# ESI® BENCHMARK REPORT

## EDITION 2023

EINE AUSWERTUNG VON ÜBER
1,7 MILLIONEN SIMULIERTEN
**SPEAR-PHISHING-ANGRIFFEN**
**AUF MITARBEITER**

## EMPLOYEE SECURITY INDEX

HORNETSECURITY

# ESI® BENCHMARK REPORT
# EDITION 2023


| | | |
|---|---|---|
| Kapitel 1: | Executive Summary | 2 |
| Kapitel 2: | Phishing: Spitzenreiter unter Cyberattacken | 3 |
| Kapitel 3: | Employee Security Index (ESI®) Benchmark für den Lernfortschritt | 5 |
| Kapitel 4: | ESI® Benchmark Report: wichtigste Ergebnisse und Best Practices | 6 |
| Kapitel 5: | Unternehmen aufgepasst: Rasches Handeln notwendig | 12 |
| Kapitel 6: | Customer Success: Wie Kunden vom Awareness Training profitieren | 17 |
| Kapitel 7: | Zusammenfassung und Ausblick | 19 |


## Kapitel 1: Executive Summary

Phishing und kein Ende: Bei der Zahl der Betrugsversuche mit gefälschten E-Mails jagt ein Rekordhoch das nächste. Immer häufiger nehmen die Phishing-Angreifer Unternehmen ins Visier, da hier das meiste Geld zu holen ist. Sie senden den Mitarbeiterinnen und Mitarbeitern vertrauenserweckende Mails, um sensible Informationen zu stehlen, Daten zu verschlüsseln oder schlimmstenfalls den gesamten Geschäftsbetrieb lahmzulegen.

Mit dem ESI® Benchmark Report möchten wir Sie über die steigenden Phishing-Gefahren für Ihr Unternehmen und wirksame Abwehrmöglichkeiten informieren. Im Fokus steht der Security Awareness Service von Hornetsecurity, mit dem Sie das Sicherheitsverhalten ihrer Mitarbeiter trainieren und eine nachhaltige IT-Sicherheitskultur etablieren können. Herzstück ist der patentierte Employee Security Index (ESI®), der eine wissenschaftlich fundierte Kennzahl zur Messung und Überwachung der Security Awareness bietet.

Wie dies genau funktioniert, zeigt unser aktueller ESI® Benchmark. Die Studie, für die wir rund 1,8 Millionen simulierte Spear-Phishing-Angriffe auf Mitarbeiter in Unternehmen aller Größen und Branchen ausgewertet haben, schafft Transparenz und gibt wichtige Handlungsempfehlungen zur Optimierung der Security Awareness Ihrer Mitarbeiter.

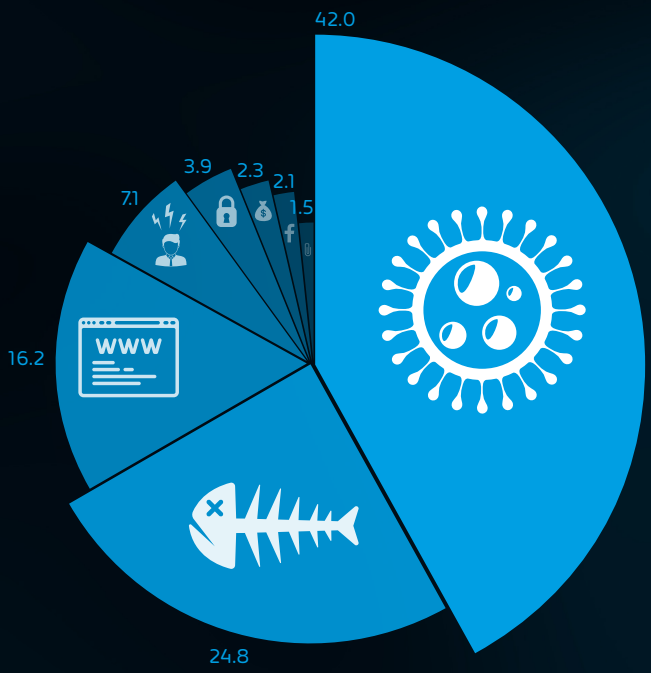
Ganz oben steht die Erkenntnis, dass Unternehmen quer durch alle Branchen ein akzeptables Sicherheitsniveau – das entspricht mindestens einem ESI® 70 – im Durchschnitt bereits nach drei Monaten Security Awareness Training erreichen. Jedoch fällt es ihnen im Trainingsfortgang schwer, dieses Niveau zu halten. Dies liegt zum einen daran, dass der Schwierigkeitsgrad der Phishing-Simulationen im Laufe der Zeit zunimmt, während gleichzeitig immer wieder neue Mitarbeiter ins Training einsteigen. Unternehmen sind daher gut beraten, sich für eine permanente Trainingslaufzeit zu entscheiden.

Ebenso aufschlussreich ist das Ergebnis, dass die erfolgreichsten Phishing-Szenarien die Autoritätsgläubigkeit von Mitarbeitern als psychologischen Einflussfaktor ausnutzen. Hier sind besonders die Führungskräfte gefragt, als Vorbild beim Thema IT-Sicherheit voranzugehen. Sie müssen die Beschäftigten motivieren, am Security Awareness Training teilzunehmen und ihre Erfahrungen untereinander auszutauschen.

## Kapitel 2: Phishing - Spitzenreiter unter Cyberattacken

Phishing ist zu einer allgegenwärtigen Bedrohung geworden. So registriert das Bundeslagebild Cybercrime des Bundeskriminalamts (BKA) für 2021 einen signifikanten Anstieg der Phishing-Zahlen und stuft den Betrug durch gefälschte E-Mails als eine der häufigsten Cyberangriffsarten ein.[1]

Mittlerweile starten über 90 Prozent aller Cyberattacken mit einer Phishing-Mail. Wie der Hornetsecurity Cyber Threat Report 2021/2022 herausfand, stellen 40 Prozent des gesamten E-Mail-Verkehrs eine potenzielle Bedrohung dar.[2] Das Spektrum reicht von wahllosen Massenaussendungen bis hin zu personenbezogenen Spear-Phishing-Mails, für die ein Opfer teilweise über Wochen oder Monate gezielt ausspioniert wird.




| ANGRIFFSTAKTIK | % |
|---|---|
| Andere | 42.0 |
| Phishing | 24.8 |
| URL | 16.2 |
| Erpressung | 7.1 |
| Executable in archive/disk-image | 3.9 |
| Advance-fee scam (Vorschussbetrug) | 2.3 |
| Brand Impersonation | 2.1 |
| Maldoc (schädlicher Anhang) | 1.5 |

**Abb. 1:** Die beliebtesten E-Mail Angriffstaktiken im 1. Halbjahr 2021

## Schlimme Folgen für Unternehmen

Für betroffene Unternehmen kann erfolgreiches Spear-Phishing hohe finanzielle Schäden und einen empfindlichen Vertrauensverlust bei Kunden und Partnern zur Folge haben. In täuschend echt wirkenden E-Mails geben sich die Betrüger als Vorgesetzte, Kollegen oder Geschäftspartner aus, um die Mitarbeiter zur Preisgabe hochsensibler Daten oder zu Klicks auf schädliche Links und Dateianhänge zu verleiten. Manche Beschäftigte werden im Namen angeblicher Vorgesetzter zu Überweisungen hoher Geldsummen auf falsche Konten veranlasst. In anderen Fällen kann ein geglückter Angriff als Einfallstor in das gesamte Unternehmensnetzwerk dienen.

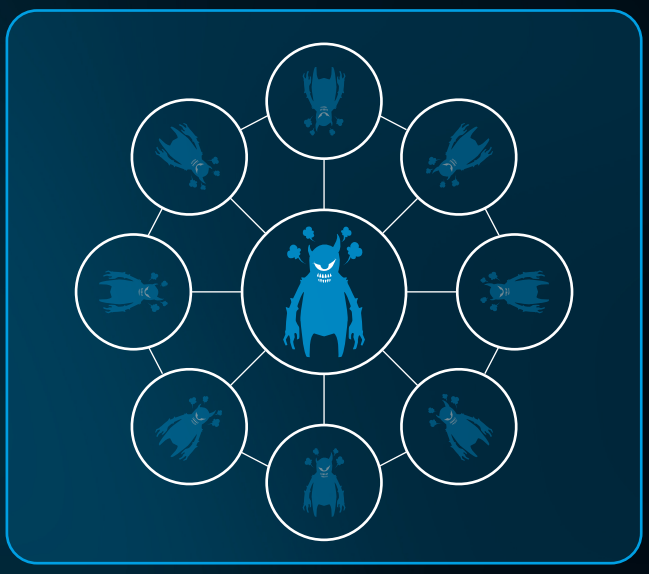

**Abb. 2:** Schäden durch Cybercrime bei Unternehmen in Deutschland laut Bitkom.

## Keine Entspannung in Sicht

Eine Entspannung der aktuellen Phishing-Zahlen ist aufgrund der Attraktivität von Phishing nicht absehbar – im Gegenteil. So hat sich bereits die Corona-Pandemie als verhängnisvoller Katalysator erwiesen, wie der Microsoft Digital Defense Report 2021 zeigt.[3]

Danach erblicken viele Cyberkriminelle ihre Chancen im Ausnutzen von Schwachstellen, die sich aus der vermehrten Homeoffice-Tätigkeit von Mitarbeitern und unzureichenden IT-Sicherheitsmaßnahmen der Unternehmen ergeben.

Eine weitere große Phishing-Welle hob mit dem Beginn der russischen Ukraine-Invasion an. Unter anderem geben sich die Cyberkriminellen als Bankinstitute aus. Sie täuschen vor, prüfen zu müssen, ob sich die Kunden an die EU-Sanktionen gegen Russland halten – und greifen deren Anmeldedaten über nachgebaute Bank-Webseiten ab. Für die Fälschung der Eingabemasken brauchen sie keine Programmierkenntnisse zu besitzen, sondern können auf Phishing-Kits zurückgreifen, die im Darknet für wenig Geld oder kostenlos zu haben sind. Mit diesen Werkzeugkästen gelingt es den Betrügern mittlerweile sogar, die herkömmliche Zwei-Faktor-Authentifizierung (2FA) zu umgehen, die bisher als eine der effektivsten Methoden zum Schutz von Online-Konten galt.



