mimecast

Behind the SCREENS:

Die sich entwickelnde Wahrnehmung von Cyber-Risiken durch den Vorstand

TEIL I

Cybersicherheit hält Einzug in die Vorstandsetage - und damit auch die wirtschaftliche Volatilität

Die moderne Arbeitsumgebung ist durch Vernetzung gekennzeichnet: Hybride Arbeitsmodelle haben die Arbeitsweise von Unternehmen verändert und die Art und Weise, wie Menschen kommunizieren, Daten austauschen und zusammenarbeiten. Teams können dank E-Mail und neuerdings auch Collaboration-Tools wie Microsoft Teams und Slack praktisch von überall aus arbeiten.

CISOs und andere Sicherheitsverantwortliche schlugen Alarm wegen des erhöhten Cyber-Risikos, das durch die moderne Arbeitsoberfläche entsteht, und dank der bekannt gewordenen Cyber-Angriffe, die sowohl an Umfang als auch an Raffinesse zunehmen, haben die Führungsetage und der Vorstand davon Kenntnis genommen.

Während E-Mail nach wie vor der wichtigste Angriffsvektor für Bedrohungsakteure ist, haben Collaboration-Tools eine neue Angriffsfläche für Cyberkriminelle geschaffen, die ein noch größeres Risiko für die Sicherheitsverantwortlichen darstellt. Es wird daher immer wichtiger, den Schutz der Unternehmenskommunikation zu gewährleisten, zumal das Volumen der E-Mail-bezogenen Bedrohungen in **82 %** der Unternehmen in den letzten **12 Monaten** zugenommen hat[1]. Ein weit verbreiteter Irrglaube vieler Unternehmensleiter ist, dass die Verwendung anerkannter, wenn auch uneinheitlicher Sicherheitslösungen ausreicht, um die Sicherheit der Unternehmenskommunikation zu gewährleisten.

Das Risiko von mehrstufigen, vektoriellen Cyberangriffen wie Ransomware und Business Email Compromise (BEC) - zusammen mit den verheerenden Auswirkungen, die sie angesichts der drohenden wirtschaftlichen Volatilität auf den Umsatz und den Ruf eines Unternehmens haben können - ist jedoch nur einen Klick entfernt.

Cybersicherheit - und der Gedanke, dass Cyberrisiken auch Geschäftsrisiken sind - muss das Verhalten der Mitarbeiter durchdringen. Cybersicherheit liegt in der Verantwortung aller, und CISOs müssen diese Botschaft an den Vorstand weitergeben, damit dieser sie erkennt und darauf reagiert.

Um mehr über die derzeitige Wahrnehmung von Cyber-Risiken durch die Führungsebene und den Vorstand zu erfahren, haben wir mit **78 Führungskräften aus 13 Ländern gesprochen**, um ihre Bemühungen, Risiken zu artikulieren, zu vertiefen und herauszufinden, was Führungskräfte tun müssen, um geschützt zu arbeiten, auch wenn sich Cyber-Angriffe häufen.

E-Mail-bezogene Bedrohungen haben in **82 %** der Unternehmen in den letzten 12 Monaten zugenommen

[1] Mimecast *State of Email Security* 2023

TEIL II

Cyber-Risiko ist Geschäftsrisiko

Sorgen Sie dafür, dass die Cybersicherheit - und die Verbindung zwischen Cyberrisiken und Geschäftsrisiken - in der Kommunikation auf Vorstandsebene im Vordergrund steht.

Auch wenn es manchmal den Anschein hat, dass die Cybersicherheit im luftleeren Raum stattfindet, kann der breitere Unternehmenskontext, in dem sie stattfindet, Schockwellen auslösen. So wird beispielsweise prognostiziert, dass Cyberrisiken mittel- und langfristig weiter zunehmen werden, wie aus Berichten des World Economic Forum's (WEF's) Jahrestagung in Davos. Tatsächlich ist 2023 das erste Jahr, in dem Cyberrisiken in die Top-10-Liste der langfristigen Probleme im jährlichen WEF-Bericht über globale Risiken aufgenommen werden. Die neue Bewertung deutet auf die Langlebigkeit der aktuellen Welle von Cyberangriffen hin.[2] "Die weit verbreitete Cyberkriminalität und -unsicherheit" wird auf der Liste der nach Schweregrad geordneten Risiken auf Platz 8 geführt, hinter globalen Problemen im Zusammenhang mit dem Klimawandel, Naturkatastrophen und unfreiwilliger Migration - aber noch vor geoökonomischen Auseinandersetzungen und Umweltschäden. Es ist vielversprechend, dass einige Vorstände jetzt regelmäßig die Risiken diskutieren, die sich aus der zunehmenden Cyberkriminalität ergeben.

"Ich glaube, dass wir anderen Banken voraus sind, weil eine Reihe von Vorstandsmitgliedern über umfassende Kenntnisse im Bereich Cybersicherheit verfügen. Der größte Vorteil dabei ist, dass diese speziellen Vorstandsmitglieder andere Vorstandsmitglieder in Fragen der Cybersicherheit schulen können."

