Oktober 2025

Marktbericht

Bericht über E-Mail-Sicherheitsverletzungen 2025

Erfahrungen und Auswirkungen von E-Mail-Sicherheitsverletzungen auf Unternehmen weltweit

Barracuda®
Your business, secured.

Inhalt

Einleitung

Dieser Bericht untersucht die Erfahrungen und Auswirkungen von E-Mail-Sicherheitsverletzungen auf Unternehmen weltweit in den letzten 12 Monaten. Er basiert auf den Ergebnissen einer internationalen Umfrage unter 2.000 IT- und Security-Entscheidern, die von Barracuda und Vanson Bourne durchgeführt wurde. Die Ergebnisse waren über alle untersuchten Länder und Branchen hinweg weitgehend einheitlich, sodass sich dieser Bericht auf die allgemeinen und größenbezogenen Ergebnisse konzentriert.

Die Ergebnisse zeigen, dass die meisten Organisationen von E-Mail-Sicherheitsverletzungen betroffen sind. Sie heben hervor, wie eine zunehmend komplexe E-Mail-Bedrohungslandschaft und interne Herausforderungen wie Qualifikationslücken und das Fehlen automatisierter Incident Response es Organisationen erschweren, Verstöße schnell zu erkennen, darauf zu reagieren und sich davon zu erholen.

Verzögerte Reaktionszeiten können Organisationen anfällig für andere Angriffe machen, wie etwa Ransomware, und zu weitreichenderen Schäden führen.

Die Auswirkungen einer E-Mail-Sicherheitsverletzung sind weitreichend und reichen von Ausfallzeiten bis hin zu Rufschädigung und Geschäftseinbußen. Die Wiederherstellungskosten treffen kleinere Unternehmen besonders hart.

Dieser Bericht soll Unternehmen dabei helfen, die Risiken und Auswirkungen von E-Mail-basierten Security-Bedrohungen besser zu verstehen und Bereiche hervorzuheben, in denen sie möglicherweise anfällig sind.

Methodik

Barracuda beauftragte das unabhängige Marktforschungsunternehmen Vanson Bourne mit der Durchführung einer globalen Umfrage unter 2.000 leitenden Sicherheitsexperten in IT- und Geschäftsfunktionen in Organisationen mit 50 bis 2.000 Mitarbeitern aus einer Vielzahl von Branchen in den USA, dem Vereinigten Königreich, Frankreich, DACH (Deutschland, Österreich, Schweiz), Benelux (Belgien, Niederlande, Luxemburg), den nordischen Ländern (Dänemark, Finnland, Norwegen, Schweden), Australien, Indien und Japan. Die Feldforschung wurde im April und Mai 2025 durchgeführt.

Zentrale Ergebnisse

78%

der Unternehmen haben in den letzten 12 Monaten eine E-Mail-Sicherheitsverletzung erlebt

71%

der Unternehmen, die eine E-Mail-Sicherheitsverletzung erlebt haben, wurden im selben Jahr auch von Ransomware angegriffen

41%

erlitten einen Reputationsschaden und viele verloren neue Geschäftsmöglichkeiten, was das Wachstum beeinträchtigte

50%

erkannten den Verstoß innerhalb einer Stunde

47%

sagen, dass fortgeschrittene Umgehungstechniken das Haupthindernis für eine schnelle Incident Response sind

44%

sagen, dass das Fehlen einer automatisierten Incident Response die Erkennung, Eindämmung und Beseitigung von Bedrohungen verzögert

217.068 USD

sind die durchschnittlichen Kosten für die Reaktion auf und die Wiederherstellung nach einer E-Mail-Sicherheitsverletzung

Die meisten Unternehmen erleben eine E-Mail-Sicherheitsverletzung

Die Umfrage ergab, dass 78 % der Befragten in den letzten 12 Monaten eine E-Mail-Sicherheitsverletzung erlebt hatten.

Opfer waren von einer Vielzahl von Angriffsarten betroffen, darunter Phishing und Spear Phishing (bei 27 % der Opfer), Kompromittierung geschäftlicher E-Mails (bei 24 %) und Account Takeover (bei 22 %).

