ACE IT Sicherheitstraining

Ausgangslage

Cybercrime – es kann jeden treffen

Die vielen Ereignisse zeigen es: Jedes Unternehmen, ob gross oder klein, wird durch die Cyberkriminalität bedroht. Die steigende Abhängigkeit von der ICT bewirkt zudem, dass diese Bedrohungen zunehmend ein existentielles Risiko für Ihr Unternehmen darstellen. Gleichzeitig werden die Attacken immer komplexer und professioneller.

Im Kampf gegen die Cyberkriminalität genügen technische Mittel alleine nicht mehr. Vielmehr müssen Massnahmen aus einem umfassenden Sicherheitskonzept implementiert werden. Dabei spielen der Faktor Mensch und die Prozesse in der IT eine wesentliche Rolle.

Unser Angebot – Ein integraler Ansatz zum nachhaltigen Sicherheitsbewusstsein und Schutz vor Cyberangriffen

Das vorliegende Angebot ist darauf ausgerichtet, Ihr Unternehmen und Ihre Mitarbeitenden auf Phishing Attacken vorzubereiten. Wir befähigen die Mitarbeitenden Phishing Attacken richtig zu erkennen und zu melden. Während dem Training beraten wir die IT Verantwortlichen auch im Bereich der Security Prozesse. So behandeln wir zum Beispiel das Thema, wie mit gemeldeten Phishing Attacken umzugehen ist und dabei die Sicherheit erhöht werden kann. Gemeinsam mit Ihren IT Verantwortlichen definieren wir auch die notwendigen Schritte, wenn trotzdem ein Angriff erfolgreich ist.

Mit Phishing Simulationen und kontinuierlichen Sicherheits-Training der Mitarbeitenden stärken den Faktor Mensch gezielt und reduzieren die Wahrscheinlichkeit eines erfolgreichen Phishing Angriffs deutlich. Die Attacken werden zunehmend raffinierter und es lohnt sich in jedem Fall, der regelmässigen Sensibilisierung der Mitarbeitenden einen hohen Stellenwert einzuräumen. Hier kann mit relativ geringem Aufwand sehr viel an Sicherheit gewonnen werden.

Was bringt das IT-Sicherheitstraining

Aktive Beteiligung der Mitarbeitenden mit dem Ziel, eine Sicherheitskultur zu schaffen, bei der Wachsamkeit und die Bereitschaft zur Meldung von Vorfällen im Zentrum stehen.

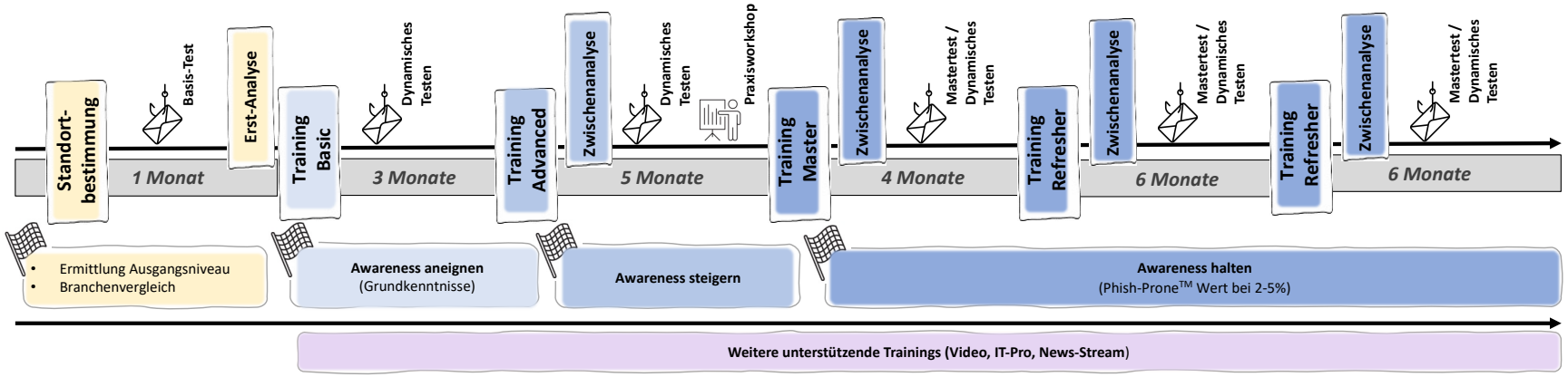
Kontinuität. Wiederkehrende Übungen und permanentes Testen gewährleisten einen bleibenden hohen Schutz.