CTO für IT und Infrastruktur, Finanzdienstleistungen, über 1.000 Mitarbeiter, Vereinigte Arabische Emirate

Diese makroökonomischen Herausforderungen werden von Tag zu Tag größer und bringen eine Vielzahl neuer Überlegungen für die einzelnen Unternehmen mit sich. |

"Ich habe den Eindruck, dass der Vorstand das Cyber-Risiko als ein weiteres Geschäftsrisiko betrachtet, das jedoch potenziell größere Auswirkungen hat. Die Hauptschwierigkeit besteht meines Erachtens darin, dass es sehr schwierig ist, das Cyber-Risiko zu quantifizieren, ohne dass ein signifikanter Verstoß stattgefunden hat, und dass sich alles schlagartig ändert, wenn es einen solchen Verstoß gibt."

CIO, in der Beratungsbranche mit über 1.500 Mitarbeitern, AUS/APAC

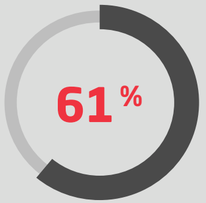
Eine Überlegung ist zum Beispiel, dass viele CISOs erkennen, dass es in ihren Gremien eine Wissenslücke gibt, die CISOs in einen Nachteil bringt, wenn sie den ROI von Cybersicherheitsinitiativen nachweisen müssen.[3] Eine weitere wichtige Überlegung ist, dass angesichts der wirtschaftlichen Unbeständigkeit, wenn die meisten Unternehmen weltweit den Gürtel in allen Geschäftsbereichen, einschließlich Marketing, Vertrieb und allgemeiner Technologie, enger schnallen, dies zu einem noch größeren Cyber-Risiko durch Schatten-IT oder Outsourcing an nicht vertrauenswürdige Dritte führen kann. Cyber-Risiken sind nicht nur ein IT-Problem - sie sind eine kritische Schwachstelle, die sich direkt auf das gesamte Geschäftsrisiko auswirkt. Angesichts rekordverdächtiger Inflationsraten, immer komplexerer Cyberangriffe und geopolitischer Spannungen können sich Unternehmen einfach keine schwache Sicherheitsarchitektur leisten, die sie anfällig für Datenschutzverletzungen macht und die Stabilität ihres Unternehmens gefährdet.

2. Global Risks Report 2023, World Economic Forum
3. Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy, *Wall Street Journal*

TEIL II

Trotz der drohenden Rezession und der Wissenslücke im Bereich der Cybersicherheit auf Vorstandsebene sind die meisten Sicherheitsverantwortlichen in dieser Umfrage der Meinung, dass sie eine Budgeterhöhung von **10 bis 20 %** benötigen, und sie halten es für wahrscheinlich, dass sie diese auch bekommen werden. In der Tat ist es unwahrscheinlich, dass in häufig angegriffenen Sektoren wie kritischen Infrastrukturen oder Finanzen die Ausgaben für Cybersicherheit gekürzt werden.[4] Um diese Chancen zu verbessern, müssen die Verantwortlichen für Cybersicherheit die Risiken und die entscheidende Rolle, die Cybersicherheit für den Schutz des Unternehmens spielt, klar kommunizieren; außerdem sollten sie mit einer genaueren Prüfung ihrer Ausgaben rechnen. Die Kosten einer Sicherheitsverletzung überwiegen alle Sparmaßnahmen, die der Vorstand ergreifen möchte. Während sich technologische Ausfallzeiten, die mit Umsatzeinbußen gleichzusetzen sind, beziffern lassen, ist der Imageschaden für Marken, die Opfer eines Cyberangriffs geworden sind, nicht leicht zu messen, darf aber nicht unterschätzt werden; der Verlust des Kundenvertrauens, das über Jahre hinweg aufgebaut werden muss, kann verheerend sein.

