Mai 2023

MARKTBERICHT

2023 Spear-Phishing-Trends

Wichtige Erkenntnisse über die Auswirkungen von Angriffen und die Herausforderungen der Bedrohungserkennung und Reaktion darauf »

Barracuda®
Your journey, secured.

Inhaltsverzeichnis

Zentrale Ergebnisse 1

Einleitung 2

Barracuda-Erkennung und -Analyse von Spear-Phishing-Angriffen im Jahr 2022 4

Auswirkungen und Kosten von Spear-Phishing-Angriffen 7

Herausforderungen bei Bedrohungserkennung und Reaktion 14

Best Practices zur Bekämpfung von Spear Phishing 19

Über Barracuda 21

Über Vanson Bourne 21

Zentrale Ergebnisse

50% der Unternehmen wurden in den letzten 12 Monaten Opfer von Spear Phishing.

An einem regulären Arbeitstag werden der IT-Abteilung eines Unternehmens durchschnittlich **10 verdächtige E-Mails** gemeldet.

Ein typisches Unternehmen erhält **5 höchst personalisierte Spear-Phishing-E-Mails** pro Tag.

Es dauert im Durchschnitt fast **zwei Tage**, um einen E-Mail-Sicherheitsvorfall zu erkennen.

Bei 1 von 4 Unternehmen wurde im Jahr 2022 mindestens ein E-Mail-Konto kompromittiert.

Hacker senden durchschnittlich **370 bösartige E-Mails** von jedem kompromittierten Konto.

Einleitung

Das Volumen von Spear Phishing bleibt gering, hat aber große Auswirkungen

Während Cyberkriminelle versuchen, viele verschiedene Angriffsvektoren auszunutzen, bleibt E-Mail einer der beliebtesten. Die 13 Arten von E-Mail-Bedrohungen, die von Barracuda-Forschern identifiziert wurden, darunter Spear Phishing, entwickeln sich ständig weiter.

Aufgrund der weit verbreiteten E-Mail-basierten Sicherheitsangriffe erleiden Unternehmen finanzielle Verluste, Rufschädigung und andere negative Auswirkungen.

Spear Phishing ist eine hochgradig personalisierte Form des E-Mail-Angriffs. Hacker recherchieren ihre Ziele und erstellen sorgfältig gestaltete Nachrichten. Dabei geben sie sich oft als vertrauenswürdige Kollegen, Websites oder Unternehmen aus. Spear-Phishing-E-Mails versuchen in der Regel, vertrauliche Informationen wie Zugangsdaten oder Finanzinformationen zu stehlen, die dann für Betrug, Identitätsdiebstahl und andere Straftaten verwendet werden.

Methodik

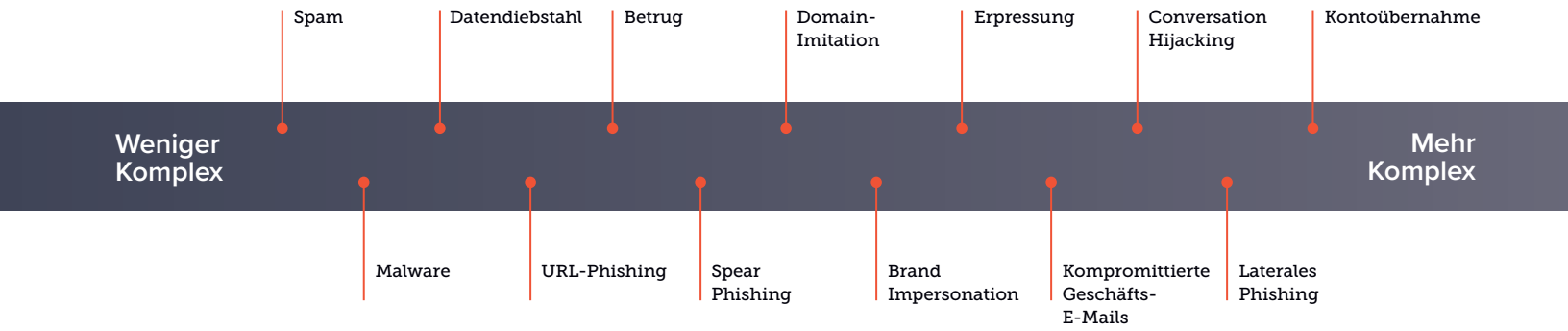
Dieser Bericht enthält proprietäre Spear-Phishing-Daten und -Analysen von Barracuda-Forschern, die auf einem Datensatz basieren, der 50 Milliarden E-Mails in 3,5 Millionen Postfächern umfasst, darunter fast 30 Millionen Spear-Phishing-E-Mails.

Der Bericht enthält auch Umfrageergebnisse aus der von Barracuda bei Vanson Bourne in Auftrag gegebenen Studie. Das unabhängige Marktforschungsunternehmen Vanson Bourne führte eine weltweite Umfrage unter 1.350 IT-Managern und technischen IT-Fachleuten, leitenden IT-Sicherheitsmanagern und leitenden IT-Führungskräften sowie IT-Sicherheitsentscheidern durch, die Unternehmen aller Größenordnungen aus einer Vielzahl von Branchen repräsentieren. Die Umfrageteilnehmer waren aus den USA, Australien, Indien und Europa. Die europäischen Befragten stammten aus dem Vereinigten Königreich, Frankreich, der DACH-Region (Deutschland, Österreich, Schweiz), den Benelux-Staaten (Belgien, Niederlande, Luxemburg) und Skandinavien (Dänemark, Finnland, Norwegen, Schweden). Die Umfrage wurde im Dezember 2022 durchgeführt.

Spear-Phishing-Angriffe, die darauf abzielen, herkömmliche E-Mail-Sicherheitssysteme wie Gateways und Spam-Filter zu umgehen, werden häufig von Domains mit hohem Ansehen oder bereits kompromittierten E-Mail-Konten versendet. Spear-Phishing-E-Mails enthalten nicht immer bösartige Links oder Anhänge. Da die meisten traditionellen E-Mail-Sicherheitstechniken auf Blocklisten und Reputationsanalysen beruhen, kommen diese Angriffe durch. Angriffe nutzen in der Regel Spoofing-Techniken und manchmal „Zero-Day"-Links. Dabei handelt es sich um URLs, die auf Domains gehostet werden, die nicht bei früheren Angriffen verwendet wurden oder die in gehackte legitime Websites eingefügt wurden. Es ist unwahrscheinlich, dass sie durch URL-Schutztechnologien blockiert werden.

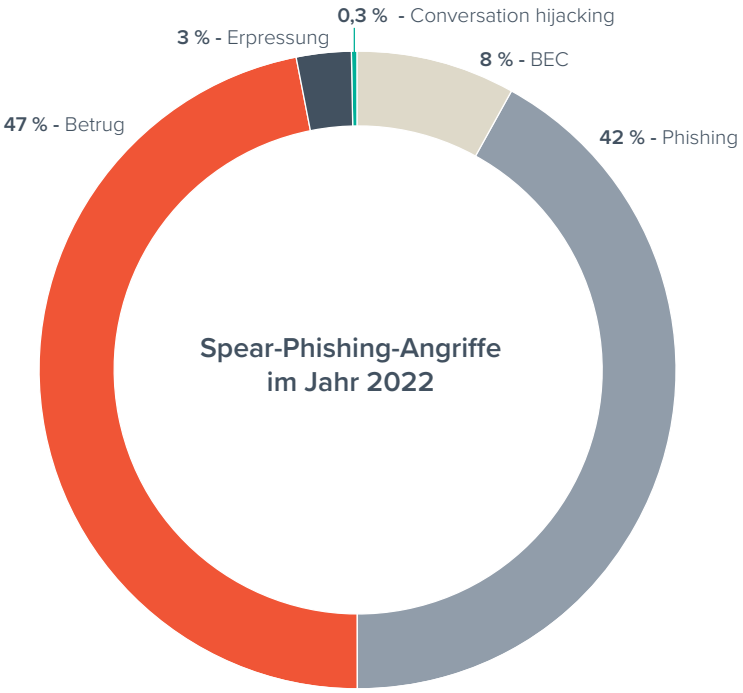
Cyberkriminelle machen sich auch Social-Engineering-Taktiken, einschließlich Dringlichkeit, Kürze und Druck, bei ihren Spear-Phishing-Angriffen zunutze, um die Erfolgswahrscheinlichkeit zu erhöhen.

