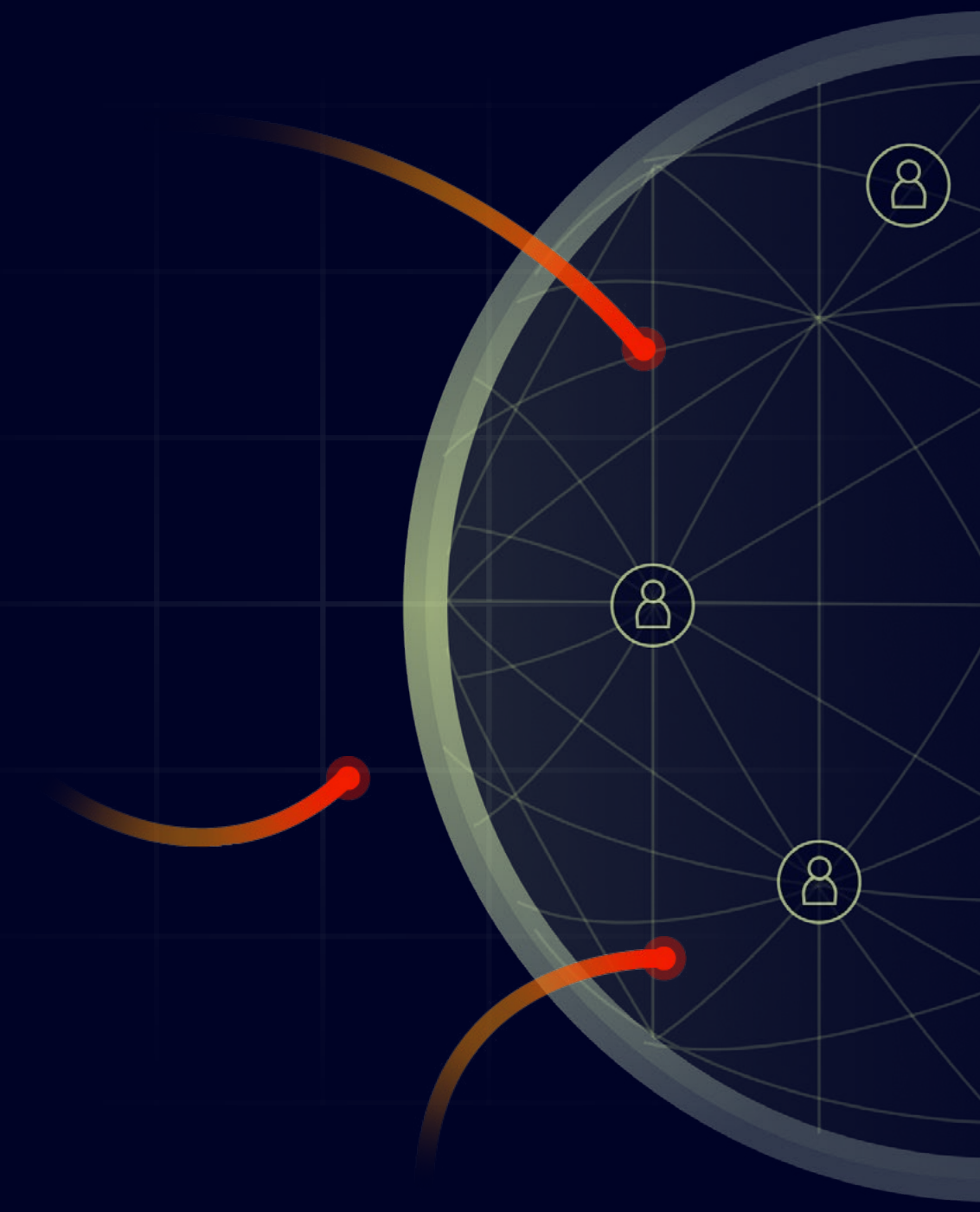
xorlab



ANALYSE

E-Mail-Sicherheit im Zeitalter von KI

Erkenntnisse aus modern geführten Penetration Tests

24 April, 2025

Über diesen Bericht

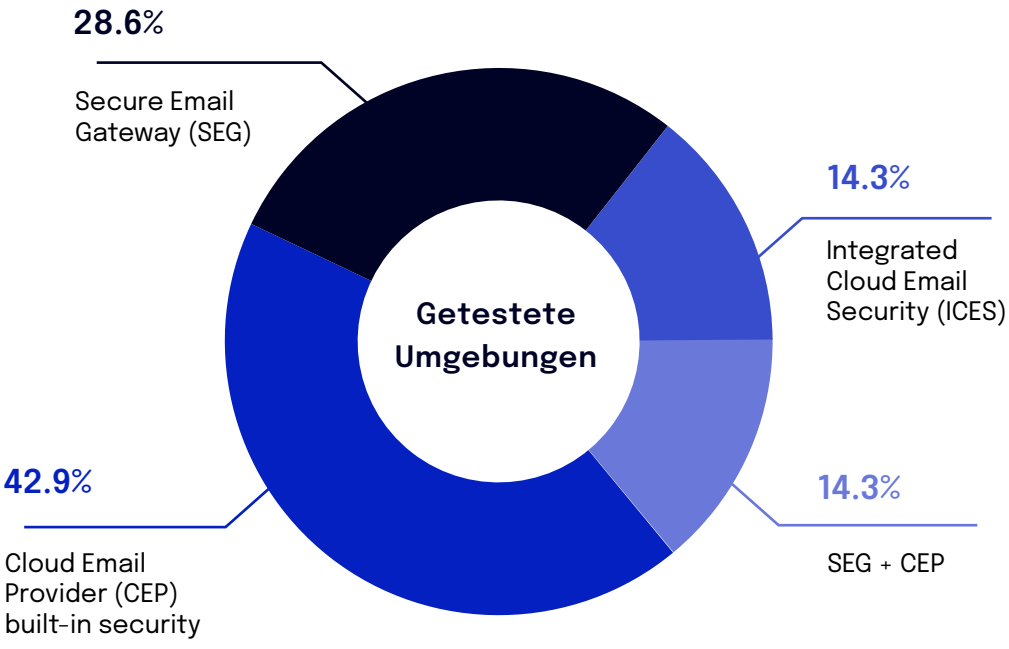
E-Mail bleibt einer der wichtigsten Angriffsvektoren für Cyberkriminelle. Fortschritte in den Bereichen Künstliche Intelligenz (KI), Automatisierung und Cybercrime-as-a-Service haben die Erfolgsrate E-Mail-basierter Angriffe erheblich erhöht. Diese Entwicklungen ermöglichen es selbst technisch unerfahrenen Angreifern, sehr zielgerichtete und ausgeklügelte Kampagnen durchzuführen, die traditionelle E-Mail-Sicherheitsmassnahmen mit alarmierender Regelmässigkeit umgehen. Infolgedessen verzeichnen Unternehmen einen Anstieg von Phishing-, Business Email Compromise (BEC)- und Ransomware-Angriffen, die unbemerkt in die Posteingänge der Nutzer gelangen.

Dieser Bericht präsentiert Ergebnisse aus über 20 E-Mail Penetration Tests, die xorlab in den letzten Monaten durchgeführt hat. Ziel war es, die Widerstandsfähigkeit verschiedener E-Mail-Sicherheitslösungen gegenüber modernen Angriffstechniken zu testen. Die untersuchten Umgebungen lassen sich grob in drei Kategorien einteilen: Secure Email Gateways (SEG), integrierte Sicherheitsfunktionen von Cloud-E-Mail-Anbietern (CEP) und erweiterte Schutzlösungen wie Integrated Cloud Email Security (ICES).

40%

der getesteten Firmen verlassen sich ausschliesslich auf die nativen Sicherheitstools ihres Cloud-E-Mail-Anbieters.

Die Ergebnisse dieser Simulationen zeigen kritische Schwachstellen in den bestehenden Sicherheitsarchitekturen auf und liefern Unternehmen konkrete Empfehlungen zur Stärkung ihrer Verteidigung gegen KI-gesteuerte Bedrohungen.