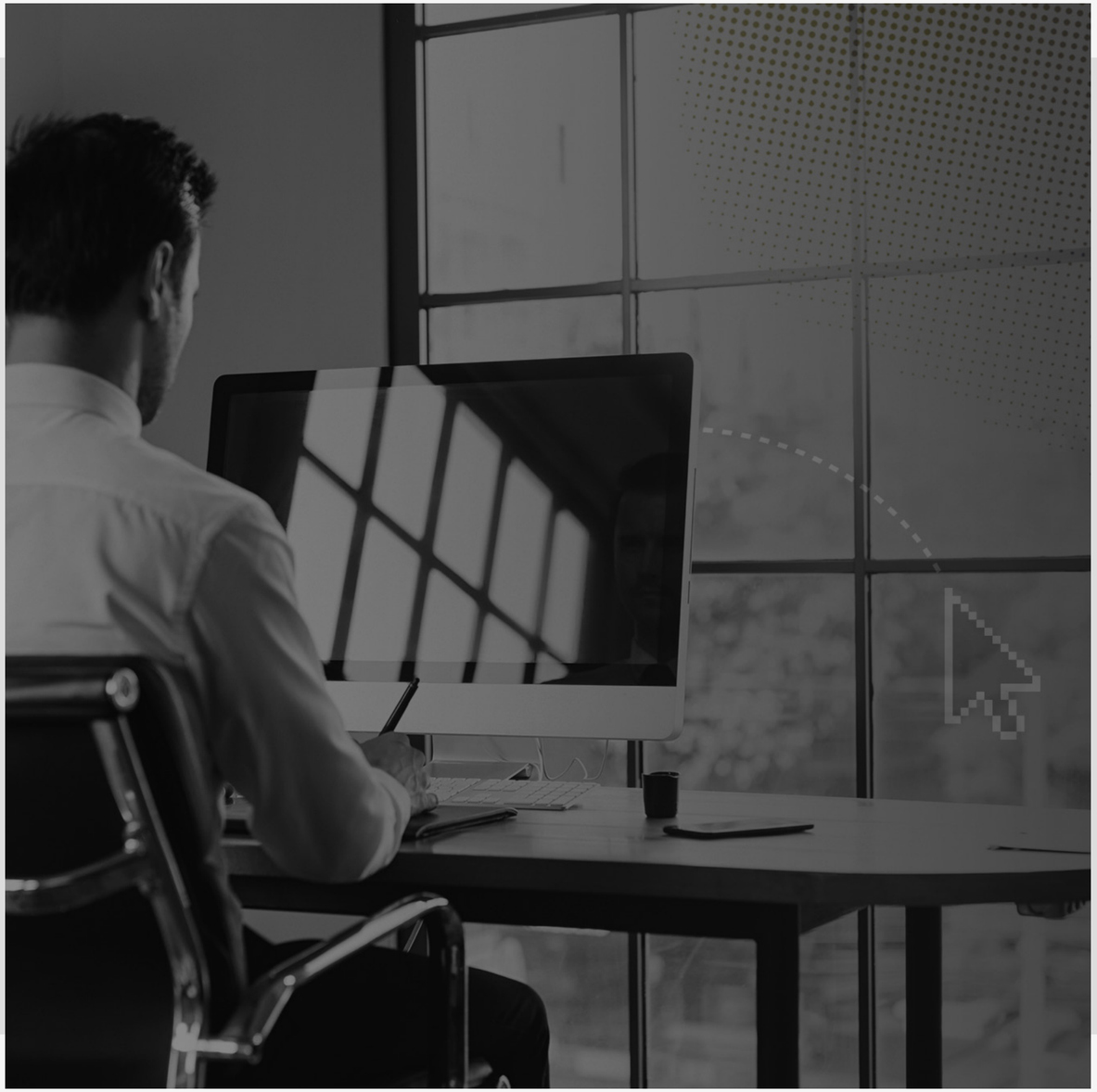
Mimecast's Brand Trust Bericht über das Markenvertrauen zeigt, dass **61 %** der Verbraucher das Vertrauen in ihre Lieblingsmarke verlieren würden, wenn diese Marke persönliche Informationen an eine gefälschte Version ihrer Website weitergeben würde. Der Vertrauensverlust spiegelt sich direkt in Umsatzeinbußen wider, da mehr als die Hälfte (**57 %**) der Befragten kein Geld mehr für ihre Lieblingsmarke ausgeben würden, wenn sie Opfer einer Phishing-Attacke würden.



der Verbraucher würden das Vertrauen in ihre Lieblingsmarke verlieren, wenn diese Marke persönliche Informationen an eine gefälschte Version ihrer Website preisgeben würde

mehr als die Hälfte der Befragten würde kein Geld mehr für ihre Lieblingsmarke ausgeben, wenn sie Opfer eines Phishing-Angriffs geworden wären

[4] Cyber Chiefs Face Scrutiny and Challenges in 2023's Uncertain Economy, *Wall Street Journal*



"Manchmal verstehen sie die Kosten einer bestimmten Art von Angriffen nicht. Dann muss ich mein betriebswirtschaftliches Gehirn einschalten (und mein technisches und sicherheitstechnisches Know-how beiseite lassen) und versuchen, ihnen zu vermitteln, wie hoch der Verlust ist und ob wir potenziell bedroht sind."

CTO, Unterhaltungsindustrie, weniger als 500 Mitarbeiter, Singapur

Hinzu kommt, dass die Bedrohungen durch Cyberkriminelle immer ausgefeilter und hartnäckiger werden, während ein kleinerer Talentpool die Arbeitgeber dazu zwingt, mehr von Cybersecurity-Analysten und -Ingenieuren zu verlangen. Im Durchschnitt dauert es 21 % länger, eine Stelle im Bereich Cybersicherheit zu besetzen als in anderen IT-Bereichen, und jährlich fehlen Zehntausende von Stellen im Bereich Cybersicherheit, die besetzt werden müssen.[5] Diese wachsenden Anforderungen führen zu mehr Stress, Burnout und Kündigungen.

