IT-SEAL
Social Engineering Analysis Labs

IT SECURITY
MADE IN GERMANY

Awareness Academy

Gemeinsam zur nachhaltigen Sicherheitskultur

Portfolio & Insights

demo.it-seal.de
Anmeldung zu Ihrer persönlichen Phishing Awareness-Simulation und Ihrem E-Learning-Testzugang

Made with ♡ in Security Valley Darmstadt

Awareness Academy

 # Patentierte Spear-Phishing-Engine: *OSINT-Phishing auf Basis öffentlich zugänglicher Informationen*

 # Awareness-Engine: *Individuelles Lernen im Autopiloten mit Hilfe des Ziel-ESI®*

 # ESI®: *Konkrete Kennzahl durch wissenschaftlichen Ansatz*

 # Bedarfsgerechtes Training: *Steigende Schwierigkeitsgrade ohne Frusterlebnis*

Ein einfacher und effektiver Workflow für die Sensibilisierung Ihrer Mitarbeiter.

9 von 10 Cyberangriffen starten mit einer Phishing-Mail und daher auch mit einem getäuschten Mitarbeiter. Als Sicherheitsverantwortlicher stehen Sie vor der Herausforderung, das Sicherheitsrisiko „Mensch" zu minimieren. Mit der IT-Seal Awareness Academy setzen Sie ganz unkompliziert und vor allem dauerhaft einen Haken an das Thema Security Awareness. Sie definieren das gewünschte Ziel-Sicherheitsniveau über den Employee Security Index (ESI®) und wir kümmern uns um den Rest.

Das kontinuierliche Trainingsprogramm beinhaltet dabei vielfältige Methoden, um unsensibilisierte Mitarbeiter effektiv zu erreichen: Von der Phishing-Simulation über E-Learnings, Kurzvideos und Online-Seminare bis hin zu Awareness-Materialien und Hinweisen am Arbeitsplatz. Das Ergebnis der Awareness Academy sind aufgeklärte Mitarbeiter, die ihre Verantwortung für die Sicherheit des Unternehmens kennen und wahrnehmen.

4 Schritte zum sicheren Mitarbeiter

Schritt 1: Lösung auswählen

- **Lite:** 4-wöchige oder dauerhafte Ist-Analyse zur Ermittlung Ihres ESI®
- **Basic, Professional und Premium:** Sie definieren Ihr gewünschtes Ziel-Niveau, wir kümmern uns um das Awareness-Training

Schritt 2: Interne Ankündigung

- Mitarbeiter, Betriebsrat und andere Stakeholder informieren
- Gerne helfen wir Ihnen mit vorgefertigten Info-Materialien und persönlichen Meetings dabei

Schritt 3: Teilnehmer hochladen

- Aus Datenschutzgründen werden die Mitarbeiter von Ihnen in Gruppen zusammengefasst
- Anschließend laden Sie die Teilnehmerlisten in einem gängigen Format hoch

Schritt 4: Zurücklehnen und steigenden ESI® beobachten

- Wir kümmern uns im Full-Service um das Training Ihrer Mitarbeiter
- Sie können das steigende Sicherheitsniveau bequem im Dashboard des Awareness Managers verfolgen

- **Transparenz:** Ihr aktuelles Sicherheitsniveau ist jederzeit im Dashboard einsehbar.
- **Nachhaltigkeit:** Sie erhalten ein dauerhaft hohes Sicherheitsniveau durch eine aktiv gelebte Sicherheitskultur.
- **Up-to-Date:** Unsere Trainingsmethoden basieren auf aktuellen wissenschaftlichen Erkenntnissen.
- **Mitarbeiterfreundlich:** Mit einer transparenten Kommunikation binden wir Mitarbeiter und Betriebsräte früh ein.
- **Planbar:** Die Investition in das Sicherheitsbewusstsein Ihrer Mitarbeiter ist vorab planbar und stets unter Kontrolle.

Dauerhaftes Training in vier Ausführungen

Security Awareness ist ein kontinuierlicher Prozess – genau wie unsere monatlich kündbaren Awareness-Lösungen.

Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Lite	**Basic**	**Professional**	**Premium**
ESI®-Messung	**Ziel-ESI®: 70**	**Ziel-ESI®: 80**	**Ziel-ESI®: 90**
Lernen Sie uns und Ihr Sicherheitsniveau kennen, um ein Bewusstsein für Awareness zu schaffen.	**Preiswertes, standardisiertes und von Profis entwickeltes Security-Awareness-Training.**	**Hochqualitatives, individuell auf den Nutzer zugeschnittenes Security-Awareness-Training.**	**Die High-End-Lösung für bestmögliche Sicherheit im Bereich Security Awareness**
4-wöchige Ist-Analyse oder kontinuierliche Phishing-Simulation	Ziel-ESI® von 70 als Zielvereinbarung	Ziel-ESI® von 80 als Zielvereinbarung	Ziel-ESI® von 90 als Zielvereinbarung
Patentierte Spear-Phishing-Engine	Alle Lite-Features inklusive	Alle Basic-Features inklusive	Alle Professional-Features inklusive
Full-Service-Setup	**Awareness-Engine: Training im Autopiloten**	Online-Seminare	Mitarbeiter-OSINT: Die beste Phishing-Simulation
	Alle E-Trainings	Awareness-Materialien	Social-Engineering-Standortbegehung inklusive

Details zu den Produkten und den enthaltenen Features finden Sie auf S. 12 – 14

Das Prinzip des Ziel-ESI®

Security Awareness ist eine zeitintensive Herausforderung. Nicht nur Sie als Sicherheitsverantwortlicher müssen Zeit investieren, um Awareness-Maßnahmen zu planen, auch Ihre Mitarbeiter benötigen Zeit, um an ihnen teilzunehmen. Unsere Full-Service-Pakete der Awareness Academy (Basic bis Premium) nehmen Ihnen diesen Aufwand ab: Sie definieren das gewünschte Sicherheitsniveau in Form des Ziel-ESI® und wir kümmern uns um den Rest. Dabei wenden wir verschiedenste Trainingsmethoden an, von der Phishing-Simulation bis zum E-Learning und mehr. Ihre Mitarbeiter sparen Zeit, indem nur dann Trainings angesetzt werden, wenn ihr Sicherheitsniveau unter dem gewünschten Ziel-Niveau liegt. Hat der Mitarbeiter den Ziel-ESI® erreicht, erhält er, mindestens bis zur nächsten Messung, eine Pause. Sie können sich währenddessen entspannt zurücklehnen und sich um Ihre anderen Aufgaben kümmern. Setzen Sie dauerhaft einen Haken an das Thema Security Awareness!