Inhaltsverzeichnis

Wie KI und Automatisierung die Bedrohungslage verändern

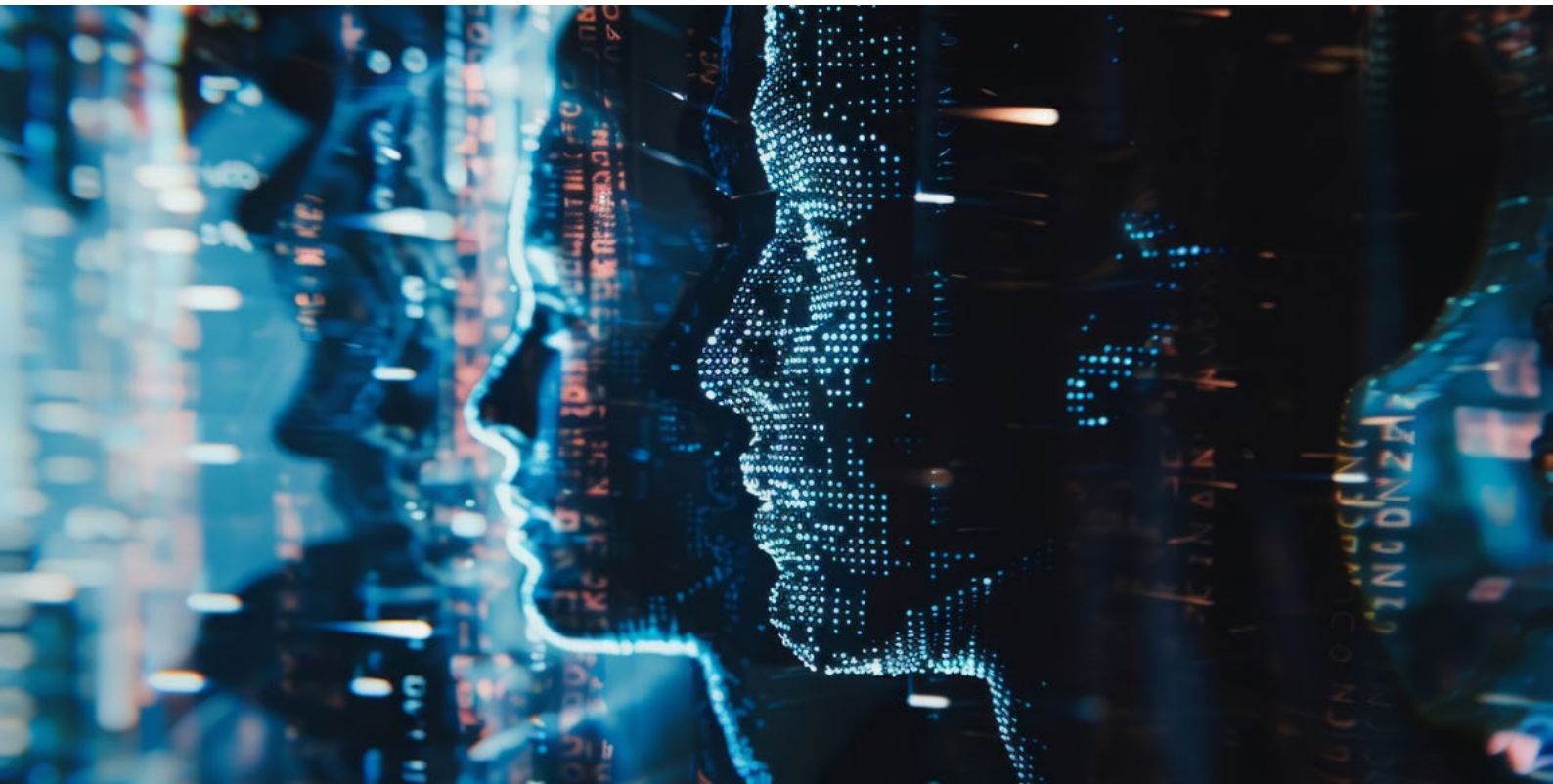
Künstliche Intelligenz (KI) und Automatisierung verändern die E-Mail-Sicherheit grundlegend. Generative KI (GenAI) ermöglicht es Cyberkriminellen, ihre Phishing-Kampagnen zu skalieren, die Qualität der Nachrichten zu verbessern und ihre Manipulationsfähigkeit zu steigern. Angreifer setzen heute KI-gesteuerte Werkzeuge ein, um Zielpersonen automatisch auszuwählen, Nachrichten zu personalisieren und mehrstufige Angriffe in Echtzeit anzupassen.

Wir beobachten, dass Akteure KI-gesteuerte Bots einsetzen, um über längere Zeit hinweg mit Opfern zu kommunizieren – was ihre Angriffe noch glaubhafter und wirksamer macht[1]. Zusätzlich sorgen KI-generierte Sprach- und Video-Deepfakes für mehr Glaubwürdigkeit bei BEC-Betrugsmaschen.

Ein aufsehenerregender Fall betraf ein britisches Ingenieurunternehmen, bei dem ein Deepfake-Videoanruf verwendet wurde, um einen Mitarbeiter zur Freigabe betrügerischer Transaktionen in Höhe von 25 Millionen US-Dollar zu verleiten. In einem anderen Fall nutzte ein Romance-Scammer KI-generierte Bilder und Nachrichten, um ein Opfer um mehr als 800.000 Euro zu betrügen. Diese Vorfälle zeigen eindrucksvoll, wie KI zur Verstärkung von Betrug und Täuschung instrumentalisiert wird.

Herkömmliche Spamfilter und in die Jahre gekommene E-Mail-Filter haben Schwierigkeiten, mit dieser Entwicklung Schritt zu halten. Die Konsequenz: Unternehmen müssen ihre E-Mail-Sicherheit aktualisieren, wenn sie in der Lage sein wollen, ausgeklügelte und KI-gesteuerte Angriffe zu erkennen. Die gute Nachricht: in den letzten Jahren hat sich viel getan in der E-Mail-Sicherheit. Mittlerweile existieren Lösungen, die KI nutzen, um verdächtige Verhaltensmuster frühzeitig zu erkennen – und damit auch gezielte Angriffe stoppen.

1 Der hin- und hergehende E-Mail-Austausch stärkt nicht nur das Vertrauen des Opfers, sondern erhöht auch die Wahrscheinlichkeit, dass E-Mail-Sicherheitssysteme den Absender als vertrauenswürdigen Kontakt einstufen.



Neue Herausforderungen für die Erkennung moderner Angriffsmethoden

4 von 10

Angriffen werden von integrierten Cloud-E-Mail-Sicherheitslösungen (ICES) übersehen.

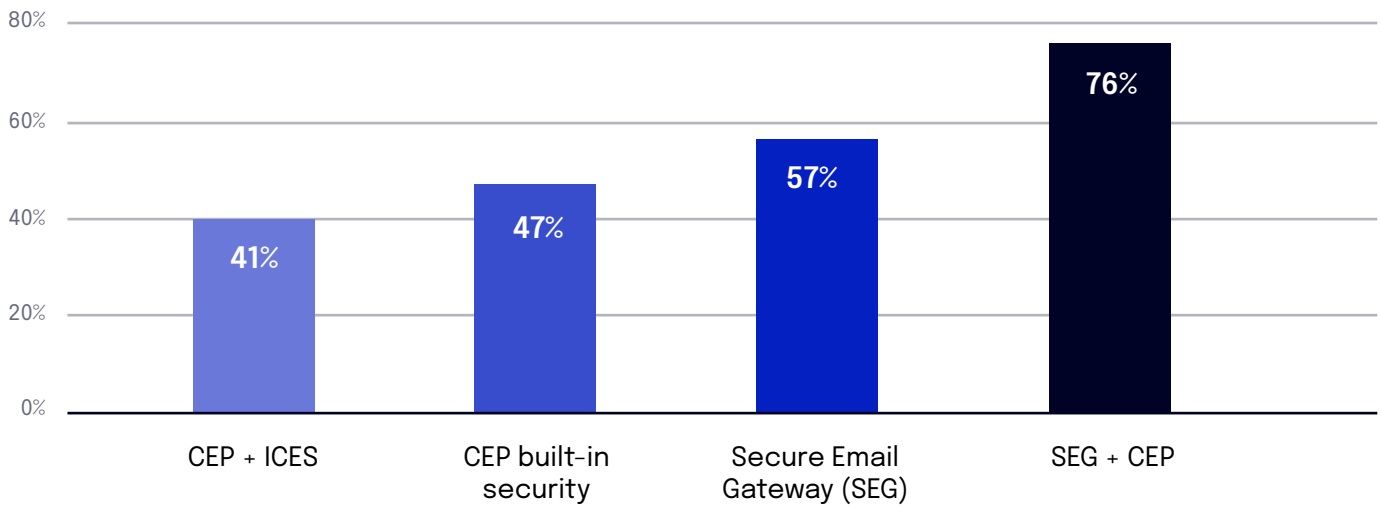
57-76%

der Angriffe landen im Posteingang, wenn ein Secure Email Gateway (SEG) vorhanden ist.

Die E-Mail Penetration Tests von xorlab ermöglichen es den Verantwortlichen in IT Security, Risk und Compliance, die Widerstandsfähigkeit ihrer Verteidigung gegenüber modernen Angriffstechniken zu bewerten. Unsere Simulationen zeigen deutlich, dass typische Sicherheitsmassnahmen einen erheblichen Anteil der Angriffe nicht erkennen oder blockieren können.

Der Einsatz eines sekundären Sicherheitsfilters als Zusatz zu den integrierten Tools des Cloud-E-Mail-Anbieters (CEP + ICES) zeigte die beste Erkennungsleistung. Dennoch: auch diese Konfiguration konnte 4 von 10 Angriffen nicht abwehren. Die nativen Sicherheitsfunktionen der Cloud-E-Mail-Anbieter verhinderten knapp 50 %, Secure Email Gateways (SEG) etwa 40 % der Angriffe. Unsere Tests zeigten die höchste Erfolgsquote für Angreifer, wenn ein SEG vor dem Cloud-E-Mail-Dienst geschaltet war – in diesem Szenario gelangten 3 von 4 Angriffen in die Postfächer.