Die versiertesten Vorstandsmitglieder wissen, dass es bei Investitionen in die Cybersicherheit nicht nur darum geht, das Risiko eines Cyberangriffs zu mindern. Durch die Aufrechterhaltung von Investitionen in die Cybersicherheit können Unternehmen den Ruf ihrer Marke schützen, das Risiko von Geldbußen und Umsatzeinbußen im Falle eines erfolgreichen Angriffs verringern und den Stress, dem Mitarbeiter im Bereich Cybersicherheit ausgesetzt sind, auf ein Minimum reduzieren. Kurz gesagt: Investitionen in die Cybersicherheit sind gleichbedeutend mit einem guten Geschäft.

"...es kann eine Herausforderung sein, talentierte Cyber-Experten zu halten. Die Cyber-Ressourcen sind begrenzt, und wir müssen einen Weg finden, um die Leute, die wir eingestellt oder ausgebildet haben, für die Zukunft zu halten. Wir haben derzeit einen Fachkräftemangel von etwa 30 %, was ein Problem darstellt - und in dieser Branche findet man keine guten Ressourcen zu einem vernünftigen Preis. Das Budget für Cybersicherheit ist angemessen, aber weil es so viele ungeschulte Leute gibt, ist es für uns schwierig, Mitarbeiter einzustellen."

CFO in einem Unternehmen mit über 1.000 Mitarbeitern in der Finanzdienstleistungsbranche, Südafrika

[5] CyberSeek

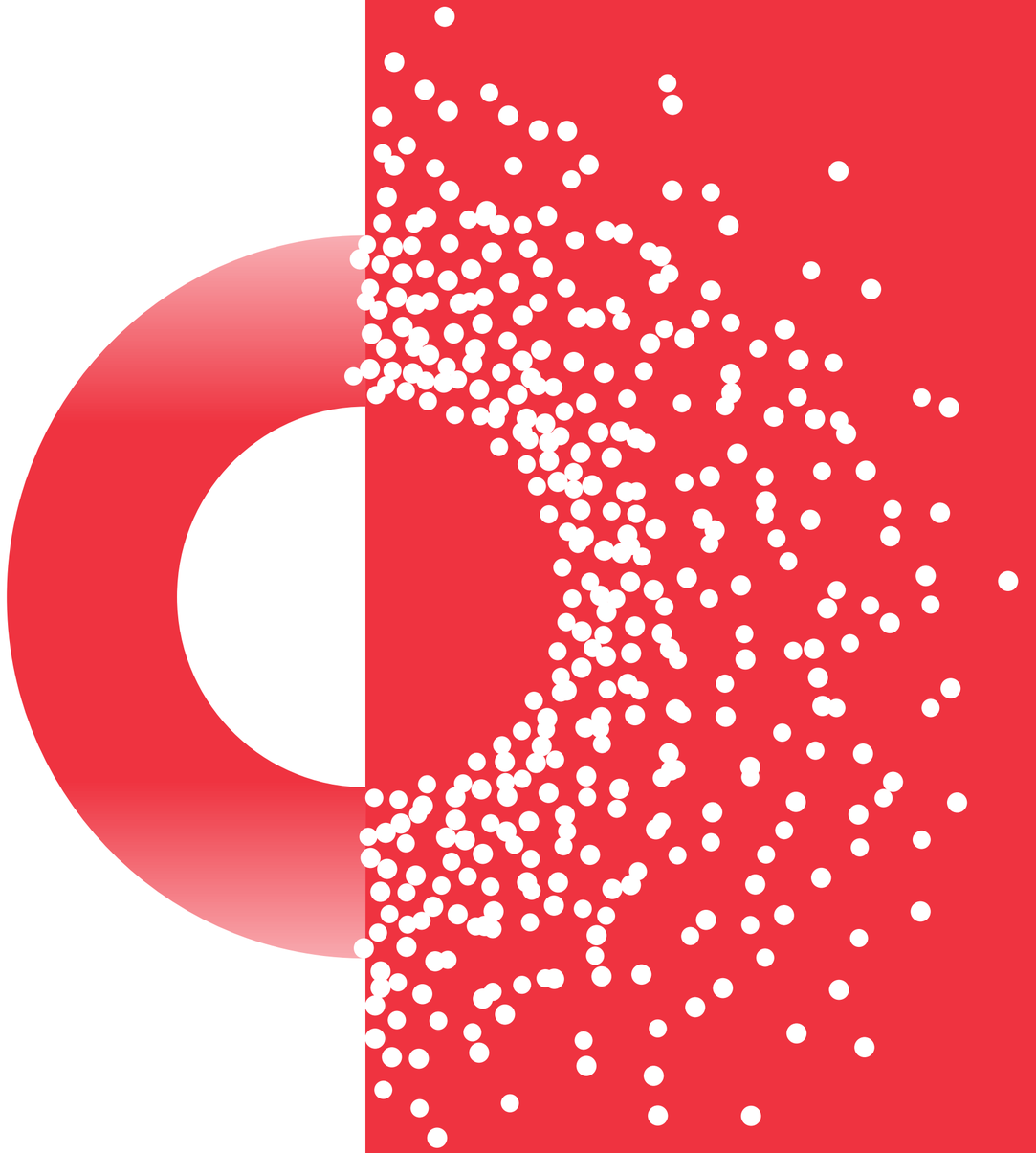
Um den Zusammenhang zwischen Cyber-Risiken und Geschäftsrisiken zu verdeutlichen, empfehlen die Befragten der Führungsebene:

1 Vermeiden Sie Fachjargon und entmystifizieren Sie das mittel- bis langfristige Risiko, das Cyber-Bedrohungen darstellen können.