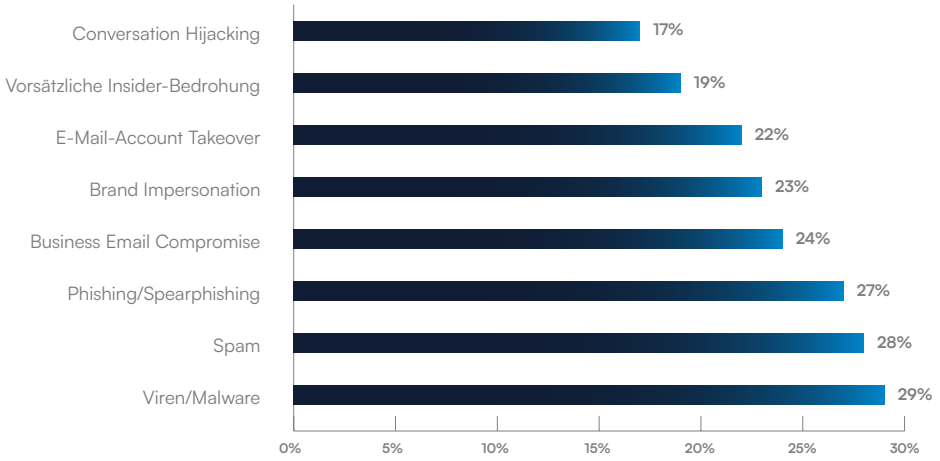


ABBILDUNG 1

Mit welcher der folgenden E-Mail-basierten Angriffsarten wurde Ihr Unternehmen in den letzten 12 Monaten erfolgreich angegriffen?

Die E-Mail-Bedrohungslandschaft wird noch dadurch komplizierter, dass viele Arten von E-Mail Angriffen miteinander verknüpft sind. Das Verständnis dieser Beziehungen ist der Schlüssel zum Aufbau einer wirksamen Verteidigung.

Phishing ist beispielsweise oft der erste Angriffspunkt und öffnet die Tür für Advanced Threats wie Business Email Compromise (BEC), Account Takeover und Ransomware. Sobald Zugangsdaten gestohlen werden, können sich Angreifer als interne Nutzer ausgeben, um ihre E-Mails vertrauenswürdiger erscheinen zu lassen und die Wahrscheinlichkeit einer weiteren Kompromittierung zu erhöhen. Spoofing-Techniken verbessern die Wirksamkeit von Phishing und BEC, indem sie vertrauenswürdige Absender nachahmen. In der Zwischenzeit kann malware, die durch Phishing eingeschleppt wird, den Angriffsprozess automatisieren, zusätzliche Zugangsdaten sammeln und sich über das Netzwerk verbreiten.

BEC ist eine gezielte und finanziell motivierte Bedrohung. Angreifer geben sich als vertrauenswürdige Personen oder Unternehmen aus, um Mitarbeiter dazu zu verleiten, Geld oder vertrauliche Informationen zu überweisen. Die Verbreitung von Malware und Ransomware wird durch Phishing-E-Mails mit bösartigen Anhängen oder Links erleichtert.

Identitätsmissbrauch und Spoofing sind Techniken, die verwendet werden, um Empfänger zu täuschen, damit sie dem Absender vertrauen. Diese Taktiken werden häufig in Phishing-, BEC- und Malware-Kampagnen eingesetzt. Angreifer können Anzeigenamen-Spoofing, Domain Spoofing oder ähnlich aussehende Domains verwenden, um legitime Kontakte zu imitieren, wodurch die Wahrscheinlichkeit erhöht wird, dass ihre Nachricht geöffnet und darauf reagiert wird.