## Weltweite Betrügerbanden aktiv

Die Beispiele zeigen, dass die Phishing-Angreifer immer skrupelloser und ihre Methoden immer ausgeklügelter werden. So gehen die Delikte zunehmend auf das Konto international organisierter Betrügerbanden, die Hunderte Mitglieder zählen und breites Spezial-Know-how bündeln, um die gesamte Angriffskette professionell abzudecken. Laut BKA bieten immer mehr Bedrohungsakteure gezielte Phishing-Angriffe sogar nach dem „Crime-as-a-Service"-Modell an.

Innerhalb der Cybergangs sind bestimmte „Experten" für die Recherche nach Informationen zuständig, die über mögliche Adressaten in den sozialen Medien und anderen Internetquellen zu finden sind, wie Jobbewertungsportale oder Unternehmenswebseiten. Gerade eifrige Social-Media-Nutzer sind eine leichte Beute für Spear-Phishing-Betrüger, wie eine gemeinsame Studie von der Technischen Universität Darmstadt und IT-Seal belegt.[4]

So werden öffentlich zugängliche Profildaten zu aktuellem Job, Ausbildung, Zertifikaten, Hobbys oder Kolleginnen und Kollegen von den Betrügern gerne herangezogen, um daraus individuell zugeschnittene Spear-Phishing-Mails anzufertigen.

Eine besondere Rolle kommt den Bandenmitgliedern zu, die für die Gestaltung der gefälschten E-Mails zuständig sind. Neben der Vorspiegelung von Insider-Wissen müssen sie die wichtigen psychologischen Tricks beherrschen, um ihre Opfer hereinzulegen. Ob Autoritätsgläubigkeit, Neugier, Hilfsbereitschaft, Zeitdruck oder Angst: Wer auf einen dieser psychologischen Einflussfaktoren setzt, kann ziemlich sicher sein, dass der Mail-Empfänger seine Aufforderungen unüberlegt befolgt.

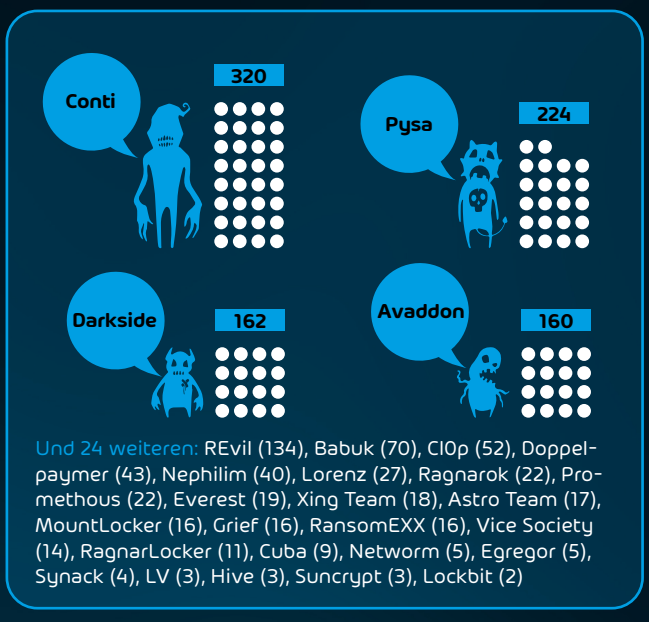



**Abb. 3:** Die Betrügerbanden mit den meisten veröffentlichten Leaks von gestohlenen oder erpressten Personendaten

## Kapitel 3: Employee Security Index (ESI®) Benchmark für den Lernfortschritt

Mit Hornetsecurity steht ein Anbieter von Security-Awareness-Trainings zur Verfügung, der Trainings-Inhalte, -Methoden und -Werkzeuge zu einem innovativen Service-Angebot kombiniert.

Zentrales Alleinstellungsmerkmal ist der patentierte Employee Security Index (ESI®) von IT-Seal, die seit Mai 2022 zur Hornetsecurity-Gruppe gehört. Damit steht ein wissenschaftlich fundierter Benchmark zur Verfügung, mit dem sich das Sicherheitsverhalten von Mitarbeitern objektiv messen und überwachen lässt.

Dies ist mit den bisherigen Messansätzen nicht möglich, da sie keine Standardisierung – und damit keine Vergleichbarkeit über längere Zeiträume hinweg oder zwischen verschiedenen Abteilungen, Rollen und Unternehmensstandorten erlauben. Damit verbunden ist das Risiko, dass einzelne Sicherheitsprobleme, Fehler oder Klicks auf Spear-Phishing-Mails überbewertet oder unterbewertet werden und die Unternehmen letztlich keine Transparenz über das Sicherheitsverhalten ihrer Mitarbeiter erhalten. Sie investieren daher häufig zu viel oder auch zu wenig, um ein angemessenes Sicherheitsniveau zu erreichen.

## Vorbereitungszeit entscheidend

Anders der ESI®, der eine realitätsnahe und reproduzierbare Methode zur Messung der Security Awareness darstellt. Zur Berechnung des ESI® werden die Spear-Phishing-Angriffe in unterschiedliche Kategorien (sogenannte „Level") unterteilt, die sich nach dem Zeitaufwand richten, die Cyberkriminelle in die Vorbereitung und Durchführung investieren müssen. Dieser Aufwand setzt sich unter anderem aus der Informationsbeschaffung aus öffentlich zugänglichen Quellen, der technischen Vorbereitung, dem Kopieren von Webseiten-Designs sowie der Bereithaltung der für einen Phishing-Angriff notwendigen IT-Infrastruktur zusammen.

So lassen sich sieben Kategorien einteilen, die jeweils einer Vorbereitungszeit von einer Stunde bis mehrere Tage und Wochen entsprechen. Der individuelle ESI® eines Unternehmens ergibt sich daraus, wie die Beschäftigten auf Phishing-Simulationen verschiedener Schwierigkeitsgrade reagieren.

Um das Sicherheitsniveau eines Unternehmens standardisiert einordnen zu können, hat Hornetsecurity Toleranzwerte für ein vorbildliches Sicherheitsverhalten der Testgruppen definiert. Diese Werte basieren auf den „Erfolgsraten" aus Sicht der Angreifer. Da „Erfolgsraten" von 0 illusorisch sind (jeder Mensch macht Fehler), liegen die Toleranzwerte jeweils an der Schnittstelle zwischen Sicherheit und Realisierbarkeit. Eine vorbildliche Testgruppe mit den niedrigsten „Erfolgsraten" erreicht auf einer Skala von 0 – 100 mindestens einen ESI® von 90.

Wird doppelt so häufig kritisches Verhalten gezeigt, erreicht die Gruppe einen ESI®-Wert von lediglich 80; bei dreifach kritischem Verhalten nur noch einen ESI® von 70. Ergebnisse unter 70 gelten als kritisch. Die von Hornetsecurity definierten Toleranzwerte basieren auf dem aktuellen Stand der Forschung und Erfahrungswerten mit Phishing-Simulationen in Unternehmen verschiedenster Branchen.

Damit bietet der ESI® den Unternehmen eine greifbare und verlässliche Kennzahl, um die einzelnen Mitarbeitergruppen standardisiert miteinander zu vergleichen. Wer ist sicherer, der Vertrieb oder die Personalabteilung, und wie steht die Geschäftsführung im Vergleich zur Buchhaltung da? Diese Informationen sind wertvoll, wenn es um die gezielte Ableitung weiterer Schulungsmaßnahmen geht.

Kapitel 4:

# ESI® BENCHMARK REPORT
# WICHTIGSTE ERGEBNISSE UND BEST PRACTICES

Wie effektiv der ESI® zur Messung und Optimierung der Security Awareness von Mitarbeitern ist, zeigt der aktuelle Benchmark-Report. Dazu wurden rund 1,8 Millionen simulierte Spear-Phishing-Angriffe ausgewertet, die im Zeitraum von Mai 2019 bis Juni 2022 auf ca. 140.000 Nutzer aus 350 Unternehmen aller Größen und Branchen ausgeführt wurden.

Betrachtet wurde das Nutzerverhalten über einen Trainingsverlauf von jeweils zwölf Monaten. Dabei wurde deutlich, welchen Einfluss unter anderem die Branchenzugehörigkeit sowie die Funktion und Position eines Mitarbeiters im Unternehmen auf die Klickraten haben. Ebenso wurden die Auswirkungen äußerer Faktoren, wie Zeitverlauf, Trainingspausen und Einsatz psychologischer Tricks, untersucht.

