DER EMPLOYEE SECURITY INDEX
SECURITY AWARENESS MESSBAR MACHEN

Der Benchmark ESI® von IT-Seal macht das Sicherheitsverhalten von Mitarbeitern in Unternehmen und Behörden standardisiert messbar, vergleichbar und trainierbar.

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, so waren es im Jahr 2018 schon 35%, Tendenz steigend. Die massenhafte Ausbreitung Schadsoftware Emotet zeigt, 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 E-Mails sind für den Laien häufig kaum noch zu erkennen.

Security Awareness stärkt die „menschliche Firewall"

Der Faktor Mensch sollte 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 Sicherheitsfeature zu verstehen: „Du bist die Firewall deines Unternehmens". Daher sollten die Nutzer mitgenommen, nicht überfordert und vor allem sollte 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" (ESI®) wird das Sicherheitsverhalten von Mitarbeitern realitätsnah, standardisiert und reproduzierbar messbar gemacht. Dieses Whitepaper erläutert den Benchmark ESI® im Detail – und präsentiert Echtdaten aus über 60 europäischen Unternehmen.

Klassifizierung von Angriffen als Grundlage für standardisierte Messmethode

Um Security Awareness messbar zu machen, ist eine realitätsnahe 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.

Kategorie	Zeitaufwand	Beispiel
1	ca. 1h	Wenig vorbereitete E-Mail in Unternehmenssprache.
2	ca. 3h	Mäßig vorbereitete E-Mail mit persönlicher Ansprache und Verwendung weniger Informationen.
3	ca. 10h	Angreifer übernimmt in E-Mail Rolle eines Kollegen oder Vertrauten der Testperson.
4	ca. 20h	E-Mail mit persönlichem Bezug, individuell vorbereiteter Telefonanruf oder einfacher physischer Angriff.
5	ca. 40h	Komplexer, mehrstufiger Angriff über mehrere Ebenen.

Abbildung 1: Übersicht der Vorbereitungszeit

Um Social Engineering-Angriffe miteinander vergleichbar zu machen, nehmen wir eine Klassifizierung in verschie-

dene Kategorien vor. Ausschlaggebend ist dabei die Vorbereitungszeit, die ein Krimineller in die Vorbereitung und Durchführung eines Angriffsszenarios investieren muss. Diese setzt sich z.B. aus der Informationsbeschaffung (OSINT), der technischen Vorbereitung, dem Kopieren von Designs (Clone Phishing), sowie der Bereithaltung der Infrastruktur zusammen. So lassen sich fünf Kategorien einteilen, welche jeweils einer Vorbereitungszeit von ca. 1, 4, 10, 20 und 40 Stunden entsprechen.

Kennzahl für Security Awareness: Der Employee Security Index

Um die Awareness einer Testgruppe zu messen, wird nun jeder teilnehmende Mitarbeiter zum Ziel zufällig ausgewählter Angriffsszenarien verschiedener Kategorien. Sowohl einmalige Bestandsaufnahmen, beispielsweise eine Angriffssimulation über vier Wochen, als auch ein kontinuierliches Monitoring der Awareness sind möglich. Für alle Kategorien wird über die Testgruppe hinweg die „Erfolgs"rate (aus Sicht der Angreifer) gemessen.

Als angestrebtes Ziel eine „Erfolgs"rate 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 Krimineller in den Angriff steckt, definieren wir Toleranzwerte, welches Verhalten noch als vorbildlich gewertet werden kann. Für die Social Engineering-Kategorien 1-3 liegen diese Toleranzwerte zwischen 1,5-6,5%. Eine vorbildliche Testgruppe mit exakt diesen Erfolgsraten erreicht auf der Skala einen Wert von 90. Wird doppelt (dreifach) so häufig kritisches Verhalten gezeigt, erreicht die Gruppe einen Wert von 80 (70). Ergebnisse unter 70 werden als kritisch bewertet (siehe Abbildung 2). Die Toleranzwerte basieren dabei auf der Erfahrungswerten.