Zustellrate nach Umgebung



Auswertung der Resultate

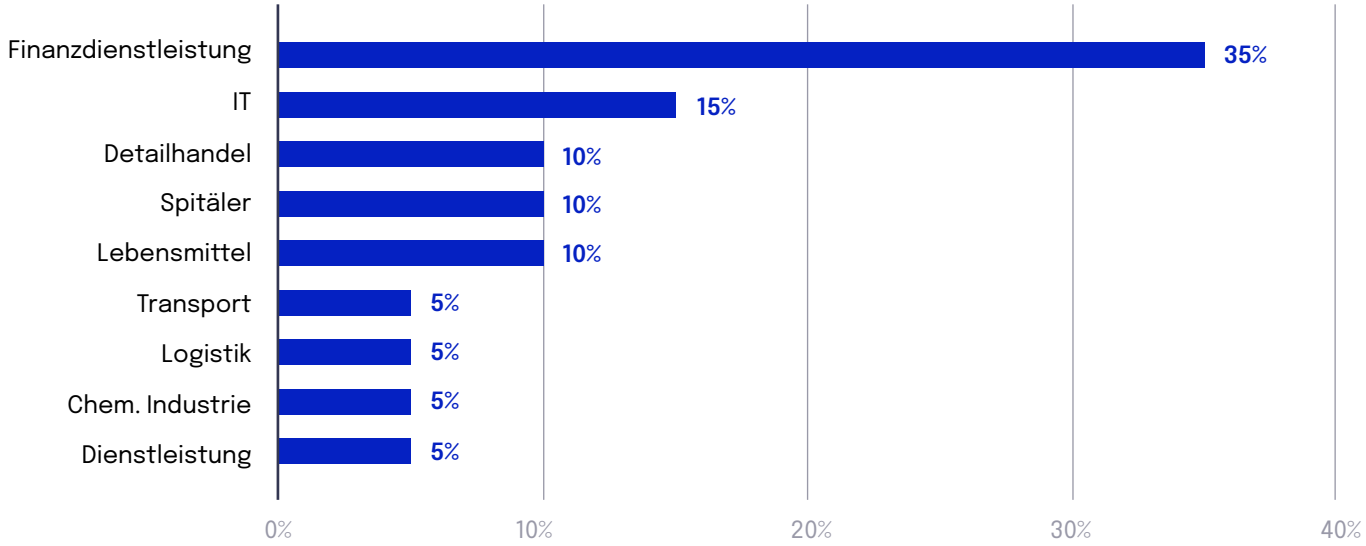
In den letzten 12 Monaten hat xorlab Email Penetration Tests mit über 20 Unternehmen aus unterschiedlichen Branchen durchgeführt. 66 % der getesteten Organisationen erzielen einen Jahresumsatz von über 100 Millionen Euro. Fast die Hälfte (48 %) beschäftigt mehr als 500 Mitarbeitende.

12
Monate

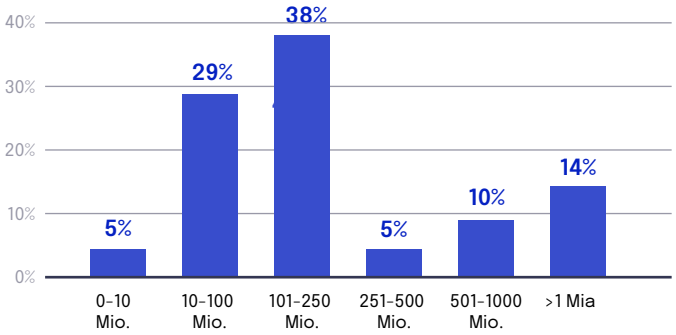
20
Unternehmen

9
Branchen

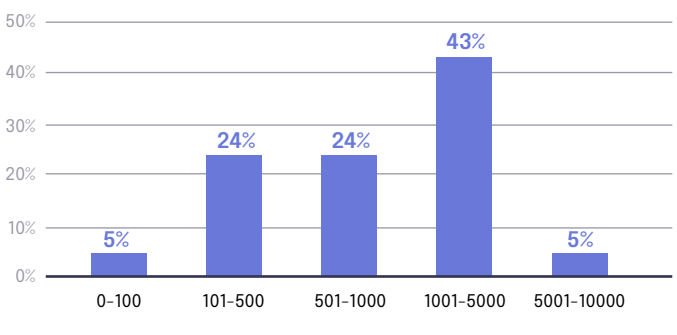
Getestete Firmen nach Industrie



Getestete Firmen nach Umsatz



Getestete Firmen nach Anzahl Mitarbeiter

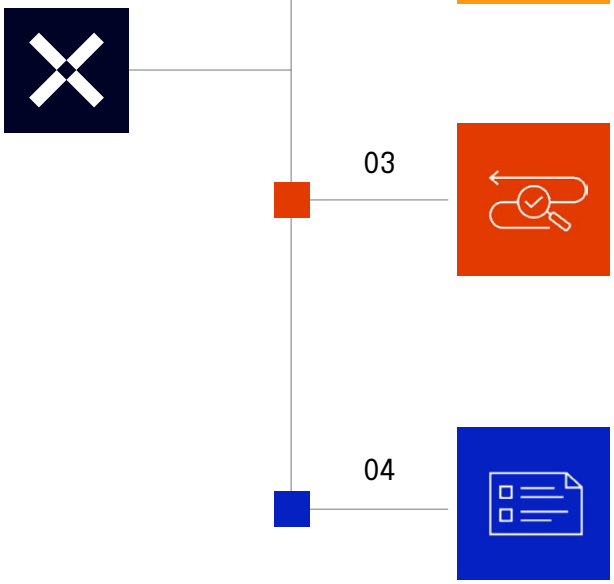


Methodik

xorlab führte die Simulationen als Blackbox Penetration Tests durch. Dabei wurden mehr als 60 speziell konstruierte E-Mails von verschiedenen E-Mail-Adressen ausserhalb der Organisation an eine E-Mail-Adresse innerhalb der Organisation verschickt, um dann die Erkennungsrate der eingesetzten Schutzsysteme zu ermitteln. Damit eine E-Mail in die Inbox ausgeliefert werden konnte, musste sie alle Filter passieren. Die E-Mails spiegeln dabei reale, moderne Angriffstechniken wider.

60+
getestete Angriffstechniken

Die Tests erfolgten in einem vierstufigen Prozess und in einer kontrollierten Umgebung:



Setup & Auswahl der Angriffe
Es wurde eine dedizierte Empfängeradresse eingerichtet. Gemeinsam mit dem Sicherheitsteam wurden die zu testenden Angriffstypen und -techniken definiert.

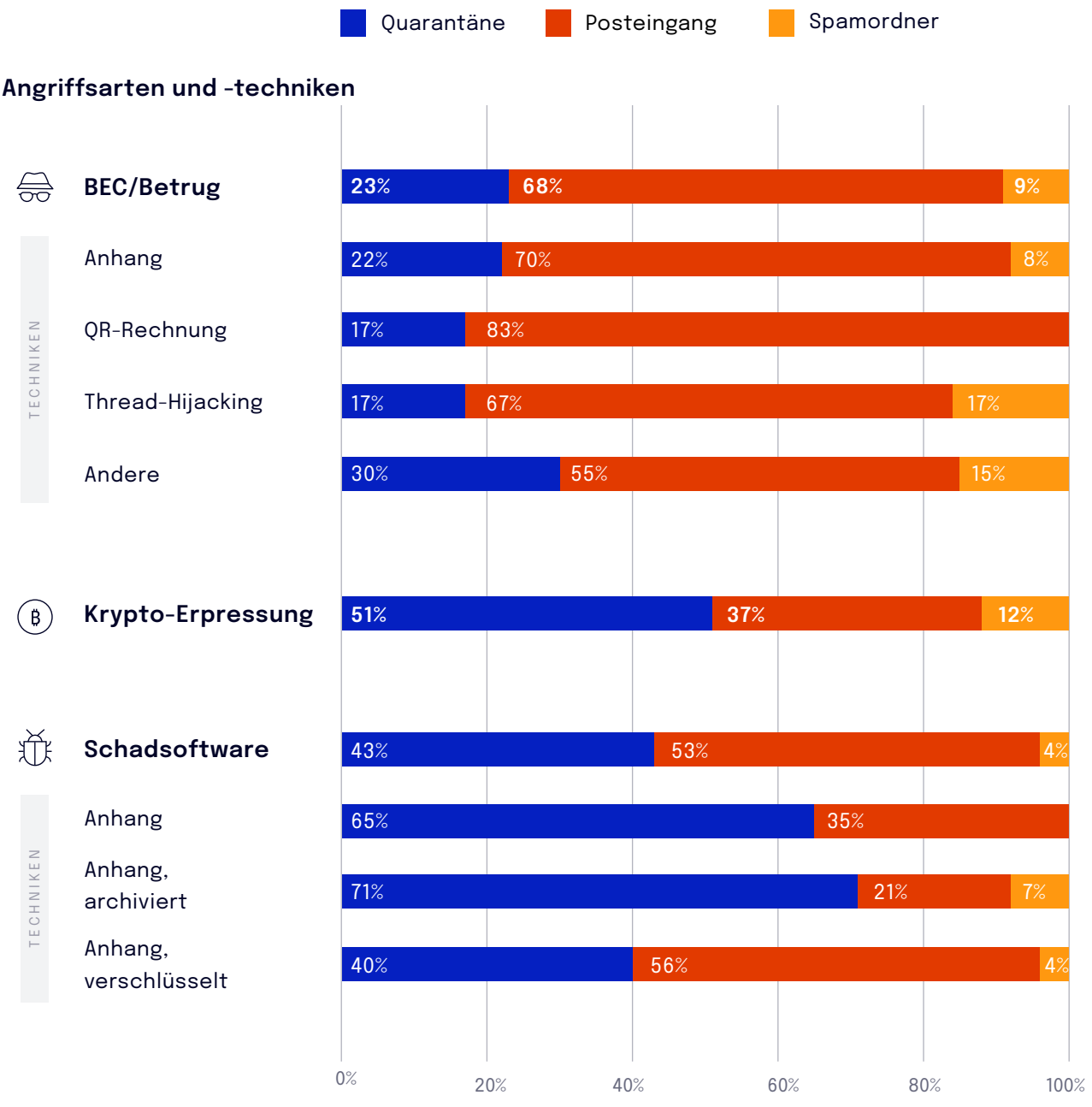
Angriffssimulation
Jede E-Mail in der Simulation testete eine Angriffsart, z.B. Phishing, und mindestens eine Angriffstechnik, z.B. Phishing mit Link, verschleiert mittels QR-Code.