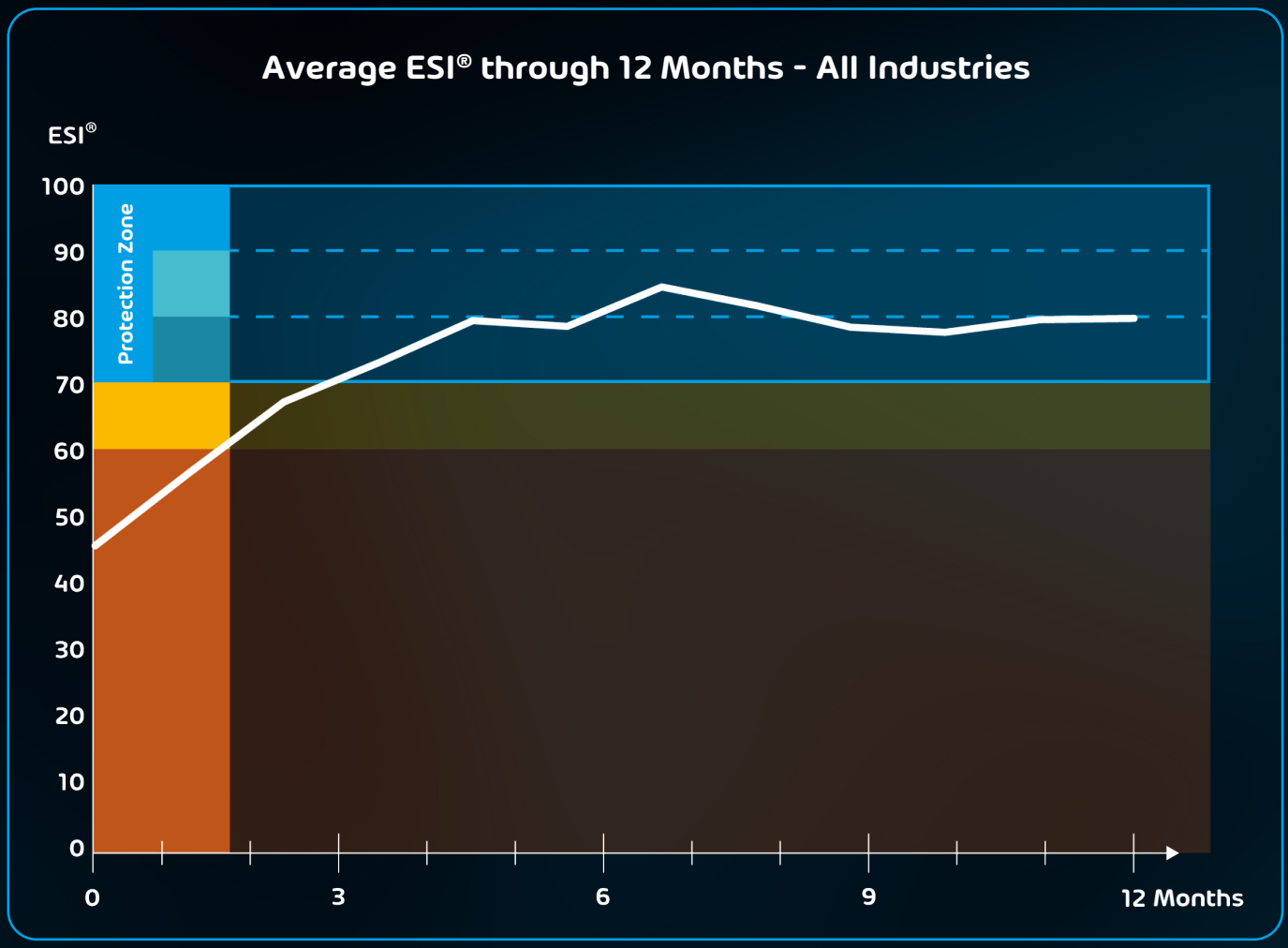
Die Ergebnisse des ESI® Benchmarks geben Aufschluss, mit welchen Awareness-Trainingsmaßnahmen ein optimales Sicherheitsbewusstsein der unterschiedlichen Nutzergruppen erreicht werden kann.

Hier eine kleine Auswahl davon.

HORNETSECURITY

IT-SEAL
Part of HORNETSECURITY group

## Auswertung 1: ESI®-Durchschnittsverlauf




## Kontinuierliches Awareness-Training erforderlich

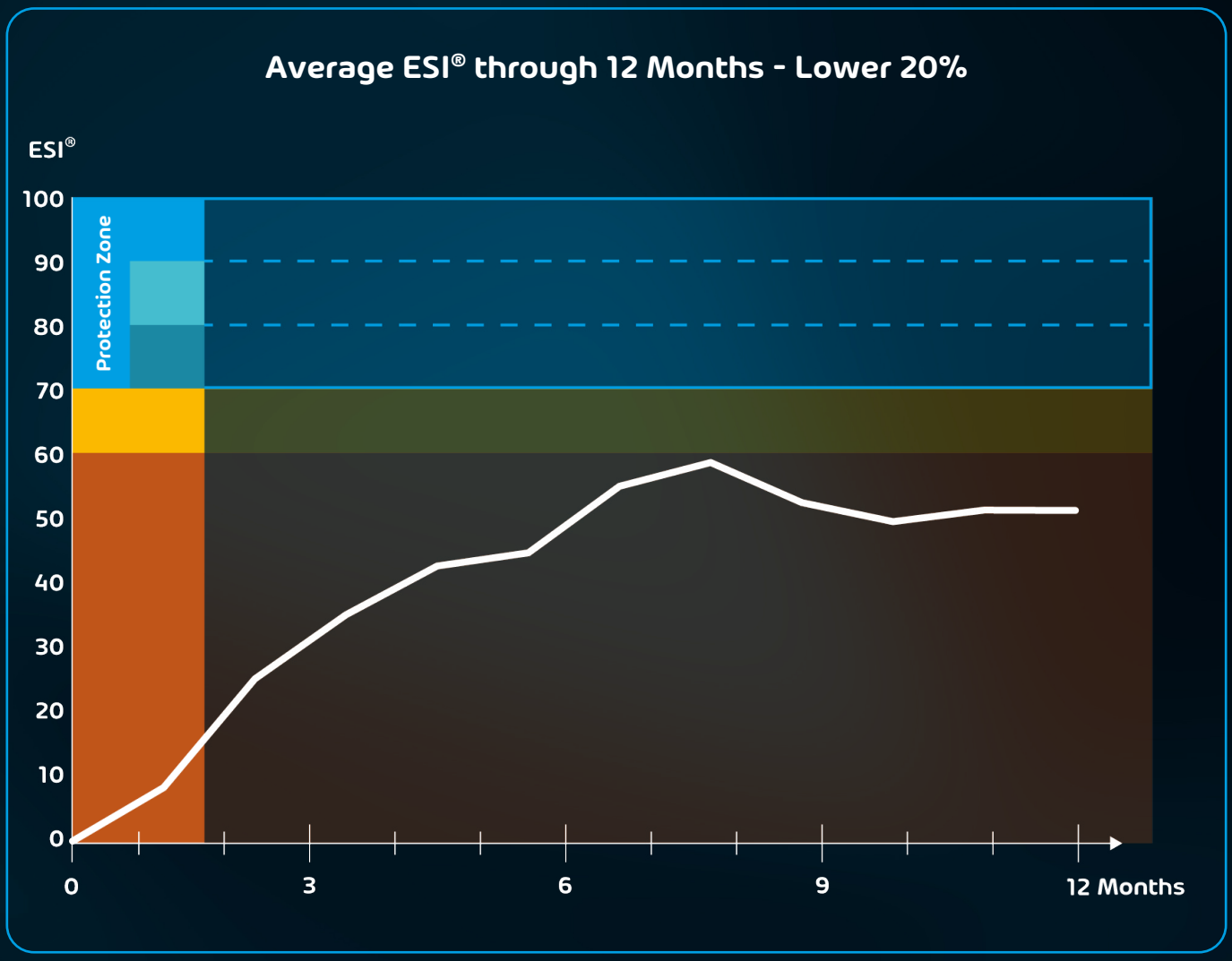
Der durchschnittliche ESI®-Verlauf über 12 Monate macht deutlich, wie wichtig ein kontinuierliches Security-Awareness-Training für die Mitarbeiterinnen und Mitarbeiter ist. Nur wenn die Spear-Phishing-Simulationen regelmäßig wiederholt und fortlaufend an die aktuellen Angreifermethoden angepasst werden, lässt sich ein hohes Sicherheitsniveau auch über einen längeren Zeitraum halten.

Wie die Grafik zeigt, steigt die ESI®-Kurve nach Beginn des Awareness-Trainings steil an und erreicht nach durchschnittlich drei Monaten ein akzeptables Sicherheitslevel. Doch fällt es den Unternehmen und Organisationen schwer, dieses Niveau dauerhaft zu halten. Dies liegt zum einen daran, dass die Beschäftigten die bei den Spear-Phishing-Simulationen erlernten Lektionen im Laufe der Zeit wieder vergessen.

Damit die Belegschaft „in Übung" bleibt, sollten die Unternehmen und Organisationen daher auf permanente Trainings-Laufzeiten setzen. Nur durch die regelmäßige Wiederholung der nachgestellten Spear-Phishing-Angriffe ist gewährleistet, dass die Mitarbeiter die Wichtigkeit der erhaltenen Informationen erkennen und im Langzeitgedächtnis ablegen.

Zum anderen stellen die Betriebe immer wieder neue Mitarbeiter ein, die für die Phishing-Gefahren sensibilisiert und im Erkennen von Fake-Mails geschult werden müssen. Mit kontinuierlichen Awareness-Kampagnen ist es möglich, auch Neuankömmlinge nahtlos in die Trainings einzubinden und in ihrer Eigenverantwortung für die IT-Sicherheit zu bestärken.