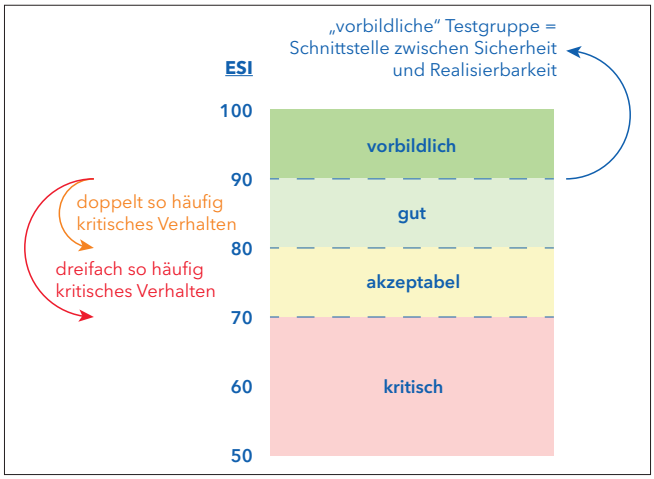

Abbildung 2: Der "Employee Security Index" (ESI) als Kennzahl für Security Awareness.

Die Ermittlung des ESI® bei über 60 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 (Social Engineering-Kategorien 1-3) in europäischen, teils 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. Die Phishing-Simulation wurde dabei so realitätsnah wie möglich durchgeführt: Alle Teilnehmer erhielten individuelle (Spear) Phishing-Angriffe zu zufälligen Zeitpunkten.

Eine Auswertung aus über 75.000 simulierten E-Mails geben einen aufschlussreichen Einblick in das Sicherheitsverhalten einzelner Fachbereiche, wie in Abbildung 3 unternehmensübergreifend dargestellt:

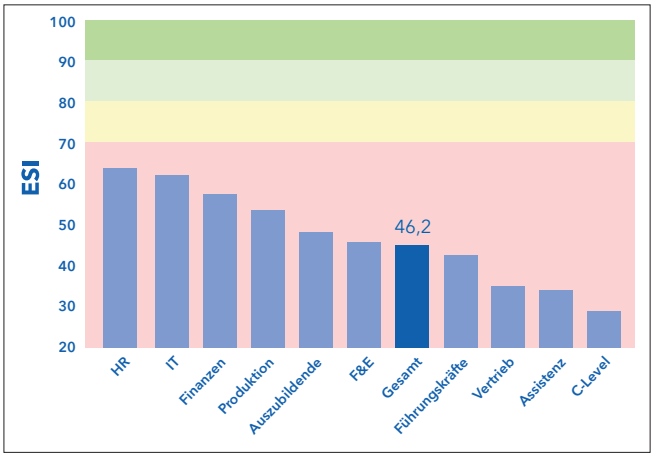

Abbildung 3: Ermittlung des Employee Security Index im Rahmen einer vierwöchigen Phishing-Simulation für verschiedene Fachbereiche.

Alle Testgruppen zeigen eine kritische Phishing Awareness, mit einem durchschnittlichen Employee Security Index von 46,2. Während die Abteilungen HR, IT und Finanzen unternehmensübergreifend überdurchschnittlich abschneiden, fallen am unteren Ende vor allem die Führungskräfte, Assistenzen und das C-Level auf.

Nachgewiesen: Kontinuierliches Training sorgt beim Nutzer für Erfolg

Während sich Abbildung 3 auf Daten aus je vierwöchigen Tests bezieht, in denen jeder Teilnehmer 2-3 Phishing-E-Mails erhielt, ist darüber hinaus insbesondere die Entwicklung der Awareness durch Trainingsmaßnahmen von Interesse. Im Rahmen von mehrmonatigen Phishing-Simulationen, wobei der Nutzer bei jedem Fehlverhalten mittels eines „teachable moment" aufgeklärt wird, konnten sich die Teilnehmer erheblich verbessern: Nach 8 Monaten erreichten sie im Durchschnitt einen ESI® von 90 (blau). Auch bei den zunächst schwächeren Untergruppen ist eine Steigerung zu verzeichnen. Besonders in der Gruppe der Auszubildenden (lila) scheint bereits eine kurze „Starthilfe" zu genügen, um dauerhaft ein gesteigertes Bewusstsein für Phishing-E-Mails zu schaffen.