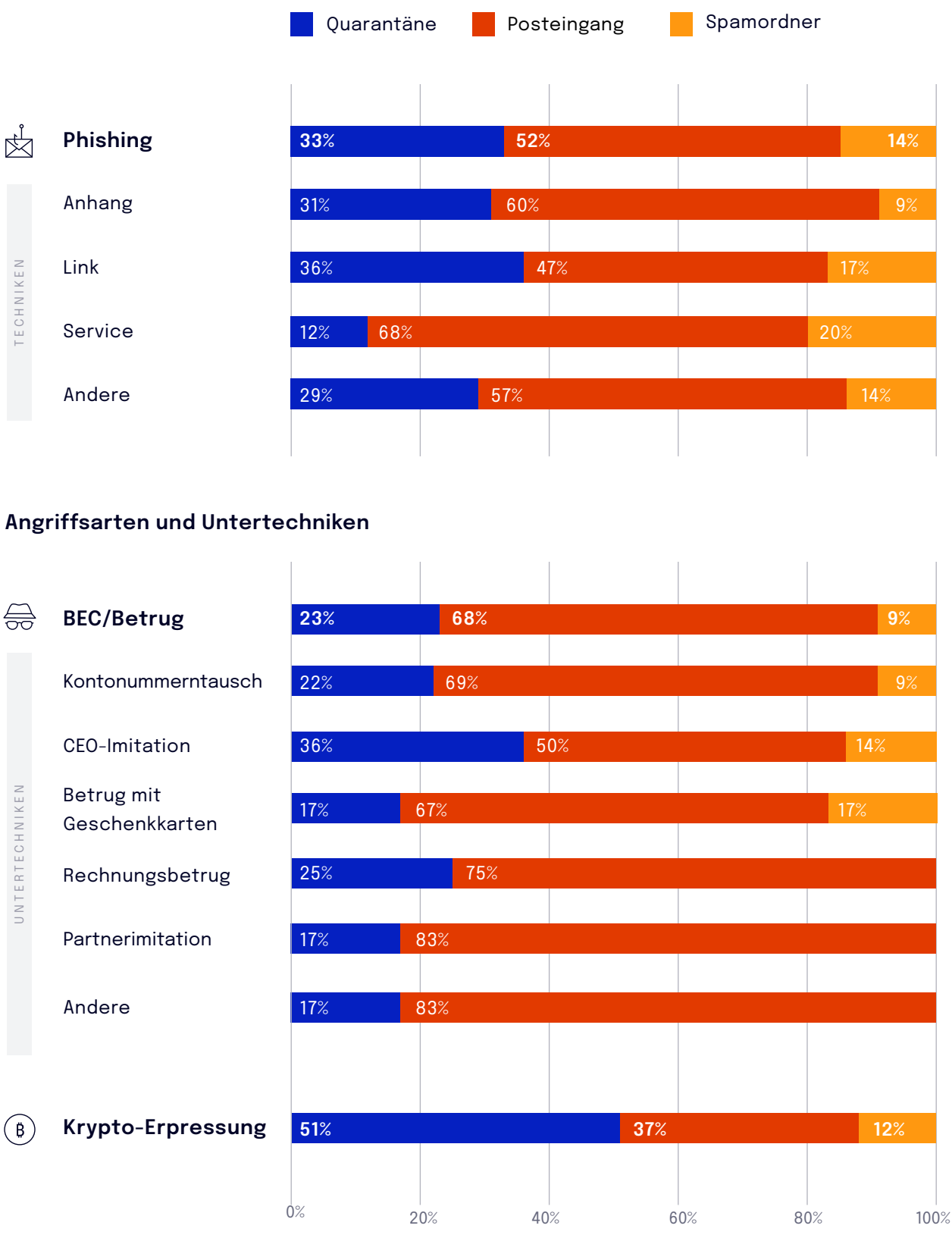
Analyse
Anschliessend wurde bewertet, wie die Sicherheitslösung auf jeden Angriff reagierte – gemessen anhand der Erkennungsrate. Mögliche Ergebnisse: “block” (Quarantäne), “junk” (Spamordner), “deliver” (Posteingang). Das Verhalten der Benutzer nach Zustellung wurde nicht analysiert.

Ergebnisse & Empfehlungen
Die Resultate wurden in einem umfassenden Bericht zusammengefasst – inklusive konkreter, datengestützter Empfehlungen, um die Organisation besser gegen moderne Bedrohungen zu schützen.