Alleinstellungsmerkmale von IT-Seal

Ziel-ESI® und Awareness Engine

Die Awareness Engine bildet das technologische Herzstück für Ihre Awareness Academy im Auto-Piloten. Sie wertet regelmäßig das Sicherheitsverhalten Ihrer Teilnehmer aus und entscheidet auf dieser Basis, welche Teilnehmergruppen in welchem Umfang weiter trainiert werden. Liegt eine Gruppe überhalb des Ziel-ESI®, so erhält sie mindestens 2 Monate Trainingspause. Falls eine Gruppe unterhalb des Ziel-ESI® liegt, werden entsprechende Traingsmaßnahmen in die Wege geleitet. Jeder Teilnehmer erhält dadurch genau so viel Training wie nötig, aber gleichzeitig so wenig wie möglich.

Full Service mit Stakeholder-Kommunikation

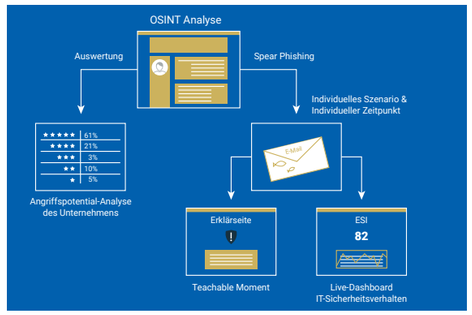
Wir kümmern uns um Ihr Awareness-Training im Full Service, sodass Sie sich enstpannt zurücklehnen und den steigenden ESI® beobachten können. Darüber hinaus kümmern wir uns schon im Vorfeld des Trainings um die Kommunikation mit relevanten Stakeholdern. Von den Mitarbeitern über den Betriebsrat und Datenschutzbeauftragten bis hin zur Führungskräften und der Geschäftsführung. Wir unterstützen Sie im gesamten Prozess mit Ihrem persönlichen Ansprechpartner.

Patentierte Spear-Phishing-Engine

Zur Vorbereitung von Spear-Phishing-Angriffen sammeln Angreifer aus öffentlich zugänglichen Quellen Informationen, um ein umfassendes Bild der Zielperson zu erhalten. Im Fachjargon der Spionage wird dies als Open Source Intelligence (OSINT) beschrieben. Wie ein echter Angreifer nutzen auch wir die öffentlich zugängliche Daten Ihrer Mitarbeiter und Ihres Unternehmens, um unsere Phishing-Simulation noch gezielter zu gestalten. So können wir von Massen- bis Spear-Phishing eine große Bandbreite an Angriffsszenarien abbilden und Ihre Gefährdungssituation umfassend analysieren.

Opt-Outs für Ihre Mitarbeiter

Lassen Sie Ihre Mitarbeiter selbst bestimmen, an welchen datenschutzrelevanten und personenbezogenen Maßnahmen des Awareness Trainings sie teilnehmen möchten oder auch nicht. Dazu können die Mitarbeiter einfach und bequem per Opt-Out entsprechenden Prozessen widersprechen. Dadurch geben Sie dem einzelnen Mitarbeiter die Entscheidung selbst in die Hand, statt den Betriebsrat über alle Köpfe hinweg pauschal entscheiden zu lassen.



4

Awareness Engine

Mitarbeiter trainieren – vollautomatisch mit der Awareness Engine

Die Sensibilisierung von Mitarbeitern für Security Awareness ist essentiell, um ein Unternehmen effektiv vor Cyber-Angreifern zu schützen, denn 90% der Cyberangriffe beginnen mit einer Phishing-Mail. Dennoch stellt diese Aufgabe viele IT-Sicherheitsverantwortliche vor eine Herausforderung, da ein nachhaltiges Mitarbeitertraining zeitaufwendig sein und viele Ressourcen in Anspruch nehmen kann.

Nicht mit uns: IT-Seal hat für Sie die innovative Awareness Engine entwickelt. Diese Awareness-Technologie trainiert Ihre Mitarbeiter bedarfsgerecht und vollautomatisiert für eine nachhaltige und effiziente Sensibilisierung. Das Ergebnis ist eine aktive Sicherheitskultur und aufgeklärte Mitarbeiter, die ihre Verantwortung für ihr Unternehmen kennen und wahrnehmen. Die Awareness Engine bildet das technologische Herzstück unserer Awareness Academy und bietet Training im Autopiloten: Jeder Teilnehmer erhält so viel Training wie nötig und so wenig wie möglich.

Arbeitszeit und Kosten sparen

Mit der Awareness Engine trainieren Ihre Mitarbeiter so viel wie nötig und so wenig wie möglich

Training im Autopiloten

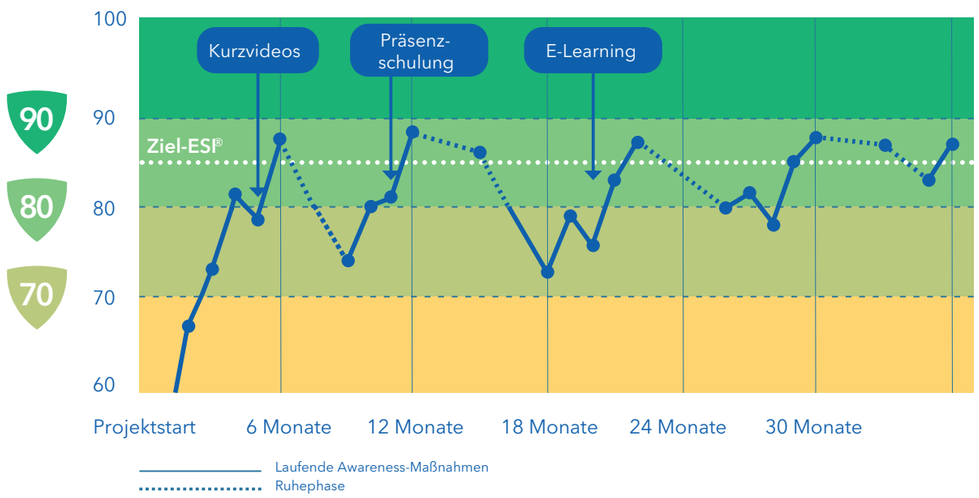
Die Awareness Engine bietet Training im Autopiloten und pausiert beziehungsweise startet das Training Ihrer Mitarbeiter automatisch

Kennzahlenbasiert, gruppenspezifisch, bedarfsgerecht

Das Awareness-Training ist zielgerichtet und kennzahlenbasiert dank Ziel-ESI®

Mit der Awareness Engine zum Ziel-ESI®

Zu Beginn der gemeinsamen Awareness Kampagne definieren Sie Ihren Ziel-ESI®, welchen Sie erreichen und langfristig halten möchten. Der ESI® stellt ein Kontrollinstrument dar, mit dem die Security Awareness im Unternehmen regelmäßig gecheckt werden kann. Somit herrscht Transparenz über den Fortschritt Ihrer Mitarbeiter. Unsere Awareness Engine nutzt Ihren Ziel-ESI®, um Ihre Mitarbeiter zielgerichtet und kennzahlenbasiert zu trainieren. Sie prüft die Effektivität einzelner Schulungsmaßnahmen und leitet konkreten Trainingsbedarf ab.