## Auswertung 2: ESI® der „Unteren 20%“




## Kein Training nach dem „Gießkannen-Prinzip“!

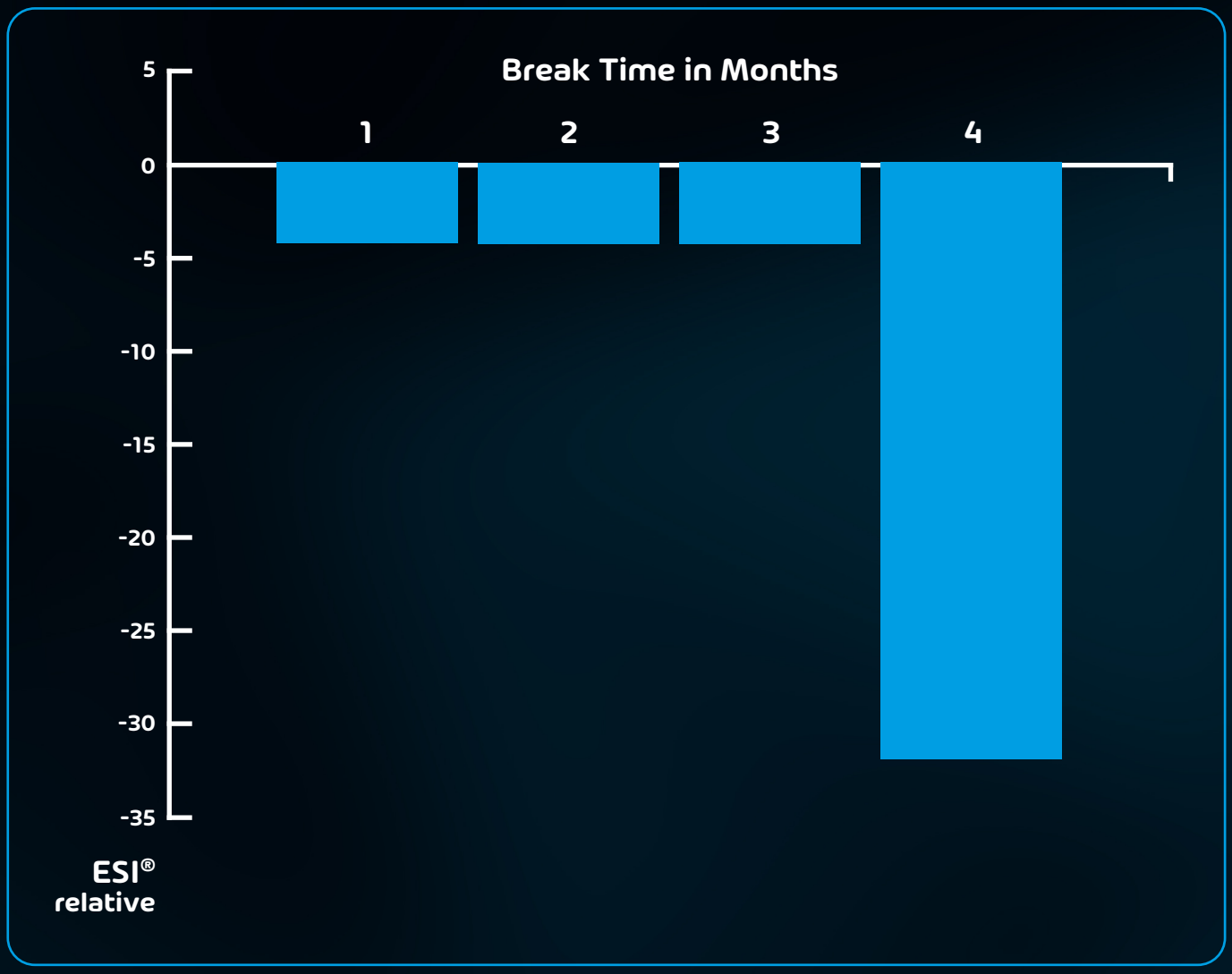
Jede Kette ist nur so stark wie ihr schwächstes Glied. Dass diese Erkenntnis gerade auch für die „menschliche Firewall“ zum Schutz vor heimtückischen Spear-Phishing-Angriffen gilt, zeigt der ESI®-Verlauf der so genannten „Unteren 20%“. Dabei handelt es sich um diejenige Nutzergruppe, die die höchsten Klickraten auf nachgestellte Spear-Phishing-Angriffe aufweist.

Zwar stellt sich auch bei den „Unteren 20%“ innerhalb von 12 Monaten ein gewisser Lerneffekt ein, wie am obigen Kurvenverlauf abzulesen ist. Jedoch kann die Gruppe in diesem Zeitraum kein einziges Mal ein angemessenes Sicherheitsniveau – also einen ESI® von mindestens 70 – erreichen. Und das, obwohl die „Unteren 20%“ dasselbe Security-Awareness-Training erhielten wie ihre Kolleginnen und Kollegen.

Die Untersuchungsergebnisse machen deutlich, dass die Sicherheitsschulungen nicht nach dem Gießkannen-Prinzip verteilt, sondern am individuellen Lernbedarf der Mitarbeiter ausgerichtet werden sollten. Denn nicht jeder Nutzer lernt auf die gleiche Weise gleich schnell und gleich gut.

Der ESI® versetzt die Unternehmen in die Lage, schnell und einfach auf die unterschiedlichen Lernbedarfe ihrer Mitarbeiter einzugehen. Denn er bietet eine greifbare und verlässliche Kennzahl, um die persönlichen Lernfortschritte zu dokumentieren und den gezielten Einsatz geeigneter Schulungsmaßnahmen abzuleiten. Zeigen Nutzer wie die „Unteren 20%“ erhöhte Klickraten, müssen sie intensiver trainiert werden.

## Auswerung 3: ESI®-Drop nach einer Pause




## Trainingspausen für nachhaltigen Wissenserwerb

Das Sicherheitsbewusstsein von Mitarbeitern lässt sich mit einem Muskel vergleichen, der ohne regelmäßiges Training erschlafft. Unterbrechen einzelne Gruppen oder Mitarbeiter für einige Zeit das Training und steigen dann wieder ein, zeigt sich ein deutlicher Abfall im Sicherheitsverhalten. So scheinen diese Nutzer wichtige Lerninhalte aus den Spear-Phishing-Simulationen wieder vergessen zu haben und deutlich nachlässiger im Umgang mit eingehenden E-Mails geworden zu sein.

Wie stark dieser Effekt ist, zeigt der ESI®-Drop in dieser Grafik, in der die „Unteren und Oberen 25%" – also Nutzergruppen mit besonders hohen und besonders niedrigen Klickraten – nicht berücksichtigt wurden. Bereits nach dem ersten Monat Trainingspause sinkt der ESI® um fünf Punkte und liegt damit schon wieder häufig unterhalb des angestrebten Sicherheitsniveaus. Nach vier Monaten ohne Awareness-Trainings sinkt der ESI® bereits um über 30 Punkte. Das heißt konkret, dass die Unternehmen beim Sicherheitsverhalten ihrer Mitarbeiter fast schon wieder am Anfang stehen.

Doch können kurze Trainingspausen durchaus auch einen pädagogischen und didaktischen Nutzen für die Unternehmen entfalten. Haben bestimmte Gruppen oder Mitarbeiter das angestrebte Sicherheitsniveau einmal erreicht, sollten sie bewusst für eine Zeit von zwei bis drei Monaten pausieren. Denn es hat sich gezeigt, dass sich einmal erworbene Lerninhalte nachhaltiger auf das Sicherheitsverhalten auswirken, wenn sie nach einer gewissen Pause wieder aufgefrischt werden. Außerdem lässt sich damit einer möglichen "Security Fatigue" bei den Mitarbeitern vorbeugen.

## Auswertung 4: Technologie-Sektor vs. Durchschnitt

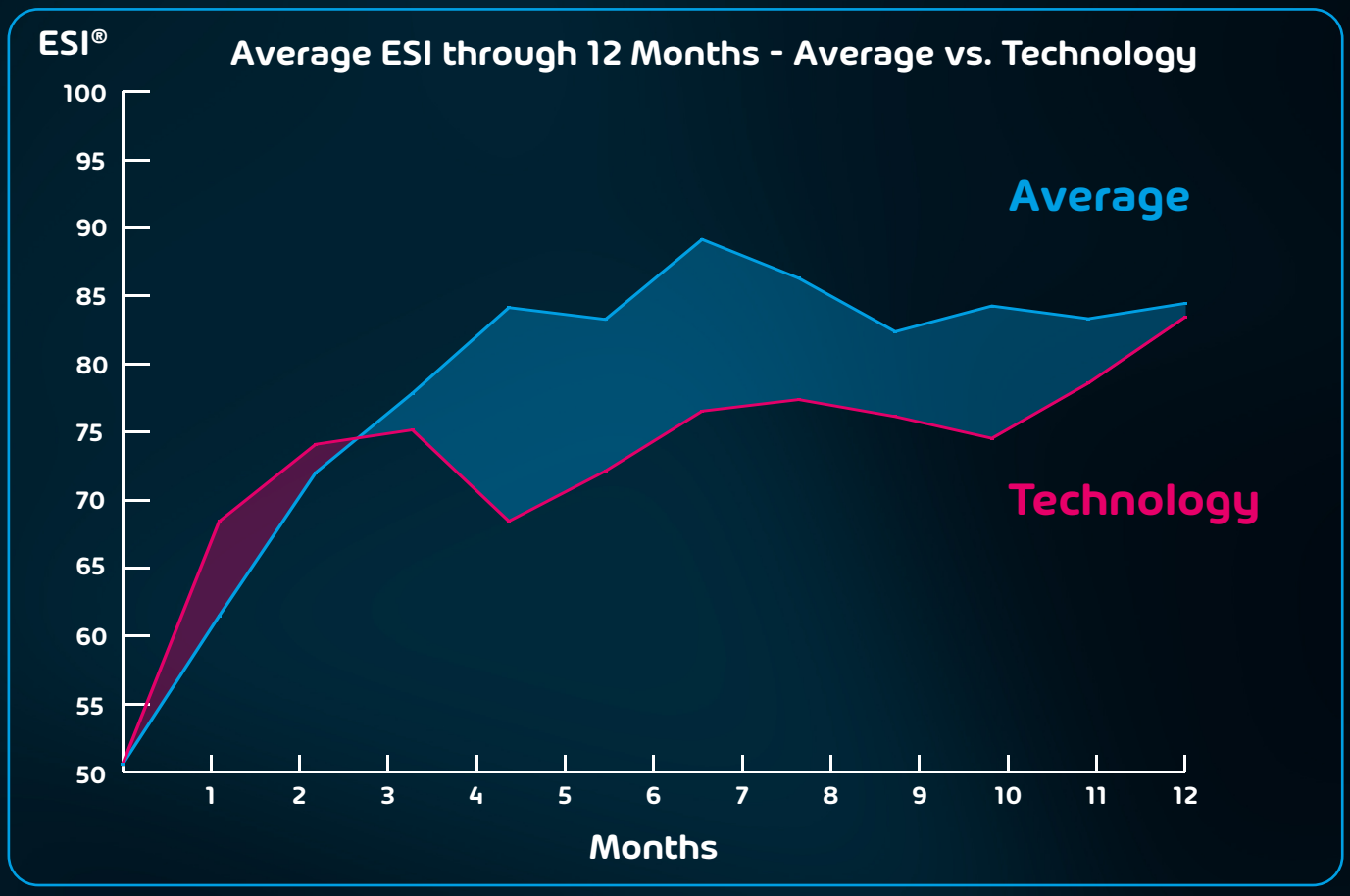



**Abb. X:** Technologie-Sektor vs. Durchschnitt ESI® Verlauf über 12 Monate

## „Technologie-affin" mit deutlicher Selbstüberschätzung

Eigentlich sollte man meinen, dass die Mitarbeiterinnen und Mitarbeiter von IT-Unternehmen deutlich versierter im Umgang mit Cyber-Risiken sind als die Angehörigen anderer Branchen. Doch erweist sich diese Annahme als Trugschluss, wie die obigen ESI®-Verlaufskurven zeigen. Danach weist der Technologie-Sektor über den gesamten Untersuchungszeitraum deutlich höhere Klickraten als der allgemeine Durchschnitt auf.