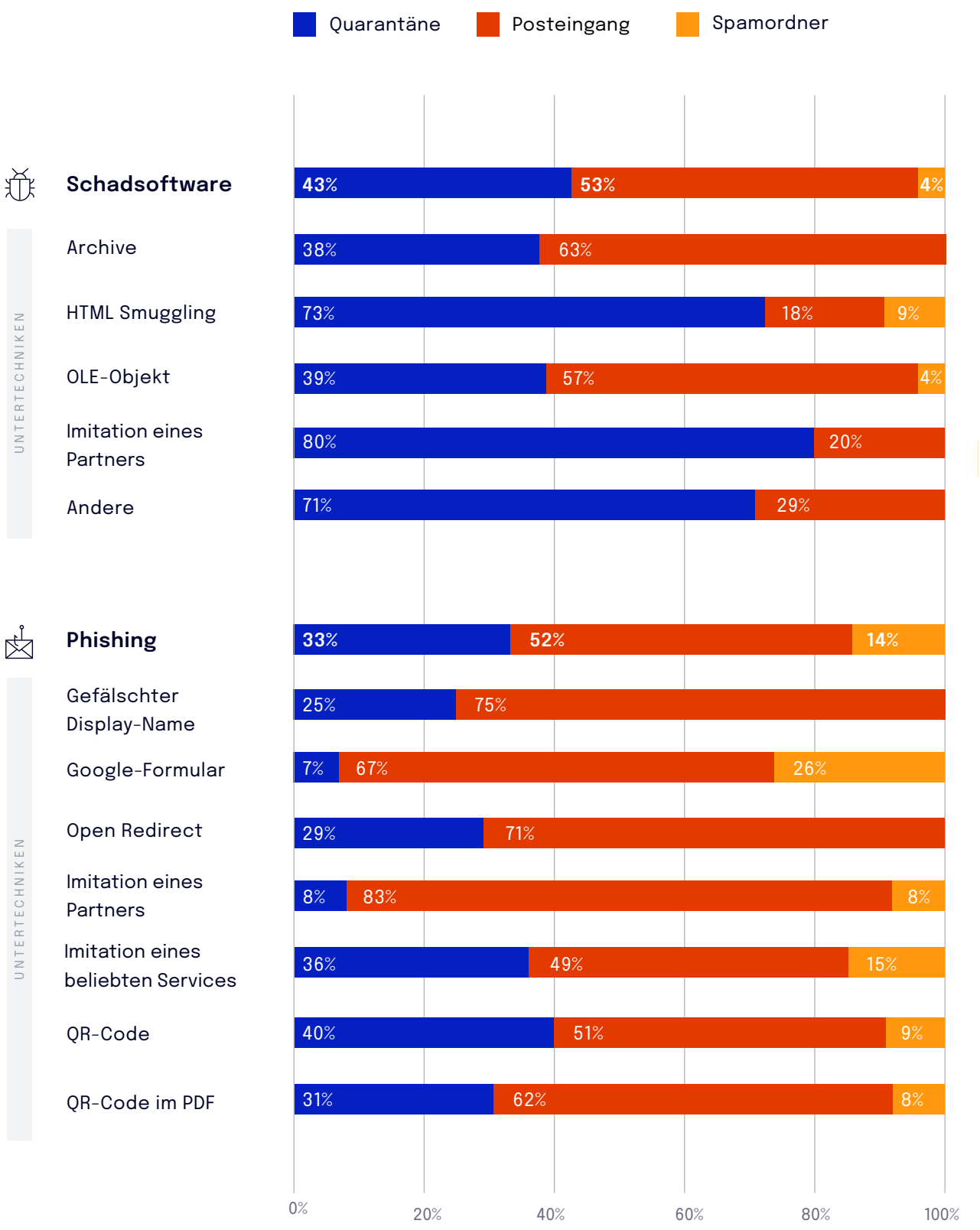
Getestete Angriffsarten und -techniken

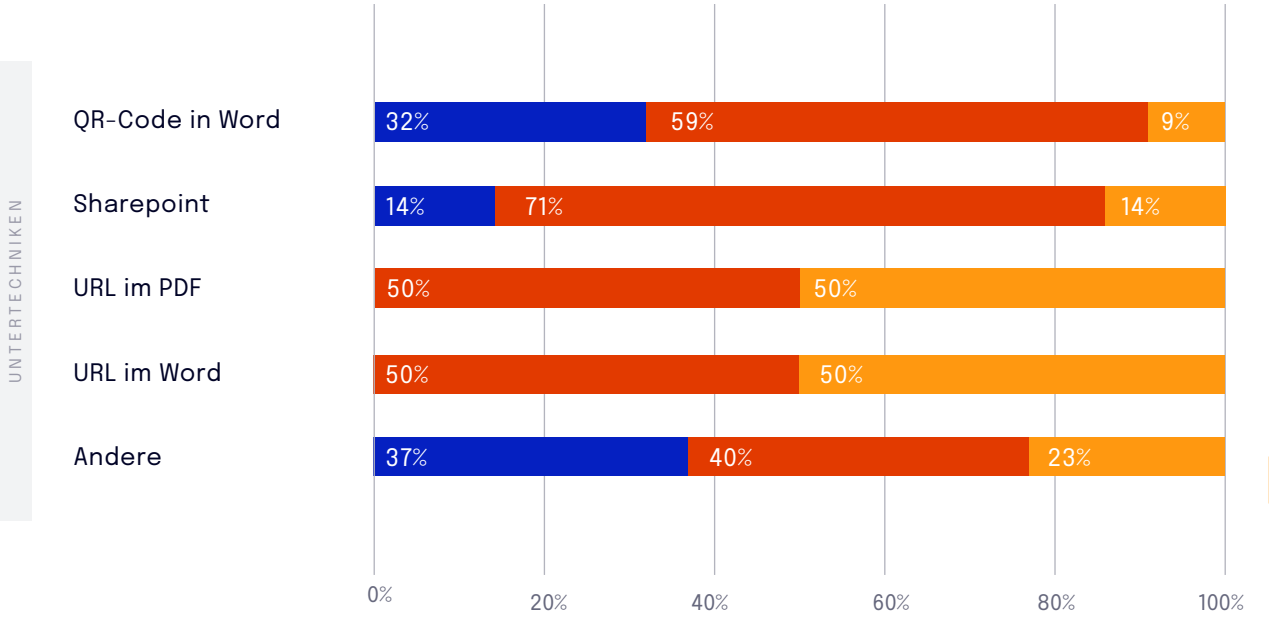
QR-Code-Rechnungen (83 % Zustellrate), manipulierte Rechnungsanhänge (70 %), Thread Hijacking (67 %) und Phishing über legitime Dienste (68 %) erwiesen sich als die grössten Bedrohungen für die getesteten E-Mail-Sicherheitssysteme. Auffällig ist, dass nur zwei von drei unverschlüsselten Malware-Anhängen erkannt wurden. Insgesamt waren über 50% unserer Angriffe erfolgreich.





Angriffsarten und Untertechniken


Quarantäne
Posteingang
Spamordner
Schadsoftware
43%
53%
4%
UNTERTECHNIKEN
Archive
38%
63%
HTML Smuggling
73%
18%
9%
OLE-Objekt
39%
57%
4%
Imitation eines Partners
80%
20%
Andere
71%
29%
Phishing
33%
52%
14%
UNTERTECHNIKEN
Gefälschter Display-Name
25%
75%
Google-Formular
7%
67%
26%
Open Redirect
29%
71%
Imitation eines Partners
8%
83%
8%
Imitation eines beliebten Services
36%
49%
15%
QR-Code
40%
51%
9%
QR-Code im PDF
31%
62%
8%
0%
20%
40%
60%
80%
100%



Getestete Arten von E-Mail-Setups

Secure Email Gateways (SEG)	• Cisco ESA • FortiMail • Barracuda • Proofpoint
Integrierte Sicherheit des Cloud-E-Mail-Anbieters	• Microsoft 365 Exchange Online Protection (EOP) • Microsoft Defender for 365 (MDO)
Kombinationen	• Cisco ESA vor EOP • EOP vor Barracuda • MDO plus Abnormal Security • MDO plus Hornet Security

Wichtigste Erkenntnisse

Jeder zweite Angriff landet im Posteingang

Unsere Daten zeigen einen besorgniserregenden Trend: Im Durchschnitt umgehen 53 % der simulierten Angriffe die bestehenden Sicherheitsfilter und landen direkt im Posteingang der Benutzer. Mit anderen Worten: Jeder zweite Angriff erreicht unbemerkt sein Ziel.

Sobald eine schädliche E-Mail im Posteingang ist, besteht eine Wahrscheinlichkeit von 25 %, dass ein Nutzer eine riskante Aktion durchführt[1] etwa das Eingeben von Zugangsdaten oder das Ausführen eines bösartigen Makros. Multipliziert man dieses Risiko mit der Anzahl an E-Mail-Angriffen, die eine Organisation jährlich erhält, wird das potenzielle Gefährdungsausmass deutlich.[2]

53%

der simulierten Angriffe umgehen Sicherheitsfilter.

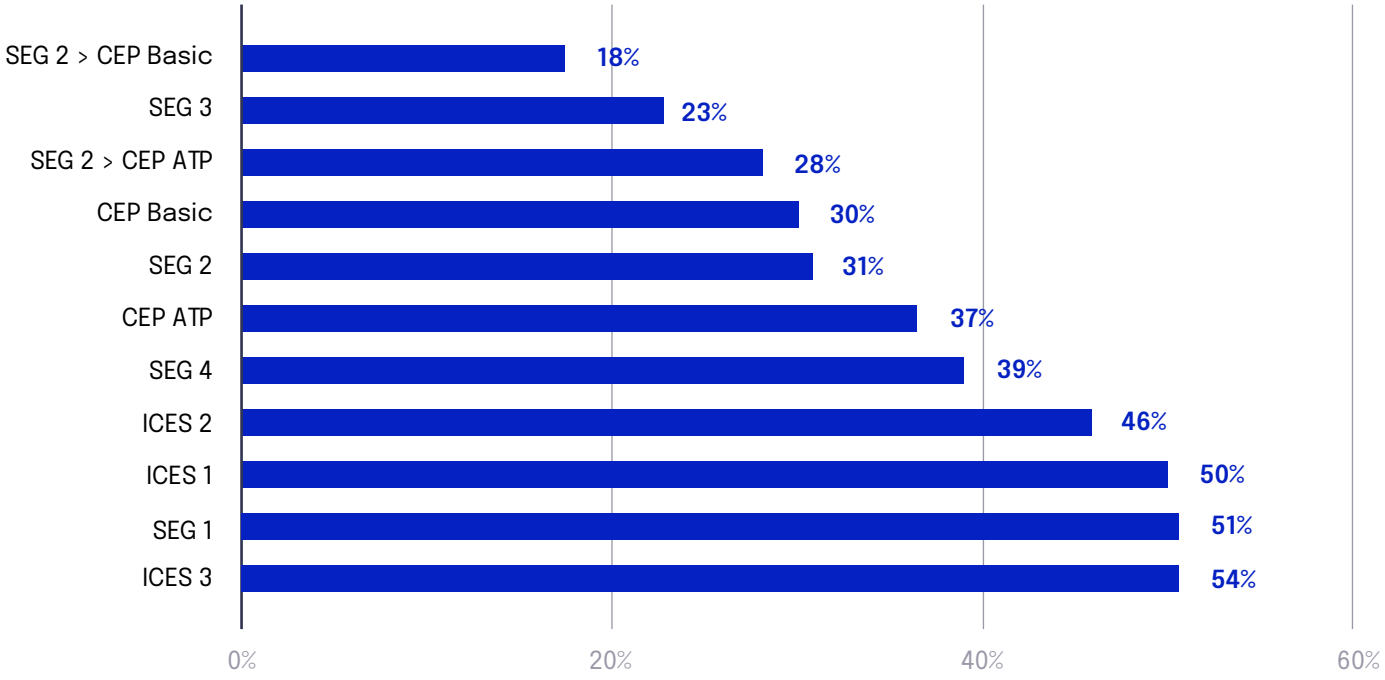
25%

Wahrscheinlichkeit, dass der Benutzer eine gefährliche Aktion ausführt[1].