2 Wenn Sie die Vorteile von Investitionen in Best-of-Breed-Lösungen kommunizieren, stellen Sie eine Verbindung zwischen Cyber-Bedrohungen und Geschäftsergebnissen her. Einige Führungskräfte empfehlen, sich nicht darauf zu konzentrieren, wie es zu einem Angriff gekommen ist, sondern sich stattdessen darauf zu konzentrieren, warum es dazu gekommen ist - zum Beispiel, weil man sich stark auf einen monolithischen Sicherheitsanbieter verlassen hat.

3 Entwickeln Sie Mechanismen, die es Ihnen ermöglichen, das Cyber-Risiko mit dem allgemeinen Geschäftsrisiko in Einklang zu bringen, um eine integrierte Cybersicherheitsfunktion zu schaffen.

4 Vermeiden Sie es, aus jedem Vorfall eine Krise zu machen - gehen Sie taktisch vor, wenn Sie dem Vorstand das Cyber-Risiko schildern, damit er es genau quantifizieren kann, ohne dass ein Verstoß die Dringlichkeit erhöhen muss.



"Mein Rat an die CISOs ist, nicht aus allem eine Krise zu machen. Seien Sie vorsichtig mit dem, was Sie ansprechen, um zu vermeiden, dass es 'Lärm' wird. Halten Sie Ihr Pulver trocken für die großen Vorfälle, die Sie ansprechen wollen, und bringen Sie den Vorstand und die Führungskräfte dazu, den Wandel zu beeinflussen."

CISO, Technologiebranche mit mehr als 180.000 Mitarbeitern, Vereinigte Staaten

TEIL III

Wert und Wirksamkeit durch mehrschichtige Cybersecurity-Rahmenwerke

Implementieren Sie Tools, die die Bedürfnisse Ihres Unternehmens abdecken, und berücksichtigen Sie dabei auch die Größe, Komplexität und Branche Ihres Unternehmens.

Unternehmen agieren in einem komplexen, unbeständigen Umfeld und sind gleichzeitig immer raffinierteren Bedrohungen ausgesetzt. Als Reaktion auf diese Marktbedingungen sind CISOs gezwungen, Budgets und Cybersicherheitstechnologien durch die bekannte Linse "Mensch, Technologie und Prozess" zu überprüfen.

Mehr als **90 % der Cyberangriffe** erfolgen per E-Mail, was daran erinnert, dass die Risikotoleranz und das Risikomanagement regelmäßig überprüft werden sollten, indem der Auftrag des Unternehmens und die zu schützenden Ressourcen identifiziert werden und der Stand des Cybersecurity-Risikos regelmäßig an die Beteiligten kommuniziert wird. Vom CISO geleitete Tabletop-Übungen sind ein weiteres Instrument zur Verbesserung der Cybersicherheitslage und der Reaktionspläne auf Vorfälle und können, wenn sie richtig kommuniziert werden, den Mitarbeitern helfen, die Folgen einer schlechten Cyberhygiene besser zu verstehen.

Mehr als 90% der Cyberangriffe erfolgen durch E-Mail

Aus technologischer Sicht müssen CISOs nach kohärenteren, umfassenderen und automatisierten Möglichkeiten suchen, um Aktivitäten zu überwachen, vor Datenexfiltration zu schützen und schneller zu handeln, um die Auswirkungen von Angriffen zu begrenzen. Es reicht nicht mehr aus, nur in Sicherheitstools zu investieren - in der Tat haben viele Unternehmen im Laufe der Zeit aufgeblähte oder unzusammenhängende Sicherheitsumgebungen erlebt.

"Wir haben einen ausgefeilten Risikomanagement-Ansatz, der sich auf technologische Prozesse und Cyber-Kontrollrahmen konzentriert und das Team finanziell unterstützt, indem wir in Systeme, Infrastruktur und neue Technologien investieren, um sichere und stabile Plattformen zu schaffen, die alle aufkommenden Bedrohungen abwehren."