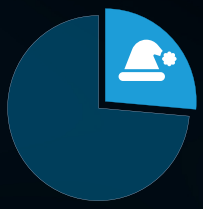
Dies lässt sich darauf zurückführen, dass Menschen ihre eigenen Fähigkeiten oft überschätzen, besonders wenn es um Themen geht, die ihnen beruflich nahestehen. In der IT-Branche kann eine solche Sichtweise beträchtliche Gefahren für die IT-Sicherheit bergen. Dies betrifft nicht nur das eigene Unternehmen, sondern auch dessen Kunden. So sind im IT-Sektor sehr viele Software- und Rechenzentrums-Anbieter ansässig, die für andere Unternehmen Anwendungen entwickeln und betreiben.

Auch in diesem Fall hilft der ESI®, die branchenspezifischen Defizite im Sicherheitsverhalten auszugleichen. IT-Unternehmen erhalten damit eine zuverlässige Kennzahl, um das Sicherheitsniveau und die Lernfortschritte der Mitarbeiter zu ermitteln und den gezielten Einsatz weiterer Schulungsmaßnahmen abzuleiten. So können die Awareness-Trainings systematisch an den erhöhten Lernbedarf von IT-Beschäftigten angepasst werden.

## Die Top 5 Spear-Phishing-Szenarien und ihre psychologischen Faktoren

**1. Autorität des Absenders & Neugier:**

Die Geschäftsführung informiert über ein neues Organigramm, welches die Verantwortlichkeiten im Unternehmen darstellt. Es kann im Intranet heruntergeladen werden.
**28% Erfolgsrate**

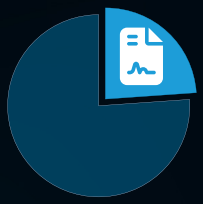


**2. Autorität des Absenders & Neugier:**

Weihnachtsszenario: Die Geschäftsleitung verschenkt ihre Lieblingsbücher aus dem aktuellen Jahr an alle Mitarbeiter.
**28% Erfolgsrate**

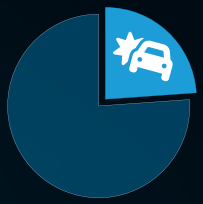
**3. Angst vor unangenehmen Konsequenzen:**

Dem Empfänger wird mitgeteilt, sein E-Mail-Konto sei voll. Unter einem Link kann Abhilfe geschaffen werden.
**24% Erfolgsrate**



**4. Pflichtbewusstsein & Angst vor unangenehmen Konsequenzen:**

Der Empfänger wird aufgefordert, die neuen Richtlinien für die Arbeit im Home Office zu unterschreiben.
**24% Erfolgsrate**



**5. Neugier & Angst:**

Der Empfänger erfährt, dass Autos auf dem Firmenparkplatz beschädigt wurden. Er soll anhand von Fotos prüfen, ob sein Auto betroffen ist.
**24% Erfolgsrate**

## Jeder hat andere „Triggerpunkte“

Wer auf welche Spear-Phishing-Mail hereinfällt, hängt von vielen verschiedenen Faktoren ab: Stress- und Trainingslevel des Nutzers, Konzentrationsvermögen, Ausgestaltung der E-Mails, Betreffzeilen etc.

Eine herausragende Bedeutung kommt jedoch den psychologischen Einflussfaktoren zu, auf die jeder Mensch unterschiedlich reagiert. So gibt es eher autoritätshörige Nutzer, die jede E-Mail sofort anklicken, wenn diese vermeintlich von ihrem Teamleiter oder der Geschäftsleitung kommt. Andere Mitarbeiter wiederum werden verstärkt durch Faktoren aktiviert, die an die Hilfsbereitschaft oder das Pflichtbewusstsein appellieren.

Neugier, Angst, Autoritätsgläubigkeit, Hilfsbereitschaft, Eitelkeit und viele andere Gefühle sind wichtige psychologische Einflussfaktoren für die Betrüger. Sie setzen sie bewusst und häufig auch in individuellen Kombinationen ein, um ihre potenziellen Opfer hereinzulegen. Damit die Mitarbeiter genau das tun, was von ihnen verlangt wird, zielen die Spear-Phishing-Angriffe geschickt auf ihr schnelles Denksystem, wie es der Psychologe und Nobelpreisträger Daniel Kahneman in seinem Bestseller dem langsamen, rationalen Denken gegenüberstellt.[5]

Wirksame Phishing-Simulationen sollten daher immer auf die Einflussfaktoren zielen, für die sich ein Nutzer als besonders anfällig erweist. Auf diese Weise lernen die Mitarbeiter im Trainingsverlauf, sich bewusst gegen die psychologischen Angreifertricks zu wappnen, für die sie besonders empfänglich sind.

## Kapitel 5: Unternehmen aufgepasst - Rasches Handeln notwendig

Wie die Ausführungen zeigen, erfordern die steigenden Phishing-Risiken von den Unternehmen ein schnelles Handeln. Sie müssen sich der Tatsache stellen, dass auch die fortschrittlichsten IT-Sicherheitstechnologien allein nicht ausreichen, um sich vor Spear-Phishing zu schützen. Denn obwohl es den IT-Abteilungen heute gelingt, täglich Millionen betrügerischer E-Mails abzufangen, schaffen es doch etliche in den Posteingang der Beschäftigten.

Daher sollten es die Unternehmen als vordringliche Aufgabe ansehen, die Mitarbeiterinnen und Mitarbeiter in ihrer Rolle als menschliche Firewall zu bestärken. Dieses Erfordernis wird auch durch eine aktuelle Studie des Bitkom-Digitalverbands untermauert, wonach ein Großteil der Cyberkriminellen den „Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette ausnutzt.[6]

Am wirksamsten ist eine IT-Sicherheitsstrategie, die die drei zentralen Bausteine einer Sicherheitskultur integriert: Mindset – Skillset – Toolset. Das heißt konkret: Die Mitarbeiter müssen für die Bedrohungslage durch Spear-Phishing-Mails sensibilisiert, in deren Erkennung geschult und mit geeigneten technischen und organisatorischen Maßnahmen bei der Abwehr unterstützt werden.

### Mindset

**Motivation und offene Kommunikation**

- Verständnis für Bedrohungslage
- Eigenverantwortung betonen
- Kommunikationshilfen für alle Stakeholder

### Skillset

**Fähigkeiten und Wissen aneignen**

- Phishing-Simulation
- E-Learning
- Online-Seminare
- Präsenzschulungen
- Awareness-Materialien

### Toolset

**Aktiv ins Geschehen eingreifen**

- Live-Dashboard
- Passwortmanager
- Sicherheitsmeldeketten
- Reporter-Button Outlook Add-In

## Mindset: Sicheres Gefühl für Gefahren wecken

Das blinde Vertrauen auf IT-Sicherheitstechnik ist unter den Beschäftigten weit verbreitet. So werden eingehende Mails bedenkenlos geöffnet und den darin enthaltenen Aufforderungen Folge geleistet, zumal die Nachrichten von vertrauenswürdigen Quellen zu stammen scheinen. Unternehmen sind daher gut beraten, einen Umdenkprozess anzustoßen, indem sie an die Eigenverantwortung und Selbstwirksamkeit der Mitarbeiter appellieren. Diese müssen verinnerlichen, dass ihr Einsatz und ihre Aufmerksamkeit mitentscheidend für das Funktionieren des gesamten Unternehmens sind.

Zur Vorbereitung auf die Security-Awareness-Trainings empfehlen sich Informationskampagnen, die vom Management initiiert und von den Führungskräften und IT-Sicherheitskräften begleitet werden.

Erfahrungsgemäß hinterlassen Zahlen und Fakten über Sicherheitsvorfälle in der eigenen Branche einen bleibenden Eindruck bei den Mitarbeitern.

Ein Beispiel bietet der österreichisch-chinesische Maschinenbauer FACC, der rund 43 Millionen Euro verlor, als ein Buchhalter auf gefälschte E-Mails des angeblichen Firmenchefs hereinfiel. Er überwies diese Summe an Internetbetrüger, die ihm vorgaukelten, es handele sich um streng vertrauliche Transaktionen für einen Firmenkauf.

Die Informationskampagnen entfalten dann eine maximale Schlagkraft, wenn sie verschiedene Kanäle bespielen sowie Team-Meetings, Videos und Rundmails umfassen.

## Skillset: Intuitive Entscheidungen fördern

Die folgenden Security-Awareness-Trainings sollten sich nicht auf klassische Präsenzschulungen, E-Learnings und Webinare beschränken. Denn diese Lernformen vermitteln nur rein theoretische Kenntnisse über Phishing-Attacken. Um die Sinne der Nutzer im Arbeitsalltag zu schärfen, haben sich praxisnahe Spear-Phishing-Simulationen bewährt.