13 Arten von E-Mail-Bedrohungen



Barracuda-Erkennung und -Analyse von Spear-Phishing-Angriffen im Jahr 2022

In einer Analyse von 50 Milliarden E-Mails in 3,5 Millionen Postfächern entdeckten Barracuda-Forscher fast 30.000.000 Spear-Phishing-E-Mails. Obwohl diese E-Mails weniger als 0,1 % aller gesendeten E-Mails ausmachen, haben sie große Auswirkungen auf Unternehmen, wenn sie erfolgreich sind. (Zum Vergleich: Angriffe mit hohem Volumen, wie z. B. Spam und Malware machen etwa 16 % der E-Mails aus, aber ihre Auswirkungen sind nicht so hoch). Die durchschnittlichen Kosten einer Datenschutzverletzung, die durch die Kompromittierung von Geschäfts-E-Mails verursacht wurde, beliefen sich im Jahr 2022 auf fast 5 Millionen US-Dollar, so IBM. Und kein Geschäft ist immun.



Die Untersuchungen von Barracuda zeigen, dass ein durchschnittliches Unternehmen täglich etwa fünf Spear-Phishing-E-Mails erhält, was über 1.700 pro Jahr entspricht. Die vielleicht schlimmste Nachricht von allen ist, dass der Analyse von Barracuda zufolge Spear-Phishing-E-Mails eine durchschnittliche Klickrate von 11 % haben. Da ein einziger erfolgreicher Angriff verheerende Folgen haben kann, ist ein mehrschichtiger Schutz gegen diese E-Mail-Bedrohungen von entscheidender Bedeutung.

Die Forscher von Barracuda haben fünf Arten von Spear-Phishing-Angriffen identifiziert:

Betrug

Betrug macht 47 % der analysierten Spear-Phishing-E-Mails aus und ist damit der häufigste Angriff. Betrug kann viele Formen annehmen, aber sie zielen alle darauf ab, private, sensible und personenbezogene Daten abzufangen, wie z. B. Bankkonto-, Kreditkarten- und Sozialversicherungsnummern. Die Angreifer bringen ihre Opfer dazu, diese Informationen preiszugeben, und verwenden sie dann, um sie zu betrügen, ihre Identität zu stehlen oder beides. Die Angriffe werden mit einer Vielzahl von Tricks ausgeführt, z. B. mit Lotteriegewinnen, nicht abgeholten Paketen, gefälschten Stellenausschreibungen, Spendenaufrufen und anderen Taktiken.

Business Email Compromise

Die Kompromittierung von Geschäfts-E-Mails, die auch als CEO-Betrug, Whaling und Überweisungsbetrug bekannt ist, macht nur 8 % der Spear-Phishing-Angriffe aus, verursacht jedoch Verluste in Milliardenhöhe. Betrüger geben sich in einer E-Mail als Mitarbeiter, Partner, Anbieter oder eine andere vertrauenswürdige Person aus und fordern eine Überweisung oder personenbezogene Daten von Mitarbeitern der Finanzabteilung oder anderen Personen mit Zugriff auf vertrauliche Informationen an. Diese zielgerichteten Angriffe sind besonders schwer zu erkennen, da sie selten eine URL oder einen bösartigen Anhang enthalten.

Brand Impersonation

Diese Art von Spear Phishing macht 42 % aller Angriffe aus und zielt darauf ab, sich als bekannte Unternehmen und häufig genutzte Geschäftsanwendungen auszugeben. Sie gehören zu den beliebtesten Arten von Angriffen, da sie gut als Einstiegspunkt für das Sammeln von Zugangsdaten und Account Takeover geeignet sind. Brand Impersonation wird in der Regel dazu verwendet, Zugangsdaten für Konten zu stehlen, aber manchmal werden auch persönliche Daten wie Kreditkarten- und Sozialversicherungsnummern gestohlen. Angreifer geben sich als große Unternehmen und beliebte Anwendungen wie Microsoft, DHL, DocuSign, WeTransfer und andere aus.

Erpressung

Erpressungsangriffe machen 3 % der Gesamtzahl der gezielten Phishing-Angriffe aus. Bei den meisten Angriffen handelt es sich um E-Mail-Erpressungen mit der Drohung der Veröffentlichung von kompromittierenden Informationen. Cyberkriminelle behaupten, kompromittierende Videos, Bilder oder andere sensible oder peinliche Inhalte zu haben, die angeblich vom Computer des Opfers aufgezeichnet wurden. Sie drohen, diese Inhalte mit all ihren E-Mail-Kontakten zu teilen, wenn kein Lösegeld gezahlt wird. Die Forderungen reichen in der Regel von einigen hundert bis zu einigen tausend Dollar und müssen in Bitcoin bezahlt werden, was schwer zu verfolgen ist.

Conversation Hijacking

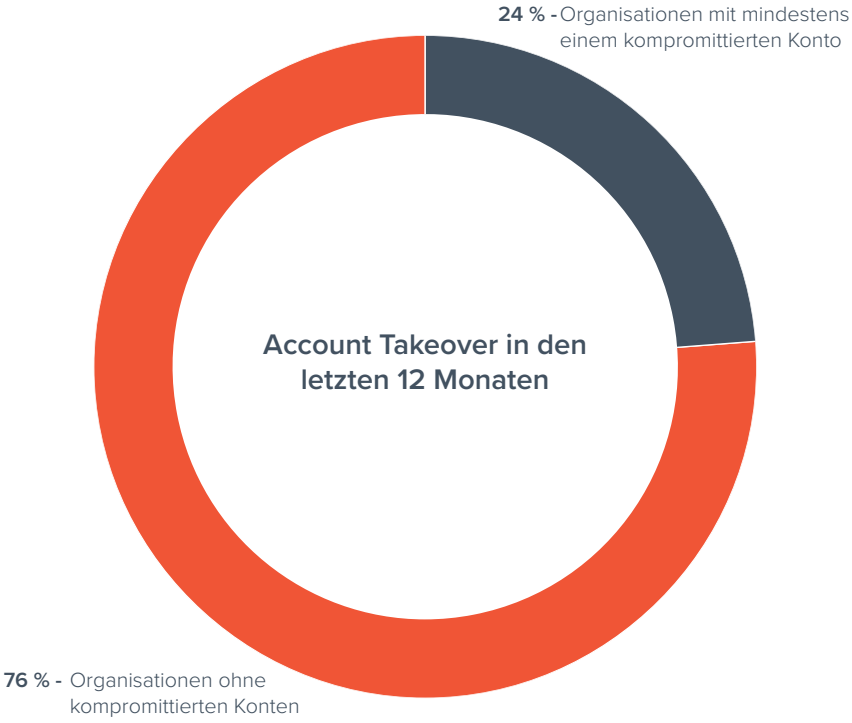
Conversation Hijacking, auch bekannt als Identitätsmissbrauch von Anbietern, kann verheerende Folgen haben. Bei diesen aufwändigen Angriffen, die nur 0,3 % aller Spear-Phishing-E-Mails ausmachen, mischen sich Cyberkriminelle in bestehende Geschäftsgespräche ein oder initiieren neue Gespräche auf der Grundlage von Informationen, die sie aus kompromittierten E-Mail-Konten oder anderen Quellen gesammelt haben.

Conversation Hijacking ist in der Regel Teil eines Account Takeover-Angriffs. Die Angreifer verwenden Phishing-Angriffe für den Diebstahl von Zugangsdaten und zur Kompromittierung von Geschäftskonten. Sie lesen E-Mails durch und überwachen das kompromittierte Konto, um den Geschäftsbetrieb zu verstehen und sich über laufende Geschäfte, Zahlungsverfahren und andere Details zu informieren. Kriminelle nutzen diese Informationen, einschließlich interner und externer Gespräche zwischen Mitarbeitern, Partnern und Kunden, um überzeugende Nachrichten zu verfassen, die sie von imitierten Domains versenden, und somit Opfer zu einer Überweisung oder Aktualisierung von Zahlungsangaben zu verleiten.

