HORNETSECURITY

EMPLOYEE SECURITY INDEX

WHITEPAPER

Social Engineering: Der Nutzer als Einfallstor

Mit dem stetigen Aufrüsten der technischen Schutzmaßnahmen im Bereich IT-Sicherheit geht ein weltweiter Aufschwung von Social Engineering-Angriffen einher: Enthielten im Jahr 2013 noch 17% aller Cyberangriffe eine Social Engineering-Komponente, wird heute bereits die überwiegende Mehrheit aller Angriffe durch Social Engineering vorbereitet. Die massenhafte Ausbreitung der Schadsoftware Emotet und ihrer Nachfolger hat gezeigt, welche Ausmaße und Qualität diese Angriffe annehmen können: Emotet liest gezielt Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus und nutzt diese Informationen zur weiteren Verbreitung. Solche Spear-Phishing-Mails sind für den Laien häufig kaum noch zu erkennen.

Security Awareness stärkt die „menschliche Firewall"

Der Faktor Mensch darf daher bei keinem Informationssicherheitskonzept fehlen – das Schlagwort heißt „Security Awareness". Security Awareness beschreibt das Ausmaß, in dem Mitarbeiter die Bedeutung von Informationssicherheit in ihrem Unternehmen sowie die Tragweite ihrer eigenen Sicherheitsverantwortlichkeit kennen und vor allem dementsprechend handeln.

Es gibt verschiedenste Maßnahmen, die eingesetzt werden können, um die Security Awareness zu steigern. Wichtig ist es, die Nutzer nicht als Risiko, sondern vielmehr als elementaren Bestandteil der IT-Sicherheitslösung zu verstehen: „Du bist die Firewall deines Unternehmens". Daher sollten die Mitarbeiter mitgenommen, nicht überfordert und vor allem sollte ihnen keine Angst gemacht werden.

Die Planung von Maßnahmen zur Steigerung des Sicherheitsbewusstseins birgt jedoch zahlreiche Herausforderungen:

- Wie stellt man sicher, dass Maßnahmen zur Security Awareness effektiv und nachhaltig sind?
- Kann ein Return on Investment angegeben werden – lohnt sich die Investition?
- Gibt es einen Benchmark oder Vergleich mit anderen Organisationen ähnlicher Branchen?
- Können Mitarbeiter in einer Organisation gezielter geschult werden als mit dem „Gießkannen-Prinzip"?

Mit dem Employee Security Index – kurz: ESI® – wird das Sicherheitsverhalten von Mitarbeitern realitätsnah, standardisiert und reproduzierbar messbar gemacht. Dieses Whitepaper erläutert das patentierte Berechnungsverfahren im Detail und präsentiert einen Benchmark aus über 60 europäischen Unternehmen.

Klassifizierung von Angriffen als Grundlage für eine standardisierte Messmethode

Um Security Awareness messbar zu machen, ist eine realitätsnahe Spear-Phishing-Simulation von Angriffen unabdingbar. Einzelne Angriffe sollten außerdem miteinander vergleichbar sein – nur so kann eine Messung über einen längeren Zeitraum Aufschluss über die Entwicklung der Security Awareness geben.

Daher nehmen wir eine Klassifizierung der zugrundeliegenden Phishing-Szenarien in verschiedene Kategorien vor. Ausschlaggebend ist dabei die Vorbereitungszeit, die ein Angreifer in die Vorbereitung und Durchführung eines Angriffsszenarios investieren muss. Diese setzt sich z. B. aus der Informationsbeschaffung (OSINT), der technischen Vorbereitung, dem Kopieren von Webseiten-Designs, sowie der Bereithaltung der Infrastruktur zusammen. So lassen sich die Phishing-Szenarien in sieben Kategorien (sogenannte Levels) einteilen, die unterschiedlich lange Vorbereitungszeiten benötigen.