Diese verwenden echte Mitarbeiter- und Unternehmensinformationen, um reale Angriffe nachzustellen. Fällt ein Mitarbeiter auf eine nachgestellte Fake-Mail herein, landet er direkt auf einer interaktiven Erklärseite mit Hinweisen auf verdächtige Merkmale der Nachricht: von Buchstabendrehern in der Adresszeile über gefälschte Subdomains bis hin zu zweifelhaften Links und Anhängen.

Spear-Phishing-Simulationen sind deshalb so wirksam, weil sie die impulsiven Entscheidungen der Mitarbeiter fördern, die für die spontanen Klicks auf die E-Mails verantwortlich sind. In seinem Bestseller „Schnelles Denken, langsames Denken" grenzt der der Psychologe und Nobelpreisträger Daniel Kahneman dieses instinktive und emotionale Denksystem des Menschen von dessen rationaler und logischer Entscheidungsfähigkeit ab.[7]

Zudem machen sich nachgestellte Spear-Phishing-Attacken den „Most Teachable Moment" eines Mitarbeiters zunutze. Indem sie ihn genau im richtigen Moment über sein potenziell schadhaftes Verhalten aufklären, wird er besonders effektiv in der Angriffserkennung geschult – und geht künftig vorsichtiger mit eingehenden E-Mails um.

Damit dieser Lerneffekt anhält, sollten die simulierten Spear-Phishing-Angriffe kontinuierlich wiederholt und an die immer neuen Angriffsmethoden angepasst werden. Ansonsten fällt das Gelernte schnell dem Vergessen anheim, wie der Psychologe Dr. Hermann Ebbinghaus bereits 1885 herausgefunden hat.[8]

So müssen nach der Ebbinghausschen Vergessenskurve Lerninhalte mehrfach wiederholt werden, bevor sie sich dauerhaft einprägen. Anhand der Häufigkeit der Wiederholung erkennt das Gehirn die Wichtigkeit der Informationen und legt diese im Langzeitgedächtnis ab. Danach müssen Security Awareness Trainings zu einem anhaltenden Prozess werden, wenn sie nachhaltig wirken wollen.

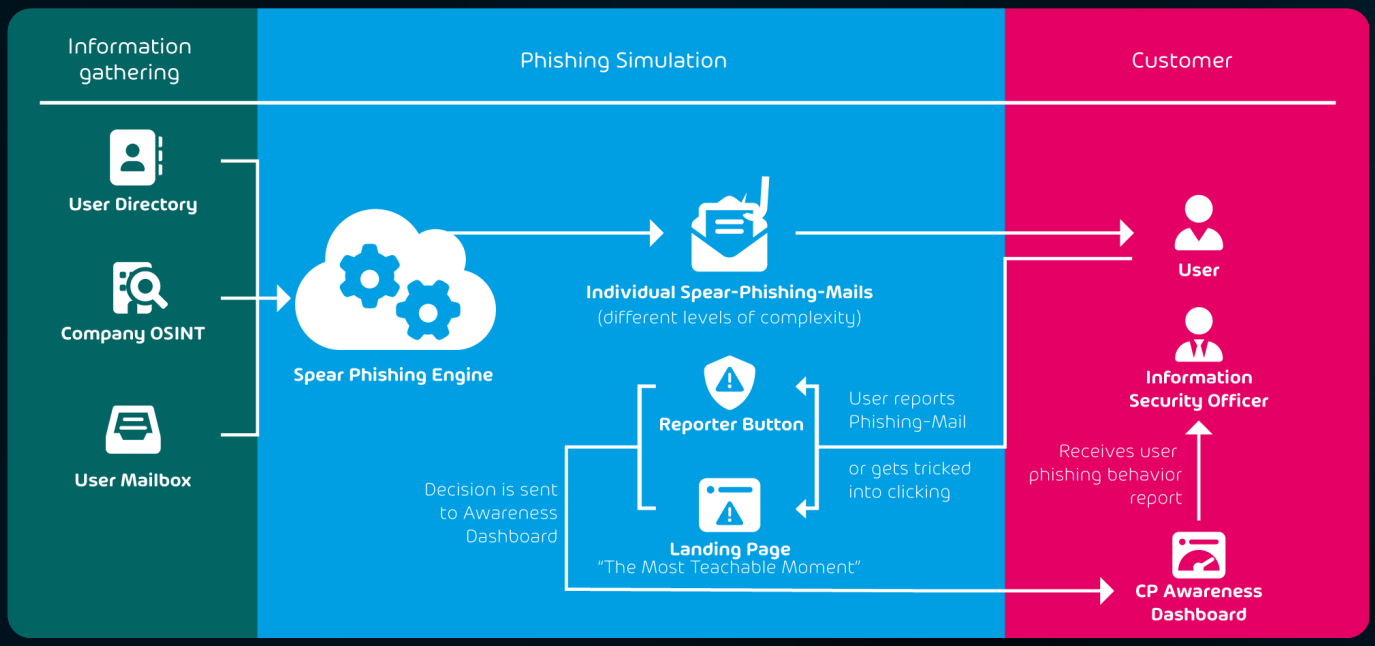



**Abb. 4:** Ablauf der Spear-Phishing-Simulation

## Toolset: i-Tüpfelchen jeder Phishing-Abwehrstrategie

Mit dem richtigen Toolset können Unternehmen ihre Spear-Phishing-Abwehr komplettieren. Von großem Vorteil sind Password Manager, die einfach in die IT-Arbeitsplatzumgebung zu integrieren sind und eine zentrale Speicherung und Verwaltung digitaler Identitäten erlauben.

Password Manager helfen zu verhindern, dass Mitarbeiter aus Bequemlichkeit immer dieselben Log-in-Daten verwenden. Gelingt es Spear-Phishing-Angreifern, ein einzelnes Password zu stehlen, greifen sie damit nicht mehr automatisch auf alle anderen Konten eines Nutzers zu.

Um der zunehmenden 2FA-Aushebelung einen Riegel vorzuschieben, sollten Unternehmen auf FIDO2 (Fast Identity Online) umsteigen.[9]

FIDO2 bietet ein innovatives 2FA-Verfahren, bei dem die Registrierung für einen Online-Dienst verschlüsselt erfolgt und selbst mit den aktuellen Hightech-Angriffsverfahren nicht geknackt werden kann.

Ein weiteres nützliches Werkzeug bietet ein direkt in Microsoft Office integrierbarer „Reporter Button". Er hilft Mitarbeitern bei der Identifizierung und Meldung zweifelhafter E-Mails.

Nutzer erhalten auf Knopfdruck nützliche Hinweise, ob eine Mail gefälscht sein könnte, und leiten diese bei Bedarf zur weiteren Prüfung an die IT-Sicherheitsverantwortlichen weiter.

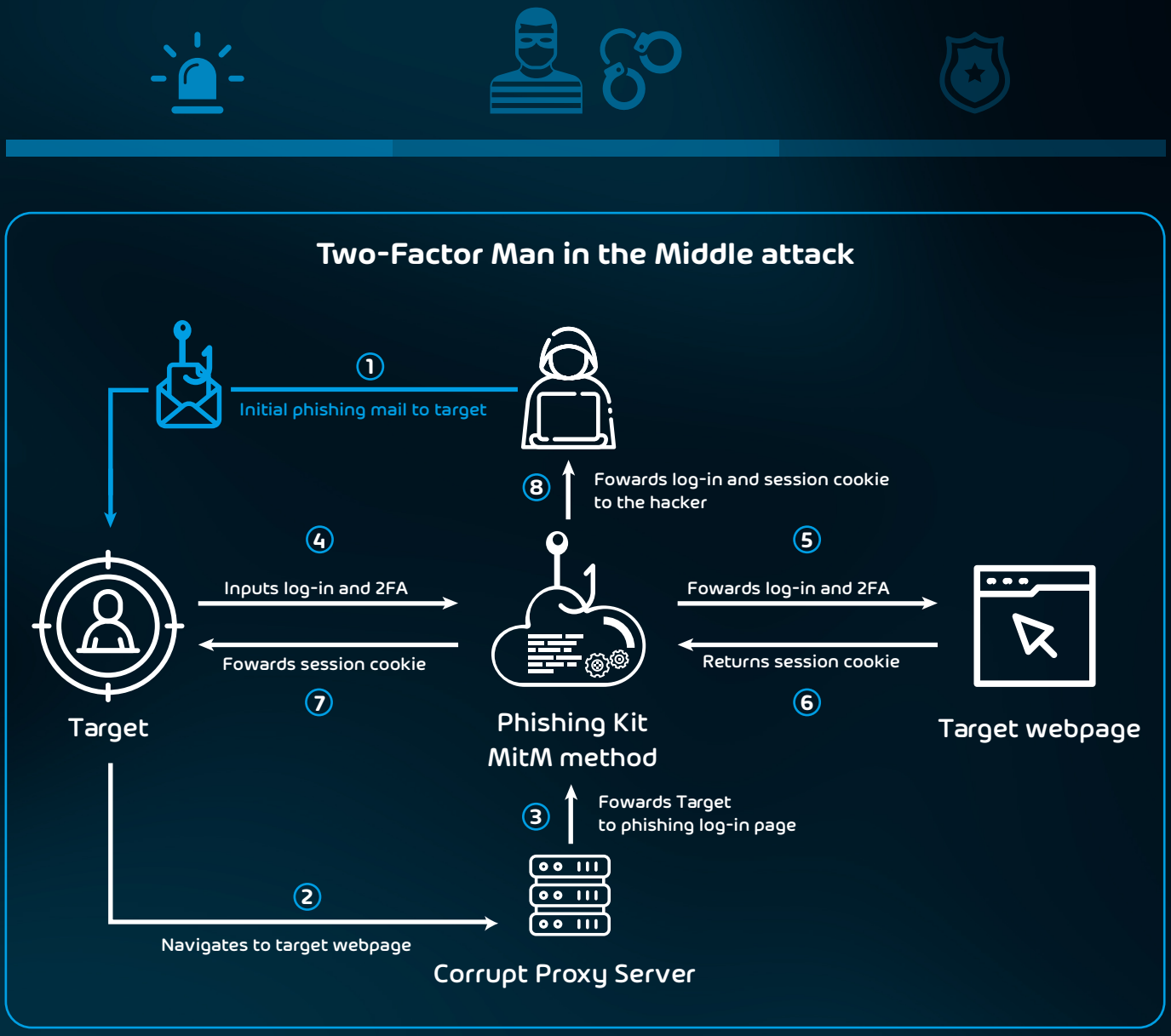



**Abb. 5:** Aufbau eines Man in the Middle Attacks gegen 2FA Authentifizierungen

## Security Awareness Service von Hornetsecurity bietet Komplett-Lösung

Für die Durchführung der Security Awareness Trainings hat Hornetsecurity eine Komplett-Lösung entwickelt, die innovative Lernformate, wie E-Training, „Most Teachable Moment" und Gamification, mit einer der fortschrittlichsten Spear-Phishing-Simulationen kombiniert. Im Rahmen von klassischen E-Learnings, Kurzvideos und Quizzen werden die Teilnehmer mit wichtigen Informationen über die wachsenden Cyber-Risiken versorgt und wie sie sich und ihr Unternehmen am besten davor schützen können.