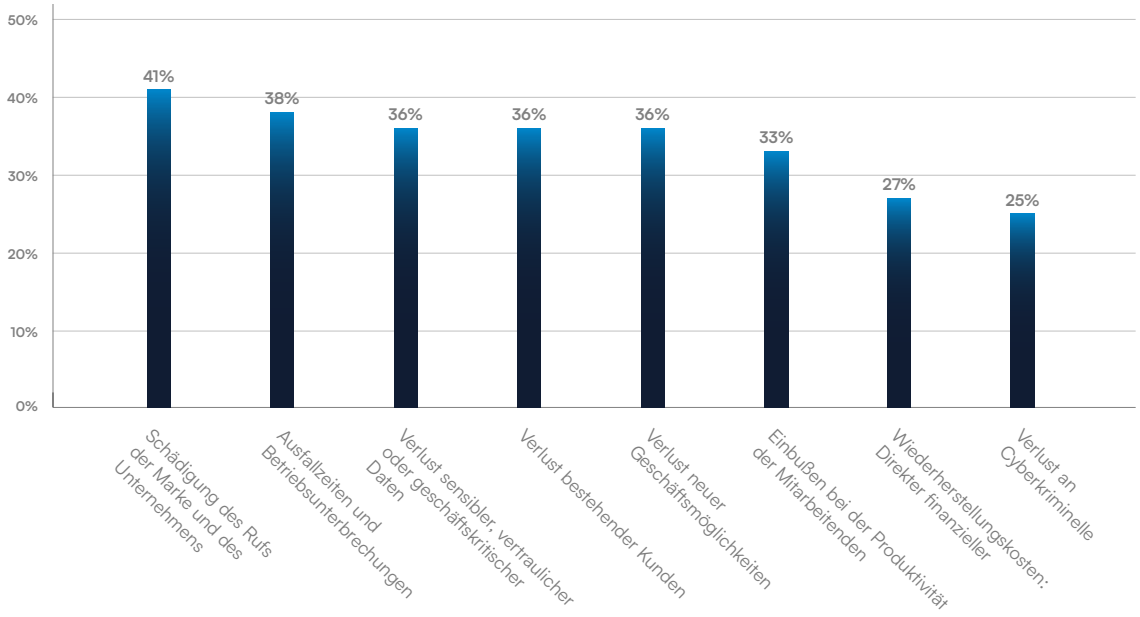
Alle Arten von E-Mail-Bedrohungen werden immer komplexer, raffinierter und weitreichender. Viele der am weitesten verbreiteten Phishing-Kampagnen werden von gut ausgestatteten Plattformen in großem Umfang entwickelt und durchgeführt. Der Schaden, den diese Angriffe anrichten können, ist beträchtlich.

Eine E-Mail-Sicherheitsverletzung schadet dem Unternehmenswachstum

Den befragten Unternehmen zufolge ist die häufigste Folge einer E-Mail-Sicherheitsverletzung eine Schädigung der Marke und des Rufs (von 41 % der Befragten genannt). An zweiter Stelle stehen die betrieblichen Auswirkungen, einschließlich Ausfallzeiten und Betriebsunterbrechungen (38 %), und die verringerte Produktivität der Mitarbeiter (36 %). Mehr als ein Drittel (36 %) verlor sensible Daten, und etwa ein Viertel verlor neue Geschäfte (27 %) und Kunden (25 %).

ABBILDUNG 2

Welche Auswirkungen hatten E-Mail-basierte Sicherheitsverletzungen auf Ihr Unternehmen (insgesamt)?



Die Folgen von Reputationsschäden können weit über die kurzfristige öffentliche Wahrnehmung hinausgehen und tiefgreifende, dauerhafte Auswirkungen auf die finanzielle Gesundheit, die Rechtslage und die strategische Ausrichtung eines Unternehmens haben.

Die Auswirkungen auf den Geschäftsbetrieb und die Produktivität sowie die finanziellen Verluste, der Datenverlust (insbesondere wenn dies zu Compliance- und Vertragsverletzungen führt), der Diebstahl geistigen Eigentums und der Vertrauensverlust können zum Verlust bestehender Kunden und neuer Geschäftsmöglichkeiten führen. Dies hat spürbare Auswirkungen auf das Umsatzwachstum.

Es mag schwierig sein, die längerfristigen Auswirkungen zu beziffern, aber es ist möglich, die Kosten für die Reaktion auf und die Behebung einer E-Mail-Sicherheitsverletzung zu beziffern.

Die Kosten für die Behebung einer E-Mail-Sicherheitsverletzung treffen kleinere Firmen härter

Die Behebung einer E-Mail-Sicherheitsverletzung kostet im Durchschnitt 217.068 USD, wobei kleinere Unternehmen unverhältnismäßig stärker betroffen sind.

Befragt wurden Unternehmen mit 50 bis 2.000 Beschäftigten. Die durchschnittlichen Kosten für die Schadensbegrenzung bei Unternehmen mit 50 bis 100 Mitarbeitern betrugen 145.921 USD. Für Unternehmen mit 1.000 bis 2.000 Mitarbeitern betrugen die durchschnittlichen Kosten für die Schadensbegrenzung 364.132 USD.

