: „Basic“ = 70, „Professional“ = 80, „Premium“ = 90. Im Paket „Lite“ ist die IT-Seal Awareness Engine nicht verfügbar.

IT-Seal Spear-Phishing-Engine

Lite | Basic | Professional | Premium

Die patentierte IT-Seal Spear-Phishing-Engine erlaubt das Versenden von Spear-Phishing-E-Mails in verschiedenen Schwierigkeits-Leveln.

Spear-Phishing-Simulationen sind besonders effektiv, um das Sicherheitsverhalten von Teilnehmer:innen zu verändern: Erstens kann durch die Erzeugung eines Effekts der „Selbsterfahrung“ das Mindset überwunden werden „Mich greift doch eh keiner an“. Zweitens bieten Phishing-Simulationen die Möglichkeit, kurze, relevante Lerninhalte in Form eines Nano-Learnings zu vermitteln: Auf der IT-Seal Erklärseite wird der Teilnehmer:in interaktiv aufgeklärt, wie er hätte erkennen können, dass diese E-Mail gefälscht war. Drittens ermöglicht eine Spear-Phishing-Simulation auf Basis der IT-Seal Spear-Phishing-Engine die Messung des aktuellen Employee Security Index (ESI®).

Die IT-Seal Spear-Phishing-Engine passt realitätsnahe Phishing-Szenarien automatisiert auf Ihr Unternehmen und Ihre Teilnehmer:innen an. Hierzu werden Spear-Phishing-E-Mails in verschiedenen Schwierigkeitsgraden versandt, bei denen unter anderem hochqualitatives Spear-Phishing (à la Emotet / QBot) mit der Simulation von gefälschtem internen E-Mail-Verkehr realisiert wird. Dazu nutzen wir unternehmens-spezifisch gefälschte Domains und nachgeahmte E-Mail-Signaturen. Zudem nehmen die Spear-Phishing-E-Mails Bezug auf die Position, den Fachbereich und die Branche des Empfängers. Es werden Dateianhänge und dynamische Phishing-Links mit verschiedenen Verschleierungstechniken eingesetzt. Die verwendeten Dateianhänge werden regelmäßig auf ihre Relevanz geprüft und umfassen momentan .docm und .xlsm. In der Testphase zu Beginn Ihres Projekts prüfen wir gemeinsam, welche Anhänge für Ihr Unternehmen geeignet sind. Selbstverständlich wird niemals Fremdsoftware durch unsere Anhänge installiert. Diese kommunizieren lediglich mit unserem Server, um das Öffnen des Anhangs zu registrieren.

Auch Spear-Phishing-E-Mails auf Basis von OSINT-Informationen sind möglich[1] (siehe „OSINT-Analyse & OSINT-Phishing“).

Die Engine wird dazu ständig durch aktuelle Angriffsszenarien erweitert, die automatisch in Ihre Awareness Academy integriert werden.

OSINT-Analyse & OSINT-Phishing[1]

Das Ziel der OSINT-Analyse ist es, die Online-Präsenz Ihres Unternehmens und der teilnehmenden Mitarbeiter:innen auf Informationen zu untersuchen, die Angreifer nutzen könnten. Die gefundenen Informationen werden anschließend von der IT-Seal Spear-Phishing-Engine für besonders ausgefeilte Angriffssimulationen genutzt.

Lite | Basic | **Professional** | Premium

Unternehmens OSINT

Für das Unternehmens OSINT können zum einen Unternehmensprofile auf dem Arbeitgeber-Bewertungsportal kununu (kununu.com) automatisiert nach Benefits für Mitarbeiter:innen durchsucht werden. Zum anderen ist es möglich auch weitere, öffentlich zugängliche Quellen (z.B. Webseite oder Social Media) zu verwenden, um Informationen zu den Benefits zu erhalten. Die gefundenen Benefits, wie z.B. Mitarbeiterrabatte, Home-Office oder Kantine werden dann in realitätsgetreuen Spear-Phishing-Simulationen eingesetzt.

[1] OSINT-Phishing ist ausschließlich auf Deutsch verfügbar.

Lite (optional) | Basic (optional) | Professional (optional) | Premium

Mitarbeiter OSINT

Für den Angriffspotential-Check durchsucht IT-Seal ausschließlich öffentlich zugängliche Quellen, die überwiegend beruflich genutzt werden. Die gefunden Informationen werden im Rahmen der Angriffspotential-Analyse bewertet und eine zusammenfassende Bewertung der Angriffsfläche erstellt.