Bei den simulierten Phishing-Angriffen kommt die ebenfalls patentierte Spear-Phishing-Engine ins Spiel, die dafür sorgt, dass die Phishing-Angriffe täuschend echt wirken.

Die Spear-Phishing-Engine basiert auf innovativen Open Source Intelligence (OSINT)-Technologien, die unternehmens-, abteilungs- und mitarbeiterspezifische Phishing-Szenarien automatisiert generieren. Für die Phishing-Inhalte werden öffentlich zugängliche Daten des Unternehmens (zum Beispiel aus Arbeitgeberportalen) und weiteren Quellen genutzt.

So lassen sich realitätsnahe Spear-Phishing-Mails anfertigen, in denen etwa der Abteilungsleiter eine Nachfrage zu einer Rechnung hat, die als Dateianhang beigefügt ist. In anderen E-Mails tarnen sich die Betrüger als Kollege oder Mitarbeiter und erinnern an ein vermeintlich geführtes Fachgespräch. Der E-Mail-Empfänger erhält zur Vertiefung einen „interessanten" Link, der in Wahrheit direkt zu einer Schadsoftware führt.

Die Beispiele zeigen, dass die Masche der Spear-Phishing-Angreifer immer die gleiche ist. Sie greifen tief in die psychologische Trickkiste und zielen so geschickt auf die Gefühle ihrer potenziellen Opfer, dass diese – ohne nachzudenken – genau das machen, was die Cyberkriminellen von ihnen verlangen.

**Mehr erfahren**

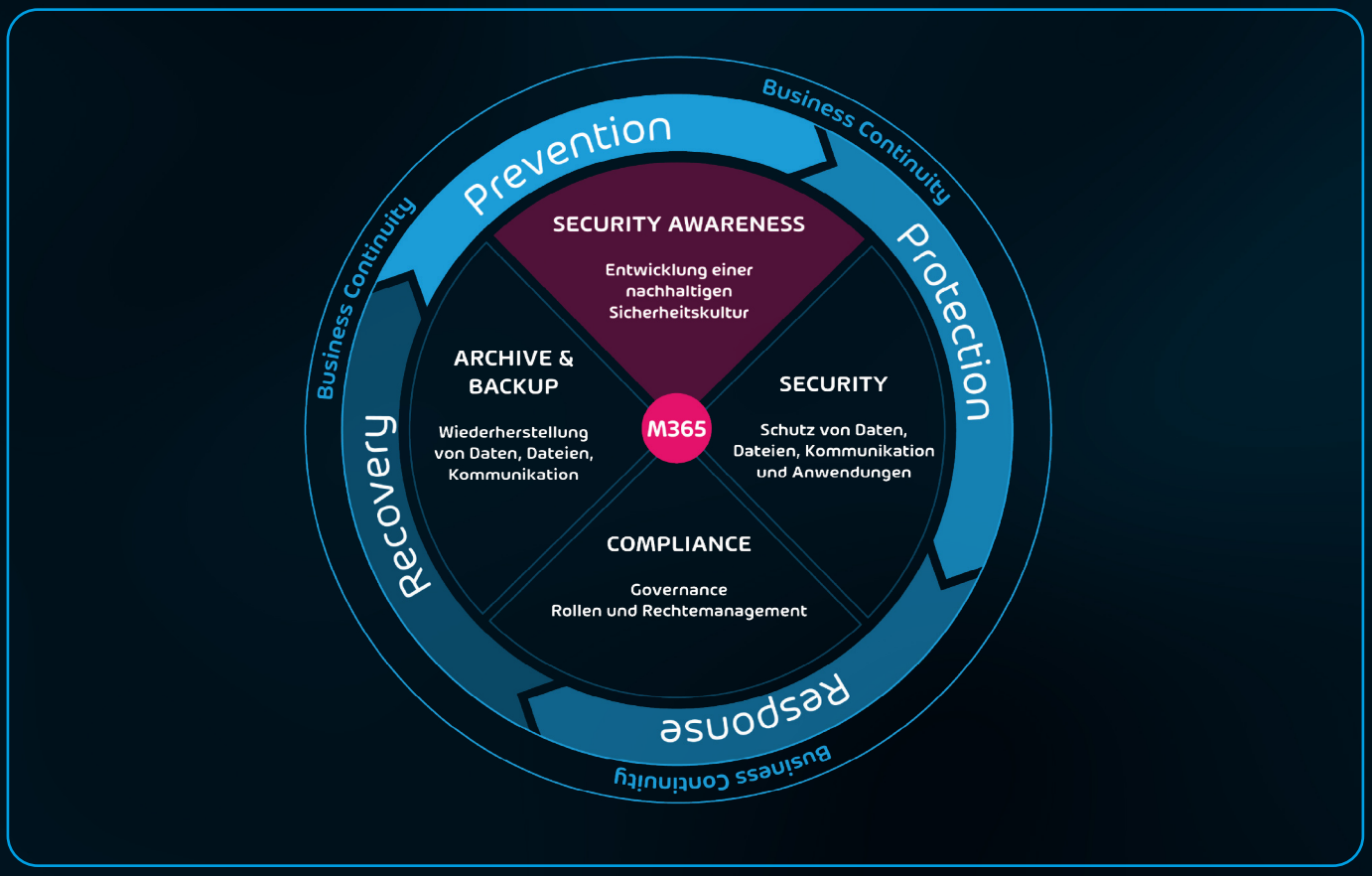



**Abb. 6:** Security Awareness als Teil der Business Continuity von Hornetsecurity

## Training im Autopiloten

Zu Beginn des Security-Awareness-Trainings sollte ein Sicherheitsniveau von mindestens ESI® 70 angestrebt werden, das dann sukzessive erhöht wird. Um den jeweiligen ESI® zu erreichen, kommt die Awareness Engine zum Einsatz.

Diese KI-basierte Engine ermöglicht Training im Autopiloten und pausiert und startet die simulierten Spear-Phishing-Angriffe automatisch – ESI®-kennzahlenbasiert und bedarfsgerecht.

Statt einheitliche Trainings nach dem Gießkannenprinzip erhält jeder Teilnehmer so viel Training wie nötig und so wenig wie möglich. Die Unternehmen sparen Zeit, Geld und wertvolle Personalressourcen, denn sie brauchen sich nicht mit der Umsetzung und Steuerung der Trainings zu beschäftigen.

In gewissen Zeitabständen werden die nachgestellten Phishing-Angriffe auf die einzelnen Mitarbeiter wiederholt und aktualisiert.

Über die laufende Awareness-Entwicklung der ESI®-Kennzahlen können sich die Manager und IT-Sicherheitsverantwortlichen über ein eigenes Frontend informieren: das Awareness Dashboard, das wie alle weiteren Lösungen von Hornetsecurity im Control Panel integriert ist. Hier sind die Awareness-Trainings-Ergebnisse jederzeit aktuell einsehbar. Die Beschäftigten selbst können ihre individuellen Lernfortschritte im so genannten User Panel verfolgen. Dabei handelt es sich um die Lernplattform des Security Awareness Service, zu der alle Teilnehmer einen eigenen Zugang haben, um ihre individuellen Trainings- und Testergebnisse abzurufen.

## Kontinuierliches Training führt zum nachhaltigen Erfolg

Bereits mehr als 1.000 Unternehmen aller Branchen und Größen vertrauen auf die bewährte Awareness-Technologie von IT-Seal, die zur Hornetsecurity-Gruppe gehört.

Um eine langfristige und nachhaltige Wirkung zu erreichen, entscheiden sich viele Kunden für eine permanente Laufzeit des Awareness Trainings. So lässt sich einerseits verhindern, dass das einmal erreichte ESI®-Niveau wieder absackt.

Stattdessen kann das Thema Security Awareness im Langzeitgedächtnis der Teilnehmer verankert werden. Zum anderen ist es auf diese Weise möglich, in die Sicherheitstrainings immer wieder neue Mitarbeiter einzubinden.

# Kapitel 6: Customer Success - Wie Kunden vom Awareness Training profitieren

Erfolgreiche Spear-Phishing-Angriffe können für Unternehmen fatale Folgen haben – ob diese aus der Finanzwirtschaft, Versicherungsbranche oder Fertigungsindustrie stammen.

Wie zwei namhafte Unternehmen ihre Abwehr mit Hilfe des Security Awareness Service stärken.

Als führender Anbieter multibankenfähiger Online- und Mobile-Banking-Lösungen in Deutschland ist die Star Finanz im hochregulierten Umfeld des Finanzsektors tätig. Häufig hat das Unternehmen mit sensiblen Finanz- und Transaktionsdaten von Endkunden und Unternehmen zu tun. Um diese vor Spear Phishing zu schützen, wurden bereits in der Vergangenheit interne Sicherheitsschulungen für die Mitarbeiter durchgeführt.

