audatis®
Datenschutz und Informationssicherheit | CERT

Anti-Phishing-Guide 2024

Der Schritt-für-Schritt-Leitfaden zur Senkung der Klickraten um mehr als 80%

Inhalt

>> Der klassische Ansatz der Security-Schulungen zeigt in der Praxis ernüchternde Ergebnisse. <<

Marcel Albrink

Senior Cybersecurity Auditor

Phishing im Mittelstand: Wie Sie Ihr Unternehmen effektiv gegen Social Engineering absichern

Executive Summary

Die Bedrohungslage durch Phishing-Angriffe hat sich fundamental gewandelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnet täglich über 450.000 neue Schadprogramm-Varianten, wobei Phishing zu den häufigsten initialen Angriffsvektoren gehört [BSI-Lagebericht 2023].

Die finanziellen Folgen sind erheblich. Laut Bitkom entstehen der deutschen Wirtschaft jährlich Schäden von 203 Milliarden Euro durch Cyberangriffe [Bitkom Wirtschaftsschutz 2023]. Bei mittelständischen Unternehmen liegt der durchschnittliche Schaden eines erfolgreichen Cyberangriffs bei 420.000 Euro [VDMA Cybersicherheit Studie 2023]. Das BKA verzeichnet dabei einen Anstieg der Phishing-bedingten Schadensfälle um 53% im Vergleich zum Vorjahr [BKA Cybercrime Bundeslagebild 2023].

Traditionelle Security-Awareness-Trainings greifen zu kurz. Das BSI stellt fest, dass rund 90% aller erfolgreichen Cyberangriffe auf menschliche Fehler zurückzuführen sind [BSI IT-Grundschutz 2023]. Unsere Erfahrung aus über 200 durchgeführten Phishing-Kampagnen zeigt: Nur durch realitätsnahe, individualisierte Simulationen lässt sich eine nachhaltige Verhaltensänderung in der Belegschaft erreichen.

Dieses Whitepaper bringt Ihnen näher:

1. Wie Sie die spezifischen Risiken für Ihr Unternehmen identifizieren
2. Welche Methodik nachweislich zu messbaren Verhaltensänderungen führt
3. Wie Sie mit begrenzten Ressourcen maximale Sicherheit erreichen
4. Wie Sie die Wirksamkeit Ihrer Maßnahmen fundiert nachweisen

Handlungsempfehlung: Etablieren Sie ein systematisches Phishing-Prevention-Programm, das sich an den tatsächlichen Angriffsmethoden

orientiert. Unsere Erfahrung zeigt: Zwei bis vier intensive, individualisierte Kampagnen pro Jahr erzielen dabei die beste Kosten-Nutzen-Relation.

Die unterschätzte Bedrohung: Modern Social Engineering

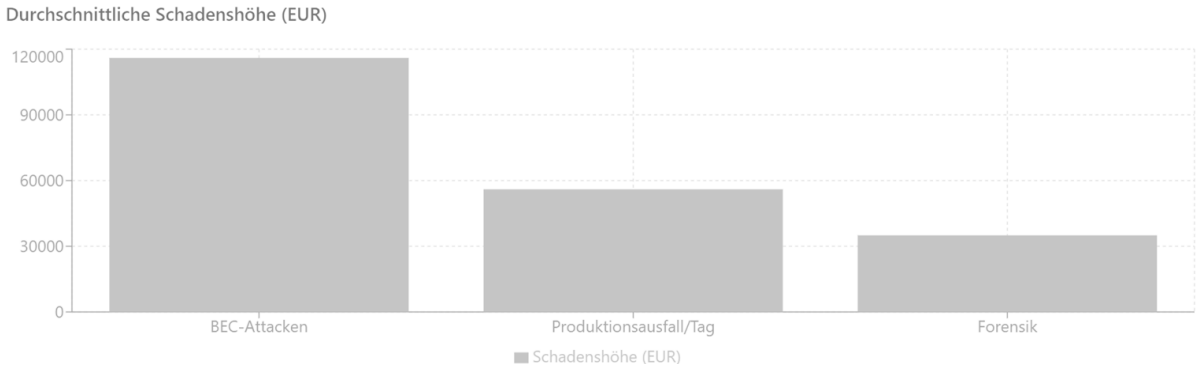
Die Evolution von Phishing-Angriffen hat in den letzten Jahren eine besorgniserregende Entwicklung genommen. Was mit offensichtlichen Massenemails begann, hat sich zu einer hochprofessionellen Bedrohung entwickelt. Das BKA berichtet von einer zunehmenden Professionalisierung der Täter mit durchschnittlichen Vorbereitungszeiten von 2-3 Wochen pro Zielunternehmen [BKA Cybercrime Bundeslagebild 2023].