Level	Beispiel	Vorbereitungszeit
1	Typische Massen-Phishing-Mail wie z. B. die Auftragsbestätigung eines bekannten Shopping-Portals	ca. 15 Minuten
2	Angebliche E-Mail vom Geschäftsführer (CEO-Fraud)	ca. 1 Stunde
3	Spear-Phishing-Mail unter Einbeziehung von öffentlichen Informationen über das Unternehmen bspw. aus Jobbewertungsportalen	ca. 2 Stunden
4	Spear-Phishing-Mail mit Bezug zur Abteilung und der Job-Position des Empfängers, E-Mail von direkten Kollegen oder Vorgesetzten.	ca. 4 Stunden
5	Gespoofte E-Mail eines Geschäftspartners, der keine Absicherung gegen E-Mail Spoofing aktiviert hat oder bei dem ein Account gehackt wurde.	ca. 6 Stunden
6	Ein Geschäftspartner oder Kollege wurde gehackt: E-Mail eines persönlichen Kontaktes, bei dem auf eine vorherige E-Mail-Konversation geantwortet wird.	ca. 12 Stunden
7	Spear-Phishing-Mail mit Bezug zu Themen, die der Empfänger selbst gerade bearbeitet, z. B. ein Status-Update zu einem laufenden Projekt, an dem der Empfänger beteiligt ist.	Mehr als 20 Stunden

Tabelle: Übersicht der Vorbereitungszeiten

Kennzahl für Security Awareness: ESI® - Der Employee Security Index

Um die Awareness einer Testgruppe zu messen, wird nun jeder teilnehmende Mitarbeiter zum Ziel zufällig ausgewählter Angriffsszenarien verschiedener Kategorien. Anschließend wird über die Testgruppe hinweg die „Erfolgsrate" (aus Sicht des Angreifers) gemessen.

Als angestrebtes Ziel eine „Erfolgsrate" von 0 zu erwarten, ist utopisch - Menschen machen Fehler. Wir definieren deshalb eine „vorbildliche" Testgruppe, welche an der Schnittstelle zwischen Sicherheit und Realisierbarkeit liegt. Abhängig von der Vorbereitungszeit, die ein Angreifer investieren muss, definieren wir Toleranzwerte, innerhalb derer das Sicherheitsverhalten der Mitarbeiter noch als „vorbildlich" gelten kann. Für die Kategorien 1 - 7 liegen diese Toleranzwerte zwischen 1,1 - 6,2%.

Eine vorbildliche Testgruppe mit exakt diesen Erfolgsraten erreicht einen ESI®-Wert von 90. Wird doppelt so häufig kritisches Verhalten gezeigt, z. B. durch Klicken auf einen schadhaften Link in einer Phishing-Mail, erreicht die Gruppe einen ESI® von 80; bei dreifach kritischem Verhalten nur noch einen ESI® von 70. Ergebnisse unter 70 werden als kritisch bewertet (siehe Abbildung 1).

