



CIO Advisory

Security Awareness

Gemeinsam Cyber-Angriffe abwehren



Cyber-Crime – niemand ist sicher

Cyber-Kriminalität hat sich mittlerweile zur mit Abstand größten Bedrohung für Unternehmen entwickelt. Weltweit wird damit mehr Geld verdient, als mit Drogenhandel und Prostitution zusammen. Dabei herrscht immer noch ein äußerst stereotypes Bild von Cyber-Kriminellen vor. Die Szene ist mittlerweile jedoch vielfältig aufgestellt, gut organisiert und finanziell hervorragend ausgestattet.

Kein Unternehmen ist für Cyber-Kriminelle uninteressant. Manche verfügen über besonders wertvolle Informationen, andere sind durch geringe Schutzmechanismen schlichtweg leichte Opfer. Cyber-Angriffe erfolgreich abzuwehren, beginnt mit der Erkenntnis, dass nicht allein die Technik, sondern vor allem die Menschen eines Unternehmens den beste Abwehrmechanismus darstellen.

Die Angreifer

Crime- bzw. sogenannte Advanced-Persistent-Threats-Gruppen setzen gezielt die Fähigkeiten ein, die zum Erreichen ihrer Ziele benötigt werden:

- Script Kiddies probieren mit beschränkten Mittel aus, ‚was so geht‘ und freuen sich bei Erfolg
- Social Engineers unterstützen andere bei der Überwindung technischer Hürden, gehen aber auch alleine weiter, sofern es Erfolg verspricht
- Hacker / Black Hats suchen sich Unternehmen gezielt aus, um an wertvolle Daten zu gelangen, die sie dann verkaufen, zerstören, oder verschlüsseln und das Unternehmen erpressen
- Spione / Späher kombinieren Social Engineering mit Hacking und überwinden physische Barrieren, um Unternehmen ‚von innen‘ anzugreifen

Die Angegriffenen

Unternehmen investieren viel in den Aufbau technischer Hürden, um Angreifer abzuwehren – und verlieren häufig das wichtigste Einfallstor aus den Augen: die Menschen im Unternehmen.

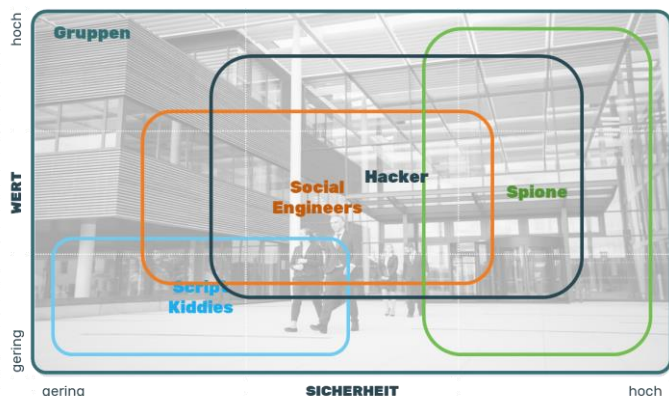
Die Unternehmensleitung missversteht das Thema als etwas Statisches und neigt dazu, punktuell auf konkrete Angriffe zu reagieren, statt sich kontinuierlich ständig ändernden Bedrohungslagen zu stellen.

Führungskräfte unterstützen das Thema selten aktiv und gehen auch nicht mit gutem Beispiel voran, da sie in ihrer Eigenwahrnehmung ‚Wichtigeres‘ zu tun haben.

Mitarbeitenden fehlt es häufig nicht nur an Knowhow, sie sind auch wenig sensibel für das Risiko und den Schaden für das Unternehmen und sie selbst, der von Angriffen ausgeht.

IT- und Sicherheitsabteilungen sprechen selten die gleiche Sprache wie die übrigen Mitarbeitenden und kommunizieren eher ad hoc statt systematisch und wertschätzend.

Bei Dienstleistern und Partnern eines Unternehmens werden geringere Anforderungen an die Widerstandsfähigkeit gegenüber Cyber-Angriffen gestellt.



Nachhaltigkeit zählt

Security Awareness bedeutet weit mehr als nur die Vermittlung von Wissen, welche Angriffsformen aktuell abzuwehren sind. Das Ziel ist eine nachhaltige Veränderung von Verhaltensweisen.





The human firewall – bevor es ernst wird

Security Awareness ist dann erfolgreich, wenn sie zielgruppenspezifisch angelegt ist, also auf die Bedürfnisse eines Unternehmens und seiner Belegschaft eingeht:

SYSTEMATISCH: Singuläre Maßnahmen können nur eine kurzfristige Wirkung haben. Erfolg versprechender ist ein Bündel von Maßnahmen, die ineinander greifen und sich gegenseitig verstärken.