Das bedeutet, dass die durchschnittlichen Wiederherstellungskosten pro Mitarbeiter bei den kleineren Unternehmen (50 bis 100 Mitarbeiter) 1.946 USD betragen, während die durchschnittlichen Wiederherstellungskosten pro Mitarbeiter bei den größeren Unternehmen (1.000 bis 2.000 Mitarbeiter) nur 243 USD betragen.

	50-100 Mitarbeite	101-250 Mitarbeite	251-500 Mitarbeite	501-1,000 Mitarbeite	1,001-2,000 Mitarbeite
Durchschnittliche Kosten pro Unternehmen zur Eindämmung der teuersten E-Mail-Sicherheitsverletzung der letzten 12 Monate	145.921 USD	157.804 USD	155.804 USD	300.751 USD	364.132 USD
Durchschnittliche Kosten pro Mitarbeiter zur Minderung der teuersten E-Mail-Sicherheitsverletzung der letzten 12 Monate	1.946 USD	898 USD	415 USD	400 USD	243 USD

Größere Unternehmen verfügen möglicherweise über bessere Abwehrmechanismen und mehr Ressourcen in Form von Fähigkeiten und Personal, um Security-Vorfälle zu erkennen und darauf zu reagieren. Dadurch sind sie besser in der Lage, Sicherheitsverletzungen schnell und effektiv zu bearbeiten und stellen sicher, dass jeder Vorfall im Vergleich zu ihrer Gesamtgröße weniger kostspielig ist. Kleinere Unternehmen sind weitaus stärker exponiert.

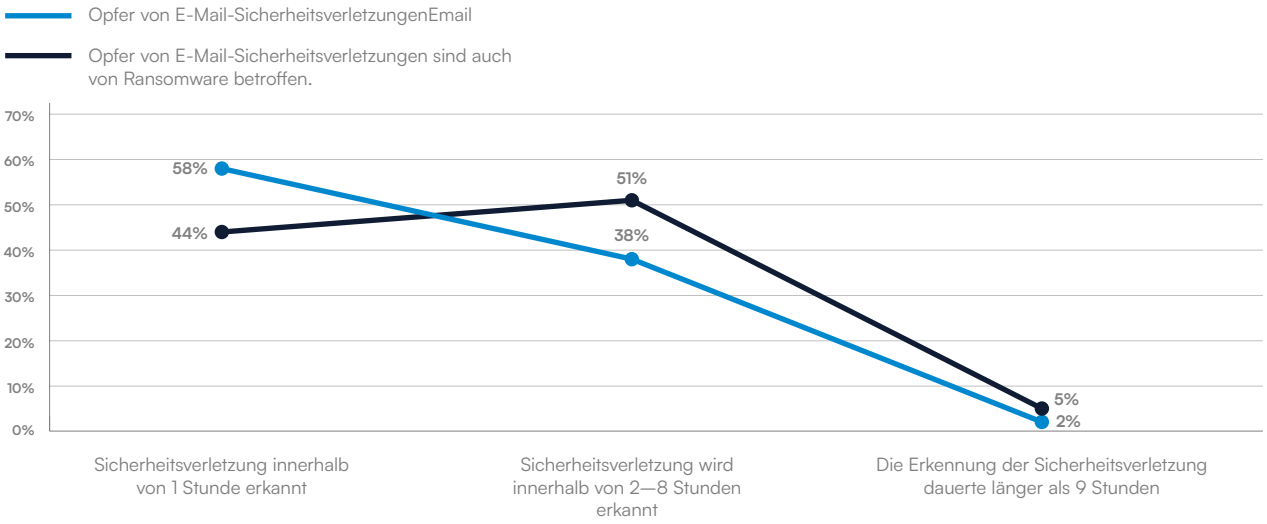
Die Fähigkeit, Security-Bedrohungen schnell zu erkennen und darauf zu reagieren, ist für die Risikominderung von entscheidender Bedeutung.

Verzögerungen in E-Mail Verletzungserkennung und Reaktionszeiten machen Ransomware wahrscheinlicher

Es besteht ein Zusammenhang zwischen der Zeit, die ein Unternehmen benötigt, um eine E-Mail-Sicherheitsverletzung zu erkennen und zu beheben, und der Wahrscheinlichkeit, ebenfalls von einem erfolgreichen Ransomware-Vorfall getroffen zu werden.