Kontokompromittierung oder Account Takeover ist oft das Ergebnis von Phishing-Angriffen. Hacker nutzen Social-Engineering-Taktiken, um Benutzer dazu zu verleiten, ihre Zugangsdaten preiszugeben, die dann verwendet werden, um in das Netzwerk einer Organisation einzudringen. Sobald sich die Hacker im Unternehmen befinden, können sie sich seitlich im Netzwerk ausbreiten und wertvollere Konten kompromittieren oder kompromittierte Konten als Startrampe für weitere Angriffe nutzen.

Im Jahr 2022 hatte fast jedes vierte Unternehmen (24 %) laut den Daten und Analysen von Barracuda mindestens ein durch Kontoübernahme kompromittiertes E-Mail-Konto. Von jedem kompromittierten Konto verschickten Hacker durchschnittlich 370 bösartige E-Mails.

Der Rest dieses Berichts befasst sich mit den Erfahrungen mit Spear Phishing auf der ganzen Welt, den Auswirkungen der Angriffe, den Herausforderungen bei der Erkennung und Reaktion sowie einer Reihe damit zusammenhängender Fragen.



Auswirkungen und Kosten von Spear-Phishing-Angriffen

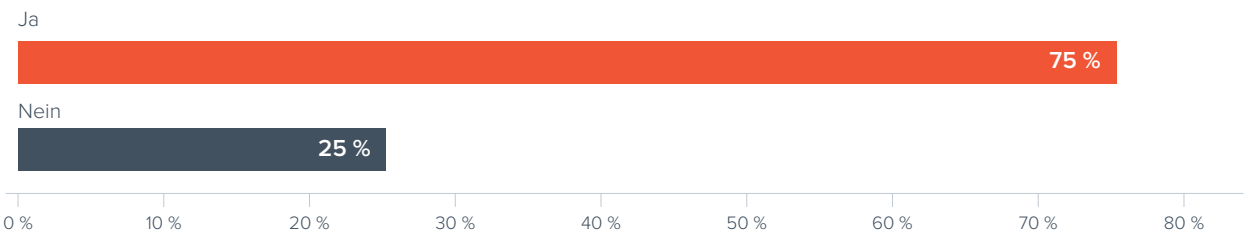
Das Volumen der Spear-Phishing-Angriffe ist zwar gering, doch sie sind im Vergleich zu anderen Arten von E-Mail-Angriffen weit verbreitet und sehr erfolgreich.

Der Erfolg von Spear-Phishing-Angriffen

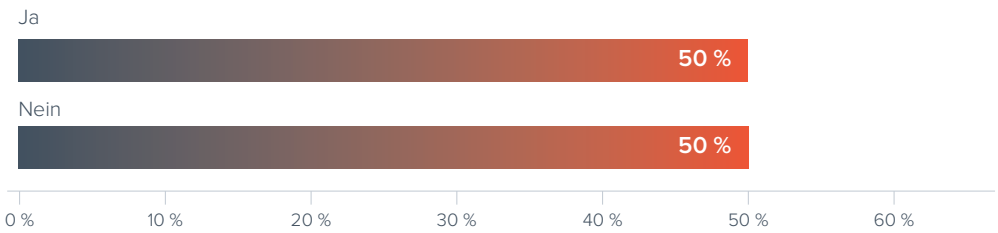
Drei Viertel der Befragten gaben an, in den letzten 12 Monaten Opfer eines E-Mail-Angriffs geworden zu sein. Die Hälfte davon waren Opfer von Spear Phishing. Das bedeutet, dass es sich bei 2 von 3 erfolgreichen E-Mail-Angriffen um Spear Phishing handelt, das personalisierte Nachrichten, Social Engineering und andere Taktiken nutzt.

Dies ist insofern von Bedeutung, da diese Angriffe nach den Daten von Barracuda nur 0,1 % aller E-Mail-basierten Angriffe ausmachen, aber für 66 % aller Sicherheitsverletzungen verantwortlich sind. Andererseits machen Angriffe mit hohem Volumen, wie Spam und Malware, 16 % der E-Mails aus, sind aber nur für ein Drittel der Sicherheitsverletzungen verantwortlich. Der Schutz vor Spear Phishing ist von entscheidender Bedeutung, da bereits ein einziger erfolgreicher Angriff verheerende Folgen haben kann.

Hat Ihr Unternehmen im letzten Jahr einen erfolgreichen E-Mail-basierten Angriff erlitten? (n=1.350)

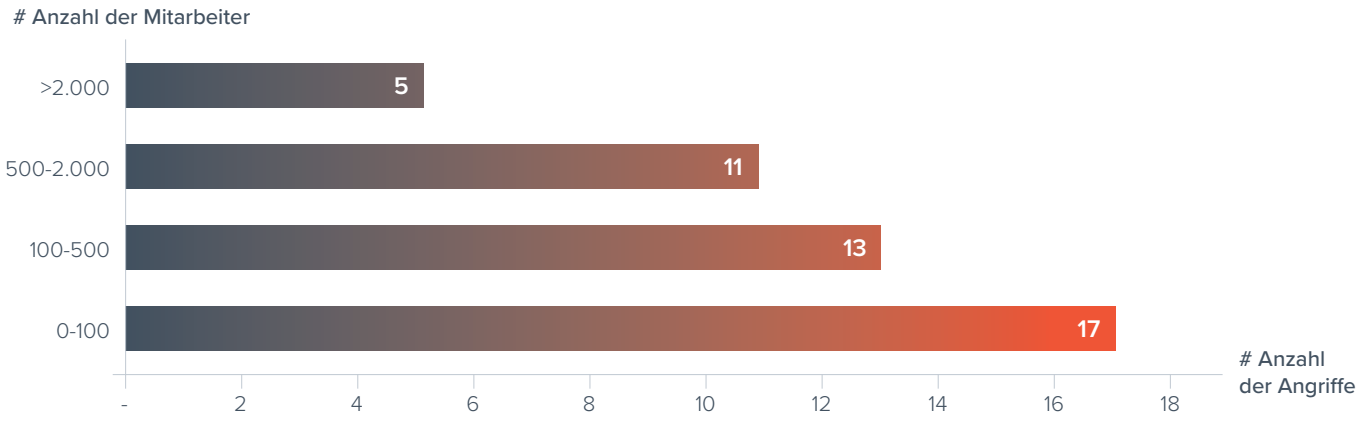


Wurde Ihr Unternehmen in den letzten 12 Monaten Opfer von Spear Phishing? (n=1.350)



Während kleinere Unternehmen weniger erfolgreiche E-Mail-Angriffe durch Spear Phishing meldeten (42 %), ergab der Barracuda-Bericht von 2022 „Spear Phishing: Top Bedrohungen und Trends (Ausgabe 7)“, dass kleinere Unternehmen mit einer höheren durchschnittlichen Anzahl von Social-Engineering-Angriffen pro Postfach überproportional angegriffen werden. Kleinere Unternehmen verfügen oft nicht über das notwendige Tool, um ausgeklügelte Angriffe zu identifizieren und zu blockieren oder sogar laufende Angriffe zu identifizieren und darauf zu reagieren. Viele sind sich möglicherweise nicht bewusst, wie viele Bedrohungen sich bereits in den Posteingängen ihrer Benutzer befinden.