In die Suche werden folgende Quellen einbezogen:

- Linkedin.com
- Xing.com

Ausdrücklich ausgeschlossen von der Durchsuchung durch IT-Seal, sind öffentlich zugängliche Datenquellen, die weniger zu beruflichen, als überwiegend zu privaten Zwecken genutzt werden oder sonst der Privatsphäre zuzuordnen sind. Insbesondere - aber nicht abschließend – werden Informationen der folgenden Internetseiten nicht genutzt:

- Facebook.com
- Instagram.com
- Twitter.com

Weiterhin ist die Erhebung oder Auswertung von Daten im Sinne von § 9 Abs. 1 DSGVO explizit ausgeschlossen.

Die Durchsuchung der vorgenannten öffentlich zugänglichen Quellen nach Informationen beinhaltet im Wesentlichen teilnehmerbezogene Daten, z. B. die Anzahl der Kontakte, ehemalige Arbeitgeber, Interessen, Wissen und Hobbys.

Die Einzelinformationen, die IT-Seal aus der Durchsuchung der öffentlich zugänglichen Quellen gewinnt, werden ausdrücklich nicht an den Auftraggeber weitergegeben, soweit nicht in der Berichtserstattung dargestellt.

Die Ergebnisse der Datensuche werden abstrahiert und für individualisierte Angriffe aufbereitet.

Spear-Phishing E-Mails: Level 1–3

Lite | Basic | Professional | Premium

Die Level der Spear-Phishing-E-Mails basieren auf standardisierten Einteilungen: je höher das Level, desto höher der Zeitaufwand eines Angreifers. Die automatisierte Auswahl der Spear-Phishing-Mails erfolgt über individuelle Personen-, Abteilungs-, Unternehmens- und Branchen-Szenarien. Sie nutzen, genau wie echte Angreifer, potenziell gefährliche Links, gefälschte Login-Seiten, Makros und verschlüsselte Dateianhänge.

Vorschlagssystem für neue Szenarien

Lite | Basic | Professional | Premium

Entwickeln wir die IT-Seal Spear-Phishing-Engine gemeinsam weiter, indem Sie uns Ihre Ideen für Phishing-Szenarien für Ihr Unternehmen oder Ihre Branche nennen. Unsere Phishing-Experten prüfen alle Vorschläge auf Umsetzbarkeit und Schwierigkeitslevel.

Aus den eingereichten Vorschlägen sowie aus aktuellen, im Umlauf befindlichen Angriffen werden jeden Monat neue Phishing-E-Mails umgesetzt und automatisch in Ihre Awareness Academy integriert.

Individuelle Spear-Phishing-Mails

Lite (optional) | Basic (optional) | Professional (optional) | Premium

IT-Seal erstellt für Ihr Awareness-Training individuelle Phishing-Mails, die nach Ihrem Wunsch konzipiert sind. Im Paket „Premium“ sind drei individuell für Ihre Organisation umgesetzte Phishing-E-Mails inklusive. In allen anderen Paketen ist diese Leistung optional buchbar.

IT-Seal Erklärseite: Most Teachable Moment

Lite | Basic | Professional | Premium

Wir liefern relevante Lerninhalte, wenn die Lernbereitschaft am größten ist – nämlich in dem Moment, wenn der Teilnehmer:in auf eine Phishing-Mail hereingefallen ist!
Auf der interaktiven Erklärseite, mit individuellen Trainingsinhalten zu der gerade simulierten E-Mail, wird in einem Nano-Learning vermittelt, wie ein echter Angriff hätte erkannt und abgewehrt werden können. Dabei werden sowohl eindeutige Erkennungszeichen sowie psychologische Tricks der Angreifer aufgezeigt.

Branding inklusive: Standardmäßig wird Ihr Logo auf der Erklärseite angezeigt, um das Vertrauen der Nutzer in die Seite zu stärken.

Gefälschte Loginseiten

Lite | Basic | Professional | Premium

Beim Credential-Phishing wird mittels nachgebauter Anmeldeseiten geprüft, wie viele Teilnehmer:innen Ihre Zugangsdaten auf einer gefälschten Webseite eingeben. Während unserer Phishing-Simulation werden dabei selbstverständlich nie Login-Daten an unsere Server übermittelt! Bei allen Paketen ist die Nutzung der drei Default-Login-Seiten, angelehnt an Microsoft Login, SAP Netweaver und Dropbox, enthalten.

Optional ist die Erstellung einer kundenspezifischen Login-Seite, basierend auf einer HTML-Vorlage, buchbar.

Reporter Outlook-Add-In

Lite | Basic | Professional | Premium

Der IT-Seal Reporter Button ist ein Outlook-Add-In für Desktop und Mobil. Er vereinfacht den Meldeprozess für reale Angriffe und liefert gleichzeitig positive Rückmeldung für korrekt erkannte Phishing-Simulationen. Der interne IT-Support wird durch unterstützende Informationen und automatisierte Antwortprozesse entlastet. Im Awareness Manager kann eingesehen werden, wie viele der simulierten Phishing-E-Mails von Mitarbeiter:innen gemeldet wurden. Der Reporter Button ist auf Deutsch u. Englisch verfügbar.