ABBILDUNG 3

Durchschnittliche Zeit bis zur Erkennung einer E-Mail-Sicherheitsverletzungan



Die Untersuchung zeigt, dass 71 % der Unternehmen, die eine E-Mail-Sicherheitsverletzung erlebt haben, berichten, dass sie in den letzten 12 Monaten auch von Ransomware betroffen waren.

Dies könnte daran liegen, dass viele Ransomware-Angriffe mit einer scheinbar harmlosen Phishing-E-Mail beginnen, die Angreifern einen Einstiegspunkt verschafft — durch gestohlene Zugangsdaten oder einen kompromittierten Endpunkt — und einen Kanal zur Übermittlung von Ransomware und anderen bösartigen Nutzlasten über Anhänge und Links bietet.

Wenn eine E-Mail-Sicherheitsverletzung nicht schnell und effektiv erkannt und eingedämmt wird, hat die Angriffskette Zeit, sich zu entfalten, und die Angreifer können Daten stehlen, Dateien verschlüsseln oder einen dauerhaften Zugriff auf das Netzwerk einrichten.

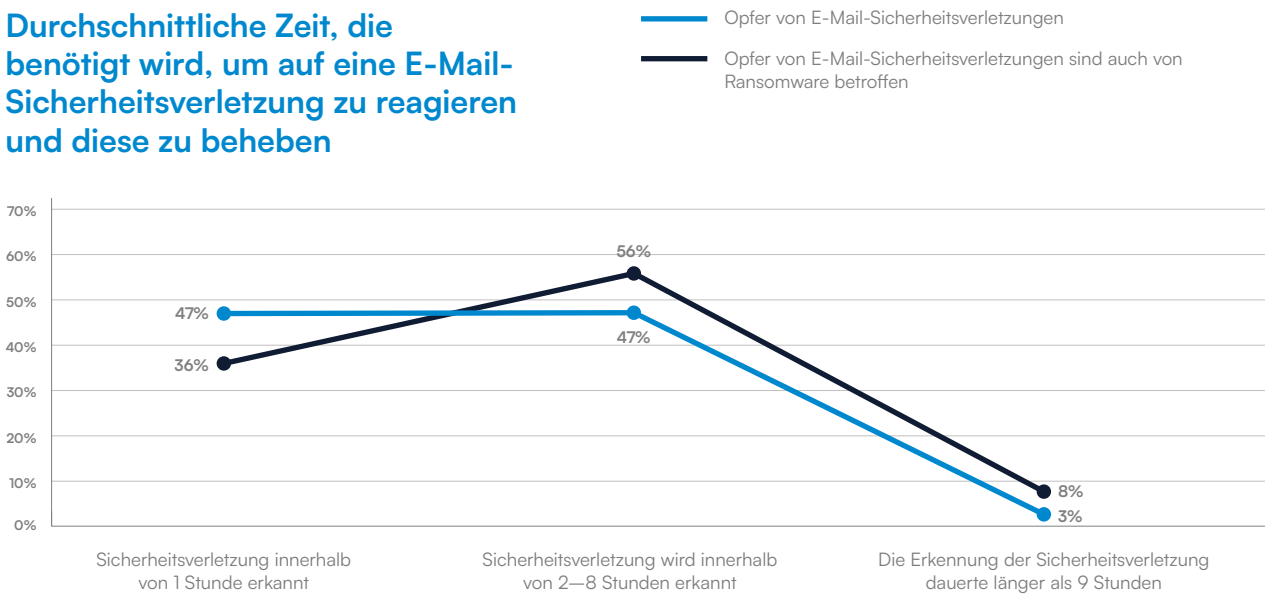
Die Ergebnisse zeigen, dass Unternehmen, die länger brauchten, um einen E-Mail-Verstoß zu erkennen und zu beheben, mit höherer Wahrscheinlichkeit auch von Ransomware betroffen waren:

- 58 % der Opfer von E-Mail-Angriffen, die nicht von Ransomware betroffen waren, brauchten weniger als eine Stunde, um den Angriff zu erkennen.
- Knapp die Hälfte (47 %) von ihnen hat die Bedrohung innerhalb einer Stunde nach ihrer Entdeckung abgewehrt.