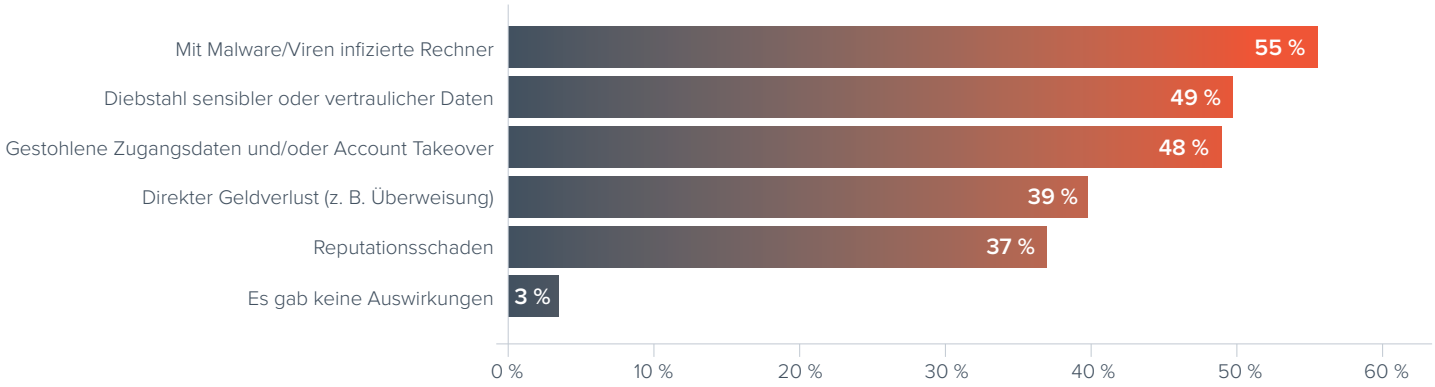
Durchschnittliche Anzahl von Social Engineering-Angriffen pro Mailbox



Unserer jüngsten Marktumfrage zufolge sind Unternehmen, die Gmail nutzen, häufiger Opfer von Spear-Phishing-Angriffen als Unternehmen, die Microsoft 365 nutzen. 57 % der Unternehmen, die Gmail nutzen, berichteten von einem erfolgreichen Spear-Phishing-Angriff, verglichen mit 41 % der Unternehmen, die Microsoft nutzen. In der Microsoft-Umgebung stehen zahlreiche Sicherheitsoptionen zur Verfügung, die einen besseren Schutz bieten.

Die Auswirkungen von Spear-Phishing-Angriffen

Welche Auswirkungen hatten die Spear-Phishing-Angriffe in Ihrem Unternehmen in den letzten 12 Monaten? (n=678)



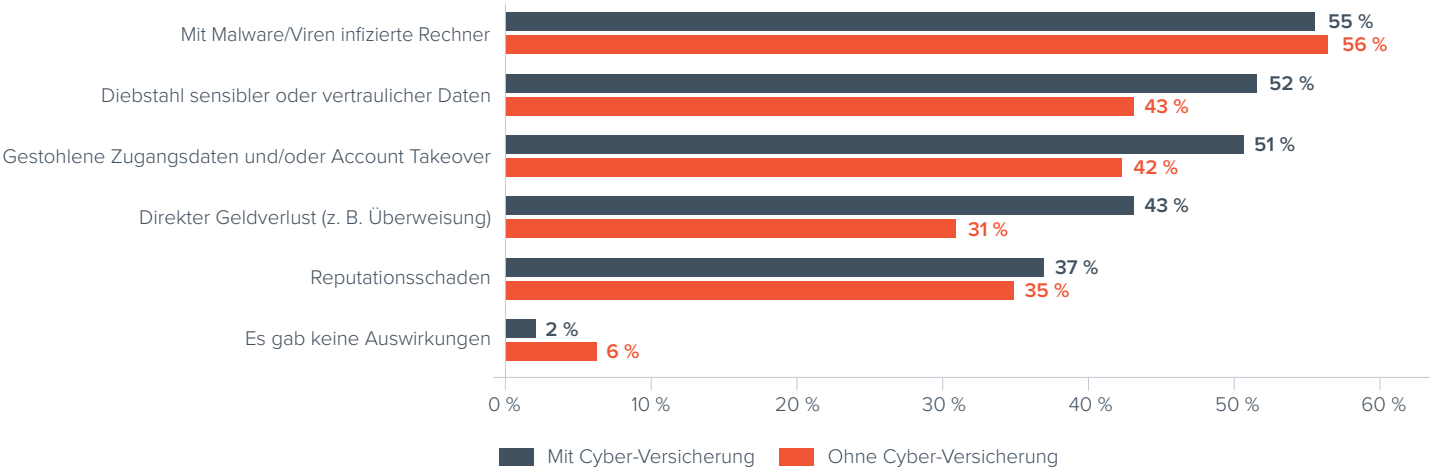
Nahezu alle Spear-Phishing-Angriffe in den letzten 12 Monaten hatten Auswirkungen auf die Unternehmen der Opfer, darunter Malware-Infektionen, Datendiebstahl und Rufschädigung. Während ein direkter finanzieller Verlust möglich ist, kann ein Angriff auch zu indirekten finanziellen Schäden für eine Organisation führen.

Hacker, die z. B. einen Malware-Angriff planen, verlassen sich häufig auf Phishing, um in ein Unternehmen einzudringen. Der Diebstahl von Zugangsdaten ist auch ein häufiges Ziel dieser Angriffe, da sich Betrüger zunehmend auf Spear-Phishing-Taktiken verlassen, um sich Zugriff zu verschaffen und dann Account Takeover durchzuführen.

Von den Opfern eines Spear-Phishing-Angriffs in den letzten 12 Monaten gab fast die Hälfte an, dass Zugangsdaten gestohlen oder sie Opfer von Account Takeover wurden.

Bei Unternehmen ohne Cyber-Versicherung waren infizierte Rechner die am häufigsten genannte Auswirkung von Spear-Phishing-Angriffen. Während Unternehmen mit Cyber-Versicherung diese Auswirkungen ebenso verzeichneten, war die Wahrscheinlichkeit für sie höher, andere Auswirkungen hinnehmen zu müssen, darunter Datendiebstahl, gestohlene Zugangsdaten und direkte finanzielle Verluste. Der Unterschied besteht vielleicht darin, dass nur Unternehmen, bei denen es sensible Informationen zu stehlen gibt, dies als Auswirkung bezeichnen würden. Es ist auch möglich, dass den Unternehmen dieses Problem nicht bewusst ist und sie nicht auf Auswirkungen wie den Verlust vertraulicher Informationen oder gestohlene Zugangsdaten achten.

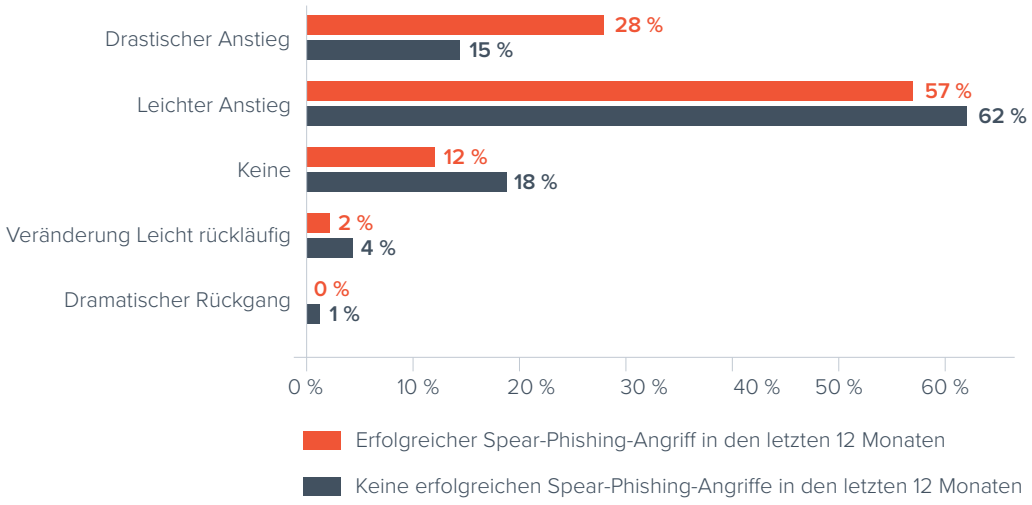
Welche Auswirkungen hatten die Spear-Phishing-Angriffe in Ihrem Unternehmen in den letzten 12 Monaten? (n=678)