Doch legte die steigende Raffinesse der Phishing-Attacken die Unterstützung durch einen professionellen Trainingsanbieter nahe. Dass die Wahl dabei auf den Security Awareness Service von Hornetsecurity fiel, liegt an der Komplett-Lösung für Awareness-Trainings, die auf dem neuesten Stand der Angreifer sind. Hinzu kommt der innovative ESI®-Benchmark, der das Sicherheitsbewusstsein der Mitarbeiter objektiv messbar macht.

starfinanz

## Spürbare Lernfortschritte messbar

Bis heute werden kontinuierlich simulierte Spear-Phishing-Angriffe und E-Trainings für die Star Finanz-Mitarbeiter durchgeführt. „Dabei wurden große Lernfortschritte erzielt und das Sicherheitsniveau der Belegschaft stieg deutlich an", zieht André Haase, Senior Security Architect bei der Star Finanz, Bilanz.

Aus datenschutzrechtlichen Gründen ist es für die Star Finanz sehr vorteilhaft, dass Hornetsecurity die Kundeninformationen in Deutschland verarbeitet. Damit sind sämtliche Trainingsmaßnahmen mit der EU-DSGVO kompatibel. Darüber hinaus kann das Unternehmen mit der Nutzung der anerkannten Sicherheitsmaßnahmen der Security Awareness Suite eine wichtige Weiche für eine mögliche ISO 27001-Zertifizierung stellen.

Für André Haase steht es außer Frage, dass der Security Awareness Service dauerhaft an Bord bleibt, um eine nachhaltige Wirkung der Awareness-Trainings zu erzielen.

André Haase
Senior Security Architect - Star Finanz

## Customer Success - Wie Kunden vom Awareness Training profitieren

KIRCHHOFF & LEHR
METALL IN BESTFORM

Wird ein Herstellerbetrieb von Phishing-Angriffen getroffen, kann die gesamte Produktion ins Stocken geraten. Entgangene Gewinne sind die Folge, zudem sinken Kundenvertrauen und Wettbewerbsfähigkeit.

Kirchhoff & Lehr, europaweit bekannter Spezialist für Profiliertechnik, kann sich solche Ausfälle nicht leisten. Neben einem breiten Produktspektrum hat sich der Hersteller durch einen hohen Qualitätsstandard, Liefertreue und Preiswürdigkeit einen Namen gemacht. Als die Zahl der gefälschten E-Mails während der Corona-Krise sprunghaft stieg, suchte das Unternehmen nach einer Lösung, um die Belegschaft für Phishing-Angriffe zu sensibilisieren.

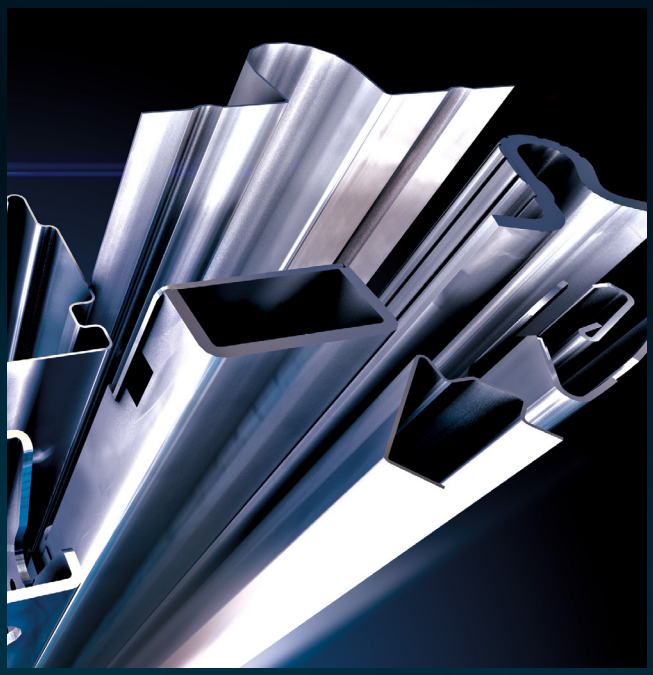
## Training wird zur Dauereinrichtung

Bereits nach kurzer Zeit entschieden die Verantwortlichen, das Security Awareness Training zu einer Dauereinrichtung für die Verwaltungsmitarbeiter zu machen. „Dies liegt vor allem an den Spear-Phishing-Simulationen, die einen hohen pädagogischen und didaktischen Nutzen bieten", unterstreicht Robert Batz, Leiter IT bei Kirchhoff & Lehr.

Bevor die Awareness-Trainings starteten, wurden die Mitarbeiter gemäß den Datenschutzregelungen informiert und um ihre Einwilligung gebeten. Seither erhalten sie regelmäßig nachgestellte Spear-Phishing-Mails. Zudem wird ihr Sicherheitsbewusstsein durch den im Security Awareness Service enthaltenen Reporter Button geschult. Erhält ein Nutzer eine zweifelhafte E-Mail, kann er diese zur technischen Prüfung direkt an die IT-Abteilung weiterleiten.

Schon nach wenigen Monaten macht der steigende ESI® große Fortschritte der Mitarbeiter bei der Phishing-Angriffserkennung deutlich. Damit diese in Übung bleiben und auch Neuankömmlinge profitieren können, werden die Trainings weit über die ursprünglich vereinbarte Vertragszeit ausgedehnt.

IT-Leiter Robert Batz ist sich sicher: „Wir haben zum Awareness Training ein überwältigendes Feedback erhalten, unsere Mitarbeiter haben ihre Verantwortung als menschliche Firewall erkannt."



Robert Batz
Leitung IT - Kirchhoff & Lehr GmbH

## Kapitel 7: Zusammenfassung und Ausblick

Trotz Einsatz modernster IT-Sicherheitstechnologien kann es keine hundertprozentige Sicherheit geben. Jedoch stehen den Unternehmen heute wirksame Maßnahmen zur Verfügung, um die Auswirkungen von Cyberangriffen zu begrenzen. So lässt sich erreichen, dass der Geschäftsbetrieb ununterbrochen weiterläuft, Angriffe zügig abgewehrt und – im Falle eines Falles – alle Systeme, Dateien und Daten rasch wiederhergestellt werden können. Zudem sorgt eine ganzheitliche Business Continuity dafür, dass die Unternehmen auch in puncto Compliance auf Nummer sicher gehen.

Sie können damit geeignete Maßnahmen ergreifen, um bei einer Cyberattacke vor Strafverfolgung und Reputationsschäden geschützt zu sein.

## Security Awareness adressiert Menschen

Hornetsecurity bietet heute bereits die fortschrittlichsten Lösungen für E-Mail Security, Backup und Compliance an, die alle Aspekte des IT-Sicherheitszyklus aus technischer Sicht abdecken – von Prevention über Protection bis zu Response und Recovery.

Allerdings zielen die meisten Cyberangriffe immer noch auf die „Schwachstelle Mensch", und letztlich sind auch die technisch sichersten Systeme und Tools immer nur so sicher, wie die Nutzer umsichtig damit umgehen.

Mit dem Security Awareness Service integriert Hornetsecurity den Faktor Mensch in die eigene Cybersecurity-Lösung und bindet ihn aktiv in den IT-Sicherheitszyklus ein. Das kontinuierliche Security Awareness Training von Hornetsecurity bereitet die Mitarbeiter systematisch auf die steigenden Cyberrisiken vor.

So lernen sie im Lauf der Zeit, auch die ausgeklügeltsten Phishing-Angriffe zu erkennen und wirksam abzuwehren. Sie beherrschen die notwendigen Maßnahmen, damit es erst gar nicht zu folgenschweren Sicherheitsvorfällen kommt und der laufende Geschäftsbetrieb jederzeit gewährleistet ist. Darüber hinaus unterstützt Hornetsecurity die Unternehmen zu Beginn des Security Awareness Trainings, bei ihren Mitarbeitern das erforderliche Security Mindset aufzubauen.

Denn nur so kann das erworbene Skillset in Kombination mit begleitenden Prozessen und Tools dazu beitragen, eine aktiv gelebte und nachhaltige Sicherheitskultur zu entwickeln.

**Mehr erfahren**

HORNETSECURITY

## Quellen


1 Bundeskriminalamt (BKA): Bundeslagebild Cybercrime 2021, Mai 2022

2 Hornetsecurity: Cyber Threat Report Edition 2021/2022, Januar 2022

3 Microsoft: Microsoft Digital Defense Report 2021, Oktober 2021

4 Anjuli Franz und Evgheni Croitor, Technische Universität (TU) Darmstadt: Who bites the Hook?

Investigating Employees' Susceptibility to Phishing: A randomized Field Experiment, 2021

5 Daniel Kahneman: Schnelles Denken, langsames Denken, 2012

6 bitkom: Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, 05. August 2021

7 Daniel Kahneman: Schnelles Denken, langsames Denken, 2012

8 Wikipedia: Hermann Ebbinghaus

9 FIDO-Allianz: FIDO-Authentifizierung. Eine passwortlose Vision

## Über die Hornetsecurity Group

Hornetsecurity ist ein führender E-Mail-Cloud-Security- und Backup-Provider, der Unternehmen und Organisationen jeglicher Größe weltweit absichert. Das preisgekrönte Produktportfolio deckt alle wichtigen Bereiche der E-Mail-Sicherheit ab: darunter Spam- und Virenfilter, Schutz vor Phishing und Ransomware, sowie rechtssichere Archivierung und Verschlüsselung. Hinzu kommen Backup, Replikation und Wiederherstellung von E-Mails, Endpoints und virtuellen Maschinen. Das Flaggschiffprodukt ist die marktweit umfangreichste Cloud-Sicherheitslösung für Microsoft 365. Mit über 450 Mitarbeitern an 12 Standorten verfügt das Unternehmen mit Hauptsitz in Hannover über ein internationales Netzwerk von mehr als 5.000 Channel-Partnern und MSPs sowie über 11 redundante, gesicherte Rechenzentren. Die Premium-Services nutzen mehr als 50.000 Kunden, darunter Swisscom, Telefónica, KONICA MINOLTA, LVM Versicherung, DEKRA und CLAAS.

HORNETSECURITY