Analyst für IT- und Infrastruktur-Support (direkte Unterstellung unter den CISO, Teamleiter), AUS, 1001 <

TEIL III

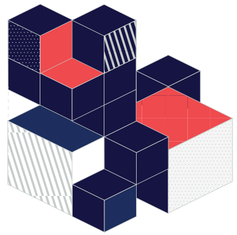
Stattdessen ist es von entscheidender Bedeutung, Platz für enge Integrationen und mehrschichtige Sicherheitsrahmen zu schaffen, um Daten im gesamten Unternehmen und während des gesamten Lebenszyklus zu schützen und gleichzeitig die Falle einer monolithischen Sicherheitsplattform mit hohem Angriffswert wie Microsoft 365 zu vermeiden. Die Anbieter von Sicherheitslösungen müssen den Anforderungen von Unternehmen gerecht werden, die mehr oder bessere Funktionen für die gleichen Kosten erwarten, was den Schwerpunkt auf Lösungen legt, die sich auf Integrationen konzentrieren, um Angriffe zu verhindern und deren Auswirkungen zu minimieren. Ein effektiver Weg, dies zu erreichen, ist die Maximierung der Partnerschaften, die Unternehmen mit bestehenden Anbietern haben, wie z. B. Technologie-API-Programme oder Allianzen; tatsächlich arbeiten **8 von 10** Unternehmen eher mit einem Cybersecurity-Anbieter mit einer offenen API-Plattform zusammen.[6]

"Die erste wäre, den Ansatz der Tiefenverteidigung zu diskutieren, von der höchsten Ebene bis zum unteren Ende der Organisationspyramide. Es ist auf jeder Ebene notwendig, die Cybersicherheit zu kennen. Und was unsere Organisation tut, um sich zu schützen."

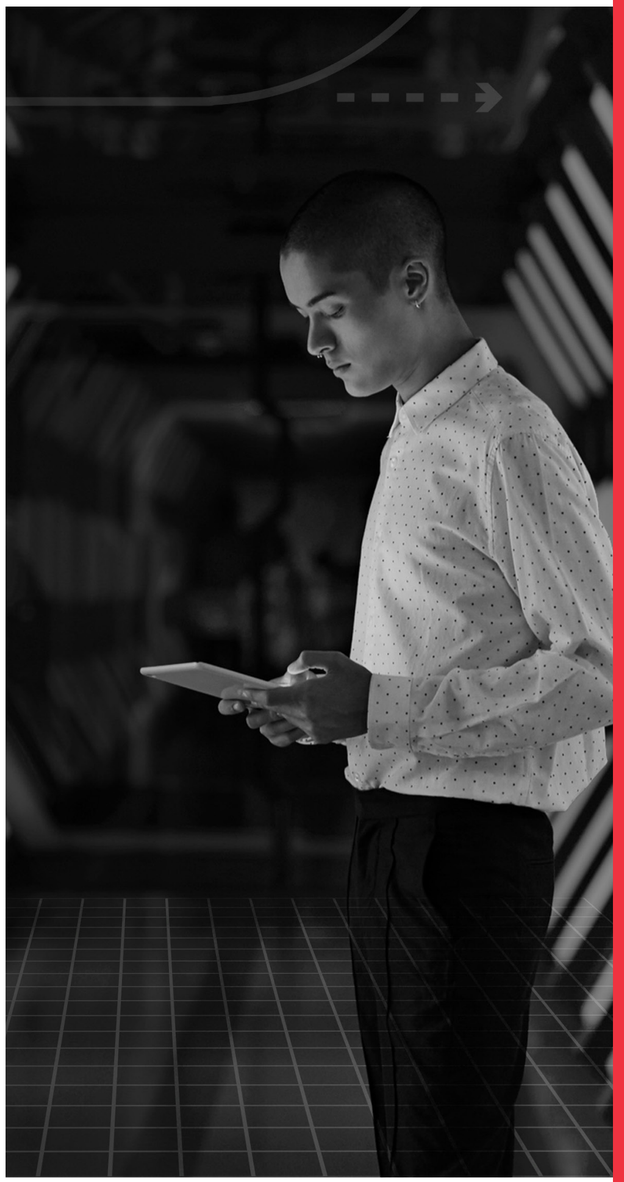
CTO, Singapur, Unterhaltungsbranche, <500 Mitarbeiter

Ziel ist es, ein Defense-in-Depth-Modell zu schaffen, das es Cybersecurity-Teams ermöglicht, Cyberbedrohungen schnell zu erkennen und zu beheben. Eine Sammlung der besten Sicherheitsprodukte, die Daten und analytische Erkenntnisse gemeinsam nutzen, bietet echte mehrschichtige Sicherheit, die SOC-Teams dabei hilft, Prävention, Erkennung, Untersuchung und Reaktion über Tools und Unternehmen hinweg zu verknüpfen. Diese Art von Modell ist eine willkommene Abwechslung zu den besten Lösungen einzelner Anbieter, die es Angreifern ermöglichen, unentdeckt in Sicherheitsumgebungen Fuß zu fassen.

Um diesen Ansatz zu unterstützen und Talente zu halten, indem die SOC-Müdigkeit verringert wird, investieren viele Unternehmen verstärkt in Automatisierungstools. Für die Implementierung und Verwaltung dieser vielschichtigen, automatisierten Tools werden jedoch weiterhin qualifizierte Mitarbeiter benötigt.