- Für jene Opfer, die auch einen Ransomware-Vorfall erlebten, dauerten Erkennung und Eindämmung jedoch oft länger: 51 % benötigten zwischen zwei Stunden und einem ganzen Arbeitstag, um die Sicherheitslücke zu erkennen, und 56 % benötigten nach der Erkennung zwei bis acht Stunden, um die Bedrohung zu beheben.
- Kurz gesagt: 64 % der Ransomware-Opfer benötigen mehr als zwei Stunden, um eine E-Mail-Sicherheitsverletzung zu beheben.

ABBILDUNG 4

Durchschnittliche Zeit, die benötigt wird, um auf eine E-Mail-Sicherheitsverletzung zu reagieren und diese zu beheben



Diese Ergebnisse unterstreichen, wie wichtig effektive E-Mail-Sicherheit, Reaktions- und Abwehrfähigkeiten in umfassenderen Cyberabwehrstrategien sind.

Die Reaktion auf Sicherheitsverletzungen wird durch die Komplexität der Angriffe, menschliche Faktoren und mangelnde Automatisierung erschwert.

Es ist nicht immer einfach, schnell und effektiv auf eine E-Mail-Sicherheitsverletzung zu reagieren, und die Umfrage zeigt die Hindernisse auf, die dabei im Weg stehen können. Diese lassen sich grob in drei Bereiche einteilen: Angriffskomplexität, menschliche Faktoren und Security-Tools.

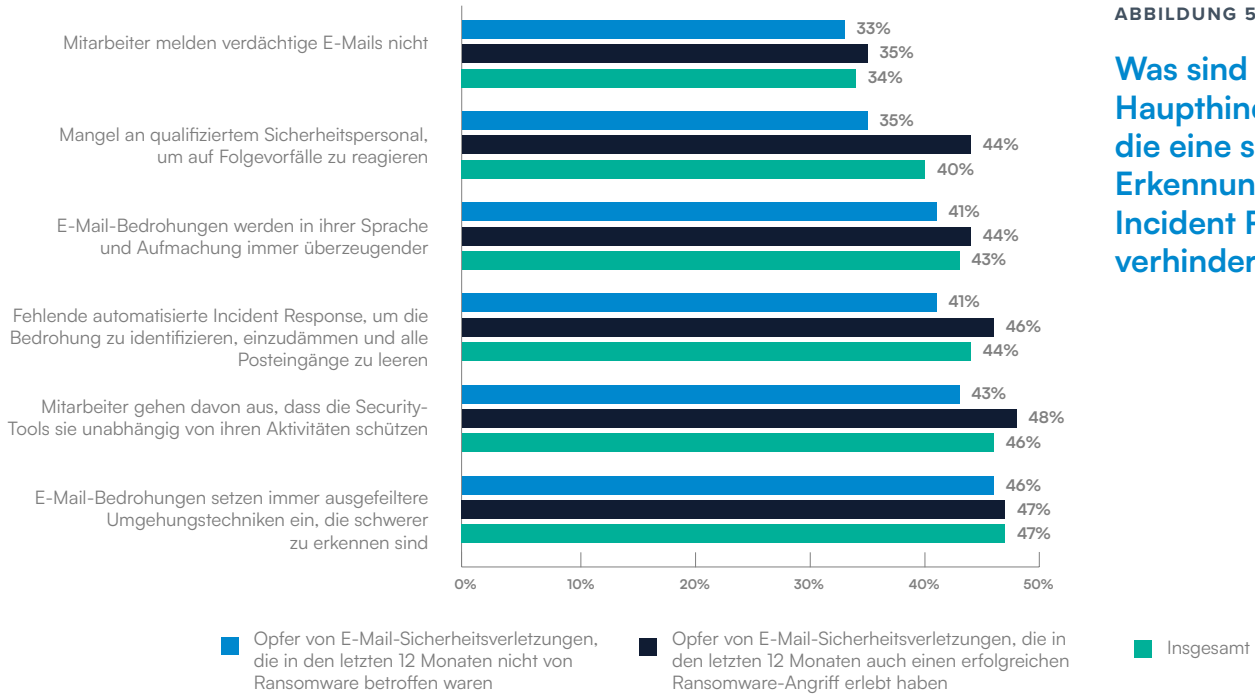


ABBILDUNG 5

Was sind die Haupthindernisse, die eine schnelle Erkennung und Incident Response verhindern?