5

Patentierte Spear-Phishing-Engine

OSINT-basierte Angriffspotential-Analyse

Heutige Phishing-E-Mails werden immer raffinierter. Zur Vorbereitung von Spear Phishing-Angriffen sammeln Angreifer aus öffentlich zugänglichen Quellen Informationen, um ein umfassendes Bild der Zielperson zu erhalten. Im Fachjargon der Spionage wird dies als Open Source Intelligence (OSINT) beschrieben.

Um einzuschätzen, wie bedroht Ihr Unternehmen durch öffentlich zugängliche Informationen auf Sozialen Medien ist, haben wir unsere Angriffspotential-Analyse entwickelt. Wie viele (kritische) Informationen geben Ihre Mitarbeiter in beruflich genutzten Sozialen Medien preis? Welche Mitarbeitergruppen sollten Sie gezielt auf die damit verbundenen Gefahren hinweisen? Wo lohnt sich eine Schulung im Umgang mit Sozialen Medien?

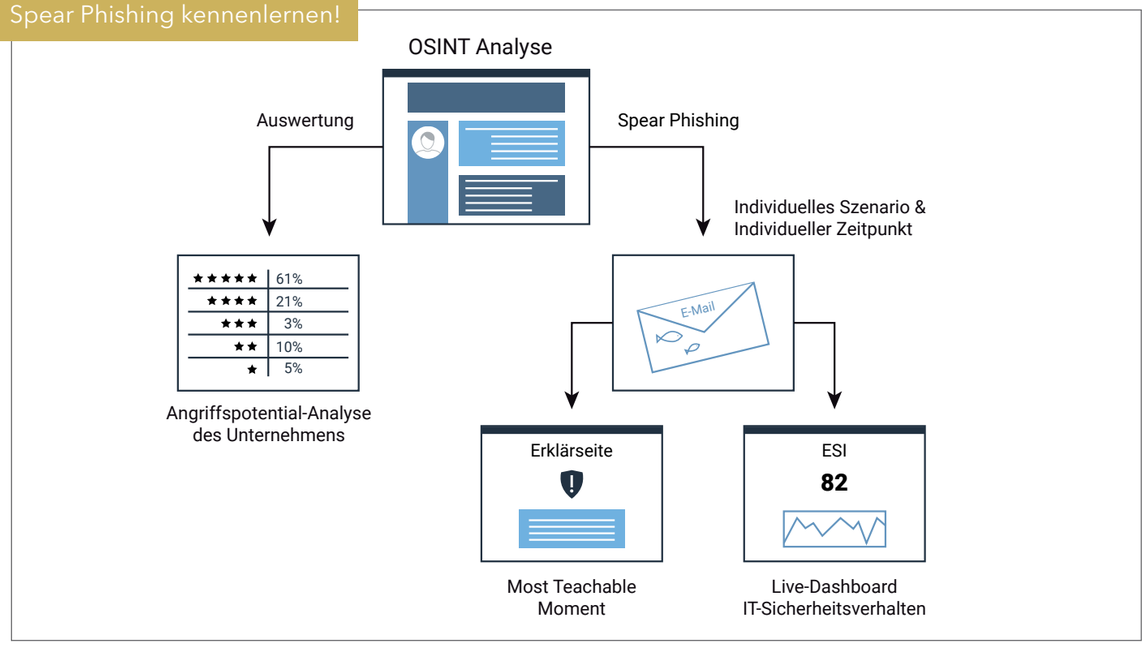
Das Thema Daten- und Mitarbeiterschutz ist dabei natürlich eine zentrale Komponente. Die Auswertung erfolgt stets gruppen-, nie personenbasiert. Wir analysieren ausschließlich Informationen, die vom Mitarbeiter selbst veröffentlicht wurden.

Massen- bis Spear Phishing

Wie ein echter Angreifer nutzen wir die gesammelten Daten, um unsere Social Engineering-Simulation noch gezielter zu gestalten: „Einladung zur Betriebssport-Wandergruppe", „Du hast doch da mal gearbeitet – was sagst Du denn zu der Meldung?"

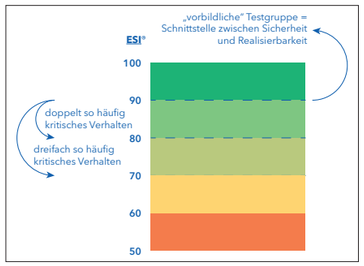
So können wir von Massen- bis Spear Phishing eine große Bandbreite an Angriffsszenarien abbilden und Ihre Gefährdungssituation umfassend analysieren. Alternativ können wir auch durch die Übergabe weniger Informationen (Abteilung, Position) automatisiert zielgerichtete Angriffe ohne OSINT simulieren.

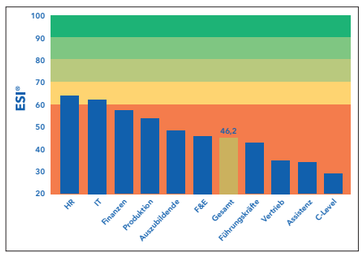
demo.it-seal.de
Jetzt selbst testen und unser Spear Phishing kennenlernen!

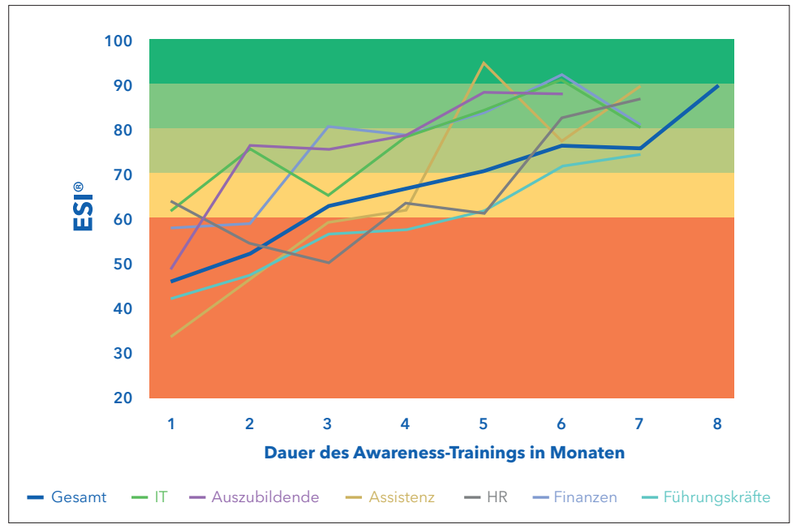


ESI®-Benchmark als KPI: Der Employee Security Index

Der ESI® bietet Transparenz und Vergleichbarkeit







Messungen des Employee Security Index (ESI®) im Rahmen der Awareness Standortbestimmung und Awareness Akademie

Sicherheit ist eine schwierig zu messende Größe

Gegen was, unter welchen Bedingungen und bis zu welchem Grad ist man sicher? Diese Frage bringt große Herausforderungen mit sich, wenn es um die Absicherung des Unternehmens und Investitionsentscheidungen geht. Für den Bereich Social Engineering- und Phishing-Awareness hat IT-Seal einen Benchmark, den „Employee Security Index" (ESI®) entwickelt. Basierend auf dem aktuellen Stand der Forschung und unserer Erfahrung mit Phishing-Simulationen in Unternehmen verschiedenster Branchen haben wir Toleranzwerte für das Verhalten von Mitarbeitern gegenüber Social Engineering-Angriffen abgeleitet. Der Toleranzwert ist dabei jeweils abhängig von der Vorbereitungszeit, die ein Angreifer für den entsprechenden Angriff aufwenden muss.