Aktuelle Angriffsmethoden

Die moderne Phishing-Landschaft ist geprägt von Angriffen verschiedener Vektoren:

- Business E-Mail Compromise (BEC): Das BSI dokumentiert, dass in 64% der erfolgreichen BEC-Angriffe die Täter zuvor mehrere Monate die Unternehmenskommunikation analysierten [BSI Lagebericht 2023].
- Spear-Phishing: Die Erfolgsquote gezielter Phishing-Angriffe liegt laut Bitkom bei 37% - dreimal höher als bei klassischen Phishing-Kampagnen [Bitkom Wirtschaftsschutz 2023].
- Voice Phishing (Vishing): Das BKA verzeichnet einen Anstieg von Vishing-Attacken um 47% im Vergleich zum Vorjahr [BKA Cybercrime Bundeslagebild 2023].

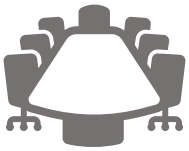
Die folgende Grafik visualisiert die Schadenshöhen und Kosten eines erfolgreichen Cyberangriffs:



Spezielle Risiken für den Mittelstand

Mittelständische Unternehmen sind besonders gefährdet. Das liegt insbesondere an den vier folgenden Gefahrenquellen. Diese sind jedoch nicht isoliert zu betrachten, sondern sie haben immer auch Wechselwirkungen untereinander:

Hohe Sichtbarkeit durch regionale Verwurzelung



direkter Zugang zur GF

Begrenzte Ressourcen

Enge, vertrauens-basierte Lieferantenbeziehungen

Warum traditionelle Schulungen oft scheitern

Der klassische Ansatz der Security-Awareness-Schulung – ein jährlicher Workshop, standardisierte Online-Trainings oder quartalsweise Newsletter – zeigt in der Praxis ernüchternde Ergebnisse. Unsere Analysen aus über 200 Phishing-Assessments belegen: Auch Unternehmen mit etablierten Schulungsprogrammen erreichen meist keine nachhaltige Verhaltensänderung.

Die Grenzen traditioneller Security-Awareness

Klassische Schulungskonzepte scheitern aus mehreren Gründen:

1. Fehlender Realitätsbezug
    - Generische Beispiele ohne Branchenbezug
    - Veraltete Angriffsmuster
    - Keine Einbindung echter Unternehmensprozesse
2. Mangelnde Nachhaltigkeit
    - "One-Shot"-Trainings ohne Follow-up
    - Keine Erfolgsmessung
    - Fehlende Wiederholung und Vertiefung
3. Geringer Praxistransfer
    - Theoretisches Wissen ohne Handlungskompetenz
    - Keine Übung unter Zeitdruck
    - Fehlendes Feedback zu eigenem Verhalten