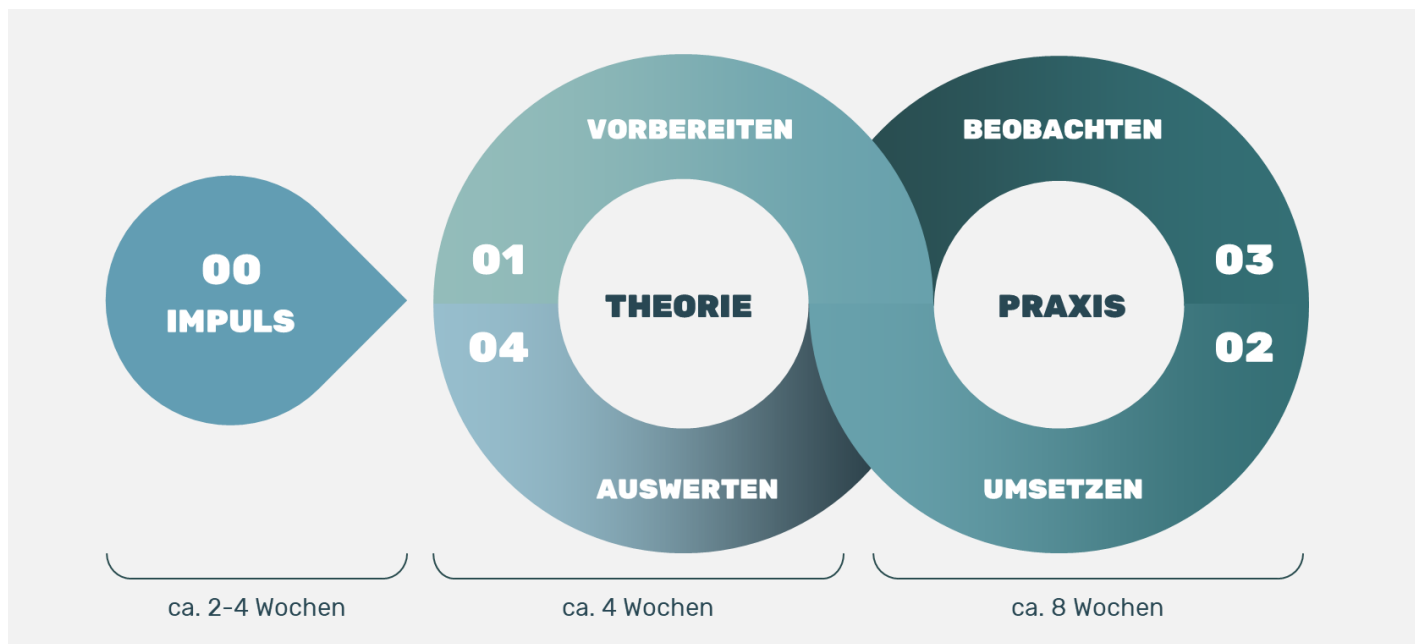
BERUHIGEND: Der Ansatz von ‚Schuld‘ und ‚Schuldigen‘ ist nicht zielführend und erzeugt unnötigen Stress bei allen Beteiligten. Stattdessen sollte an das Gemeinschaftsgefühl werden.

INTERAKTIV: Weder Top-Down noch Frontal sind langfristige Ansätze – sie führen eher zu Blockaden statt Akzeptanz. Beteiligte müssen wertgeschätzt und auf ihre Signale transparent reagiert werden.

UMSETZUNGSORIENTIERT: Allgemeingültige Ansätze tragen wenig zur Identifikation mit dem Thema bei. Awareness entsteht dann, wenn das Thema mit dem Alltag der Betroffenen verbunden wird.

KULTURKONFORM: Es gibt keine Standardkultur – jedes Unternehmen tickt anders. Security Awareness benötigt einen Baukasten, aus dem man sich die Elemente entnimmt, die zu der eigenen Kultur passen.

Eine nachhaltige Security Awareness zu erreichen ist ein Veränderungsprozess, der im Vorhinein nicht durchgeplant werden kann. Vielmehr geht es darum, iterativ das Niveau zu erhöhen. Auf vorhandenen Erfahrungen aufbauend, sollte praxisorientiert Wissen vermittelt und verankert werden. Dabei wird kontinuierlich sensibilisiert, die Wirkung beobachtet und bei Bedarf nachjustiert.



Vorhaben vorbereiten

- Festlegung der Ziele
- Identifikation und Charakterisierung aller Zielgruppen
- Abstimmung von (Kern-)Botschaften
- Auswahl und Vorbereitung geeigneter Formate
- Planung und Organisation der Umsetzungsphase

Maßnahmen umsetzen

- Durchführung klassischer wie digitaler medialer Maßnahmen
- Ansprache der Zielgruppen auf vertrautem Terrain
- Motivation und Austausch in Dialogformaten
- Sensibilisierung in spielerischer Form

Entwicklung beobachten

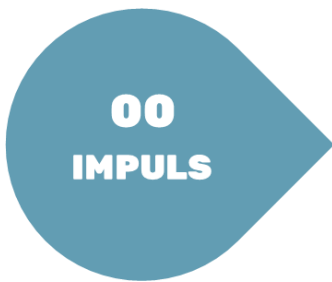
- Motivation von Rückmeldungen
- Gespräche mit Vertretern aller Zielgruppen
- Besuche und/oder Begleitung von Zielgruppen in ihrem Arbeitsalltag
- Aufnahme von Ideen und Vorschlägen für Verbesserungen

Ergebnisse auswerten

- Einsatz geeigneter Instrumente zur Messung des Fortschritts
- Analyse der Rückmeldungen
- Bewertung und Priorisierung der Ideen und Vorschläge zur Verbesserung
- Auswahl der Eckpfeiler für den nächsten Durchlauf



Bereit für Ihren ersten Impuls?