Eingespielte Prozesse. Handlungsfähigkeit ist sichergestellt, wenn trotzdem einmal etwas passiert.

Stärkung einer positiven Fehlerkultur. Positive Rückmeldungen auf die Meldung von Fehlern und Vorfällen stärkt das Vertrauen, baut auf und erhöht dabei die IT-Sicherheit wesentlich.

Das ACE IT-Sicherheitstraining im Überblick

Trainings- und Simulationsprogramm für alle Mitarbeitenden

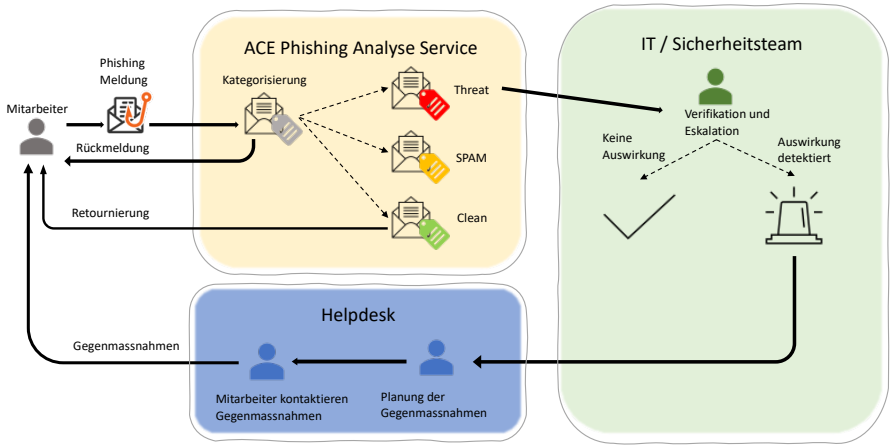


Unterstützt durch

KnowBe4
Human error. Conquered.

weltweit führender Anbieter von Sicherheitstrainings und Phishing-Tests

Phishing Meldeprozess und Analyseservice



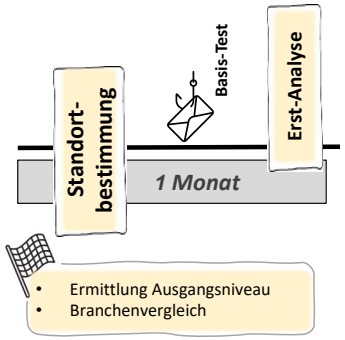
Praxisworkshops

- Passwortschutz
- Datenschutz
- E-Mail
- Die Rolle der Mitarbeitenden
- Open Source Intelligence

ACE IT-Sicherheitstraining im Detail

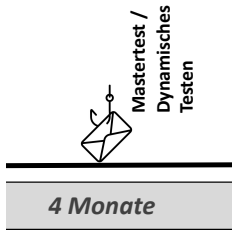
Die Standortbestimmung

Mit einer ersten simulierten und unangekündigten Phishing-Kampagne ermitteln wir, wie anfällig Ihre Mitarbeitenden für Angriffe sind. Die Anfälligkeit wird mit dem Phish-Prone™ Prozentsatz gemessen. Mit der Erst-Analyse erhalten Sie eine erste Einschätzung im Vergleich zu Unternehmen aus der gleichen Branche und eine erste Beratung zur Verbesserung der Sicherheit. Der erste Test ist zudem ein wesentliches Element, um die Notwendigkeit eines Trainings im gesamten Unternehmen schaffen zu können.



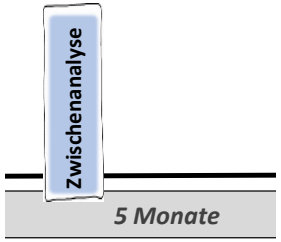
Die Mastertests

Ab dem zweiten Halbjahr führen wir halbjährlich Mastertests durch. Dabei analysieren wir Informationen aus frei verfügbaren, offenen Quellen und nutzen diese, um gezielte Phishing und Social Engineering Angriffe durchzuführen.