Das Problem der nachhaltigen Verhaltensänderung

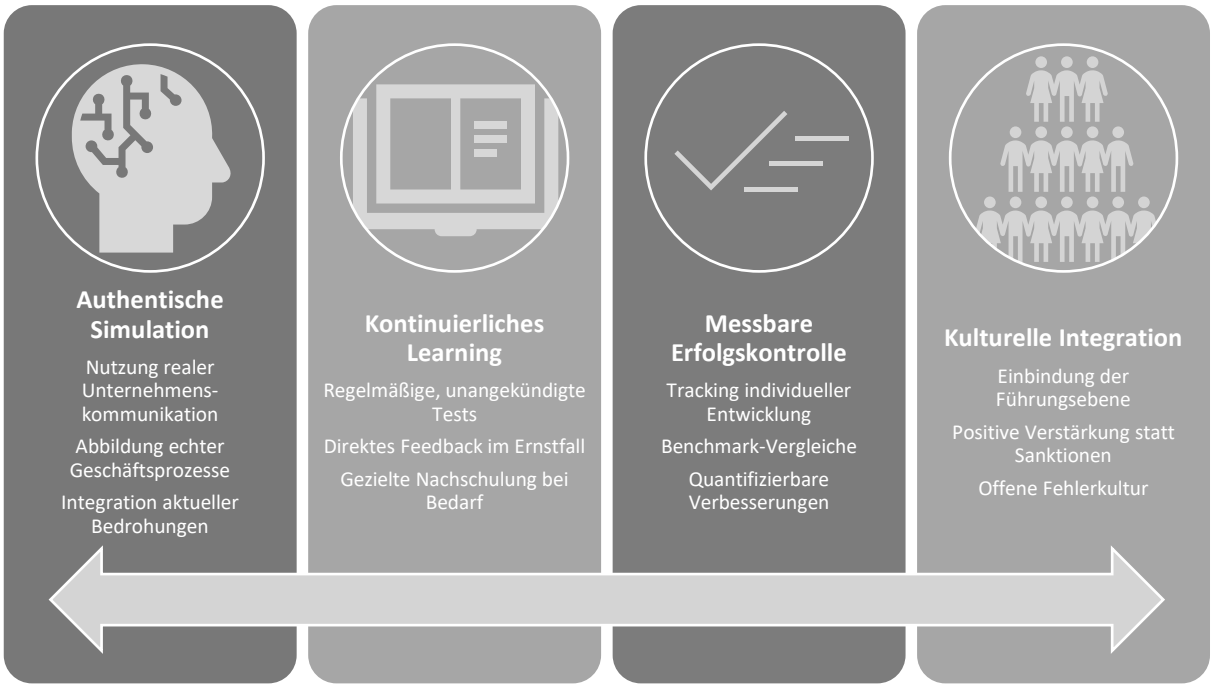
Die größte Herausforderung in der IT-Sicherheit liegt oft nicht in der Technik, sondern in der menschlichen Psychologie. Mitarbeiter tendieren dazu, ihr persönliches Risiko systematisch zu unterschätzen – ein Phänomen, das durch die "Das passiert mir nicht"-Mentalität noch verstärkt wird. Gleichzeitig werden Sicherheitsrichtlinien häufig als lästige Hindernisse im Arbeitsalltag wahrgenommen, die den gewohnten Workflow stören. Unter Zeit- und Arbeitsdruck greifen Mitarbeiter dann oft auf risikobehaftete Verhaltensweisen zurück, die sich über Jahre eingeschliffen haben. Diese Gewohnheitsmuster zu durchbrechen, erweist sich als besonders schwierig, da sie tief in der täglichen Arbeitsroutine verankert sind.

Diese psychologischen Faktoren werden bei typischen Sicherheitsinvestitionen häufig nicht ausreichend berücksichtigt. Viele IT-Leiter setzen auf kostspielige E-Learning-Plattformen, die zwar

umfangreiches Wissen vermitteln, aber keine effektive Erfolgskontrolle bieten. Auch standardisierte Phishing-Simulationen, die keinen echten Bezug zum Geschäftsalltag der Mitarbeiter haben, verfehlen oft ihre Wirkung. Besonders problematisch sind isolierte Awareness-Maßnahmen, die nicht in eine übergeordnete Sicherheitsstrategie eingebettet sind, sowie generische Schulungsinhalte, die die spezifischen Anforderungen und Risiken verschiedener Abteilungen und Mitarbeitergruppen ignorieren. Diese Fehlinvestitionen führen nicht nur zu verschwendeten Ressourcen, sondern auch zu einer gefährlichen Scheinsicherheit im Unternehmen.

Der notwendige Paradigmenwechsel

Erfolgreiche Sensibilisierung erfordert einen grundlegend anderen Ansatz:



Fazit

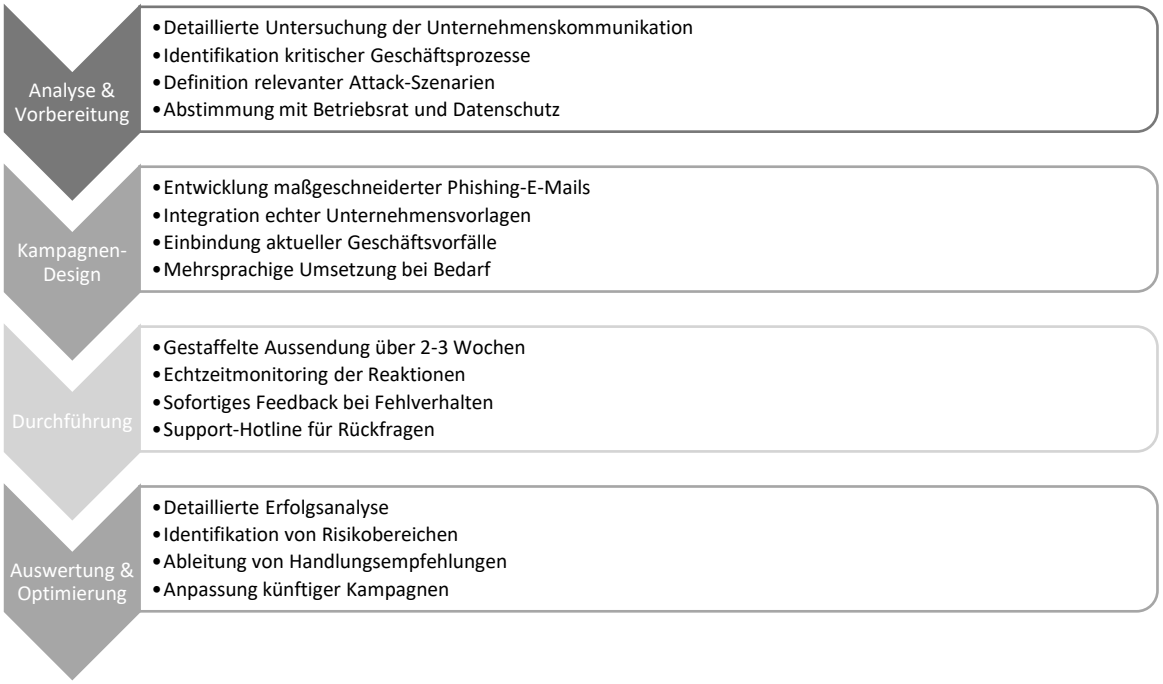
Die Zeit isolierter Security-Schulungen ist vorbei. Moderne Phishing-Prävention muss Teil einer ganzheitlichen Sicherheitsstrategie sein, die kontinuierliches Lernen mit realistischer Gefahrensimulation verbindet.

Der simulierte Ernstfall: Individualisierte Phishing-Kampagnen

In einer Zeit, in der Angreifer wochenlang Ihr Unternehmen analysieren, bevor sie zuschlagen, reichen standardisierte Phishing-Tests nicht mehr aus. Individualisierte Kampagnen simulieren präzise die Methoden echter Angreifer - und bereiten Ihre Mitarbeiter so optimal auf den Ernstfall vor.

Methodik und Vorgehensweise

Im Optimalfall erfolgen Phishing Kampagnen in mehreren Phasen, die aufbauend aufeinander, die Zielerreichung der gesamten Sensibilisierungskampagne sicherstellen:



Dabei sollten Phishing-Kampagnen insgesamt verschiedene Angriffstypen simulieren:

Die Auswahl der passenden Angriffsmethodik kann je nach Zeitpunkt variieren. Im Rahmen einer Mehrjahresplanung ist es hier sinnvoll, die Angriffsvektoren zu variieren, um die Sensibilität auf die verschiedenen Punkte auszurichten.

Erwarten Mitarbeitende zum Beispiel eine Ankündigung der Geschäftsführung, so ist der Executive-Fraud das geeignete Mittel. Sollte der Zugriff auf bestimmte Informationen, wie etwa einen Projektabschluss, absehbar sein, so kann ein Angriff mittels Credential Phishing über einen Kollegen der richtige Weg sein.

Individualisierung sticht standardisierte Schulungen aus

Die Entscheidung zwischen standardisierten Security-Schulungen und individualisierten Phishing-Kampagnen hat weitreichende Auswirkungen auf die Cybersicherheit von Unternehmen. Während klassische E-Learning-Ansätze seit Jahren etabliert sind, zeigt sich in der Praxis:

Nur was im eigenen Unternehmenskontext getestet und geübt wird, führt zu nachhaltigen Verhaltensänderungen und somit zu einer Verbesserung der Cyber-Sicherheitslage.

Die folgende Gegenüberstellung verdeutlicht die wesentlichen Unterschiede beider Ansätze. Sie basiert auf unserer Erfahrung aus über 200

durchgeführten Phishing-Kampagnen und dem direkten Feedback unserer Kunden, die zuvor auf standardisierte Schulungen setzten.

Besonders bemerkenswert: Während klassische Schulungen primär Wissen vermitteln, schaffen individualisierte Kampagnen echte Handlungskompetenz im Ernstfall.