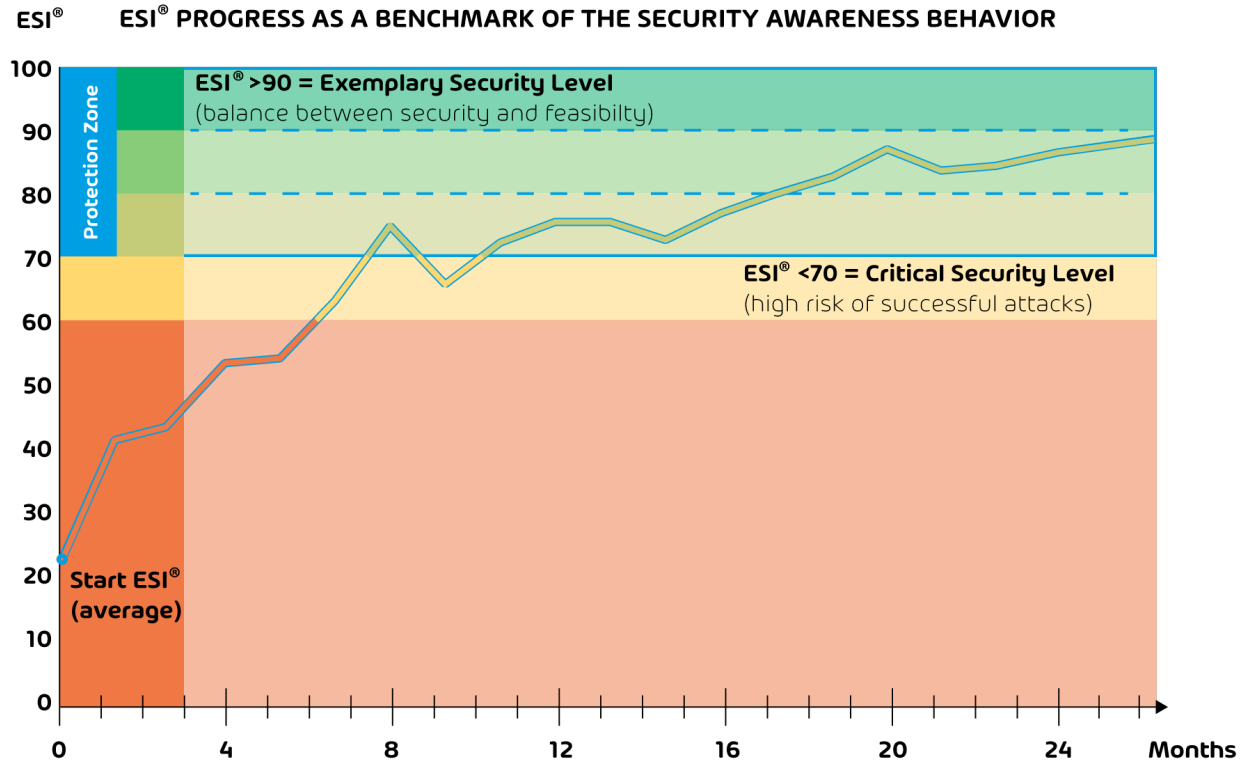

Abbildung 1: Ein Beispiel für die zeitliche Entwicklung des ESI®-Verlaufs als Benchmark der Sicherheitskultur

Die Ermittlung des ESI® bei europäischen Unternehmen zeigt: Die Security Awareness ist mangelhaft – aber ein signifikanter Lernerfolg messbar.

Der Employee Security Index wird seit Mitte 2018 im Rahmen von Phishing-Simulationen in international tätigen Unternehmen und Behörden ermittelt. Konkret wird hier die Klickrate auf Links und Dateianhänge gemessen. Beispiele für die simulierten Angriffe sind eine angebliche Meldung des Postfachs, der Speicher sei voll (Kategorie 1), die E-Mail eines zufälligen Kollegen, der einen Link zu einem lustigen GIF sendet (Kategorie 2), oder die Nachfrage des Abteilungsleiters zu einer Rechnung, welche als Dateianhang beigefügt ist (Kategorie 4). Die Phishing-Simulation wurde dabei so realitätsnah wie möglich durchgeführt: Alle Teilnehmer erhielten individuelle Spear-Phishing-Angriffe zu zufälligen Zeitpunkten.

Eine Auswertung aus über 1,7 Millionen simulierten Phishing-Angriffen geben einen aufschlussreichen Einblick in das Sicherheitsverhalten der Mitarbeiter aus Unternehmen aller Branchen und Größen, wie in Abbildung 2 im Zeitraum von 12 Monaten dargestellt.