Die am häufigsten genannten Hindernisse zeichnen ein klares Bild von der zunehmenden Komplexität von E-Mail-Bedrohungen und den internen Herausforderungen, mit denen Unternehmen konfrontiert sind, wenn die Angreifer einmal durchgebrochen sind.

Angriffsraffinesse

- Das größte Hindernis für eine schnelle Incident Response ist laut 47 % der E-Mail-Sicherheitsopfer die sich weiterentwickelnde und zunehmend schwer zu erkennende Natur von E-Mail-Bedrohungen, die es schwieriger macht, sie zu erkennen und aus den Posteingängen zu entfernen, sobald sie sich erfolgreich Zugang verschafft haben.
- Erschwerend kommt hinzu, dass die Phishing-E-Mails selbst immer raffinierter werden. Angreifer verfassen sprachlich ausgefeilte, kontextuell relevante und visuell überzeugende Nachrichten, die oft die interne Kommunikation oder vertrauenswürdige Marken imitieren. Laut 43 % der Befragten wird es dadurch sowohl für Nutzer als auch für Security-Tools schwieriger, bösartige E-Mails von legitimen zu unterscheiden.

Der menschliche Faktor

- Die Ergebnisse deuten auf ein gewisses Maß an Selbstgefälligkeit unter den Mitarbeitern hin, wobei 46 % der Befragten angeben, dass Kollegen davon ausgehen, dass Security-Tools sie schützen, egal was passiert.
- Rund ein Drittel (34 %) gibt an, dass Mitarbeiter verdächtige E-Mails nicht melden. Dies kann auch dazu führen, dass Bedrohungen im Posteingang verbleiben und ein Zeichen dafür sein, dass die Mitarbeiter nicht wissen, an wen sie verdächtige E-Mails melden sollen.
- Beide Faktoren können durch Schulung zur Stärkung des Risikobewusstseins, Anreize, Feedback, einfache Meldemechanismen und die Förderung einer Kultur des proaktiven Cybersecurity-Bewusstseins angegangen werden.

Security-Tools

- Für 44 % der Befragten stellt das Fehlen automatisierter Incident Response ein erhebliches Hindernis dar. Ohne automatisierte Tools, die Bedrohungen in den Posteingängen der Nutzer schnell identifizieren, isolieren und beseitigen können, sind die Security-Teams zu manuellen Prozessen gezwungen, die langsam und fehleranfällig sind. Diese Verzögerung gibt Angreifern mehr Zeit, die Sicherheitslücke auszunutzen, ihre Berechtigungen zu erweitern oder sich seitlich im Netzwerk zu bewegen.

Mangelnde Kompetenz

- Ein Mangel an qualifiziertem Security-Personal ist für 40 % der Befragten eine Herausforderung.
- In diesem Bereich ist die Kluft zwischen Unternehmen, die ebenfalls von einem erfolgreichen Ransomware-Angriff betroffen waren, und solchen, die nicht betroffen waren, am größten: 44 % der Unternehmen, die Opfer beider Arten von Angriffen wurden, gaben an, dass dies ein Hindernis darstellt, verglichen mit 35 % der Unternehmen, die nicht von Ransomware betroffen waren. Wenn Unternehmen nicht über das Fachwissen oder die Kapazität verfügen, um effektiv auf eine erkannte Sicherheitsverletzung zu reagieren, kann dies zu einer verzögerten Eindämmung oder unvollständigen Behebung führen, sodass Angreifer im Netzwerk bleiben und ihre Angriffe fortsetzen können.

Fazit

Die große Bandbreite an E-Mail-Bedrohungen, die auf Unternehmen abzielen, die spürbaren Auswirkungen, die erheblichen Kosten und die zunehmende Komplexität der Cyberbedrohungslandschaft unterstreichen, wie wichtig es ist, die E-Mail-Sicherheit zu einem integralen Bestandteil plattformbasierter Cyberabwehrstrategien zu machen.

Ein ganzheitlicher Ansatz zur E-Mail-Sicherheit sollte fortschrittliche, KI-gestützte Erkennungstechnologien mit Nutzerschulung, automatisierter Reaktion und einer starken Security-Kultur kombinieren.