Je nach Ausprägung Ihrer bisherigen Erfahrungswerte mit Security Awareness (SAW) bieten wir drei Optionen zur Vorbereitung Ihrer weiteren Ausrichtung und Entwicklung an. Dabei kombinieren wir gängige deutsche wie internationale Standards des Information-Sicherheit-Managements mit Praxis-Erfahrungen aus Ihrer Branche.

Unsere Awareness-Projekte werden wann immer möglich interdisziplinär zusammengesetzt. Wir können hierfür aus allen relevanten Kompetenzfeldern Kollegen beisteuern – je nach Bedarf: Sicherheitsexperten, Branchenkenner, Transformationsspezialisten und auch Regulatorikprofis.

Unsere Einstiegsangebote

Das **SONAR** ist unser Angebot für Unternehmen, die noch unsicher sind, ob überhaupt und falls ja, wo es Potenziale für SAW geben könnte und mit welchem Mehrwert dies verbunden wäre.

Es handelt sich um eine standardisierte Breitenuntersuchung an neuralgischen Punkten und stellt eine reine Außen-Betrachtung dar, in der Regel dokumentenbasiert. Die Ergebnisse werden dann mit Best Practices und den Empfehlungen des BSI abgeglichen.

Unser **ECHOLOT** eignet sich für Unternehmen, die bereits punktuell im Bereich SAW aktiv waren und nun wissen möchten, ob sie auf dem richtigen Weg sind, oder wo sie noch besser werden können – der Favorit unserer Kunden.

Hierbei handelt es sich um eine standardisierte Tiefenuntersuchung von persönlichen Erfahrungen an neuralgischen Stellen. In Interviews und Workshops mit Schlüsselpersonen und Teams in Anlehnung an CISA laufen Außen- und Innenbetrachtung zusammen.

Mit unserem **KOMPASS** adressieren wir Unternehmen, die ihre Organisation konsequent und nachhaltig an den Zielen ihrer SAW-Strategie ausrichten wollen und die schon langjährige Erfahrungswerte sammeln konnten, die es nun zu schärfen gilt.

Diese Untersuchung ist individuell und geht zielorientiert auf alle relevanten Aspekte Ihrer SAW-Strategie ein.

Unsere Referenzen – beispielhafte Projektinhalte

- Reifegradermittlung und Analyse (vorbelasteter) Zielgruppen im Unternehmen – SONAR, ECHOLOT, KOMPASS
- Konzeption und Planung Awareness steigernder Maßnahmen – Kanäle, Botschaften, Kennzahlen
- Auswahl und Gestaltung von Schulungs- und Kommunikationsformaten – persönlich, online und klassisch
- Zielgruppengerechte Aufbereitung der schriftlich fixierten Ordnung – Sicherheitsrichtlinien, Arbeitsanweisungen, Prozessbeschreibungen etc.
- Begleitung und Moderation von Schulungen, Workshops und Events
- Sensibilisierung von Führungskräften zur Bedeutung von Informationsrisiken
- Durchführung von Angriff-Simulationen und Übungen mit Beteiligten
- Formatübergreifendes Feedback-Management
- Beobachtung, Steuerung und Auswertung aller Maßnahmen eines ‚Security Awareness Office‘ – in Abstimmung mit dem Security Operations Center

Ihr Mehrwert

Unsere Angebote und deren Mehrwert für Sie bauen größtenteils aufeinander auf. Bereits im SONAR werden Ihre ersten Handlungsfelder identifiziert und Nutzenpotenziale aufgezeigt. Schon in wenigen Tagen erhalten Sie die Ergebnisse in den Händen.

Mit dem ECHOLOT erfolgt dies noch detaillierter, auch der Abgleich mit Best Practices erfolgt nach mehr Kriterien. Außerdem bekommen Sie bereits eine erste Planungsskizze mit konkreten Optimierungsansätzen. Das dauert in der Regel etwa einen Monat, je nach Verfügbarkeit Ihrer Ansprechpartner.



Wesentlich spezifischere Ergebnisse erhalten Sie mit dem KOMPASS, nämlich nicht nur eine Roadmap für die nachhaltige Transformation, sondern auch die Planungsskizze für die ersten Schritte. Die Dauer dafür richtet sich stark nach Umfang und Qualität der Ergebnisse Ihrer bisherigen Aktivitäten. Meistens ist der KOMPASS aber auch nach etwa einen Monat beendet, auch wenn er mehr Abstimmungen beinhaltet als die anderen beiden Angebote.