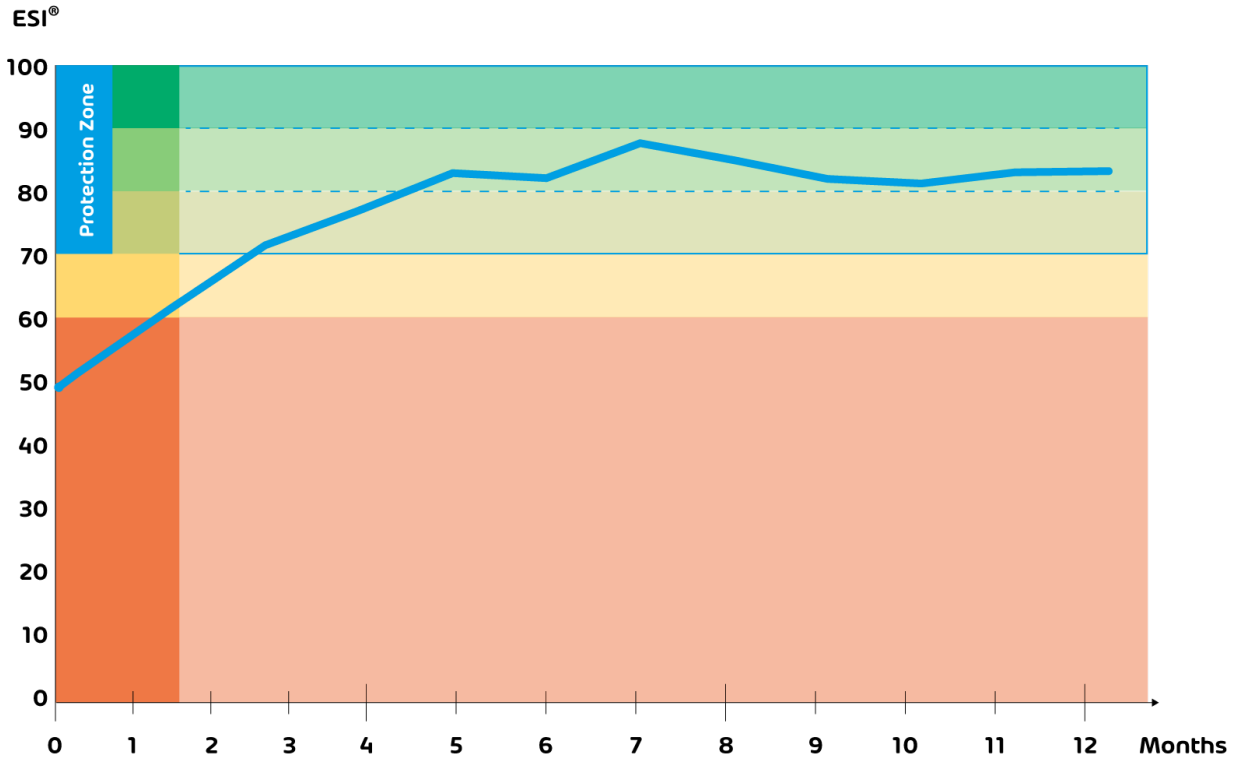

Abbildung 2: Ermittlung des Durchschnitts-ESI® aus der Phishing-Simulation.

Kontinuierliches Awareness-Training erforderlich

Der durchschnittliche ESI®-Verlauf macht bereits in den ersten 12 Monaten deutlich, warum ein kontinuierliches Training notwendig ist, um ein gutes Sicherheitsniveau auch über einen längeren Zeitraum zu halten. Während die ESI®-Kurve am Anfang steil ansteigt und schon bald ein akzeptables Sicherheitsniveau erreicht, fällt es mit zunehmend ausgeklügelteren Spear-Phishing-Szenarien deutlich schwerer, das Niveau zu halten - besonders wenn neue Mitarbeiter fortlaufend hinzukommen oder einzelne Gruppen und Mitarbeiter das Training pausieren, wie man in Abbildung 3 sehen kann.