Technische Voraussetzung für die Nutzung: Outlook-Client-Version ab 2021, Outlook Retail Lizenz bereits ab 2019, Exchange Online / Office 365 sowie Outlook Web Access, Outlook für Macintosh und Mobile.

E-Training Module

Lite (optional) | Basic | **Professional** | Premium

Die IT-Seal E-Trainings vermitteln Teilnehmer:innen unterhaltsam, anschaulich und verständlich Grundinhalte zu verschiedenen Themen der IT-Security Awareness.

In den Trainings liegt der Fokus auf Inhalten, die auch von technischen Laien im Alltag direkt erkannt und umgesetzt werden können. Zu jedem Thema stehen 1-3 Lernmodule, in Form eines interaktiven E-Trainings, Kurzvideos oder PDF's, zur Verfügung. Zusätzlich bieten wir Auffrischungsmodule an, um bereits absolvierte Inhalte bei den Teilnehmer:innen wieder ins Gedächtnis zu rufen.

- **Interaktive E-Trainings** sind immer in mehrere Module à 2 bis 10 Minuten gegliedert (ausgenommen Datenschutz; das Modul hat einen Umfang von ca. 20 Minuten). Der Fortschritt wird dabei gespeichert, sodass jedes Modul vom Teilnehmer:in am Stück oder in mehreren Sitzungen bearbeitet werden kann.
- In den **Kurzvideos** wird in 60 bis 90 Sekunden die Motivation der Lernenden adressiert und gesteigert sowie einzelne Lernziele wiederholt und vertieft.
- Unsere **PDF's** enthalten unterstützende Informationen zu den E-Trainings, die Ihre Mitarbeiter:innen für den Schnellzugriff abspeichern oder auch ausdrucken können.
- Um das Wissen Ihrer Mitarbeiter:innen auffrischen zu können, bieten wir Auffrischungsmodule, sogenannte **Memo-Rays** an. Diese fassen Lerninhalte zu bereits absolvierten Trainings kurz und anschaulich zusammen.

Neben den klassischen E-Trainings bieten wir in unserem Trainingsportfolio auch Quizze zur Kenntnisprüfung an – diese heißen bei uns Quick-Checks. Quick-Checks werden im Nachgang zu einem Training ausgerollt und sollen eine spielerische Überprüfung des eigenen Kenntnisstands ermöglichen und Konzepte auffrischen, die drohen in Vergessenheit zu geraten.

Die Sprachenverfügbarkeit der E-Training-Module ist im Anhang dargestellt.

Die Pakete „Basic" „Professional" und „Premium" enthalten alle Inhalte, die bei IT-Seal zur Verfügung stehen.
Im Paket „Lite" sind die E-Training-Module optional buchbar.

Lerninhalte können entweder über den Security Hub von IT-Seal oder in einem eigenen LMS ausgerollt werden.

Awareness Material

Lite (optional) | Basic (optional) | **Professional** | Premium

Ziel der Awareness-Materialien ist es, die Aufmerksamkeit der Teilnehmer:innen im Alltag immer wieder auf wichtige Verhaltensregeln der IT-Sicherheit zu lenken. Zu Beginn einer Awareness Academy erhalten Sie daher, abhängig von der Anzahl der Teilnehmer:innen, ein Paket von Awareness-Plakaten.

Mit Hilfe der Awareness-Materialien, wie Poster und Flyer, kann ein Grundbewusstsein erreicht und somit die Aufmerksamkeit im Alltag erhöht werden. Awareness-Materialien sind ausschließlich auf Deutsch verfügbar.

Online-Seminar

Lite (optional) | Basic (optional) | **Professional** | Premium

Unsere Erfahrungen haben gezeigt, dass ergänzende Schulungen in vielen Fällen ein effektives Mittel sind, um Wissen zu vermitteln und das Sicherheitsverhalten dauerhaft zu verbessern.

In Online-Seminaren erhalten Teilnehmer:innen mit besonderem Schulungsbedarf von unseren Awareness Consultants die Grundlagen sicheren Verhaltens am Arbeitsplatz vermittelt. Dabei wird darauf eingegangen, welche Rolle der Teilnehmer:in in der IT-Sicherheit spielt, wie Angreifer vorgehen (inkl. Live Phishing), woran man Angriffe erkennt und wie man sich schützen kann.