Individuelle Phishing-Kampagnen	Standard Security Schulungen / E-Learnings
Relevanz & Realitätsnähe	
✅ Basierend auf echten Geschäftsprozessen	❌ Generische Beispiele ohne direkten Bezug zum Unternehmensalltag
✅ Integration in Geschäftsprozesse und -abläufe	❌ Losgelöst von tatsächlichen Unternehmensprozessen
✅ Berücksichtigung von Branchenrisiken und -besonderheiten	❌ Allgemeine Inhalte ohne Branchenfokus
Lerneffekte & Nachhaltigkeit	
✅ Unmittelbares, reales Feedback	❌ Verzögertes, generisches Feedback ohne Praxisbezug
✅ Konkrete Handlungsanweisungen	❌ Allgemeine Sicherheitsrichtlinien und Best Practices
✅ Langfristige Verhaltensänderung durch reale Erfahrungen	❌ Kurzfristige Wissensvermittlung ohne Verhaltensänderung
Analyse & Auswertung	
✅ Auswertung nach Abteilungen, Teams und Risikobereichen	❌ Oberflächliche Gesamtauswertung ohne spezifische Details
✅ Identifikation von Schwachstellen in Prozessen und Verhalten	❌ Keine oder nur begrenzte Schwachstellenanalyse
✅ Fundierte Datenbasis für strategische Sicherheitsentscheidungen	❌ Begrenzte Aussagekraft für strategische Entscheidungen

Einbettung in die Gesamt Cybersecurity-Strategie

Die Durchführung der Kampagnen müssen Teil der ganzheitlichen Cybersecurity Strategie des jedes Unternehmens sein. Es muss eine Integration in bestehende Awareness-Programme, eine Abstimmung mit technischen Schutzmaßnahmen und eine Verknüpfung mit Incident-Response-Prozessen erfolgen.

Insgesamt bilden die Ergebnisse der Kampagnen und der ganzheitlichen Strategie die Basis für strategische Security-Entscheidungen.

Best Practice: Der optimale Kampagnen-Rhythmus

Unsere Erfahrung zeigt, dass der folgende allgemeine Ansatz sich für jedes Unternehmen eignet, darauf eine geeignete Awareness-Strategie aufzubauen. Dieser Ansatz stärkt den Faktor Mensch nachhaltig:

- 2-4 Hauptkampagnen pro Jahr (Standard E-Mail Phishing und Spear-Phishing über E-Mail und Telefon kombiniert)
- Zusätzlichen Ad-hoc-Tests bei aktuellen Bedrohungen
- Gezielten Nachschulungen für Risikogruppen
- Regelmäßigen Erfolgsmessungen

Messbare Erfolge und ROSI

Die Investition in individualisierte Phishing-Kampagnen muss sich rechnen. Unsere Datenbasis aus über 200 durchgeführten Kampagnen zeigt: Die Kombination aus präziser Messung und kontinuierlicher Optimierung führt zu nachweisbaren Verbesserungen der Unternehmenssicherheit.

KPIs und Erfolgsmessung

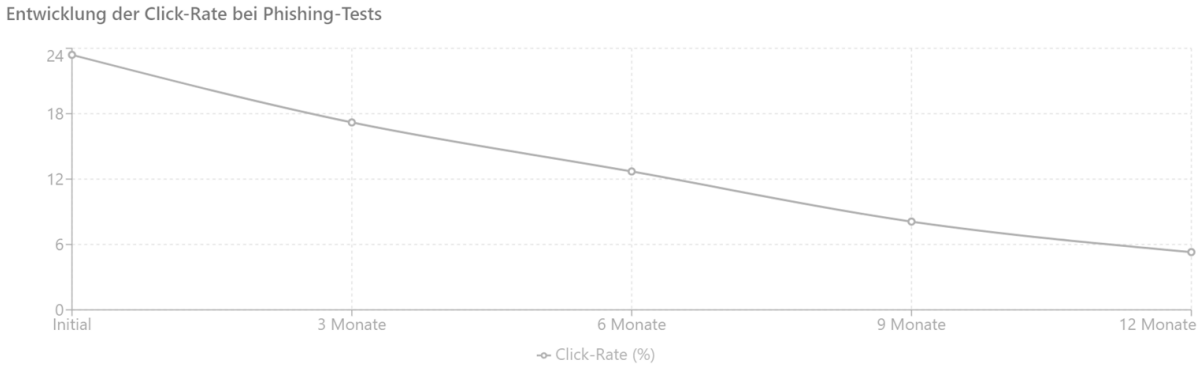
Zur erfolgreichen Ausrichtung von Kampagnen und Maßnahmen ist die geeignete Erhebung von KPI unerlässlich. Folgende Messwerte haben sich dabei als praxisrelevant herausgestellt und sollten bei der Durchführung und der späteren Bewertung unbedingt in Betracht gezogen werden:

1. Reaktionsquoten
    - Click-Rate auf Phishing-Links
    - Eingabe von Zugangsdaten
    - Öffnen gefährlicher Anhänge
    - Weiterleitung an Kollegen
2. Verhaltensänderung
    - Meldequote verdächtiger E-Mails
    - Reaktionszeit bei Vorfällen
    - Nutzung von Meldesystemen
    - Qualität der Verdachtsmeldungen
3. Abteilungsspezifische Entwicklung
    - Risikobereiche im Unternehmen
    - Fortschritte einzelner Teams
    - Effektivität von Nachschulungen
    - Vergleich mit Branchenbenchmarks

Erfolgsfaktoren und Benchmark-Daten

Die folgenden Daten und die dazugehörige Grafik zeigen eine typische Entwicklung über 12 Monate:

- Initial: 20-30% Click-Rate
- Nach 3 Monaten: 12-15% Click-Rate (46 % Verbesserung)
- Nach 6 Monaten: 8-10% Click-Rate (64% Verbesserung)
- Nach 12 Monaten: <5% Click-Rate (>80% Verbesserung)



Return on Security Investment – Der messbare Mehrwert der Sicherheitsinvestition

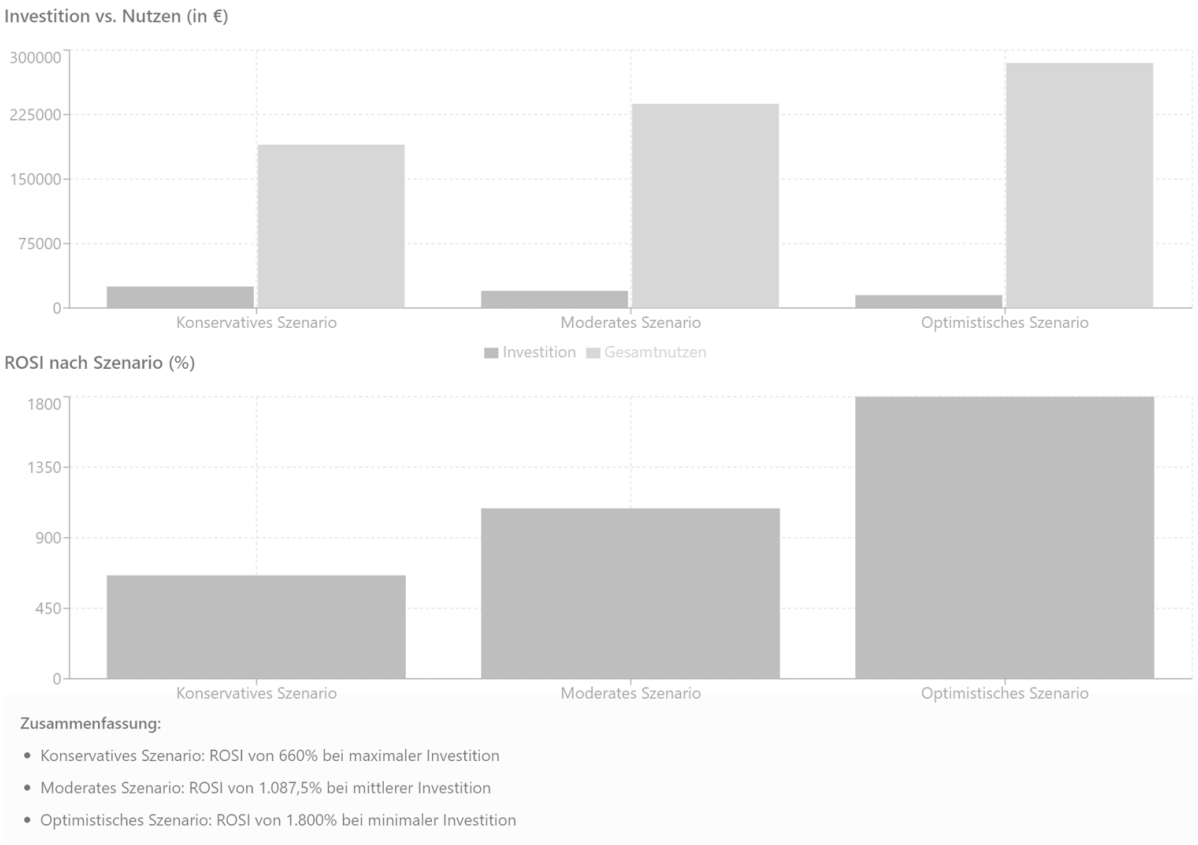
Die Investition in IT-Sicherheit wird oft als reiner Kostenfaktor wahrgenommen. Dabei lässt sich der Mehrwert von Sicherheitsmaßnahmen durchaus quantifizieren. Der Return on Security Investment (ROSI) macht genau dies möglich: Er zeigt auf, welchen konkreten finanziellen Nutzen Ihre Investition in Cybersicherheit bringt.