An der Schnittstelle zwischen absoluter Sicherheit und Realisierbarkeit definieren wir ein „sicheres" Unternehmen, welches auf einer Skala von 0-100 einen Wert von 90 erreicht. Welchen ESI® erreicht Ihr Unternehmen im Vergleich? Wer ist sicherer, Vertrieb oder Buchhaltung? Transparent und vergleichbar ermitteln wir den ESI® für einzelne Mitarbeitergruppen, um Gefahrenpotential aufzuzeigen und weitere Schulungsmaßnahmen planbar zu machen. Die Mindestgruppengröße beträgt zum Schutz der Mitarbeiter 30 Personen.

„Der ESI® ist die erste und einzige IT-Security-Kennzahl, die es in unsere Unternehmens-KPIs geschafft hat!"
– Kunde aus der Energiebranche –

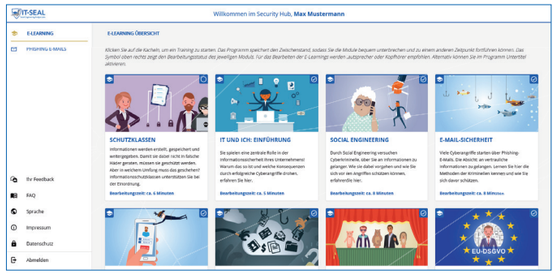
Kompatibel und kommunizierbar

Unser Konzept macht Social Engineering-Angriffe reproduzierbar. Die zeitliche Entwicklung der Awareness in Ihrem Unternehmen können Sie mit dem ESI® bequem per API in Ihr SOC einbinden. Auch für das Management ist unsere Kennzahl einfach verständlich und macht das Thema Awareness greifbar.

Weitere Awareness-Technologien

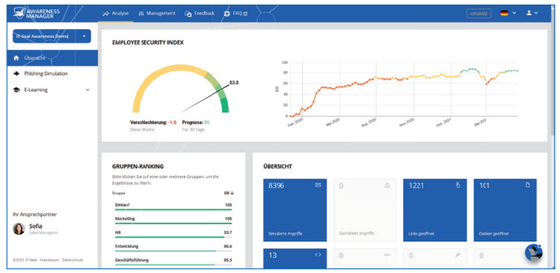
Security Hub

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



Awareness Manager

Erhalten Sie jederzeit einen Live-Überblick zum Status Ihrer Awareness-Kampagne und des aktuellen Sicherheitsniveaus im Awareness Manager. Die Ergebnisse können projektweit und auf Gruppenbasis eingesehen werden. Außerdem sehen Sie, wie viele Links und Dateianhänge geöffnet wurden und welcher ESI® daraus resultiert. Auch die konkret versendeten Phishing-Szenarien samt Erfolgsquote sowie der Mitarbeiter-Fortschritt für die versendeten E-Learnings sind einsehbar.

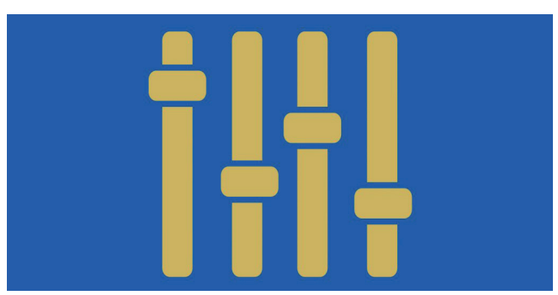


Bedarfsgerechtes Training

Unsere Phishing-Simulation fängt mit einfachen Szenarien an und steigert sich bei einer erfolgreichen Abwehr durch den Mitarbeiter individuell – bis hin zu immer aufwendiger gestalteten Spear-Phishing-Mails. Dadurch vermeiden wir sowohl demotivierte Mitarbeiter, die frustriert einen Misserfolg nach dem anderen erfahren, als auch Security Fatigue: Mitarbeiter erhalten genau den richtigen Schwierigkeitsgrad zwischen Langeweile und Überforderung.

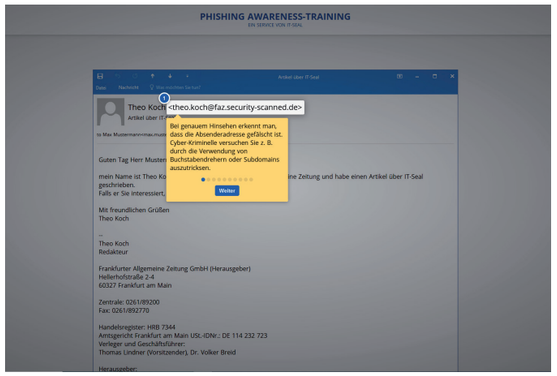
Phishing-Intensität bestimmen

Bestimmte Ereignisse oder Phasen außerordentlicher Belastung können Gründe sein, die Phishing-Simulation für Ihre Mitarbeiter zu drosseln. In manchen Fällen kann auch eine dauerhaft niedrige Versandrate von simulierten Phishing-Mails sinnvoll sein. In Absprache mit Ihrem Awareness Consultant können Sie einfach und schnell die Intensität aller versendeten Phishing-E-Mails global auf die Bedürfnisse Ihrer Mitarbeiter anpassen.



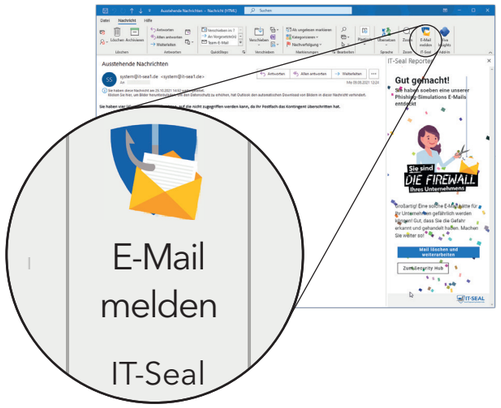
Individuelle Erklärseite

Öffnet ein Mitarbeiter einen risikobehafteten Link beziehungsweise Dateianhang oder gibt Login-Daten auf gefälschten Seiten ein, wird er auf die IT-Seal Erklärseite weitergeleitet. Am exakten Beispiel der eben geöffneten E-Mail wird konkret aufgezeigt, wie er den Phishing-Versuch hätte erkennen können. In diesem Moment des Fehlverhaltens ist der Mitarbeiter besonders empfänglich für eine nachhaltige Aufklärung: Der sogenannte „Most Teachable Moment" kann seine Lernwirkung voll entfalten. Auch auf häufig genutzte psychologische Tricks (Neugier, Angst, Gewohnheit, …) wird hingewiesen.