Eine Social Engineering Awareness Schulung umfasst ein Online-Seminar à 60 Minuten. Die Anzahl der Teilnehmer:innen ist dabei grundsätzlich unbeschränkt. Online-Seminare sind in deutscher und englischer Sprache verfügbar.

Präsenzschulung

Lite (optional) | Basic (optional) | **Professional (optional)** | Premium

Unsere Präsenzschulungen bieten den Teilnehmer:innen im Gegensatz zu Online-Seminaren die Möglichkeit, im geschützten Umfeld Fragen zu stellen. Unsere Awareness Consultants können dann noch individueller auf die Teilnehmer:innen eingehen.

In Präsenzschulungen erhalten Teilnehmer:innen mit besonderem Schulungsbedarf von unseren Awareness Consultants die Grundlagen sicheren Verhaltens am Arbeitsplatz vermittelt. Dabei wird darauf eingegangen, welche Rolle der Teilnehmer:in in der IT-Sicherheit spielt, wie Angreifer vorgehen (inkl. Live Phishing), woran man Angriffe erkennt und wie man sich schützen kann.

Zu Beginn erhält jeder Teilnehmer:in Schulungsunterlagen und nach Abschluss des Workshops ein Zertifikat. Die Anzahl der Teilnehmer:innen ist auf 20 Personen pro Schulungstermin beschränkt. Präsenzschulungen sind ausschließlich in Deutschland, in deutscher oder englischer Sprache, verfügbar. IT-Seal entscheidet im Einzelfall, ob eine Präsenzschulung oder ein Online-Seminar für die Projektsituation am geeignetsten ist.

Individuelles Branding: Auf Ihr Unternehmen angepasst

Lite | Basic | **Professional** | Premium

Die Anpassung der Lerninhalte an Ihr Unternehmens-Branding stärkt das Image bei den Teilnehmer:innen und steigert das Vertrauen in die Inhalte.

Dazu passen wir auf Wunsch den Security Hub inkl. der E-Training-Module und die Awareness-Materialien an Ihre Corporate Identity an und übernehmen Farben und Logo.

Individuelle Konfiguration: Auf Ihre Mitarbeiter:innen angepasst

Lite | Basic | Professional | Premium

Konfigurieren Sie das Awareness-Training nach Ihren individuellen Vorstellungen oder ergänzen Sie eigene Inhalte: Von der Anzahl der simulierten E-Mails (Phishing-Intensität), bis hin zu individuellen Textelementen in Ihren E-Trainings.

Sprachen

Lite | Basic | Professional | Premium

Unsere **Phishing Simulation** ist in den folgenden Sprachen verfügbar:

- Deutsch, Schweizerdeutsch, Chinesisch, Englisch, Französisch, Holländisch, Italienisch, Polnisch, Portugiesisch, Rumänisch, Slowakisch, Spanisch, Tschechisch, Türkisch, Ungarisch

Die IT-Seal **Erklärseite** ist in den folgenden Sprachen verfügbar:

- Deutsch, Arabisch, Chinesisch, Dänisch, Englisch, Französisch, Hindi, Holländisch, Italienisch, Japanisch, Kroatisch, Norwegisch, Polnisch, Portugiesisch, Rumänisch, Russisch, Schwedisch, Slowakisch, Spanisch, Tschechisch, Türkisch, Ungarisch

Der **Security Hub** ist in den folgenden Sprachen verfügbar:

- Deutsch, Chinesisch, Englisch, Französisch, Italienisch, Polnisch, Portugiesisch, Rumänisch, Spanisch, Tschechisch, Türkisch, Ungarisch

Der **Awareness Manager** ist in den folgenden Sprachen verfügbar:

- Deutsch, Englisch

In den Paketen sind alle verfügbaren Sprachen inklusive.

Die für die E-Training Module verfügbaren Sprachen, entnehmen Sie bitte aus dem Anhang „E-Training Module“. Hier sind in allen Paketen alle verfügbaren Sprachen inklusive.

Administration und Setup

Lite | Basic | Professional | Premium

Ihr persönlicher Awareness Consultant unterstützt Sie bei der erfolgreichen Einrichtung Ihres Security Awareness Programms. Dazu gehört die interne Kommunikation mit den Stakeholdern (Datenschutzbeauftragter, Personal- oder Betriebsrat, IT-Support, Teilnehmer:innen, Geschäftsleitung), die Konfiguration des Projekts, Unterstützung beim Whitelisting und Test-E-Mails sowie verschiedene Materialien zur internen Ankündigung und datenschutzfreundlichen Umsetzung des Projekts.