Die Kosten von Spear-Phishing-Angriffen

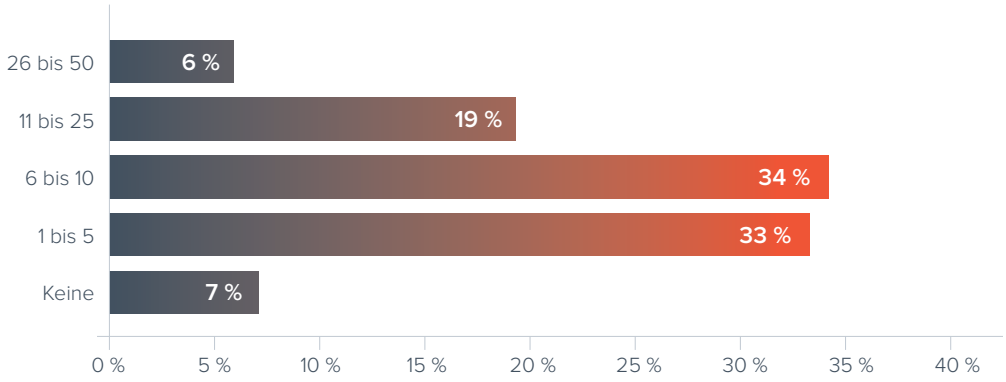
Unternehmen, die Opfer eines Spear-Phishing-Angriffs wurden, gaben mit größerer Wahrscheinlichkeit an, dass die mit einer E-Mail-Sicherheitsverletzung verbundenen Kosten im letzten Jahr dramatisch gestiegen sind: 28 % gegenüber 15 % der Unternehmen, die kein Opfer von Spear Phishing waren. Die Wahrscheinlichkeit, dass diese Unternehmen bei dem teuersten Angriff, den sie erleiden, mehr Kosten für die Wiederherstellung und die Auswirkungen haben, ist ebenfalls höher – durchschnittlich 1,1 Mio. USD im Vergleich zu 760.882 USD für diejenigen, die Opfer anderer Arten von E-Mail-Angriffen waren.

Wie haben sich die Gesamtkosten von E-Mail-Sicherheitsverletzungen in den letzten 12 Monaten verändert? (n=1.003)



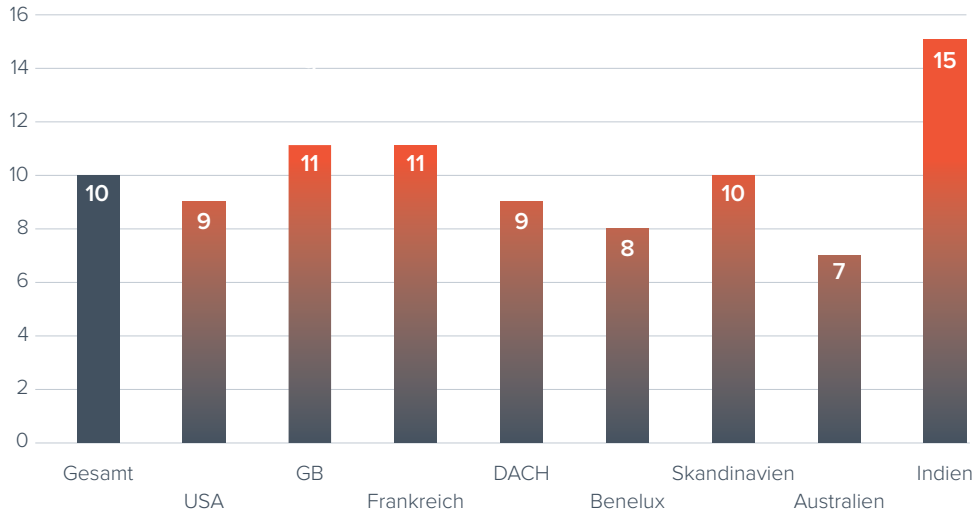
Bei 93 % der Unternehmen meldeten Benutzer verdächtige Nachrichten nach der Zustellung

Wie viele verdächtige E-Mails werden der IT Ihres Unternehmens an einem typischen Arbeitstag gemeldet? (n=1.350)



An einem typischen Arbeitstag werden der IT durchschnittlich 10 verdächtige E-Mails gemeldet

Wie viele verdächtige E-Mails werden der IT Ihres Unternehmens an einem typischen Arbeitstag gemeldet? (n=1.350)



Nach Region melden Nutzer in Indien die höchste durchschnittliche Anzahl verdächtiger E-Mails pro Tag – 50% mehr als der weltweite Durchschnitt. Dies könnte ein Beweis dafür sein, dass Unternehmen Schwierigkeiten haben, E-Mail-basierte Angriffe zu verhindern, oder dass Unternehmen in Indien verdächtigen E-Mails mehr Aufmerksamkeit schenken und deshalb im Durchschnitt mehr davon entdecken und melden. Eine große Anzahl von gemeldeten Nachrichten ist jedoch nicht immer ein gutes Zeichen. Es könnte auch bedeuten, dass die Benutzer eine Menge an Graymail oder unerwünschter Nachrichten melden und nicht etwa bösartige E-Mails.

Bei 7 % der Unternehmen weltweit werden von ihren Benutzern keine E-Mails gemeldet. In DACH und Australien sind die Zahlen besonders hoch: 14 % geben an, dass keine E-Mails gemeldet werden. In diesen Regionen ist auch die Akzeptanz computerbasierter Schulungen zur Stärkung des Sicherheitsbewusstseins unterdurchschnittlich. Während der weltweite Durchschnitt bei 42 % liegt, sind es in Australien 28 % und in der DACH-Region 37 %. Geringere Investitionen in das Sicherheitsbewusstsein könnten dazu beigetragen haben, dass die Benutzer weniger wachsam sind oder eine potenzielle E-Mail-Bedrohung weniger gut erkennen können.

Aufgrund der hochgradig personalisierten Natur von Spear-Phishing-E-Mails und der potenziell schwerwiegenden Auswirkungen eines erfolgreichen Angriffs sollte jedes Unternehmen, unabhängig von seiner Größe und seinem Standort, die entsprechenden Vorkehrungen zur Verhinderung dieser Angriffe treffen.

Im Verhältnis dazu melden Benutzer in größeren Unternehmen weniger verdächtige E-Mails

Die Anzahl der von Benutzern gemeldeten Angriffe steht nicht im Verhältnis zur Größe ihrer Organisationen. In Unternehmen mit 100 bis 249 Mitarbeitern werden durchschnittlich sieben verdächtige E-Mails pro Tag gemeldet, während in Unternehmen mit 1.000 bis 2.500 Mitarbeitern durchschnittlich zwölf E-Mails pro Tag gemeldet werden. Wie wir bereits gesehen haben, sind kleinere Unternehmen im Verhältnis zu ihrer Größe tatsächlich einem größeren Volumen an Spear-Phishing-Angriffen ausgesetzt.

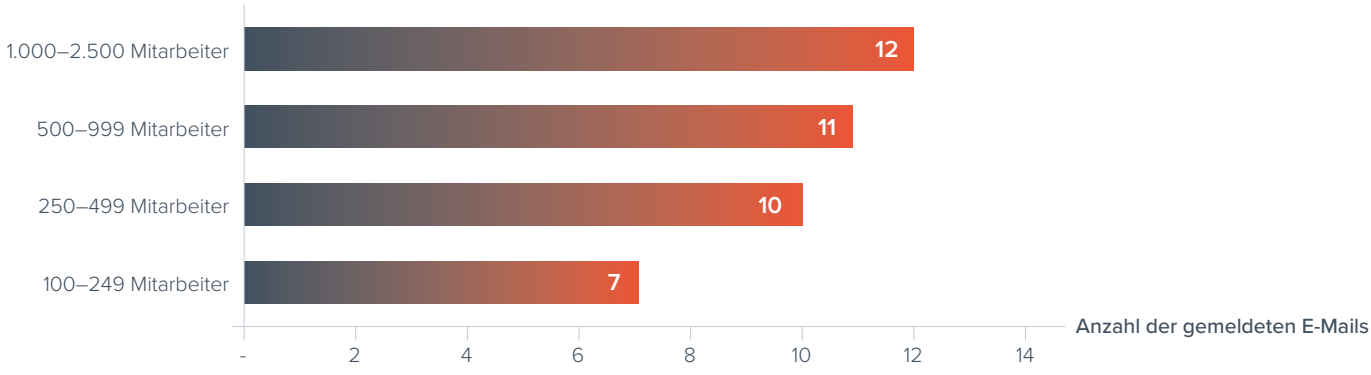
Diese größere Anzahl von Angriffen und einige potenziell übermäßige Meldende könnten bedeuten, dass IT-Teams eine größere Anzahl von Nachrichten bearbeiten müssen. Leider haben kleinere Unternehmen kleinere IT-Teams, sodass sie nicht immer über genügend Tools und Ressourcen verfügen, um alle potenziellen Vorfälle zu bearbeiten.