1 Eine grossangelegte Studie der ETH Zürich hat gezeigt, dass 32% der Mitarbeiter mindestens einmal auf einen Phish hereinfallen und 80% davon die darauf folgende, riskante Aktion durchführen.

2 Für die meisten Organisationen liegt die Wahrscheinlichkeit, dass innerhalb eines Jahres niemand auf eine Phishing-E-Mail klickt oder eine gefährliche Aktion durchführt, bei null (Beispiel: Wenn in Ihrem Unternehmen 50 Phishing-E-Mails den Posteingang erreichen, beträgt die Wahrscheinlichkeit, dass niemand eine gefährliche Aktion ausführt, 0,00004 %).

Die Erkennungsraten verschiedener Security-Setups im Vergleich



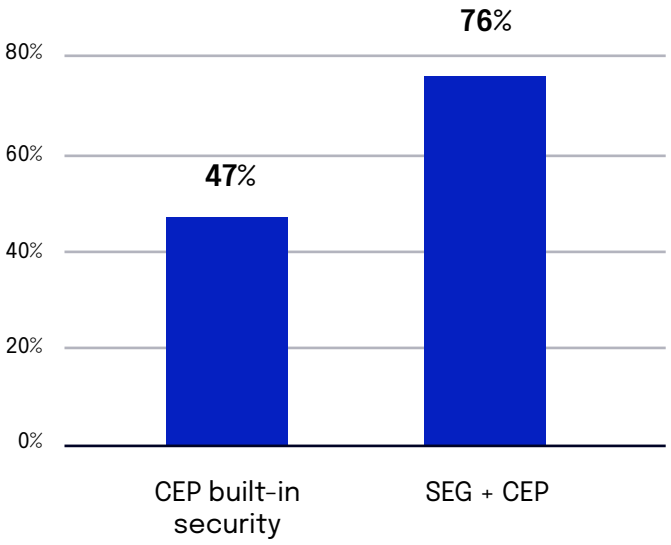
Secure Email Gateways (SEG) können mehr schaden als nützen

SEGs gelten oft als zentrales Element in der Verteidigung, doch unsere Tests zeigen: Sie bieten nur begrenzten Schutz – teils verschlechtern sie sogar die Erkennungsrate.

So liess Microsoft ohne SEG 47 % der Angriffe durch, mit vorgeschaltetem SEG stieg die Zustellrate auf 76 %.

Das zeigt, wie wichtig eine durchdachte Konfiguration hybrider Sicherheitslösungen ist – sonst entstehen blinde Flecken, die mehr Bedrohungen durchlassen.

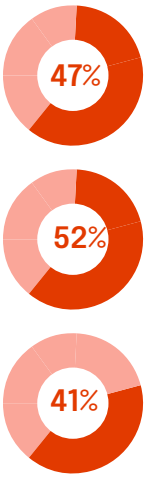
Zustellrate im Vergleich: SEG + CEP vs. CEP mit integrierter Security



Die integrierte Sicherheit von Microsoft 365 weist Lücken auf

Microsoft 365 war die am häufigsten getestete Plattform – passend zur weiten Verbreitung. Trotz fortlaufender Verbesserungen blieb die Erkennung lückenhaft: MDO liess 47 %, EOP 52 % der Angriffe durch. Ein zusätzlicher ICES-Filter verbesserte die Erkennung, doch 41 % der Angriffe gelangten weiterhin in den Posteingang. Das zeigt die Bedeutung eines mehrschichtigen und sorgfältig abgestimmten Sicherheitsansatzes.

Angriffe im Posteingang



Microsoft Defender for Office 365 (MDO)

Exchange Online Protection

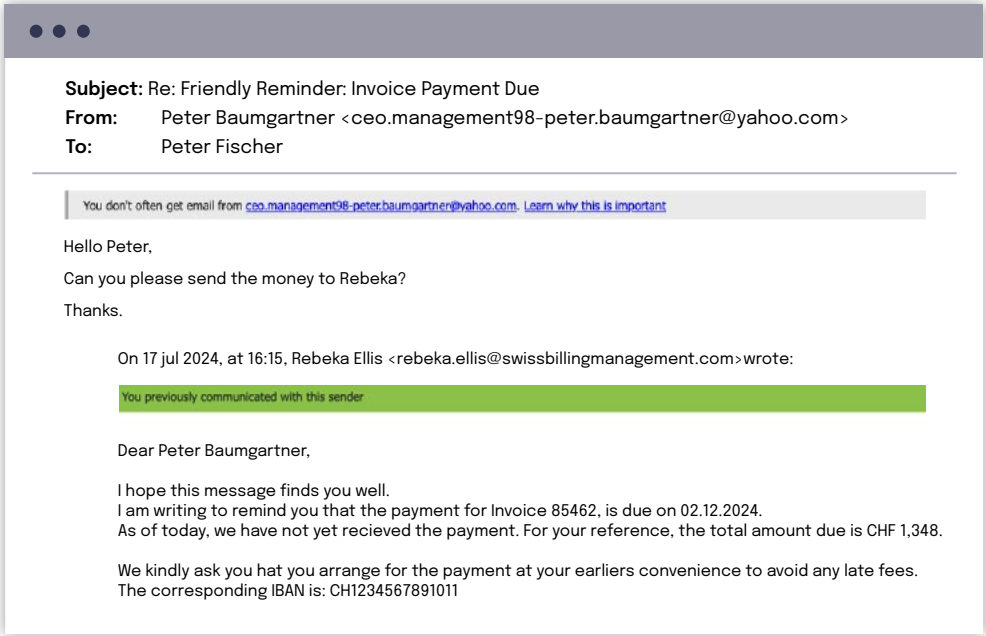
Extra ICES Filter

BEC und Betrug stellen das grösste Risiko dar

In allen durchgeführten Tests erwies sich Business Email Compromise (BEC) bzw. VIP Fraud als Unterkategorie als besonders schwer zu erkennen – 68 % dieser Angriffe gelangten durch die Sicherheitsfilter. Das Problem: In den meisten Fällen enthalten BEC-E-Mails keine bösartigen Anhänge oder Links und werden dementsprechend von herkömmlichen E-Mail-Sicherheitslösungen nicht erkannt.

Im Gegensatz zu klassischen Phishing-Angriffen basieren BEC-Angriffe häufig auf ausgefeilten Social-Engineering-Taktiken. Dazu gehört beispielsweise das Nachahmen von Führungskräften (engl. VIP Impersonation), Lieferanten oder vertrauenswürdigen Geschäftspartnern, um Mitarbeitende zur Freigabe unautorisierter Geldtransaktionen oder zur Weitergabe sensibler Informationen zu verleiten.

Darüber hinaus nutzen Angreifer Techniken wie E-Mail-Spoofing, kompromittierte Konten oder Thread Hijacking, um ihre Nachrichten legitim wirken zu lassen.



Subject: Re: Friendly Reminder: Invoice Payment Due
From: Peter Baumgartner <ceo.management98-peter.baumgartner@yahoo.com>
To: Peter Fischer

You don't often get email from ceo.management98-peter.baumgartner@yahoo.com. Learn why this is important

Hello Peter,

Can you please send the money to Rebeka?

Thanks.

On 17 jul 2024, at 16:15, Rebeka Ellis <rebeka.ellis@swissbillingmanagement.com>wrote:

You previously communicated with this sender

Dear Peter Baumgartner,

I hope this message finds you well.
I am writing to remind you that the payment for Invoice 85462, is due on 02.12.2024.
As of today, we have not yet recieved the payment. For your reference, the total amount due is CHF 1,348.

We kindly ask you hat you arrange for the payment at your earliers convenience to avoid any late fees.
The corresponding IBAN is: CH1234567891011

Die Grenzen traditioneller E-Mail-Filter

Traditionelle E-Mail-Sicherheitslösungen basieren in hohem Masse auf signaturbasierter Erkennung sowie der Qualität der integrierten Threat Intelligence. Diese Verfahren funktionieren gut bei bekannten Bedrohungen, stossen jedoch schnell an ihre Grenzen, wenn es um neue oder ausgefeiltere Angriffstechniken geht. Da diese Methoden auf vordefinierten Mustern und Datenbanken bekannter Bedrohungen beruhen, scheitern sie oft bei der Erkennung neuartiger oder stark angepasster Angriffe, die nicht zu bestehenden Signaturen passen. Dieser reaktive Ansatz lässt Organisationen gegenüber fortgeschrittenen Bedrohungen verwundbar zurück – insbesondere, da sich diese schneller weiterentwickeln als herkömmliche Abwehrmechanismen. In unseren Simulationen konnten durchschnittlich 53 % der E-Mail-Angriffe die Sicherheitsfilter umgehen und direkt in die Posteingänge gelangen.