Security Hub

Lite | Basic | Professional | Premium

Der Security Hub fasst die persönlichen Lerninhalte der Mitarbeiter:innen zentral und bequem an einem Ort zusammen. Mitarbeiter:innen werden automatisch eingeloggt und müssen sich keine Zugangsdaten merken. Sie erhalten dort Zugriff auf ihre gebuchten und zugewiesenen E-Trainings und andere Lerninhalte. Der Security Hub speichert alle Zwischenstände der Trainings und die Mitarbeiter:innen können auch bereits abgeschlossene Lerninhalte jederzeit anschauen. Mitarbeiter:innen können außerdem eine personalisierte Auswertung über die erhaltenen Phishing-Mails von IT-Seal einsehen. Der FAQ-Bereich versorgt die Mitarbeiter:innen zusätzlich mit Informationen aus unserer Wissensdatenbank. Mitarbeiter:innen können über den Security Hub ihr Widerspruchsrecht wahrnehmen und flexibel anpassen.

Live-Dashboard: Awareness Manager

Lite | Basic | Professional | Premium

Über den IT-Seal Awareness Manager erhalten Sie Zugang zu einem Dashboard, das Ihnen jederzeit Einblick in den aktuellen Stand der Simulations- und Trainingsfortschritte und in das aktuelle Sicherheitsverhalten der Teilnehmer:innen gibt.

Im Awareness Manager können Sie in einer gesicherten Umgebung die Phishing- und E-Training-Ergebnisse einsehen, den aktuellen ESI® auf Unternehmens- und Gruppen-Ebene auswerten, sowie auf verschlüsseltem Wege Dateien austauschen. Zusätzlich gibt es eine Whitelisting-Anleitung inkl. interaktivem Whitelisting-Test. Sie können außerdem eine Phishing-Übersicht für den IT-Support freischalten, wo dieser prüfen kann, ob eine als Angriff gemeldete Nachricht Teil unserer Phishing-Simulationen ist oder nicht.

Zusammenfassung der Ergebnisse und Handlungsempfehlungen in regelmäßigen Berichten

Lite | Basic | Professional | Premium

Ergänzend zur Live-Einsicht im IT-Seal Awareness-Manager werden im Abstand von 3 Monaten Zwischenberichte erstellt und von Ihrem persönlichen Awareness Consultant vorgestellt. Darin enthalten sind Auswertungen nach Nutzergruppen, die Entwicklung des ESI® über die Zeit und konkrete Handlungsempfehlungen für Ihr Unternehmen.

Die Ergebnisse werden dabei auf die einzelnen Gruppen aufgeschlüsselt, nicht jedoch auf einzelne Teilnehmer:innen.

Tiefgehende Analyse und Interpretation der Ergebnisse

Professional | Premium

Ihr Awareness Consultant sichtet die Ergebnisse detailliert und erarbeitet tiefgehende Einblicke zum Teilnehmerverhalten, dem Umgang mit gefälschten Login-Seiten, der Evaluation der Führungskräfte, zu besonders effektiven psychologischen Tricks sowie einen Branchen-Benchmark.

Bei der Buchung einer OSINT-Analyse (Professional (Optional), Premium) wird dargestellt, wie stark die Teilnehmergruppen in den öffentlich zugänglichen Quellen präsent sind.

Berichte für Geschäftsleitung

Professional | Premium

Als IT-Sicherheitsverantwortlicher ist es wichtig, Ihre Ansprechpartner kurz und präzise zu informieren, wie sich das Sicherheitsniveau aktuell entwickelt und welche Fortschritte Sie erzielen konnten.

Für das Reporting an die Geschäftsleitung/den Vorstand wird von Ihrem persönlichem Awareness Consultant im Abstand von 3 Monaten ein angepasster Bericht mit den Ergebnissen & Fortschritten sowie konkreten nächsten Schritten vorbereitet.

Berichte für Teamleiter und Führungskräfte

Premium

Teamleiter und Führungskräfte gelten als Multiplikatoren für die Sicherheitskultur bzw. können sie diese auch komplett untergraben. Um das Potential der Führungskräfte zu nutzen und die Sicherheitskultur zu stärken, erstellt Ihr Awareness Consultant jeweils gesonderte Berichte für die Teamleiter der Gruppen mit besonderem Nachholbedarf. Hierbei werden sowohl die Abteilungs-Ergebnisse als auch konkrete Tipps zur Kommunikation mit den Teammitgliedern zur Verfügung gestellt.

Unternehmenszertifikat als Nachweis für Auditierung nach ISO 27001

Lite | Basic | Professional | Premium

Sie erhalten ein Unternehmenszertifikat, das als Nachweis für Sicherheitsaudits (ISO27001, TISAX, BSI IT-Grundschutz, …) und für Kunden dienen kann.