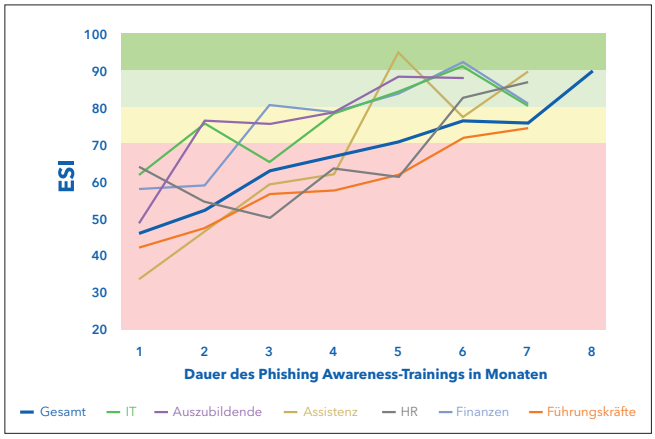

Abbildung 4: Entwicklung der Phishing Awareness unterschiedlicher Fachbereiche während eines kontinuierlichen Awarenss-Trainings im Rahmen einer Phishing-Simulation. Die Daten sind unternehmensübergreifend.

Es ist geplant, neben dem Sicherheitsbewusstsein gegenüber Phishing in den Employee Security Index weitere Faktoren einzubinden, beispielweise andere Angriffsvektoren (Telefon-Phishing) oder der Umgang mit gefälschten Login-Seiten. Das Melden von Vorfällen an die IT soll hingegen positiv eingerechnet werden. Auch Analysen zur Passwortkultur könnten ebenso in die Kennzahl einfließen.

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 anonymisierte Auswertung der Ergebnisse auf Gruppenbasis trägt dabei dem Mitarbeiterschutz zu. 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.

Unsere Awareness Standortbestimmung

Um das IT-Sicherheitsverhalten Ihrer Belegschaft zu prüfen, senden wir Phishing-E-Mails an Ihre Mitarbeiter. Jeder Teilnehmer erhält über einen Zeitraum von vier Wochen 2-3 E-Mails mit individuellen Szenarien zu individuellen Zeitpunkten. Um die Ergebnisse greifbar zu machen, wird das IT-Sicherheitsbewusstsein Ihrer Mitarbeiter in der Kennzahl "Employee Security Index" (ESI®) zusammengefasst und dargestellt.

Über IT-Seal

Die IT-Seal GmbH ist ein erfolgreiches Cyber-Security-Startup, das an der digitalen Selbstverteidigung und menschlichen Firewall ansetzt. Sie testet und trainiert das IT-Sicherheitsbewusstsein, denn aufmerksame Mitarbeiter sind der effektivste Schutz. Das Unternehmen hat 2016 den europaweiten Social Engineering Award gewonnen, es beim internationalen Wettbewerb der SBA Research unter die Top 10 der Cybersecurity Startups Europas geschafft und wurde Ende 2018 als Bestes Cybersecurity Startup (aus D/A/CH) ausgezeichnet.

vertrieb@it-seal.de
www.it-seal.de
06151 493 89 90
@it_seal
Hilpertstraße 31 | 64295 Darmstadt

Wir feuen uns auf Ihre Nachricht!

EMPOWERING SECURITY AWARENESS.

- SECURITY AWARENESS-MESSUNGEN & -TRAININGS
- PHISHING-SIMULATIONEN
- SOCIAL ENGINEERING ZUSATZLEISTUNGEN
- MODULARES E-LEARNING & KURZVIDEOS
- WEBINARE & PRÄSENZSCHULUNGEN

MEHR INFORMATIONEN:
WWW.IT-SEAL.DE

@it_seal

IT-Seal GmbH | Hilpertstr. 31 | 64295 Darmstadt | 06151 493 89 90 | vertrieb@it-seal.de | www.it-seal.de