Heutzutage nutzen Angreifer oftmals legitime Infrastruktur für ihre kriminellen Aktivitäten. Kompromittierte E-Mail-Konten kommen genau so zum Einsatz wie kommerzielle Dienstleister wie zum Beispiel Microsoft 365 und Sendgrid. Da diese E-Mails von scheinbar vertrauenswürdigen Quellen stammen, entgehen sie häufig der Erkennung durch herkömmliche Schutzmechanismen. Das erschwert es erheblich, zwischen legitimen Geschäftsnachrichten und geschickt getarnten Angriffen zu unterscheiden. Diese Methode ist besonders effektiv bei BEC-Betrugsmaschen, bei denen Angreifer gezielt Vertrauen ausnutzen, um Empfänger zur Überweisung von Geldern oder zur Preisgabe vertraulicher Informationen zu bewegen. In unseren Tests wurden 68 % der BEC-E-Mails von den bestehenden Schutzmass-nahmen nicht erkannt.

68%

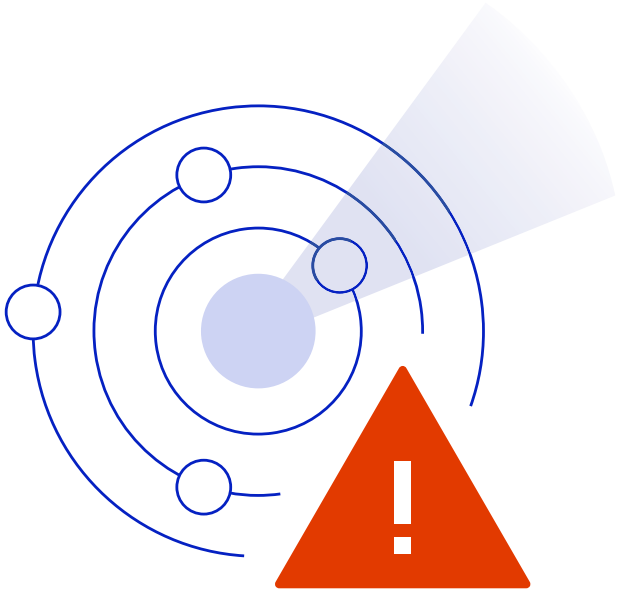
der BEC-Tests umgingen traditionelle Sicherheitslösungen.

Secure Email Gateways (SEGs) und cloudbasierte E-Mail-Sicherheitslösungen stehen vor der ständigen Herausforderung, mit den sich schnell verändernden Bedrohungen Schritt zu halten. Angreifer verfeinern kontinuierlich ihre Taktiken, Techniken und Verfahren (TTPs) – darunter KI-gestütztes Social Engineering, adaptive Phishing-Kampagnen und polymorphe Malware, deren Code sich verändert, um der Erkennung zu entgehen. Ohne verhaltensbasierte Analyse, einem Verständis für den eigenen Kontext und adaptive maschinelle Lernmodelle haben traditionelle E-Mail-Sicherheitslösungen grosse Schwierigkeiten, diese neuen Angriffe zu erkennen und abzuwehren. In unseren Tests zeigten SEGs eine sehr niedrige Erkennungsrate von 20 % bis 40 %, und auch Cloud-E-Mail-Sicherheitslösungen konnten die Erkennungsrate nicht über 53 % hinaus steigern. Daher sollten Organisationen einen proaktiveren, KI-gestützten Ansatz zur E-Mail-Sicherheit in Betracht ziehen – über die traditionellen Abwehrmechanismen hinaus.

Handlungsempfehlungen

Um diesen sich weiterentwickelnden Bedrohungen wirksam zu begegnen, müssen Organisationen auf eine proaktive Sicherheitsstrategie setzen:

Best Practices für eine proaktive E-Mail-Sicherheit



1 Führen Sie regelmässig Email Penetration Tests durch

Cyberbedrohungen entwickeln sich ständig weiter, und Angreifer verfeinern laufend ihre Methoden, um Sicherheitsmechanismen zu umgehen. Regelmässige Email Penetration Tests (auch Angriffssimulation genannt) helfen Unternehmen dabei, Schwachstellen frühzeitig zu erkennen.

So setzen Sie es um:

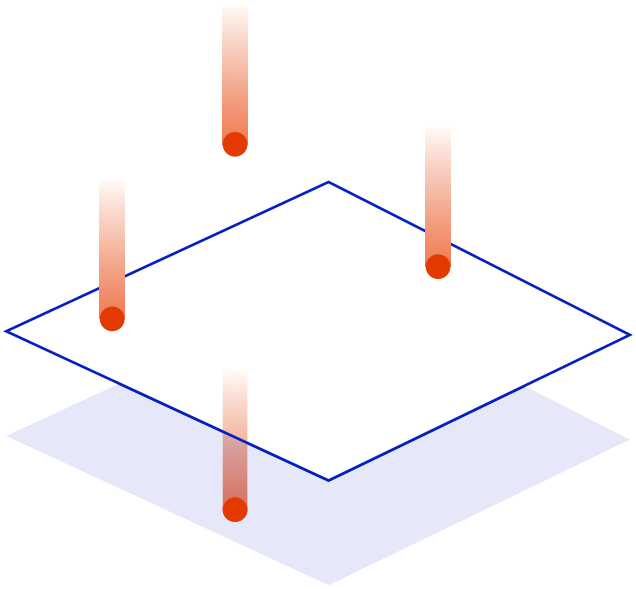
Angriffssimulationen:
Arbeiten Sie mit Penetrationstestern zusammen oder nutzen Sie eine dedizierte E-Mail-Angriffssimulation, um Ihre Sicherheitsmechanismen ganzheitlich zu testen und mögliche Blindspots frühzeitig zu identifizieren. Achten Sie darauf, die gesamte Bandbreite an Angriffstypen sowie aktuelle Techniken abzudecken.

BEC-Drills:
Simulieren Sie CEO-Fraud- oder Nachahmer von Lieferanten, um die Fähigkeit der Organisation zur Erkennung und Abwehr von Betrugsversuchen zu überprüfen.

Massnahmen nach der Simulation:
Verwenden Sie die gewonnenen Erkenntnisse, um Sicherheitsrichtlinien zu optimieren, Prozesse zu aktualisieren und Mitarbeiterschulungen gezielt auszubauen.

Ergebnis:

Eine erhöhte Widerstandsfähigkeit gegenüber modernen E-Mail-Bedrohungen – und damit ein geringeres Risiko für Phishing-, BEC- und Ransomware-Angriffe.



Ergebnis:

Reduziertes Risiko nicht erkannter Angriffe und verbesserter Schutz gegenüber KI-gestützten sowie auf Social Engineering basierenden Bedrohungen (Deepfake, BEC, Zero-Hour Phishing).

2 Ergänzen Sie die Sicherheit von Microsoft 365

Die integrierten Sicherheitsfunktionen von Microsoft 365 reichen nicht immer aus, um moderne Bedrohungen zuverlässig zu erkennen. Unsere Tests zeigen, dass selbst Organisationen mit Microsoft Defender for Office 365 mit einer erheblichen Anzahl nicht erkannter Angriffe konfrontiert sind.

So setzen Sie es um:

Mehrstufige Abwehr:
Ergänzen Sie Microsofts native Sicherheitsfunktionen durch eine zusätzliche Sicherheitslösung wie etwa eine Integrated Cloud Email Security (ICES)-Plattform.

Verhaltensanalyse (KI-basiert):
Wählen Sie Lösungen, die das Verhalten von Benutzern, Kommunikationsmuster sowie weitere kontextbezogene Signale analysieren – um neuartige oder besonders gezielte Bedrohungen zu erkennen.

Stärken Sie Ihr SEG:
Wenn Sie Ihre E-Mail-Umgebung noch nicht in die Cloud migrieren können, erweitern oder ersetzen Sie das Secure Email Gateway mit zusätzlichen Abwehrfunktionen.

3 Schulen Sie Ihre Mitarbeiter

Menschliches Fehlverhalten bleibt ein zentraler Erfolgsfaktor für E-Mail-basierte Angriffe. Die Sensibilisierung und Entscheidungsfähigkeit der Mitarbeitenden zu stärken, ist entscheidend, um erfolgreiche Angriffe zu verhindern.

So setzen Sie es um:

Security-Awareness-Schulungen:
Schulen Sie Ihre Mitarbeitenden regelmässig im Erkennen von Phishing, BEC und Social-Engineering-Techniken.