Schriftlich fixierte Ordnung

Lite (optional) | Basic (optional) | Professional (optional) | Premium

Um den Anforderungen von Auditoren zu entsprechen, liefern wir Ihnen eine Vorlage zur schriftlich fixierten Ordnung für Ihr Organisationshandbuch. Hier wird dokumentiert, wann und wie das Sicherheitsverhalten trainiert wird, und welche Maßnahmen bei einer Teilnehmergruppe mit besonderem Nachholbedarf ergriffen werden.

CISO-Workshop zur Sicherheitskultur

optional

Gemeinsam mit einem erfahrenen Spezialisten wird bei Bedarf einmal jährlich ein Workshop durchgeführt, bei dem aktuelle Herausforderungen an die Sicherheitskultur besprochen und weitere Handlungsempfehlungen zur Steigerung der Sicherheitskultur erarbeitet werden.

Verunreinigte Datenspeicher (USB-Sticks)

Lite (optional) | Basic (optional) | Professional (optional) | Premium

IT-Seal präpariert USB-Sticks mit einer manipulierten Datei und misst, wie oft die Datei geöffnet wird. Die USB-Sticks können per Post an, von dem Auftraggeber ausgewählte, Personen/Postfächer zugesandt werden. Alternativ werden sie dem Auftraggeber von IT-Seal bereitgestellt, um von diesem vor Ort eigenhändig platziert zu werden. Die Inklusivleistung in „Premium“ umfasst pro Quartal 15 USB-Sticks für je 500 gebuchte Mitarbeiter:innen. In den anderen Paketen können Staffelungen von je 15 USB-Sticks gebucht werden.

Telefon Phishing-Kampagne (Vishing)

Lite (optional) | Basic (optional) | Professional (optional) | Premium

Vishing steht für “Voice Phishing” und wird vermehrt von Kriminellen genutzt, um zusätzlichen Druck und Stress aufzubauen – beispielsweise beim CEO-Fraud. Wir simulieren diesen Angriffsweg, um Ihnen zu helfen, Schwachstellen im Sicherheitskonzept Ihres Unternehmens zu entdecken. Bei Bedarf schulen wir Ihre Mitarbeiter:innen, um diese Schwachstellen zu schließen.

Wie ein realer Angreifer, simulieren wir Angriffe per Telefon und prüfen beispielsweise:

- ob Mitarbeiter:innen Zugangsdaten und Passwörter weitergeben
- ob Mitarbeiter:innen sich verleiten lassen, Software zu installieren oder Dateien zu öffnen
- ob Mitarbeiter:innen persönliche Daten von sich oder ihren Kollegen weitergeben

Die Inklusivleistung bei „Premium“ umfasst pro Quartal für je 1.000 gebuchte Mitarbeiter:innen 20 Anrufe an ausgewählte Zielpersonen. In den Paketen Lite, Basic und Professional können unsere Vishing Anrufe optional gebucht werden. Die Wählversuche beschränken sich auf eine Anzahl von 4 Versuchen pro Anruf. Die Aufklärung nach einem Vishing-Anruf ist optional. Hierbei lösen wir die Situation auf und bestätigen das Verhalten oder geben Tipps zum korrekten Umgang mit Vishing.

Social Engineering-Begehung

Lite (optional) | Basic (optional) | Professional (optional) | Premium

Bei der Social Engineering-Begehung handelt es sich um eine Vor-Ort-Begehung beim Kunden. Ein Social-Engineering-Spezialist führt eine Überprüfung des Kundenobjektes durch und prüft das technisch organisatorische Sicherheitskonzept des Kunden. Dabei wird, von außen nach innen, systematisch nach möglichen Schwachstellen gesucht, die ein Social Engineer nutzen könnte, um sich Zugang zum Unternehmen und danach Zugang zu Sicherheitsbereichen, der EDV, der Produktion oder anderen neuralgischen Bereichen zu verschaffen.

Die Vor-Ort-Begehung dauert ca. 6-8 Stunden. Nach der Durchführung der Begehung erstellt der Ausführer der Social Engineering-Begehung einen Bericht über die identifizierten möglichen Schwachstellen und gibt Handlungsempfehlungen. Sollte es sich um mehr als ein Objekt handeln oder sollte dieses Objekt zu groß für eine Tagesbegehung sein, wird eventuell ein weiterer Tag notwendig sein.

Die Social Engineering-Begehung ist im „Premium“-Paket ab 30 Mitarbeiter:innen einmal jährlich inklusive.

Social Engineering Penetrationstest

Lite (optional) | Basic (optional) | **Professional (optional)** | Premium (optional)

Ziel des Penetrationstests ist die Betrachtung der physischen sowie technisch-organisatorischen Sicherheitsmaßnahmen eines Objektes aus der Sicht eines Angreifers. Mögliche identifizierte Schwachstellen werden mit einem simulierten Angriffsszenario auf die Verwundbarkeit überprüft.