Größere Unternehmen nutzen eher Tools und Ressourcen, um Vorfälle zu priorisieren, die behoben werden müssen, und um schnell den Unterschied zwischen harmlosen und bösartigen E-Mails zu erkennen.

Benutzer in Unternehmen mit mehr als 50 % externen Beschäftigten berichten von einer höheren Anzahl verdächtiger E-Mails – im Durchschnitt zwölf pro Tag, verglichen mit neun pro Tag bei Unternehmen mit weniger als 50 % externen Mitarbeitenden. Unternehmen mit einer größeren Anzahl von externen Beschäftigten, die an verschiedenen Orten arbeiten, sind gegenüber potenziellen Bedrohungen anfälliger. Da sie mit größerer Wahrscheinlichkeit Opfer eines Spear-Phishing-Angriffs werden, könnten sie eine übermäßige Berichterstattung ihrer Benutzer begrüßen.

In Unternehmen, die von mehreren Ransomware-Angriffen betroffen sind, berichten die Mitarbeiter auch von einer höheren Anzahl verdächtiger E-Mails: Durchschnittlich 17 verdächtige E-Mails pro Tag in Unternehmen, die von drei oder mehr Ransomware-Angriffen betroffen sind. Nach Ransomware-Angriffen wird das Sicherheitsbewusstsein der Benutzer in Organisationen wahrscheinlich zunehmen, was möglicherweise zu einer Überberichterstattung der Benutzer führt.

Wie viele verdächtige E-Mails werden der IT Ihres Unternehmens an einem typischen Arbeitstag (durchschnittlich) gemeldet? (n=1.350)



Herausforderungen bei Bedrohungserkennung und Reaktion

Keine Security ist zu 100 Prozent wirksam. Wenn eine Bedrohung durchkommt, müssen Sicherheitsteams schnell handeln, um sie zu erkennen und darauf zu reagieren, bevor sie sich ausbreitet und großen Schaden anrichtet. Schnellere Erkennungs- und Reaktionszeiten verringern das Risiko einer Sicherheitsverletzung.

Im Durchschnitt benötigen Unternehmen fast 100 Stunden, um eine E-Mail-Bedrohung nach der Zustellung zu erkennen, darauf zu reagieren und sie zu beheben.

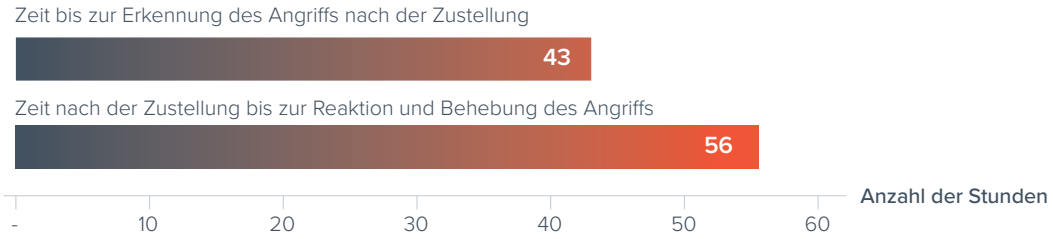
Mit einer durchschnittlichen Erkennungszeit von 43 Stunden und einer durchschnittlichen Reaktions- und Behebungszeit von 56 Stunden für E-Mail-Bedrohungen nach der Zustellung benötigen Unternehmen fast 100 Stunden für die Bewältigung eines E-Mail-Sicherheitsvorfalls.

1 von 5 Unternehmen (22 %) braucht länger als 24 Stunden, einen E-Mail-Angriff zu erkennen. Dieser lange Zeitraum gibt Benutzern ausreichend Zeit und Gelegenheit, auf einen schädlichen Link zu klicken oder auf eine E-Mail zu antworten. Wenn dies geschieht, können Hacker das kompromittierte Konto nutzen, um in das Netzwerk einzudringen und möglicherweise weitere Konten zu kompromittieren.

Als ob die langen Erkennungszeiten nicht schon besorgniserregend genug wären, gaben 38 % der Befragten an, dass sie über 24 Stunden benötigen, um auf die Angriffe zu reagieren und sie zu beseitigen, sobald sie davon Kenntnis erlangen.

Die Erkennungs-, Reaktions- und Behebungszeiten sind bei größeren Organisationen, die in der Regel über mehr Ressourcen verfügen und schneller reagieren können, im Durchschnitt kürzer. Während ein Unternehmen zwar möglicherweise aufgrund seiner Größe anfälliger für mehr Bedrohungen ist, steht wahrscheinlich ein größeres Team zur Verfügung, das bei der Erkennung, Reaktion und Behebung der Auswirkungen von Angriffen hilft.

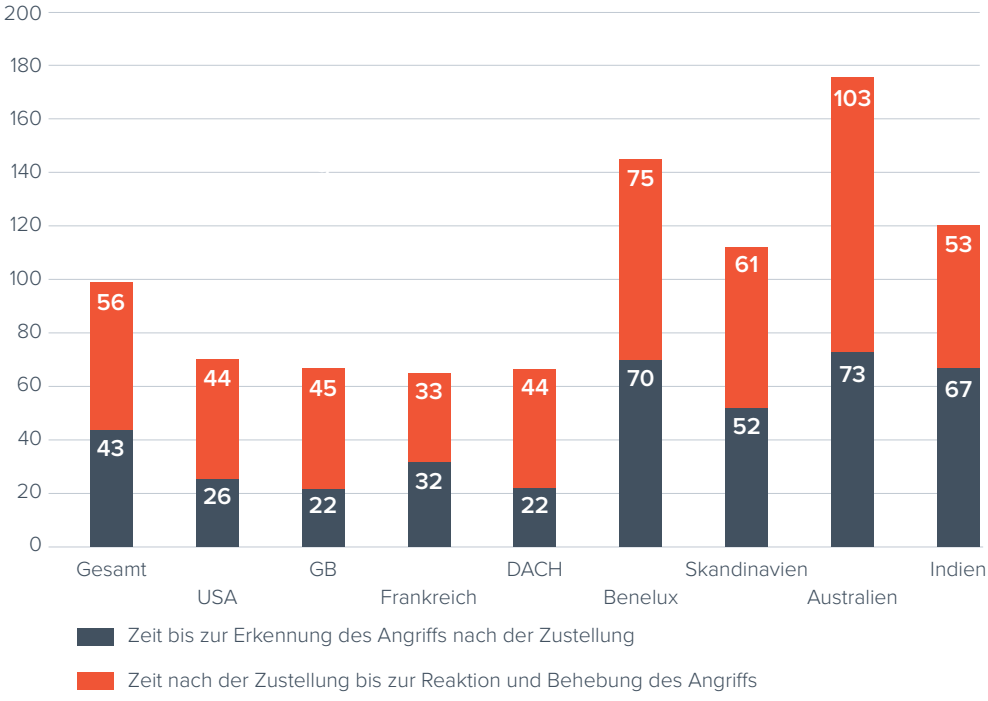
Wenn Sie an die Erkennungs- und Reaktionszeiten nach der Zustellung oder der gemeldeten E-Mail-Vorfälle denken, wie lange dauert es ungefähr (in Stunden), bis Ihr Unternehmen Folgendes erledigt? (n=1.350)



Investitionen in Automatisierung und Sicherheitstraining verkürzen die Reaktionszeiten

Die geringe Akzeptanz der automatisierten Incident Response in Australien (24 %) kann durchaus ein Grund für die langen Reaktionszeiten sein. Australien hat auch die niedrigsten Akzeptanzraten computergestützter Schulungen zur Stärkung des Risikobewusstseins. Die Verantwortung für die Aufdeckung von und die Reaktion auf Bedrohungen nach der Zustellung liegt größtenteils bei der IT-Abteilung, was ohne die erforderlichen Tools zu lange dauert – in Australien im Durchschnitt 175 Stunden.