8 von **10** Unternehmen arbeiten eher mit einem Cybersicherheitsanbieter mit einer offenen API-Plattform zusammen.



"Als CIO muss ich sicherstellen, dass das Unternehmen über die modernsten Systeme und Technologien verfügt, die eine solide Grundlage für die Abwehr von Cyberangriffen bilden."

CIO, Finanzdienstleister, Deutschland 500- 1.000 Mitarbeiter

6. Mimecast *State of Email Security* 2023

Die Befragten der Führungsebene empfehlen, die Sicherheitsvorkehrungen durch mehrschichtige Cybersicherheitsrahmen zu verstärken:

1 Bestimmen Sie die wichtigsten Bedrohungen für das Unternehmen und erstellen Sie ein Risikoprofil des Unternehmens. E-Mail-basierte Angriffe wie Phishing und die Übernahme von Konten sind äußerst besorgniserregend. Daher ist es wichtig, eine Lösung zu wählen, die die Branche, die Komplexität der Sicherheitsumgebung und die rechtlichen Rahmenbedingungen berücksichtigt.

2 Maximieren Sie die Beziehungen zu den Anbietern, um ein möglichst schlankes Defense-in-Depth-Modell zu erstellen.

3 Sobald das Risikoprofil fertiggestellt ist, entwickeln Sie einen Rahmen für die Cybersicherheit, der alle wichtigen Aspekte berücksichtigt, und bauen Sie die Cybersicherheitsebenen auf, die zur Bekämpfung der ermittelten Bedrohungen erforderlich sind. Implementieren Sie wichtige Leistungsindikatoren, überwachen Sie das Rahmenwerk und passen Sie es unter Mitwirkung der Unternehmensleitung entsprechend an.

4 In komplexeren Umgebungen können Sicherheitsverantwortliche Datenverluste mit weniger Ressourcen verhindern, indem sie mehr Intelligenz über Technologien des maschinellen Lernens und herkömmliche Analysen einsetzen; sie können auch mehr Automatisierung anwenden, einschließlich der Auslagerung sich wiederholende manuelle Aufgaben, die die Mitarbeiter im Bereich Cybersicherheit auslaugen und den Fachkräftemangel verschärfen können.

"In den Vorstandssitzungen legen wir Wert auf die Entwicklung einer starken IT-Infrastruktur und auf Mitarbeiter mit guten Kenntnissen im Bereich Cybersicherheit. Die Diskussion umfasst alle Parameter der IT-Infrastruktur, die Sicherheitsüberwachung, die Virtualisierung von Rechenzentren, die Migration von Firewalls und die Frage, welche neuen Verfahren zu unserem aktuellen System hinzugefügt werden können, um unser Unternehmen vor Datenverletzungen zu schützen."

CTO, Kanada, Pharmaindustrie

TEIL IV

Phishing-Schutz ist ein Teamsport

Sichern Sie Ihr Unternehmen durch Schutz vor Phishing und Investitionen in Sicherheitsschulungen für Mitarbeiter.

E-Mail-basierte Angriffe sind bei drei von vier Unternehmen auf dem Vormarsch, und ebenso viele rechnen im kommenden Jahr mit ernsten Folgen eines solchen Angriffs.[7] Als Reaktion darauf hat sich die Führungsetage auf die Schaffung einer unternehmensweiten Sicherheitskultur eingestellt,[8] genauer gesagt, Investitionen in Sensibilisierungsmaßnahmen in Verbindung mit mehrschichtigen Cybersicherheitsrahmen, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren.

"Unser Vorstand ist sich darüber im Klaren, dass E-Mail immer noch einer der Hauptangriffsvektoren ist, weshalb wir erheblich in die E-Mail-Sicherheit investiert haben."

CISO, britischer Einzelhandelssektor mit über 1.000 Mitarbeitern

E-Mails sind aufgrund ihrer Allgegenwärtigkeit und ihres Umfangs sowohl innerhalb als auch außerhalb des Arbeitsplatzes ein attraktives Angriffsziel für Cyberkriminelle. Und selbst mit den besten Cybersicherheitslösungen wird menschliches Versagen immer eine Lücke hinterlassen, durch die Angreifer spazieren können.

"E-Mail ist derzeit die größte Bedrohung, und Phishing-E-Mails sind der häufigste Weg, um Informationen aus dem Unternehmen zu stehlen. Das ist einer der größten Risikobereiche und der Bereich, der mir am meisten Sorgen bereitet. Wir hatten schon einmal einen Angriff mit Phishing-E-Mails, bei dem die Mailboxen von Mitarbeitern gehackt wurden, und wir melden solche Szenarien dem Information Commissioner's Office (ICO)."