Analyse und Beratung

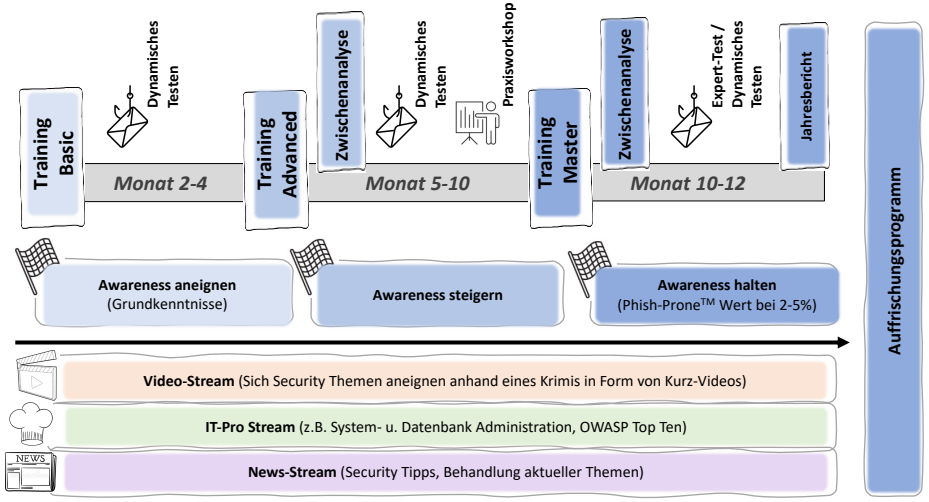
Während der Trainingsphase werden die Resultate der Phishing Tests und der Verlauf der Trainings zusammen mit dem Kunden analysiert und der weitere Verlauf der Kampagne abgestimmt. Zudem wird jeweils die aktuelle Situation des Kunden beurteilt und es werden Massnahmen zur Verbesserung der Sicherheit vorgeschlagen. Dies erfolgt unter anderem in Themen wie Anfälligkeit der IT Infrastruktur auf Ransomware, Incident Detection und Response Prozesse, Notfall- und Wiederherstellungspläne. Sämtliche Analysetätigkeiten und Beratungen werden in einem Bericht zusammengefasst.



ACE IT-Sicherheitstraining im Detail

Das Trainingsprogramm

Nach der Standortbestimmung wird das kontinuierliche Training und Testing eingeleitet. Das von uns vorbereitete Trainingsprogramm lässt sich gut in den Arbeitsalltag integrieren. Kurze und interessante Lernmodule, die auf den einzelnen Benutzer abgestimmt sind, bewirken, dass das Sicherheitsbewusstsein geschaffen und schrittweise vertieft wird. Die Kontrolle und Steuerung des Trainingsprogramms wird von unserem Kampagnenleiter übernommen. Der Kunde kann dabei stets auf den Inhalt und Ablauf Einfluss nehmen. Im Trainingsprogramm durchläuft jede/r Mitarbeitende folgende Stufen:



- **Basic** – zum Aneignen der Grundkenntnisse (Gesamtdauer ca. 70min)
- **Advanced** – zur Vertiefung von IT-Sicherheitsthemen (Gesamtdauer ca. 60-90min)
- **Master** – um auf dem aktuellen Stand bei Sicherheitsthemen zu bleiben

Weiter stehen für die Mitarbeitenden optionale Programme zur Verfügung:

- **Video** Trainingsprogramm, bei welchem die Sicherheitsthemen in einer spannenden Krimi-Serie nähergebracht werden
- **News** Informationsprogramm, bei welchem aktuelle Sicherheitshinweise und Tipps präsentiert werden
- für IT-Fachleute ein **IT-Pro** Trainingsprogramm zur Vertiefung von technischen Themen in der IT-Sicherheit

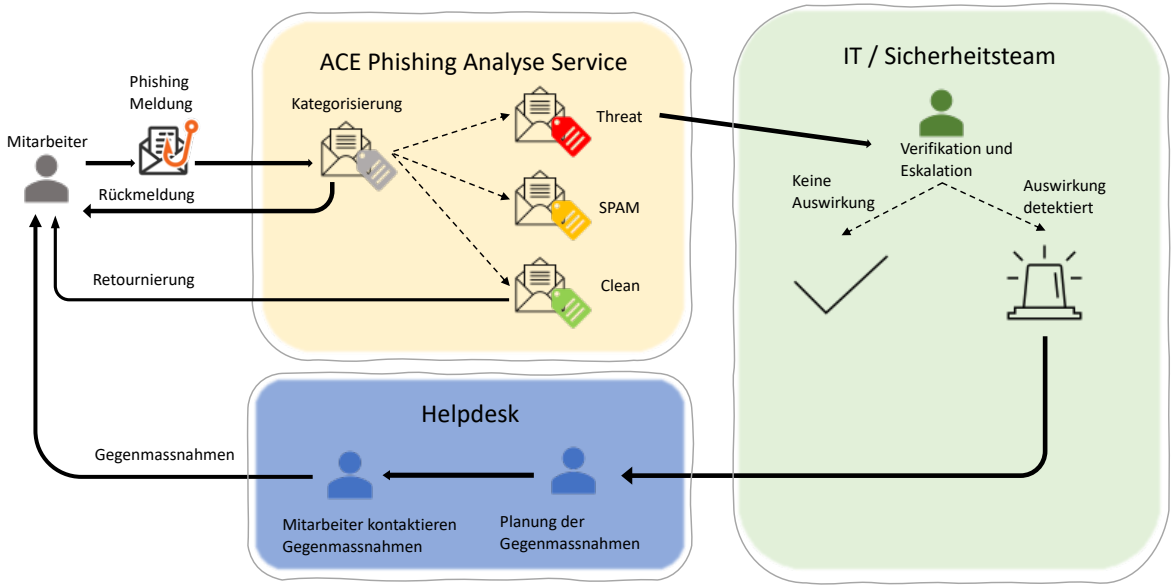
Phishing Meldeprozess und Analyseservice