Das Ergebnis des Penetrationstests wird Ihnen in einem Bericht präsentiert. Die Ergebnisse sind anonymisiert, sodass weder Namen noch Fotos von Personen auftauchen.

Unser Vorgehen

Der Ansatz zur physischen Social Engineering Penetration gliedert sich in vier Phasen:

1. OSINT (Open Source Intelligence) & grundlegende Erkundung

Die Phase OSINT & grundlegende Erkundung hat den Zweck, einen grundsätzlichen Überblick über die möglichen Angriffsobjekte und mögliche Methoden eines Angriffs zu geben. Ziel der Phase ist es, dass sowohl geeignete Zugänge zum Zielobjekt gefunden werden, als auch eine Angriffsmethode bestimmt werden kann, sodass in der folgenden Phase die Detailplanung beginnt.

Wir führen OSINT wie folgt durch:

- Auswertung der, durch den Kunden bereitgestellten, Informationen auf den eigenen Webseiten, Blogs, Sozialen Medien etc.
- Identifizierung von Mitarbeiter:innen der Zielorganisation in geschäftlichen, sozialen Netzwerken
- Sammlung von Zeitungsartikeln über aktuelle Themen, Rahmenverträge, Events und Kampagnen der Organisation
- Recherche nach externen Firmen, zur Unterstützung der Zielorganisation (Zulieferer, Technischer Support, Facility Management etc.)

Wir führen die grundlegende Erkundung wie folgt durch:

- Erkundung des Umfelds möglicher Zielobjekte und Zugänge
- Erkundung des Nahbereichs, mit Dokumentation der Infrastruktur und Sicherheitsmaßnahmen am Objekt
- Legendierte Begehung der Zielobjekte
- Observation der geeigneten Zielobjekte, mit dem Ziel, Informationen über den Tagesablauf zu erhalten (Wo verbringen die Kollegen gemeinsam ihre Pausen, ihren Feierabend, Lieferdienste, Reinigungspersonal, Wartungsfirmen etc.)
- Dokumentierte Ansprache möglicher Zielpersonen

2. Spezifische Erkundung & Aufklärung

Die Phase Spezifische Erkundung & Aufklärung bildet den Schwerpunkt der Vorbereitungen. Hier wird spezifisch für die ausgewählte Methode erkundet sowie am und im Objekt aufgeklärt. Mögliche Zugänge werden erkannt und dokumentiert. Sofern von der Anriffsmethode gefordert, werden Verbindungen zu Personen aufgebaut.

Mögliche Angriffsmethoden:
(Wünsche/Einschränkungen können hierbei nach Absprache berücksichtigt werden)

Person:

- Identifizierung von Zielpersonen
- Ansprache und Kontaktaufbau
- Gemeinsamkeiten schaffen (Rapport)
- Legende aufbauen

Drittfirma:

- Identifizierung der Firma
- Legendierte Ansprache der Drittfirma
- Informationen sammeln (Namen, Zutrittsberechtigung, Ablauf beim Inprocessing)
- Abfotografieren der Arbeitskleidung etc.

Eigeninfiltration:

- Legende als Drittfirma
- Anzeige aufgeben
- Als Bewerber auftreten
- Als Paketdienst auftreten
- Auskunft erbitten
- u.v.m.

Autorisierter Zugang:

- Durch Anbahnung von Mitarbeiter:innen den Zugang bekommen
- Legendiert den Zugang einfordern (Bsp. Arbeitssicherheitsüberprüfung)
- Internet stören und als Internet /Teletechniker ausgeben
- Gefälschte Zutrittsberechtigung nutzen

3. Angriff

Der Angriff erfolgt auf Grundlage der, in den vorangegangenen Phasen gewonnenen, Erkenntnisse. Zu diesem Zeitpunkt sind das genaue Vorgehen sowie die Ziele, Personen, Zeiten und Gewohnheiten bekannt.

Folgende Besonderheiten sind während des Angriffs zu berücksichtigen:

- Kaum ein Angriff lässt sich zu 100% planen. Daher ist die Kreativität des Testers sowie Flexibilität gefragt.
- Die Angriffe werden auf Wunsch mit Kameras dokumentiert, um später Informationen aus Gesprächen und dem Videomaterial zu generieren.
- Hoch eingestufte und interne Informationen der Zielorganisation können nach Absprache genutzt werden.