Wenn Sie an die Erkennungs- und Reaktionszeiten nach der Zustellung oder der gemeldeten E-Mail-Vorfälle denken, wie lange dauert es ungefähr (in Stunden), bis Ihr Unternehmen Folgendes erledigt? (n=1.350)

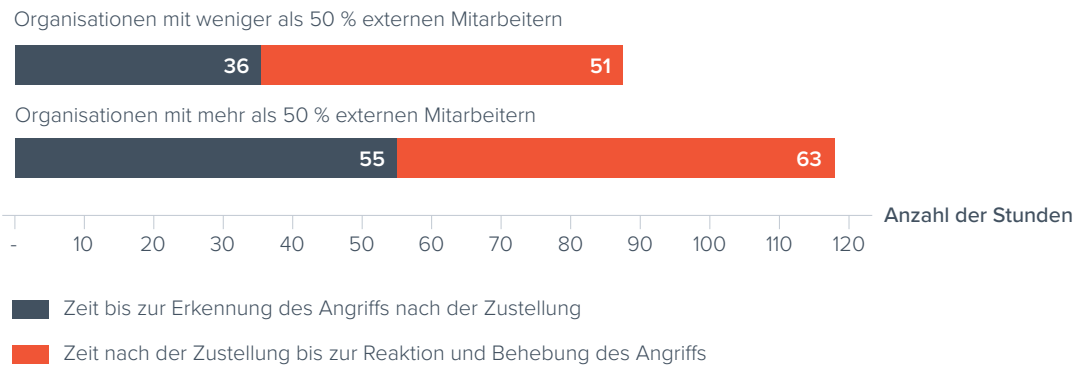


Auf der anderen Seite verwenden 36 % der Unternehmen in den Vereinigten Staaten eine automatisierte Reaktion auf Vorfälle, und 45 % nutzen computerbasierte Schulungen zur Stärkung des Risikobewusstseins. Sie berichten außerdem von durchschnittlich schnelleren Reaktionszeiten, was bedeutet, dass sie weniger IT-Ressourcen verbrauchen und diese Ressourcen sich auf andere Aufgaben konzentrieren können.

Die Erkennungs- und Reaktionszeit erhöht sich bei mehr externen Mitarbeitern

Unternehmen mit mehr externen Mitarbeitern brauchen länger, um E-Mail-Sicherheitsvorfälle zu erkennen und darauf zu reagieren. Unternehmen mit weniger als 50 % externen Mitarbeitern hatten eine durchschnittliche Erkennungszeit von 36 Stunden, während Unternehmen mit mehr als 50 % externen Beschäftigten durchschnittlich 55 Stunden benötigten, um einen E-Mail-Sicherheitsvorfall zu erkennen. Das Gleiche gilt für die Behebung: Bei Unternehmen mit weniger als 50 % externen Mitarbeitern betrug die durchschnittliche Reaktions- und Entschärfungszeit 51 Stunden, während Unternehmen mit mehr als 50 % externen Mitarbeitern durchschnittlich 63 Stunden für die Reaktion auf einen E-Mail-Sicherheitsvorfall und dessen Entschärfung benötigten.

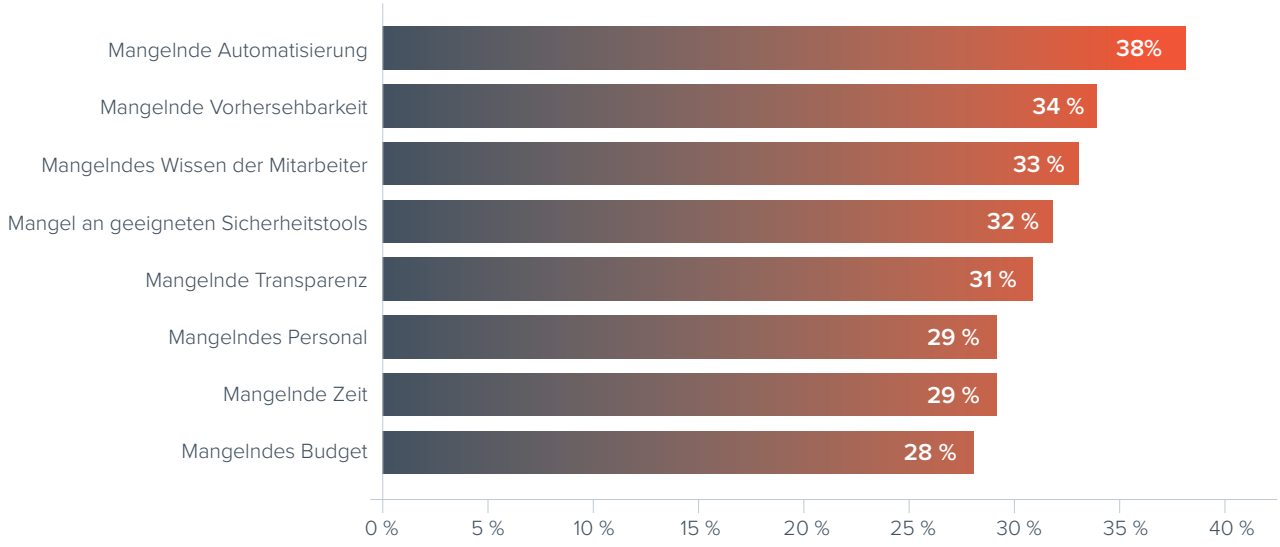
Wenn Sie an die Erkennungs- und Reaktionszeiten nach der Zustellung oder der gemeldeten E-Mail-Vorfälle denken, wie lange dauert es ungefähr (in Stunden), bis Ihr Unternehmen Folgendes erledigt? (n=1.350)



Mangelnde Automatisierung ist Haupthindernis

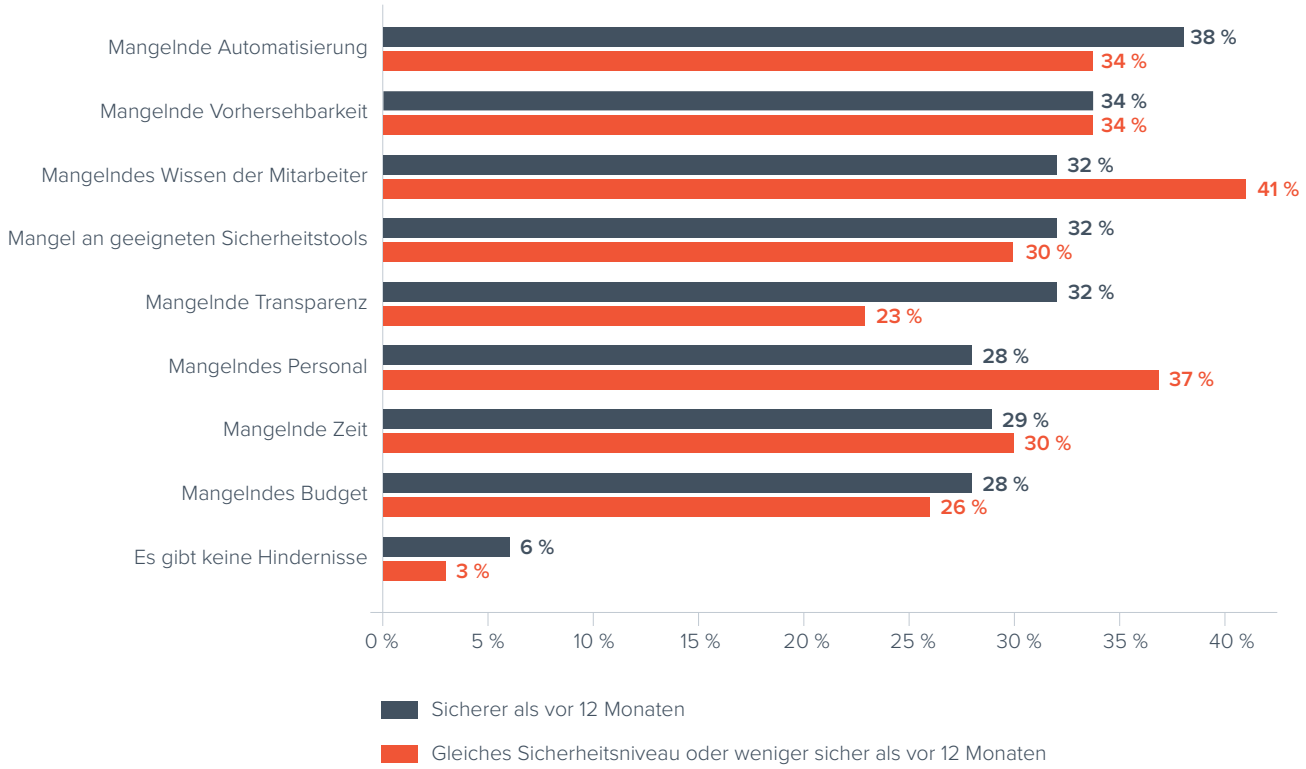
Größere Unternehmen nennen mangelnde Automatisierung als das wahrscheinlichste Hindernis, das einer schnellen Reaktion auf einen Vorfall im Weg steht: 41 % für Unternehmen mit über 250 Mitarbeitern im Vergleich zu 28 % für Unternehmen mit 100 bis 249 Mitarbeitern. Diese kleineren Unternehmen nennen fast zu gleichen Teilen weitere Gründe, darunter den Mangel an Vorhersehbarkeit (29 %), an Mitarbeiterwissen (32 %) und an geeigneten Sicherheitstools (32 %). Kleinere Unternehmen scheinen noch dabei zu sein, geeignete Tools einzuführen, und haben offenbar Schwierigkeiten, sachkundige Mitarbeiter einzustellen und zu halten. Sobald Unternehmen über die richtigen Mitarbeiter, Prozesse und Technologien verfügen, können sie die Vorteile der verfügbaren Mechanismen nutzen, um die Reaktionsarbeit zu beschleunigen, einschließlich der Automatisierung.