Gerade bei Phishing-Prävention ist die Berechnung besonders aussagekräftig, da sich sowohl die Kosten eines erfolgreichen Angriffs als auch die Wirksamkeit der Präventionsmaßnahmen präzise messen lassen. Individualisierte Phishing-Kampagnen erzielen dabei einen deutlich höheren ROSI als standardisierte Schulungsmaßnahmen.

Die folgende Berechnung basiert auf realen Durchschnittswerten mittelständischer Unternehmen und zeigt transparent auf, wie sich Ihre Investition in moderne Phishing-Prävention rechnet.

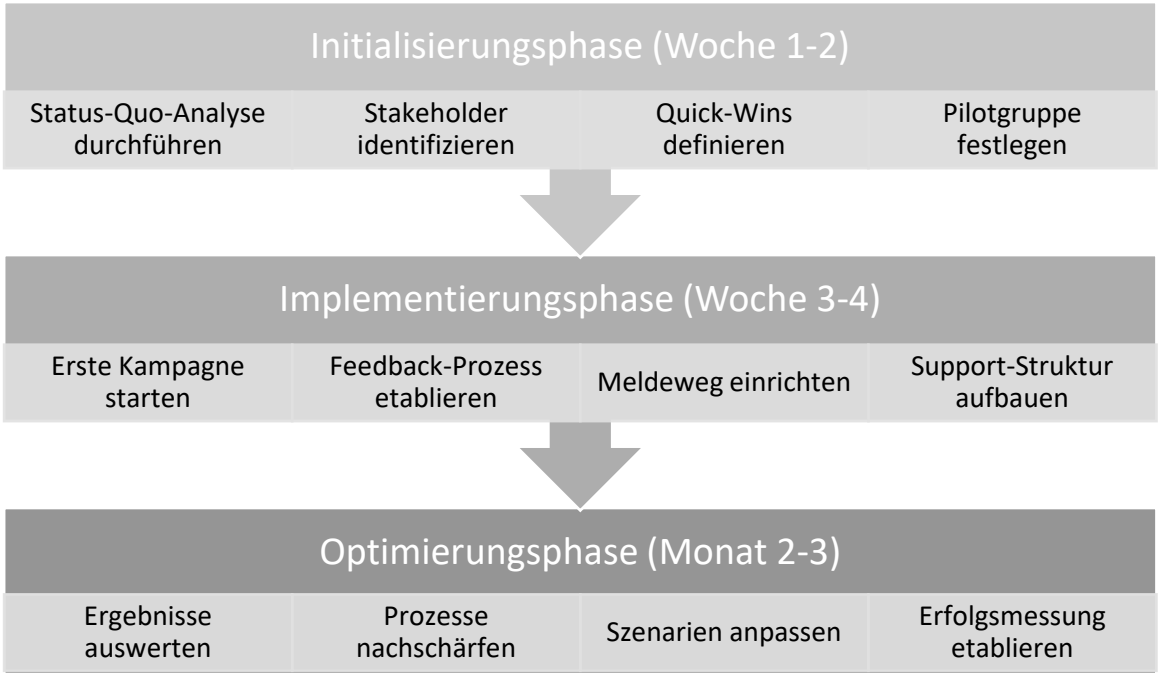
Investition pro Jahr	15.000-25.000€
Verhinderte Schadensfälle	2-3 pro Jahr
Eingesparte Folgekosten	170.000-255.000€
Zusätzliche Effizienzgewinne	20.000-30.000€

Der ROSI liegt damit bei über 500% im ersten Jahr. Die folgenden Grafiken visualisieren dabei die Berechnung des ROSI mit den oben genannten Zahlen:



Ausblick und Handlungsempfehlungen

Die Bedrohungslandschaft entwickelt sich kontinuierlich weiter. Phishing-Simulationen und -Kampagnen müssen sich diesen Veränderungen dynamisch anpassen. Das folgen aufbereitete Flussdiagramm zeigt exemplarisch, wie Sie für Ihr Unternehmen eine nachhaltige Sicherheitsstrategie für den „Faktor Mensch“ etablieren.