Der Angriff kann, je nach verwendeter Methode, auf verschiedene Weisen unterstützt werden.
Hierzu zählen:

- Abhörtechniken (nach Absprache)
- Auslesetechniken (nach Absprache)
- Falschaussagen
- Stören von Internetverbindungen mit Hilfe von Jammern (nach Absprache)

4. Auswertung, Darstellung & Schulung

Die Phase Auswertung, Darstellung & Schulung bildet den Abschluss des Penetrationstests. In einem internen Prozess wird die Durchführung des Angriffs mit der Planungsgrundlage abgestimmt und mit den Ergebnissen anderer Tests verglichen. Dem Kunden wird eine Dokumentation der Arbeitsschritte vorgelegt. Die Darstellung erfolgt gegenüber dem Kunden umfassend, unter der Prämisse, dem Auftraggeber ein detailliertes Bild von der erkannten Situation liefern zu können.

Unsere Maßstäbe in der Phase Auswertung, Darstellung & Schulung

Auswertung:

- Jeder Angriff wird in einer Situationsbeschreibung schriftlich dokumentiert
- Alle identifizierten Schwachstellen werden bewertet
- Jedes Objekt wird zusätzlich einzeln bewertet
- Erkundung = Angriff
- Psychologische Bewertung der ausgenutzten menschlichen Schwächen

Darstellung:

- Der Report wird, soweit nicht anders besprochen, ohne die Angabe von Namen der getesteten Zielpersonen an den Kunden übergeben
- Bild und Tonmaterial wird nach dem Test vernichtet, kann aber auf Wunsch vorher von dem Kunden eingesehen werden
- Auf Wunsch des Kunden, werden die Ergebnisse des Penetrationstest als Vortrag präsentiert

Schulung: Halbtages-Workshop nach Abschluss der Tests (optional)

In einem abschließenden Halbtages-Workshop werden die Lehren des Penetrationstests mit einem zu bestimmenden Personenkreis besprochen und weitere Schlüsse/Maßnahmen diskutiert.

Vertrag zur Auftragsdatenverarbeitung

In Ergänzung zu dem vorliegenden Angebot schließen die Parteien einen Vertrag, welcher die datenschutzrechtliche Auftragsdatenverarbeitung regelt.

Individuelle Opt-Out-Lösungen

Lite | Basic | **Professional** | Premium

Um die Prozesse datenschutzfreundlich zu gestalten, haben Ihre Mitarbeiter:innen diverse Möglichkeiten, um bestimmten Maßnahmen zu widersprechen. Dadurch erhalten Sie die Möglichkeit, jede:n Teilnehmer:in individuell und wunschgerecht abzuholen und möglichen Bedenken entgegenzuwirken.

Referenz

Der Auftraggeber genehmigt, dass sein Name als Referenzkunde genannt und sein Logo auf der Internetseite von IT-Seal als Referenz verwendet werden dürfen.

Datenschutz, Schweigepflicht

Die Parteien sind sich einig, dass der Schutz der Mitarbeiter:innen eine zentrale Rolle spielen muss. An den Auftraggeber werden anonymisierte Ergebnisse und Daten übermittelt. Die Informationen, die während der Social Engineering-Awareness Maßnahmen gesammelt werden, werden abstrahiert gespeichert.

Der Auftraggeber verpflichtet sich, alle ihm in Nutzung dieses Angebotes zur Verfügung gestellten Arbeitsdokumente nur für den unternehmensinternen Gebrauch einzusetzen, nicht an Dritte weiterzugeben und keine Inhalte, die den Angebotsgegenstand betreffen, in irgendeiner Form an Dritte zu vermitteln.

Anhang: Content Auflistung unserer Sprachenverfügbarkeit

E-Training Module

Thema	Anzahl Module	Sprachen (ISO-639-1)	Sprachen - geplant
IT und ich: Einführung	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Social Engineering	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
E-Mail-Sicherheit	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Passwörter und Authentisierung	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Soziale Medien	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Vishing (Telefon-Phishing)	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Sicher im Home-Office	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Datenschutz	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Schutzklassen	2	DE, EN	FR
Vorfälle melden	3	DE, EN	FR
Mobile Sicherheit	2	DE, EN	FR
Informationssicher im Internet	2	DE, EN	FR
Reporter Button	1	DE, EN	
Makros	1	DE, EN, FR[2]	
Gefälschte Login-Seiten	1	DE, EN, FR[2]	
Als Führungskraft Informations-sicherheit vorleben	1	DE, EN, FR[2]	

[2] Französische Untertitel

Quick-Checks

Thema	Sprachen (ISO-639-1)	Sprachen - geplant
IT und ich	DE, EN	
Passwörter und Authentisierung	DE, EN	
Schutzklassen	DE, EN	
E-Mail-Sicherheit	DE, EN	

Memo-Rays (Auffrischungsmodule)

Thema	Sprachen (ISO-639-1)	Sprachen - geplant
Vishing	DE, EN	
Phishing	DE, EN	