Reporter Button für Outlook

Die Meldekette ist ein zentrales Element der IT-Sicherheit im Unternehmen. Als Unterstützung dafür, bietet IT-Seal den Reporter Button, als Add-In für Outlook Desktop und Mobil. Er ermöglicht es Mitarbeitern, eine verdächtige E-Mail mit einem Klick an eine vorher definierte Stelle weiterzuleiten. Handelt es sich dabei um eine IT-Seal Spear-Phishing-Simulation, erhalten die Mitarbeiter direkt ein positives Feedback. Stammt die E-Mail nicht von IT-Seal, wird sie automatisch als Anhang zur Analyse an den kundeninternen IT-Support weitergeleitet. Ziel ist es, das Melden von Phishing-Vorfällen zu vereinfachen sowie den unternehmensinternen Aufwand mit der Phishing-Simulation gering zu halten. Im IT-Seal Awareness Manager kann eingesehen werden, wie viele der simulierten Phishing-E-Mails von Mitarbeitern gemeldet wurden.



ISO27001-konformes Reporting

Alle Teilnehmer, die ihre vorgesehenen E-Learning-Module und Phishing-Simulationen erfolgreich abschließen, erhalten ein personalisiertes Teilnahme-Zertifikat, das im Rahmen der ISO 27001 als Nachweis genutzt werden kann. Auch das Unternehmen selbst erhält ein gültiges Zertifikat über die durchgeführten Maßnahmen, um den Nachweis zu erbringen.

Modulare E-Trainings

E-Learnings und Kurzvideos für zeitgemäßes Lernen

Interaktives E-Learning

Unsere E-Learning-Module sind vielseitig einsetzbar. Sie decken dabei unterschiedliche Themen auf anschauliche Art und Weise ab, um die Mitarbeiter ungebunden und flexibel im Bereich IT-Security fortzubilden: Von den Tricks der Social Engineers und anschaulichen Beispielen echter Sicherheitsvorfälle bis hin zu Know-How, welches beruflich und privat angewandt werden kann – stets mit dem „Faktor Mensch" im Fokus. Interaktiv, unterhaltsam und verständlich für alle Zielgruppen gestaltet.

Auch das Monitoring spielt bei uns eine zentrale Rolle. Im Learning-Management-System (LMS) kann das Training verwaltet und der Lernfortschritt eingesehen werden. Alle Teilnehmer, die ihre vorgesehenen E-Learning-Module erfolgreich abschließen, erhalten ein personalisiertes Teilnahme-Zertifikat, das im Rahmen der ISO 27001 als Nachweis genutzt werden kann. Darüber hinaus können Sie wählen, ob das E-Learning bequem in unserem hauseigenen Learning-Management-System zur Verfügung gestellt werden soll oder ob die Inhalte dynamisch in Ihr Unternehmens-LMS eingepflegt werden. Alle E-Learning-Module sind in den Sprachen Deutsch, Englisch und Französisch verfügbar. Weitere Sprachen nach Absprache.

Relevant und umsetzbar
Lerninhalte sind sofort im Alltag anwendbar

Unsere Erfahrung ist Ihr Vorteil
Trainings erstellt von Security Awareness-Experten, basierend auf langjähriger Erfahrung.

Persönliche Mitarbeiterzertifikate
Alle Mitarbeiter können personalisierte Zertifikate erhalten, welche die Teilnahme an den abgeschlossenen Modulen bescheinigen

IT und ich: Einführung

Social Engineering

Passwörter und Authentisierung

E-Mail-Sicherheit

Soziale Medien

Homeoffice

Vishing

Datenschutz

Informationsschutzklassen

Cyberangriffe melden

Auszug aus unserem vielfältigen E-Learning Angebot

Mitarbeiter-Quizze: Stellen Sie Ihre Mitarbeiter auf die Probe

Sie möchten sicher gehen, dass ihre Mitarbeiter die Themen zur Informationssicherheit auch wirklich verinnerlicht haben? Stellen Sie ihre Kenntnisse mit Quizzen auf die Probe. In verschiedenen Aufgaben werden die Teilnehmer herausgefordert, ihr Wissen zu überprüfen und ihre Kenntnisse an typischen (Arbeits-)Situationen anzuwenden.

- Als Teilnehmer erhalten Sie Einblick in Ihren Wissensstand und können Lücken proaktiv schließen.
- Als Verantwortlicher erhalten Sie einen Überblick über die Kenntnisse im Unternehmen und können den Bildungsbedarf Ihrer Kollegen und Mitarbeiter erkennen und ableiten.

Kurzvideos für Zwischendurch

Integrieren Sie einfache und kurzweilige Lerninhalte direkt in den Arbeitsalltag Ihrer Mitarbeiter. Mit einminütigen Kurzvideos bringen wir aktuelle Themen aus der Informationssicherheit auf den Punkt. Die Videos sind jederzeit bequem im Security Hub abrufbar.

Die Kurzvideos behandeln aktuelle Bedrohungslagen und ergänzen die E-Learnings um spezifisches IT-Sicherheitswissen wie beispielsweise Emotet und gefälschte Loginseiten. Dabei werden die Themen regelmäßig erweitert und sind stets auf dem neuesten Stand.

Die prägnanten Lernmodule sind unterhaltsam gestaltet und für alle Zielgruppen leicht verständlich.

Kurze Lernvideos sind perfekt für den Arbeitsalltag
Digitales Lernen per Video passt sich der sich immer schneller verändernden Arbeitswelt optimal an

Konsistentes Lernkonzept
Inhalte abgestimmt mit Lerneinheiten der IT-Seal Phishing-Simulation.

BSI IT-Grundschutz
Sensibilisierung der Mitarbeiter für InfoSec gemäß BSI IT-Grundschutz

Gefährliche Makros: Emotet und die Makroviren-Pandemie

- Was sind Makroviren und wie erreichen sie mich?
- Welche Gefahr geht durch Emotet aus?
- Wie kann ich mich vor Makroviren schützen? Wer greift an – und warum mich?

Nicht anbeißen: Login-Seiten als Köder

- Welche Gefahr geht durch gefälschte Login-Seiten aus?
- Wie kann ich mich schützen?
- Woran erkenne ich, ob die Login-Seite von einer validen Quelle stammt?

Vorbild sein! Als Führungskraft Informationssicherheit vorleben

- Warum betrifft Informationssicherheit nicht nur IT-Experten?
- Welche Rolle spiele ich als Führungskraft?
- Wie kann Informationssicherheit Teil der Unternehmenskultur werden?