Langfristige Strategie

Entwickeln Sie Ihre Phishing-Prävention systematisch weiter:

1. Quartal 1
    - Basis-Kampagnen etablieren
    - Kennzahlen definieren
    - Teams einbinden
    - Erste Erfolge messen
2. Quartal 2-3
    - Szenarien erweitern
    - Prozesse optimieren
    - Nachschulungen integrieren
    - Benchmarks aufbauen

3. Quartal 4
    - Fortgeschrittene Angriffe simulieren
    - Abteilungsübergreifend testen
    - Automatisierung ausbauen
    - ROI nachweisen

Checkliste für IT-Entscheider

Sofort umsetzen:

☐ Management-Commitment einholen durch datenbasierte Präsentation der Bedrohungslage mit konkreter ROSI-Berechnung und Definition messbarer Sicherheitsziele für das nächste Jahr

☐ Budget für 12 Monate sichern mit quartalsweiser Meilensteinplanung und klarer Kostenaufstellung für Kampagnen, Schulungen und technische Integration

☐ Pilotgruppe definieren aus besonders exponierten Abteilungen wie Finanzen, Einkauf und Vertrieb, mit Abstimmung durch Betriebsrat und Datenschutz

☐ Erste Kampagne planen basierend auf Analyse der realen Unternehmenskommunikation und Priorisierung der kritischsten Angriffsvektoren

Innerhalb von 3 Monaten:

☐ Vollständiges Programm aufsetzen mit definiertem Eskalationsprozess, Incident Response Plan und Integration in bestehende Sicherheitsrichtlinien

☐ Metriken etablieren zur Messung von Click-Raten, Meldequoten, Reaktionszeiten und abteilungsspezifischen Entwicklungen

☐ Feedback-Loops implementieren durch automatisierte Sofort-Rückmeldungen bei Fehlverhalten und monatliche Auswertungsgespräche

☐ Erfolge dokumentieren mittels standardisierter Reporting-Templates und Vergleich mit Branchen-Benchmarks

Innerhalb von 6 Monaten:

☐ Programm skalieren auf alle Unternehmensbereiche mit angepasstem Schwierigkeitsgrad und individuellen Lernpfaden

☐ Szenarien erweitern um Voice Phishing, Spear Phishing und Social Engineering Varianten basierend auf aktuellen Bedrohungen

☐ Teams schulen durch praxisnahe Workshops zur Erkennung von Angriffsmustern und korrektem Verhalten im Verdachtsfall

☐ Prozesse optimieren durch Automatisierung der Auswertung, Integration in Ticketsysteme und Anpassung der Eskalationswege

Fazit

Die Bedrohung durch Phishing-Angriffe wächst täglich. Mit individualisierten Phishing-Kampagnen schaffen Sie eine nachhaltige Verteidigungslinie, die messbar zur Unternehmenssicherheit beiträgt. Die Zahlen sprechen für sich: Ein Return on Security Investment von 660% bis 1.800% macht deutlich, dass sich gezielte Prävention nicht nur sicherheitstechnisch, sondern auch finanziell rechnet.

Während standardisierte Schulungen oft an der Realität vorbeigehen, bieten maßgeschneiderte Kampagnen genau die Vorbereitung, die Ihre Mitarbeiter im Ernstfall brauchen. Mit unserem bewährten Implementierungsplan erreichen Sie innerhalb von sechs Monaten eine nachweisbare Reduzierung Ihres Unternehmensrisikos.

Vereinbaren Sie jetzt Ihr persönliches Erstgespräch

Finden Sie heraus, wie verwundbar Ihr Unternehmen wirklich ist. In einem 30-minütigen Erstgespräch analysieren wir gemeinsam Ihre spezifische Risikosituation und zeigen Ihnen konkrete Handlungsoptionen auf.

Kontakt

Marcel Albrink

Senior Cybersecurity Auditor
E-Mail: m.albrink@audatis.de

>>Hier kostenlosen Termin vereinbaren<<

audatis CERT GmbH

Luisenstraße 1 | 32052 Herford
Fon: 05221 87292-0 | Fax: 05221 87292-49
E-Mail: info@audatis.de
www.audatis.de