Die folgenden Empfehlungen können hilfreich sein:

Unterstützung von Mitarbeitern

1. **Schulen Sie Mitarbeiter regelmäßig** darin, Phishing, Social Engineering und verdächtiges E-Mail-Verhalten zu erkennen.
2. **Machen Sie es den Mitarbeitern leicht, verdächtige E-Mails zu melden, u**nd stellen Sie sicher, dass die Berichte zur Untersuchung und schnellen Prüfung an das richtige Team weitergeleitet werden.
3. **Beschränken Sie den Zugriff auf vertrauliche Systeme und Daten** basierend auf den jeweiligen Aufgabenbereichen. So minimieren Sie die Auswirkungen von Anmeldedatendiebstahl und lateraler Bewegung nach einem E-Mail-Angriff.

Security-Tools

4. **Implementieren Sie die Multi-Faktor-Authentifizierung (MFA)** für E-Mail und andere kritische Systeme. Selbst wenn Zugangsdaten durch Phishing gestohlen werden, fügt MFA eine starke Verteidigungsebene gegen unbefugten Zugriff hinzu.
5. **Setzen Sie E-Mail-Sicherheitslösungen ein, die KI/ML verwenden,** um Phishing, Malware und Identitätsmissbrauch zu erkennen. Diese Tools sollten in der Lage sein, das Absenderverhalten, den Nachrichteninhalt und Anhänge in Echtzeit zu analysieren.
6. **Implementieren Sie branchenübliche E-Mail-Authentifizierungsprotokolle** wie SPF, DKIM und DMARC , um die Identität des Absenders zu überprüfen und Spoofing zu verhindern. Diese Protokolle helfen sicherzustellen, dass nur autorisierte Absender Ihre Domain verwenden können.
7. **Automatisieren Sie die Incident Response** mit Tools, die bösartige E-Mails nach der Zustellung automatisch identifizieren und unter Quarantäne stellen, sie aus Posteingängen entfernen und Eindämmungs-Workflows einleiten können. Dies reduziert die Verweildauer von Angreifern und begrenzt die Gefährdung.

Längerfristige Maßnahmen

8. **Nutzen Sie Threat Intelligence-Feeds,** um über neue E-Mail-Bedrohungen, bösartige Domains und Angreifer-Taktiken auf dem Laufenden zu bleiben. Integrieren Sie diese Daten in Ihre umfassenderen Erkennungssysteme und Ihre Security-Plattform.
9. **Führen Sie regelmäßige Überprüfungen** der E-Mail-Sicherheitskonfigurationen durch und simulieren Sie Angriffsszenarien (z. B. Phishing, BEC), um Ihre Erkennungs- und Reaktionsfähigkeiten zu testen.
10. **Verstehen und erfüllen Sie regulatorische Anforderungen,** indem Sie sicherstellen, dass Sie die entsprechenden E-Mail-Sicherheitsmaßnahmen für eine robuste Erkennung, Reaktion und Data Protection haben. Dies wird auch bei den Anforderungen der Cyberversicherung helfen.

In der heutigen dynamischen und vernetzten Bedrohungslandschaft geht es bei der E-Mail-Sicherheit nicht nur darum, Spam oder Phishing zu stoppen — es geht darum, zu verhindern, dass der erste Dominostein einer Kette fällt, die zu Betriebsstörungen, **Datenverlust, Rufschädigung und längerfristigen Auswirkungen auf das Geschäft führen könnte.**

Über Barracuda

Barracuda ist ein weltweit führendes Cybersecurity-Unternehmen, das umfassenden Schutz vor komplexen Bedrohungen für Unternehmen aller Größen bietet. Unsere KI-gestützte Plattform BarracudaONE schützt E-Mails, Daten, Anwendungen und Netzwerke mit innovativen Lösungen, einem Managed XDR-Service sowie einem zentralen Dashboard. Das sorgt für maximalen Schutz und stärkt die Cyber-Resilienz. Von Hunderttausenden von IT-Experten und Managed Service Providern weltweit als vertrauenswürdig angesehen, bietet Barracuda leistungsstarke Abwehrmaßnahmen, die einfach zu kaufen, bereitzustellen und zu verwenden sind.

Informationen 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.