Academy-Features im Detail

Nachhaltige Sicherheitskultur

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Nachhaltige Sicherheitskultur: Unser gemeinsames Ziel Unser gemeinsames Ziel ist eine nachhaltige Sicherheitskultur. Dafür holen wir alle Mitarbeiter:innen Schritt für Schritt ab und zeigen die Relevanz sowohl im beruflichen als auch privaten Kontext auf. Sie lernen das 1x1 der Cybersicherheit, um gemeinsam an einem Strang zu ziehen – dadurch kennen sie ihre Verantwortung am Arbeitsplatz und nehmen diese effektiv wahr. Wir unterstützen Ihre Mitarbeiter:innen bedarfsgerecht, kennzahlen- und gruppenbasiert: So viel wie nötig, so wenig wie möglich.	✓	✓	✓	✓

ESI® und Ziel-ESI® (Employee Security Index)

Features	Lite	Basic	Professional	Premium
ESI® und Ziel-ESI® (Employee Security Index): Ihr Benchmark Der ESI® ist ein wissenschaftlicher Benchmark, um die Sicherheitskultur branchenübergreifend messen zu können. Mit dem Ziel-ESI® wählen Sie Ihr Sicherheitsniveau, das als gemeinsame Ziel-Vereinbarung gilt. Dabei wird jede Gruppe kennzahlenbasiert und bedarfsgerecht trainiert. Erreicht eine Gruppe den Ziel-ESI®, wird das Training pausiert, bevor der ESI® nach 3 Monaten erneut gemessen wird. Gruppen, die mehr Unterstützung benötigen, erhalten mehr Hilfestellung durch zusätzliche Trainings. Als KPI benchmarkt Sie der ESI® im Vergleich zu Unternehmen der selben Branche und Größe.	ESI®	70 Ziel-ESI®	80 Ziel-ESI®	90 Ziel-ESI®

Awareness Engine

Features	Lite	Basic	Professional	Premium
Awareness Engine: Unser technologisches Herzstück Die Awareness Engine ist unser technologisches Herzstück und wertet live das Sicherheitsverhalten Ihrer Teilnehmer aus. Sie ist immer aktiv, wobei einzelne Gruppen aktiv oder pausiert sind. Sie entscheidet auf Basis des Ziel-ESI®, welche Gruppen welches Training zu welchem Zeitpunkt erhalten. Jeder Teilnehmer erhält dadurch genau so viel Training wie nötig, aber gleichzeitig so wenig wie möglich.		✓	✓	✓
Full-Service durch unsere Awareness-Expert:innen Die strukturierte Kommunikation mit den Stakeholdern ist der Schlüssel zu einer nachhaltigen Sicherheitskultur. Dabei unterstützt Sie Ihr persönlicher Awareness Consultant mit Best Practices von hunderten erfolgreichen Kunden bei der Einrichtung und Pflege Ihres Security-Awareness-Programms. Dazu gehört die interne Kommunikation mit den Stakeholdern (Mitarbeiter:innen, Geschäftsführung, Betriebs- oder Personalrat, Datenschutzbeauftragte:r, IT-Support), die Konfiguration des Projekts, Unterstützung beim Whitelisting und bei Testmails sowie Material zur internen Ankündigung.	✓	✓	✓	✓
Security Hub: One-Stop-Shop für Training & Kommunikation Damit wir am besten lernen, benötigen wir eine bequeme und konsistente Lernerfahrung. Der Security Hub fasst die persönlichen E-Trainings Ihrer Mitarbeiter:innen zentral an einem Ort zusammen. Dabei setzen wir auf individuelle Lernpfade, denn wir wissen wie individuell jede:r Einzelne lernt. Mitarbeiter:innen können ihre E-Trainings an jedem Ort aufrufen und die eigenen Phishing-Szenarien Revue passieren lassen. Ihre Mitarbeiter:innen werden automatisch per Magic Link eingeloggt und müssen sich keine Zugangsdaten merken.	✓	✓	✓	✓

Awareness Engine

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
"Most Teachable Moment": Aufklärung im richtigen Moment Der „Most Teachable Moment" ist pädagogisch und didaktisch ein wertvoller Moment, um besonders effektiv zu lernen und Mitarbeiter:innen über das potenziell schadhafte Fehlverhalten aufzuklären. Beispielsweise zeigt eine interaktive Erklärseite anhand der tatsächlich geklickten Phishing-Mail auf, worauf zu achten ist und welcher psychologische Trick angewendet wurde.	✓	✓	✓	✓
Interaktive E-Trainings, die Spaß machen Das IT-Seal E-Training vermittelt Teilnehmern unterhaltsam, kurzweilig und verständlich Inhalte zu Sicherheitskultur, Informationssicherheit und Datenschutz in Form von E-Learnings, Kurzvideos und Most-Teachable-Moments.	optional	✓	✓	✓
Unternehmenszertifikat als Nachweis für ISO 27001 u.ä. Sie erhalten ein Unternehmenszertifikat, das als Nachweis für Sicherheitsaudits (ISO27001, TISAX, BSI IT-Grundschutz, …) und für Kunden dient. Weiter erhalten Mitarbeiter:innen Teilnahmezertifikate.	✓	✓	✓	✓
Individuelles Branding: Auf Ihr Unternehmen angepasst Die Anpassung des E-Trainings, des Security Hubs, der Benachrichtigungs-Mails und der Awareness-Materialien an Ihr Unternehmensbranding stärkt das Image bei den Mitarbeitern. Zusätzlich erhält die Erklärseite Ihr Unternehmenslogo, um Vertrauen zu schaffen.	✓	✓	✓	✓
Individuelle Konfiguration: Auf Ihre Mitarbeiter:innen angepasst 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.	✓	✓	✓	✓
Online-Seminare & „Bleib wachsam!"-Awareness-Material In interaktiven Online-Seminaren bekommen Teilnehmer:innen die Grundlagen sicheren Verhaltens am Arbeitsplatz durch einen Awareness-Coach vermittelt. Unser Awareness-Material beinhaltet Plakate, Flyer, Webcamcover, Mousepads, Schreibblöcke, Traubenzucker und Energydrinks.	optional	optional	✓	✓
Präsenzschulungen & Social-Engineering-Standortbegehung In Präsenzschulungen erhalten Teilnehmer die Grundlagen sicheren Verhaltens am Arbeitsplatz persönlich bei Ihnen vor Ort vermittelt. Für die Social-Engineering-Standortbegehung nehmen wir die Rolle eines Angreifers ein und prüfen, wie angreifbar Ihr Standort ist.	optional	optional	optional	✓
Telefonangriffe (Vishing) & manipulierte USB-Sticks Mit gefaketen Telefonangriffen versuchen wir sensible Informationen herauszufinden oder Zahlungen anzuweisen. Dabei klären wir die betroffenen Mitarbeiter:innen direkt und sensibel auf. Die manipulierten USB-Sticks werden als weiterer Angriffsvektor eingesetzt.	optional	optional	optional	✓