Phishing Meldeprozess

Ein wesentlicher Schritt zur aktiven Beteiligung der Mitarbeitenden ist die Einführung des Phishing-Meldeprozesses. Die Trainingsphase ist der ideale Zeitpunkt, um diesen Prozess bei den Mitarbeitenden zu etablieren.

Add-on: Phishing Analyseservice

Der ACE Phishing Analyseservice analysiert gemeldete und eskaliert Bedrohungen an die definierte Stelle. Die Mitarbeitenden erhalten zudem eine Rückmeldung zur Einstufung der gemeldeten E-Mail als Threat, Spam, Clean. Clean E-Mails werden an die Meldenden zurückgestellt. E-Mails, welche als Bedrohung eingestuft werden, werden an das IT- bzw. Sicherheitsteam des Kunden weitergeleitet.



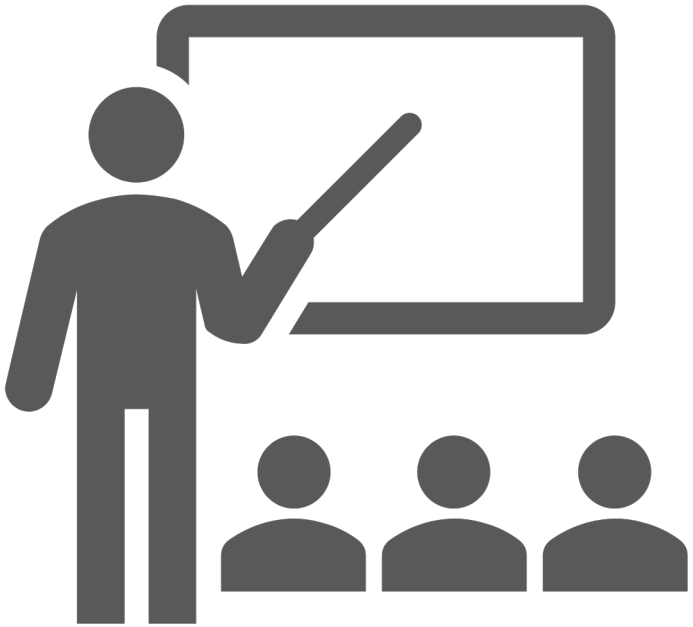
Add-on: Praxisworkshop

Praxisworkshop

Als Option führen unsere Sicherheitsspezialisten ein oder mehrere Praxisworkshops beim Kunden vor Ort durch. Ein Praxisworkshop besteht aus 3-5 frei wählbaren Modulen und kann von bis zu 50 Mitarbeitenden besucht werden. Idealerweise findet ein Workshop 3-4 Monate nach dem Start des Trainings statt.

Die Durchführung solcher Praxisworkshops zusätzlich zum IT-Sicherheitstraining haben den Vorteil,

- die Rolle der Mitarbeitenden in der IT-Sicherheit des Unternehmens zu stärken,
- die Fähigkeit Gefahren und Angriffe mithilfe von Praxisübungen richtig zu erkennen und
- das Gelernte während dem Workshop im eignen Umfeld anzuwenden und dabei Problemfelder und Schwachstellen aufzudecken und direkt zu besprechen.



Module

Folgende Module stehen zur Verfügung:

- **Passwort -** Verwendung und Umgang mit sicheren Passwörtern, Databreach Kontrolle
- **Daten -** Datenschutz, sicherer Datentransfer, Neues DSG
- **E-Mail -** Gefahren und Angriffe richtig erkennen (Red Flags)
- **Die Rolle der Mitarbeitenden -** Eigenes Verhalten, Mitwirkung, Security Prozesse in der IT
- **Open Source Intelligence -** öffentlicher Fussabdruck im Internet, Anonymität