Was sind die Haupthindernisse, die eine schnelle Erkennung von und Reaktion auf E-Mail-Bedrohungen nach der Zustellung in Ihrem Unternehmen verhindern? (n=1.350)



Unternehmen, die sich sicherer fühlen, sagen auch, dass mangelnde Automatisierung das wahrscheinlichste Hindernis für eine schnelle Reaktion auf Vorfälle ist. Im Gegensatz dazu verweisen Unternehmen, die sich weniger sicher fühlen, auf einen Mangel an fachkundigem Personal. Gut ausgebildete Mitarbeiter sind eine Voraussetzung für ein starkes Programm zur Reaktion auf Vorfälle, und die Automatisierung kann diese Reaktion erheblich beschleunigen.

Was sind die Haupthindernisse, die eine schnelle Erkennung von und Reaktion auf E-Mail-Bedrohungen nach der Zustellung in Ihrem Unternehmen verhindern? (n=1.350)



Best Practices zur Bekämpfung von Spear Phishing

Da sich E-Mail-Angriffe weiterentwickeln und immer ausgefeilter werden, sehen sich Unternehmen mit ernsthaften Bedrohungen durch gezielte Spear-Phishing-Angriffe konfrontiert. Die Auswirkungen eines einzigen erfolgreichen Angriffs können verheerend sein. Um Ihr Unternehmen zu schützen, müssen Sie in Technologien investieren, die Angriffe abwehren, und in Schulungen, die den Mitarbeitern helfen, als letzte Verteidigungslinie zu agieren.

Technologie

- **Vorteile der künstlichen Intelligenz nutzen.** Betrüger passen E-Mail-Taktiken an, um Gateways und Spamfilter zu umgehen, daher ist es wichtig, eine Lösung zu haben, die eine Erkennung und den Schutz vor Spear-Phishing-Angriffen bietet, einschließlich kompromittierte Geschäfts-E-Mails, Identitätsmissbrauch und Erpressungsangriffe. Setzen Sie speziell entwickelte Technologien ein, die sich nicht nur auf die Suche nach bösartigen Links oder Anhängen verlassen. Verwenden Sie maschinelles Lernen, um normale Kommunikationsmuster in Ihrem Unternehmen zu analysieren und Anomalien zu erkennen, die auf einen Angriff hindeuten könnten.

- **Schutz vor Kontoübernahmen implementieren.** Es muss sichergestellt werden, dass Hacker keine kompromittierten Konten in Ihrem Unternehmen dazu nutzen können, um Spear-Phishing-Angriffe zu starten. Nutzen Sie Technologie mit künstlicher Intelligenz, um zu erkennen, wenn Konten kompromittiert sind, und die in Echtzeit das Problem beheben, indem sie die Benutzer warnen und bösartige E-Mails von den kompromittierten Konten entfernen.

- **Posteingangsregeln und verdächtige Logins überwachen.** Nutzen Sie Technologien, um verdächtige Aktivitäten zu erkennen, einschließlich Logins von ungewöhnlichen Orten und IP-Adressen, was ein mögliches Anzeichen für ein kompromittiertes Konto ist. Überwachen Sie E-Mail-Konten auch auf bösartige Posteingangsregeln, da diese häufig dazu verwendet werden, E-Mails zu verstecken oder zu löschen, die im Rahmen eines Angriffs zur Übernahme des Kontos gesendet wurden.

- **Multifaktor-Authentifizierung verwenden.** Bieten Sie über Benutzername und Passwort hinaus eine zusätzliche Sicherheitsebene, z. B. einen Authentifizierungscode, einen Fingerabdruck oder eine biometrische Authentifizierung.

- **DMARC-Authentifizierung und -Berichterstellung implementieren.** Dies hilft gegen Domain-Spoofing, eine der häufigsten Techniken, die bei Identitätsmissbrauch verwendet werden. Stoppen Sie Domain-Spoofing und Marken-Hijacking mit DMARC-Authentifizierung und -Durchsetzung. Legen Sie mit Hilfe von DMARC-Berichten und -Analysen genaue Durchsetzungsregeln für Ihr Unternehmen fest.

- **Automatisierte Incident Response.** Mit einer automatisierten Incident-Response-Lösung können Sie alle Bedrohungen, die in den Posteingängen gefunden werden, schnell bereinigen und die Behebung für alle zukünftigen Nachrichten effizienter gestalten.

- **Mitarbeiterschulungen zur Erkennung und Meldung von Angriffen.** Schulen Sie Benutzer über Spear-Phishing-Angriffe, indem Sie diese in Schulungen zur Stärkung des Risikobewusstseins thematisieren. Stellen Sie sicher, dass Mitarbeiter diese Angriffe erkennen, ihre betrügerische Natur verstehen und wissen, wie sie sie melden können.

- **Schutz vor Datenverlusten optimieren.** Mit der richtigen Kombination aus Technologien und Unternehmensrichtlinien wird eine Blockierung ausgehender E-Mails gewährleistet, die vertrauliche, personenbezogene und andere sensible Daten enthalten.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir glauben, dass jedes Unternehmen Zugang zu Cloud-First-Sicherheitslösungen auf Unternehmensniveau verdient hat, die einfach zu kaufen, zu implementieren und zu verwenden sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit der Entwicklung unserer Kunden wachsen und sich anpassen.

Mehr als 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Daher können Sie sich darauf konzentrieren, Ihr Unternehmen auf die nächste Stufe zu heben.

Weitere Informationen finden Sie unter barracuda.com.

Über Vanson Bourne

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung im Technologiesektor. Der Ruf des Unternehmens für robuste und glaubwürdige forschungsbasierte Analysen beruht auf strengen Forschungsprinzipien und der Fähigkeit, die Meinungen hochrangiger Entscheidungsträger in allen technischen und geschäftlichen Funktionen, in allen Geschäftsbereichen und allen wichtigen Märkten einzuholen.

Weiter Informationen erhalten Sie unter vansonbourne.com.

Barracuda
Your journey, secured.

2023 SPEAR-PHISHING-TRENDS • DE 1.0 • Copyright 2023 Barracuda Networks, Inc. • barracuda.com
Barracuda Networks und das Logo von Barracuda Networks sind eingetragene Marken der Barracuda Networks, Inc. in den USA. Alle anderen Namen sind Eigentum der jeweiligen Rechteinhaber.