Academy-Features im Detail

Patentierte Spear-Phishing-Engine

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Patentierte Spear-Phishing-Engine: Die beste Phishing-Simulation Auf Basis frei verfügbarer Informationen generiert unsere patentierte Spear-Phishing-Engine individuell zugeschnittene Phishing-Angriffe (Spear-Phishing/Dynamite Phishing). Dies erfolgt für Sie vollautomatisiert: Jeder Mitarbeiter:in erhält zu individuellen Zeitpunkten individuelle Szenarien.	✓	✓	✓	✓
Unternehmens-OSINT: Open-Source-Intelligence Unser Unternehmens-OSINT durchsucht Ihre Website, Jobportale, Arbeitgeberbewertungsportale oder berufliche Soziale Netzwerke nach individuellen Unternehmensmerkmalen. Die gewonnenen Informationen dienen als Grundlage für unternehmensspezifische Spear-Phishing-Mails.	✓	✓	✓	✓
Mitarbeiter-OSINT: Open-Source-Intelligence Unser Mitarbeiter-OSINT durchsucht berufliche Soziale Netzwerke nach verwertbaren Informationen. Dabei sammeln wir Informationen Ihrer Mitarbeiter:innen, die aufgrund ihrer Datenschutzeinstellungen mehr Informationen nach außen preisgeben. Die gewonnen Informationen dienen als Grundlage für mitarbeiterspezifische Spear-Phishing-Mails.	optional	optional	optional	✓
Spear-Phishing-Mails: Level 1–3 Die Level unserer Spear-Phishing-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 Branchenszenarien. Sie nutzen genau wie echte Angreifer potenziell gefährliche Links, gefälschte Login-Seiten, Makros und verschlüsselte Dateianhänge.	✓	✓	✓	✓
Reporter Button für Outlook Der Reporter Button ist ein Add-In für Outlook Desktop und Mobil. Er unterstützt den Meldeketteprozess für reale Angriffe. Zudem erhalten Mitarbeiter:innen eine positive Rückmeldung für erkannte Phishing-Simulationen.	✓	✓	✓	✓
Individuelle Spear-Phishing-Mails Wir erstellen Phishing-Mails, die nach Ihrem Wunsch individuell konzipiert sind.	optional	optional	optional	✓

Mitarbeiterfreundlichkeit & Datenschutz besonders im Fokus

Features	Lite	Basic	Professional	Premium
Security and Privacy by Design Der Mitarbeiter- und Datenschutz steht im Vordergrund, weshalb die Ergebnisse der Phishing-Simulation stets gruppenbasiert ausgewertet werden. Unsere Prozess- und Datenbankstrukturen sind von Anfang an nach dem Prinzip „Security and Privacy by Design" erschaffen worden.	✓	✓	✓	✓
Respektvolle und sensible Kommunikation Wir haben von Anfang an verstanden, dass wir alle Mitarbeiter:innen Schritt für Schritt abholen müssen und dabei respektvoll und sensibel kommunizieren. Gemeinsam mit Ihren Mitarbeiter:innen möchten wir an einem Strang ziehen und das Ziel einer nachhaltigen Sicherheitskultur erreichen.	✓	✓	✓	✓
Individuelle Opt-Out-Lösungen Um die Prozesse so datenschutzfreundlich wie möglich zu gestalten, haben Ihre Mitarbeiter diverse Möglichkeiten, um bestimmten Maßnahmen zu widersprechen. Dadurch erhalten Sie die Möglichkeit, jeden Teilnehmer:in individuell und wunschgerecht abzuholen.	✓	✓	✓	✓

Persönliche Eindrücke

89% der Teilnehmer geben an, dass die Maßnahmen ihre Security Awareness geschärft haben.

» Ich dachte eigentlich, dass ich Phishing-Mails direkt erkennen würde. Die Kampagne hat mich eines Besseren belehrt. Nun bin ich noch achtsamer. «

98% bewerten die Awareness-Maßnahme als sinnvoll.

» Viel besser, als „nur" Online-Schulungen mitzumachen! «

100% haben sich mit Kollegen über das Security-Awareness-Training ausgetauscht.

» Gut konstruierte E-Mails mit steigendem Anspruch. «

» In der Projektarbeit erlebe ich, dass unsere Ansprechpartner unseren Full Service-Ansatz sehr schätzen. Der regelmäßige Austausch mit unseren Kunden ermöglicht es uns, direkt auf aktuelle Bedürfnisse zu reagieren. «

Antje
Customer Success Managerin

» Die für Cyberattacken genutzten Angriffsmethoden entwickeln sich permanent weiter. Das stellt uns täglich erneut vor die Aufgabe, eine möglichst realitätsnahe Simulation für das optimale Training unserer Kunden zu erschaffen. Diese Herausforderung nehme ich gerne an! «

Christian
Technischer Leiter

Kunden über uns

Vom Mittelstand zum DAX-Konzern – zu unseren Kunden zählen namhafte Unternehmen aus zahlreichen Branchen. Aus Datenschutzgründen haben wir darauf verzichtet, den Firmennamen zu nennen.

Gerne stellen wir Ihnen auf Anfrage die komplette Referenz sowie einen Ansprechpartner aus einer Branche Ihrer Wahl zur Verfügung.

Mehr unter www.it-seal.de/referenzen

»Über die Dauer der Kampagne konnten wir unseren ESI® (Employee Security Index) signifikant steigern ...«

– Industriepark. Teilnehmer: 700

Nachdem wir uns intern entschieden hatten, eine Weiterbildungsmaßnahme zum Thema Phishing Awareness durchzuführen, haben wir diese mit IT-Seal umgesetzt. Neben dem nachhaltigen Training und der Sensibilisierung unserer Mitarbeiter konnten wir so eine unabhängige und konkrete Analyse unserer Sicherheitskultur erhalten. Die Projektdurchführung mit IT-Seal war reibungslos und hat uns intern sehr wenig Aufwand gekostet.

Die Phishing-Simulation orientiert sich an aktuellen Bedrohungen. Über die Dauer der Akademie konnten wir unseren ESI® (Employee Security Index) signifikant steigern und erzielten bereits nach 3 Monaten ein Ergebnis, mit dem wir uns sicher fühlen. Dabei haben wir besonders die nichtinvasive Art der Weiterbildungsmaßnahme geschätzt, die ohne zusätzlichen Zeitaufwand im Arbeitsalltag stattfindet und den Mitarbeiter auf seinem bisherigen Kenntnislevel abholt.

Für jede Branche die passende Awareness-Kampagne

Maschinenbau · Finanzen · Gesundheit · Energie · Logistik

Universität · Onlinehandel · Kanzlei · Industriepark · Automotive

»Nachdem wir uns lange auf den technischen Teil der IT-Sicherheit konzentriert hatten, wollten wir als nächsten Schritt auch unsere Mitarbeiter verstärkt mit einbeziehen ...«

– Finanzbranche. Teilnehmer: 250

Aus diesem Grund haben wir nach einem zuverlässigen Partner gesucht und diesen in IT-Seal gefunden. IT-Seal hat bei uns eine Security Awareness-Strandortbestimmung durchgeführt, bei der Social Engineering-Angriffe simuliert wurden, um das aktuelle Sicherheitsniveau der Mitarbeiter zu messen. Auf diese Weise konnten sie das Sicherheitsverhalten unserer Mitarbeiter beurteilen und weiteren Handlungsbedarf hervorheben. Dabei wurden Maßnahmen mit Priorisierungen besprochen, um unsere Sicherheit weiter zu erhöhen. Die Phishing-Szenarien von IT-Seal haben das, was uns bisher durch echte Phishing-Versuche erreicht hat, sehr gut abgebildet.