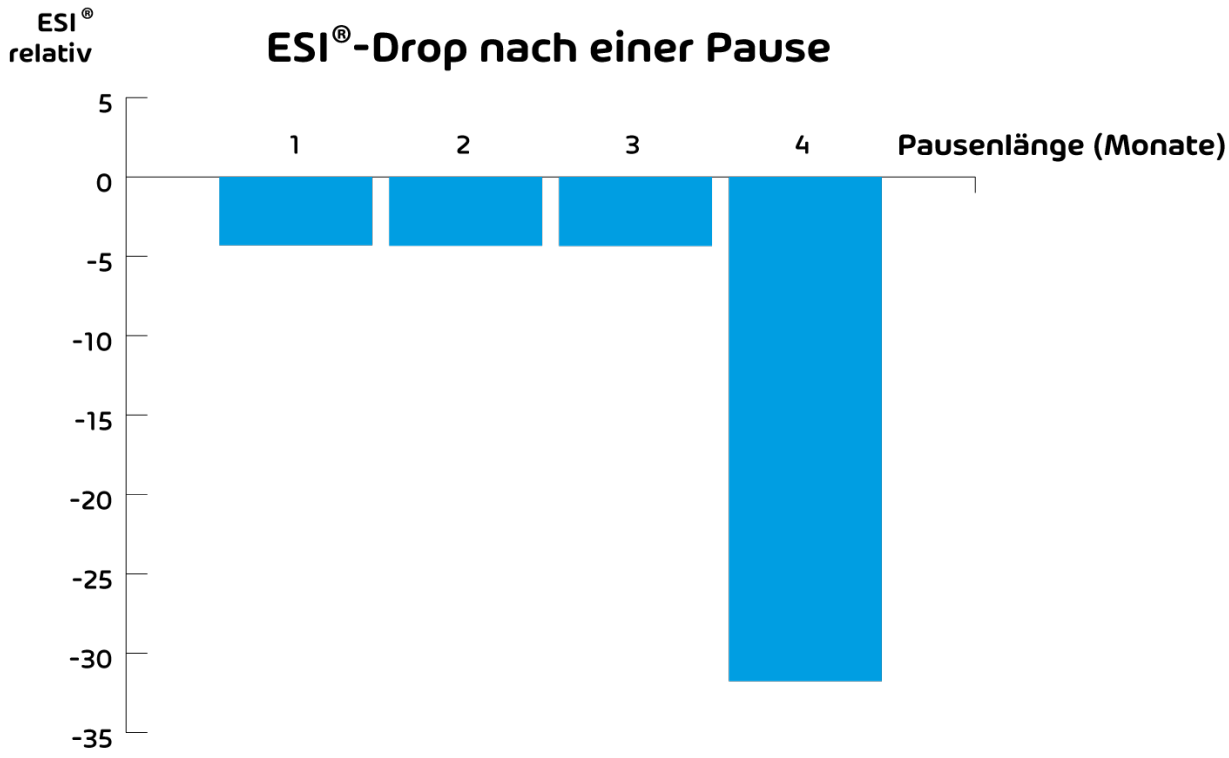

Abbildung 3: ESI®-Drop nach einer Pause des Trainings

Trainieren gegen das Vergessen

Awareness ist wie ein Muskel, der regelmäßig trainiert werden muss, sonst erschlafft er. Unterbrechen einzelne Gruppen oder Mitarbeiter das Awareness Training und steigen dann später wieder ein, zeigt sich ein deutlicher Abfall im Sicherheitsverhalten: ohne Training, während der Pausen werden sie wieder nachlässiger und haben wichtige Lerninhalte bereits wieder vergessen. Wie erschreckend groß dieser Effekt ist, zeigt der ESI®-Drop in dieser Grafik: Bereits nach dem ersten Monat Pause sinkt der ESI® um 5 Punkte und damit häufig schon wieder unterhalb des angestrebten Sicherheitsniveaus. Nach 4 Monaten sinkt der ESI® bereits um über 30 Punkte - und man steht fast wieder am Anfang des Awareness Trainings.

Kontrollinstrument als Entscheidungsgrundlage für weitere Security Awareness-Maßnahmen

Der ESI® stellt damit ein Kontrollinstrument dar, mit welchem die Security Awareness in Unternehmen kontinuierlich überwacht werden kann. Die Effektivität einzelner Schulungsmaßnahmen kann überprüft und konkreter Bedarf festgestellt werden. Die Kommunikation sowohl mit dem Management als auch mit der Belegschaft wird durch eine greifbare Kennzahl erleichtert: Eine quantitative Analyse der Security Awareness bietet einen direkten Vergleich mit anderen Unternehmen ähnlicher Branchen und kann so als Entscheidungsgrundlage für weitere Investitionen genutzt werden.

Mitarbeiter trainieren – vollautomatisch mit dem Security Awareness Service

Die Sensibilisierung von Mitarbeitern für Security Awareness ist essenziell, um ein Unternehmen effektiv vor Cyberattacken zu schützen. Denn sicherheitstechnische Maßnahmen allein reichen nicht aus, wenn Hacker gezielt die menschliche Schwachstelle auszunutzen wissen.

Dennoch stellt diese Aufgabe viele IT-Sicherheitsverantwortliche vor eine Herausforderung, da ein nachhaltiges Mitarbeitertraining zeitaufwendig sein und viele Ressourcen in Anspruch nehmen kann. Unser Security Awareness Service nimmt Ihnen den Großteil dieser Arbeit ab.

Unser Security Awareness Service trainiert Ihre Mitarbeiter ESI®-kennzahlenbasiert, bedarfsgerecht und vollautomatisiert für eine nachhaltige und effiziente Sensibilisierung. Das kontinuierliche Trainingsprogramm beinhaltet dabei vielfältige Methoden, um Mitarbeiter effektiv zu erreichen: Von der Phishing-Simulation über E-Trainings und Kurzvideos bis hin zu Awareness-Materialien. Das Ergebnis ist eine aktive Sicherheitskultur und aufgeklärte Mitarbeiter, die ihre Verantwortung für das Unternehmen kennen und wahrnehmen. Die Awareness Engine bildet das technologische Herzstück unseres Security Awareness Services und bietet für jeden das richtige Pensum an Training: Jeder Teilnehmer erhält so viel Training wie nötig und so wenig wie möglich.