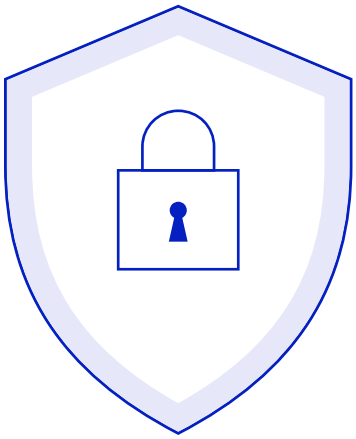
Simulierte Angriffe:
Führen Sie Phishing-Simulationen durch, um die Erkennungs- und Meldefähigkeiten Ihrer Mitarbeitenden zu überprüfen und gezielt zu fördern.

Klare Meldewege:
Erleichtern Sie die Meldung verdächtiger E-Mails mit One-Click-Reporting-Tools und definierten Prozessen zur Vorfallbehandlung.

Ergebnis:

Mitarbeitende werden zu aktiven Verteidigern statt weiterhin als Schwachstellen in der Sicherheitsarchitektur wahrgenommen zu werden - das reduziert durch menschliches Fehlverhalten verursachte Sicherheitsvorfälle und fördert eine nachhaltige Sicherheitskultur.

Taktische und strategische Massnahmen für CISOs und SOC-Leiter



1 Überprüfen Sie Ihre aktuelle Sicherheitsarchitektur

Da sich Cyberbedrohungen ständig weiterentwickeln, ist es für CISOs und SOC-Verantwortliche entscheidend, regelmässig zu prüfen, ob die bestehenden Sicherheitslösungen noch mit dem heutigen Bedrohungsumfeld Schritt halten.

So setzen Sie es um:

Audit der bestehenden E-Mail-Sicherheitssysteme:
Überprüfen Sie, wie gut Ihr Secure Email Gateway (SEG), Microsoft 365, DNS-Filter, Web-Proxy und Ihre Endpoint-Lösung gegen fortgeschrittene Bedrohungen bestehen.

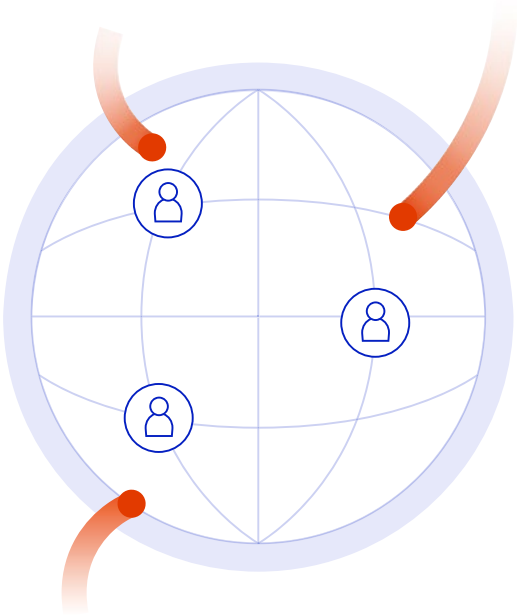
Potentialanalyse:
Identifizieren Sie Möglichkeiten zur Optimierung, z. B. in Bereichen wie KI-gestützter Phishing-Erkennung, Verhaltensanalyse oder API-basierter Email Security.

Benchmarking:
Vergleichen Sie Ihre Sicherheits-architektur mit Best Practices der Branche und Compliance-Standards (z. B. DORA, NIS2, DSGVO, CISA Zero Trust Prinziples).

Anbieterevaluation:
Prüfen Sie, ob Ihre aktuellen Sicherheitsanbieter mit den Bedro-hungsentwicklungen Schritt halten und das identifizierte Potential abdecken – oder ob ein innovativerer Anbieter notwendig ist.

Ergebnis:

Ein klarer Fahrplan zur Verbesserung der Sicherheitslage – mit priorisierten Investitionen in moderne, adaptive Sicherheitstechnologien.



Ergebnis:

Ein robuster Incident-Response-Plan und eine schnelle Einsatzbereitschaft.

2 Führen Sie einen modernen Email Penetration Test durch, um ein klares Bild der Lücken Ihres Unternehmens zu erlangen

Standard-Phishing-Tests reichen nicht aus. Fortgeschrittene Angriffssimulationen bieten tiefere Einblicke in die möglichen Schwachstellen Ihrer Sicherheitsinfrastruktur.

So setzen Sie es um:

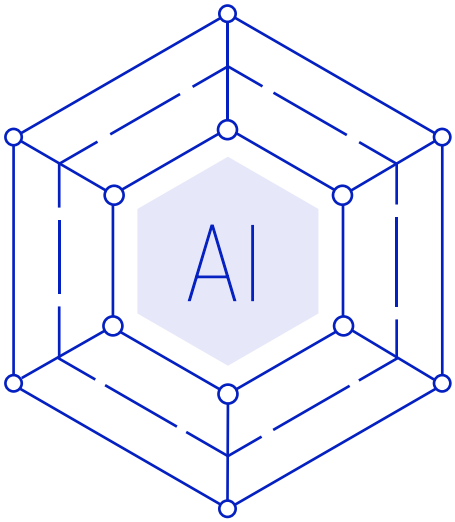
Externe Perspektive einholen:
Beauftragen Sie externe Experten mit der Durchführung eines realitätsnahen Penetration Tests. Hierbei ist es wichtig, dass das Gesamtsystem und moderne Angriffstechniken getestet werden (mit dem Blackbox-Ansatz).

Fortgeschrittene Taktiken, Techniken und Verfahren (TTPs) testen:
Simulieren Sie Malware, Credential Phishing und KI-gestützte BEC-Angriffe.

Teamübergreifende Zusammenarbeit:
Integrieren Sie SOC-, IT-Sicherheits- und Incident-Response-Teams zur Verbesserung der Koordination.

Analyse der Incident-Response-Fähigkeit:
Beurteilen Sie, wie schnell und effektiv Ihr Sicherheitsteam E-Mail-basierte Bedrohungen erkennt, eindämmt und neutralisiert.and mitigates email-based threats.

3 Ziehen Sie eine flexible, KI-gestützte E-Mail-Sicherheitslösung in Betracht



Traditionelle E-Mail-Sicherheitslösungen setzen noch immer auf signaturbasierter Erkennung – und sind damit anfällig gegenüber sich schnell entwickelnden Bedrohungen. KI-gestützte Lösungen erkennen Anomalien (z.B. im Verhalten) und neuartige Angriffsmuster, bevor Schaden entsteht.

So setzen Sie es um:

Einführung KI-/ML-basierter Bedrohungserkennung:
Implementieren Sie verhaltensbasierte Anomalieerkennung, um Phishing-, BEC- und Malware-Angriffe in Echtzeit zu identifizieren.

Kontext nutzen:
Verwenden Sie adaptive Sicherheitsmodelle, die das individuelle Benutzerverhalten verstehen und ungewöhnliche Kommunikationsmuster automatisch erkennen.

Integration in XDR/SIEM-Plattformen:
Stellen Sie sicher, dass Verdachtsfälle übergreifend korreliert werden können, indem Sie E-Mail-Sicherheitsdaten mit Extended Detection & Response (XDR) und Security Information & Event Management (SIEM) verbinden.

Ergebnis:

Ein proaktiver, zukunftssicherer E-Mail-Sicherheitsansatz, der sich dynamisch an neue Bedrohungen anpasst – und den Bedarf an manuellen Eingriffen erheblich reduziert.

Fazit

Unsere Ergebnisse zeigen, dass herkömmliche E-Mail-Abwehrmassnahmen nicht mehr ausreichen, um Schutz vor KI-gesteuerten Angriffen zu bieten. Cyberkriminelle nutzen KI und Automatisierung, um ihre Aktivitäten zu skalieren und ihre Erfolgsquoten zu steigern – daher ist es für Organisationen unerlässlich, ihre Sicherheitslage neu zu bewerten. Die Ergebnisse unserer Email Penetration Tests unterstreichen die dringende Notwendigkeit, dass Sicherheitsverantwortliche umgehend handeln und in fortschrittliche E-Mail-Sicherheitslösungen investieren, die KI-gestützte Bedrohungserkennung und Verhaltensanalysen integrieren.

Organisationen, die sich nicht anpassen, werden weiterhin eine Zunahme erfolgreicher Angriffe erleben. Wer heute proaktive Massnahmen ergreift, sorgt für eine stärkere und widerstandsfähigere Verteidigung gegenüber den KI-gesteuerten Bedrohungen von morgen.

xorlab

xorlab ist auf die Erkennung neuer und bislang unbekannter E-Mail-Bedrohungen spezialisiert. Unsere Plattform befähigt Security Analysten, die Erkennung von xorlab mit eigenen Regeln zu verfeinern – für schnellere Reaktionen auf neue Bedrohungen und mehr Kontrolle über die Angriffsfläche ihrer Organisation.

Erfahren Sie mehr auf xorlab.com

Email Penetration Test anfordern