Der Projektablauf wurde unkompliziert auf unseren Bedarf zugeschnitten. Durch die Standortbestimmung haben wir einen direkten Einblick in das Verhalten der verschiedenen Mitarbeitergruppen erhalten.

Die Vishing-Simulation zeigte uns Schwachstellen im Sicherheitsverhalten unserer Mitarbeiter auf und ist die Grundlage für eine Anpassung unserer Richtlinien und deren Umsetzung.

»Von Vertragsabschluss bis Projektende hatten wir großes Vertrauen in den von IT-Seal gepflegten Datenschutz ...«

– Stadtwerke. Teilnehmer: 200

Wir waren mit IT-Seal als Partner zum Messen des IT-Sicherheitsbewusstseins unserer Mitarbeiter sehr zufrieden. Das Thema Phishing-Analyse stand bei uns schon länger auf der Agenda. Leider konnten wir jedoch vorher nie einen Anbieter finden, mit dem wir es mitarbeiterfreundlich umsetzen konnten.

Das Projekt gab uns zudem einen spannenden Einblick in die Informationen, die über unsere Mitarbeiter und unser Unternehmen öffentlich einsehbar sind. Dies hilft uns, unsere Richtlinien zu aktualisieren und zeigte auch den Kollegen auf, wie wichtig die richtigen Datenschutzeinstellungen im Netz sind.

Von Vertragsabschluss bis Projektende hatten wir stets großes Vertrauen in den von IT-Seal gepflegten Datenschutz. Alle datenschutzrelevanten Themen waren kompetent vorbereitet: Die Auswertung der Phishing-Simulation wurde konsequent gruppenbezogen berichtet. Alle mitarbeiterbezogenen Daten wurden verschlüsselt übertragen, die Verwendung der Daten war transparent.

Überzeugen Sie sich selbst, auf der unabhängigen Bewertungsplattform Proven Expert, von der Zufriedenheit unserer Kunden

Eine Auswahl unserer Kunden

DEUTSCHE BUNDESBANK EUROSYSTEM · Schwan STABILO · DATEV · infraserv höchst

 # 1. Platz – Bestes Cybersecurity Start-Up Deutschlands @it-sa [4]

#1. Platz Europaweiter Social Engineering Wettbewerb @TREsPASS_Project [1]

 # 1.Platz beim Best Student Award @BSI [2]

Wir sind IT-Seal

 # Top 10 der besten Cybersecurity Start-Ups Europas @SBA_Research [3]

Sehr geehrte Damen und Herren,

Innovation und das Streben nach einer sicheren digitalen Welt stecken uns im Blut.

Die IT-Seal GmbH ermöglicht es Unternehmen, Social Engineering-Angriffen vorzubeugen. Wir simulieren im respektvollen und geschützten Rahmen Phishing- und andere IT-Sicherheitsangriffe auf Ihre Mitarbeiter und trainieren diese durch eine sofortige interaktive Aufklärung.

Diese Dienstleistung basiert auf unserem in universitärer Forschung entwickelten standardisierten und reproduzierbaren Rahmenwerk für Social Engineering-Angriffe.

David Kelm

Alex Wyllie

Yannic Ambach

Gründer der IT-Seal GmbH

Made with ♡
in Security Valley Darmstadt

1) https://www.trespass-project.eu/node/236
2) https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/David_Kelm_Best_Student_Award_16052013.html
3) https://www.sba-research.org/
4) https://www.it-sa.de/de/up18

IT-Seal GmbH | Hilpertstr. 31 | 64295 Darmstadt | 06151 862 70 00 | www.it-seal.de

Wir freuen uns auf ein persönliches Gespräch!
Ihr Team von IT-Seal

Stellen Sie sich selbst auf die Probe: demo.it-seal.de
Kostenfrei und ungefährlich.

IT SECURITY
MADE IN GERMANY

DEUTSCHLANDS ERSTE LOKALE CYBER-SECURITY-KAMPAGNE FÜR BÜRGERINNEN UND BÜRGER

digitales.hessen · IT-SEAL Social Engineering Analysis Labs · HESSEN Hessische Ministerin für Digitale Strategie und Entwicklung · HESSEN Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen · Wissenschaftsstadt Darmstadt

Gemeinsam: Digital und sicher

UNSERE VISION

Jede Technologie ist darauf ausgerichtet, den Menschen zu bereichern. Wenn ein Mensch in der Lage ist, eine Technologie zu nutzen, kann er Großartiges erreichen.

Man hat oft das Gefühl, dass gerade die IT-Sicherheit das Gegenteil bewirkt: IT-Sicherheitssysteme stehen der Produktivität des Anwenders im Wege und Anwender sind die größte Bedrohung für die IT-Sicherheit.

Wir glauben, dass es an der Zeit ist, die IT-Sicherheit wieder mit dem Anwender zu vereinen.

Wir glauben, dass Menschen durch die Ermächtigung ihrer selbst die Freiheit und das Vertrauen zurückgewinnen können, mit moderner Technologie mehr zu erreichen.

Wir glauben, dass jeder Mensch die IT-Sicherheit fördern kann – und auch umgekehrt.

UNSERE WERTE

Respekt
Der Schutz der uns anvertrauten Mitarbeiterdaten und Firmeninterna steht zentral. Dem Know-How unserer Kunden treten wir mit Respekt gegenüber und wertschätzen die uns entgegengebrachte Arbeitszeit.

Professionalität
IT-Seal zeichnet sich durch fundiertes, aktuelles Fachwissen und einen wissenschaftlichen Ansatz aus. Wir legen Wert auf klare Kommunikation.

Offenheit
Wir führen eine offene Kommunikation und sprechen Ideen, Vorschläge und Probleme frühzeitig und klar an. In der Zusammenarbeit pflegen wir eine umfassende Feedbackkultur. Unseren Kunden liefern wir eine transparente Risikoanalyse.

Flexibilität
Wir sehen es als Stärke unseres Start-Up-Charakters, unsere Leistung flexibel an die Bedürfnisse unserer Kunden und Partner anzupassen.

Wir freuen uns auf ein persönliches Gespräch mit Ihnen!

Tel.: 06151 862 70 00
E-Mail: kontakt@it-seal.de

IT-Seal GmbH | Hilpertstr. 31 | 64295 Darmstadt | www.it-seal.de

Made with ♡ in Security Valley Darmstadt

IT-SEAL
Social Engineering Analysis Labs