Direktor für Technologie in einem Unternehmen mit über 1.000 Mitarbeitern im öffentlichen Dienst, Großbritannien

Phishing ist eine der ursprünglichen Cyber-Bedrohungen, und sie hält sich hartnäckig, weil die Angreifer ihre Vorgehensweise ständig anpassen können. Darüber hinaus machen es Automatisierungstools und Phishing-Kits für weniger erfahrene Cyberkriminelle einfacher, ein größeres Netz auszuwerfen, das Unternehmen größeren Schaden zufügen kann. Vor dem Hintergrund der globalen Pandemie hat der jüngste *State of Email Security Report* gezeigt, dass **97 %** der Unternehmen bereits mit Phishing-Angriffen konfrontiert waren, und **59 %** der Unternehmen berichten von einem deutlichen Anstieg der Phishing-Bedrohungen, denen sie ausgesetzt sind.

7. Cyber Risk and the C-Suite in the State of Email Security, Mimecast
8. Cyber Risk and the Board: Support Fuels Cyber Awareness Training, Mimecast

TEIL IV

“Es ist menschliches Versagen, und man kann nicht analysieren, was in den Köpfen der Menschen vorgeht. Wir können unsere Mitarbeiter nur darin schulen, nicht auf unnötige Links zu klicken, aber es liegt an ihnen, ob sie es ernst nehmen oder nicht. Solange E-Mail-Kompromittierung und Phishing existieren und funktionieren, wird es also immer eine Lücke in der Cybersicherheit geben.”

CISO in einem Unternehmen mit über 1.000 Mitarbeitern im Einzelhandel, Australien

Um diese anhaltenden und anpassungsfähigen Bedrohungen einzudämmen, konzentrieren sich CISOs auf die Entwicklung einer sicherheitsbewussten Kultur im gesamten Unternehmen - einschließlich der Vorstandsmitglieder. Doch das menschliche Verhalten zu ändern, ist weder einfach noch schnell. Schulungen zum Cyber-Bewusstsein und Abhilfemaßnahmen brauchen Zeit, um Ergebnisse zu erzielen, verglichen mit der Implementierung von E-Mail-Sicherheit oder anderen Technologie-Tools. Aus diesem Grund erkennen immer mehr Führungskräfte, wie wertvoll eine Kultur, die der Cybersicherheit Priorität einräumt, für die langfristige Sicherheit ist. Die Schaffung einer solchen Kultur erfordert jedoch Ausdauer, Kreativität und ein deutlich sichtbares Engagement der Führungsebene.

Schwachstellen in der Lieferkette, die zunehmende Online-Zusammenarbeit und die wachsende digitale Vernetzung sind die Hauptgründe dafür, dass die Cyberlandschaft immer tückischer wird. Die Erklärung dafür ist einfach: Die Kreuzung von Kommunikation, Menschen und Daten birgt ein enormes Risiko, da böswillige Akteure die moderne Arbeitsoberfläche ausnutzen. Die digitale Transformation, die Unternehmen vor der Pandemie durchführten, führte bereits zu einer rekordverdächtigen Anzahl von Datenverletzungen. Doch als die Unternehmen im Zuge der Pandemie ihre digitalen Kommunikationskanäle rasch ausbauten, vergrößerten sie unbeabsichtigt auch die Angriffsfläche für böswillige Akteure.

TEIL IV

“Auf Vorstandsebene würde ich mir mehr Diskussionen über die Psychologie des Umgangs mit Cyberangriffen wie Ransomware-Angriffen wünschen. Ein Blick auf die nichttechnische Perspektive dieser Ereignisse wäre von Vorteil. Wir müssen auch darüber diskutieren, wie wir die Cybersicherheit zum Problem aller machen können, nicht nur zum Problem des IT-Leiters.”

IT-Leiter, General Manager, Infrastruktur, 2.500+ Mitarbeiter, Australien

Einfach nur zu wissen, wie eine Spam- oder Phishing-E-Mail aussehen kann, reicht nicht aus. Deshalb können kontextbezogenes Wissen und die volle Unterstützung des Unternehmens, dass Sicherheit in der Verantwortung jedes Einzelnen liegt, dazu beitragen, den Nutzen von Sensibilisierungsschulungen zu maximieren.

Unternehmen aller Art befinden sich in einer entscheidenden Phase, und ein umfassender Wandel scheint unvermeidlich. Doch die Festlegung einer Strategie, die sich mit kritischen Fragen der Cybersicherheit befasst - von der Gewährleistung der Sicherheit interner Systeme und Kunden bis hin zur Entlastung der Cybersicherheitsexperten - wird keine leichte Aufgabe sein. Und sie erfordert die aktive Beteiligung nicht nur des Vorstands, sondern jedes Einzelnen im Unternehmen.

Um sich vor Bedrohungen durch E-Mails zu schützen und eine sicherheitsbewusste Kultur zu entwickeln, empfehlen die Befragten der Führungsebene:

1 Phishing ist ein Problem, das nicht verschwinden wird, unabhängig von der Branche, der Unternehmensgröße oder der Region Ihres Unternehmens. Sorgen Sie dafür, dass alle Mitarbeiter eine bessere Cyber-Hygiene betreiben und sich sicher fühlen, wenn sie potenzielle Cyber-Bedrohungen mitteilen. Diese Praktiken sind ein entscheidender Aspekt für die Fähigkeit jedes Unternehmens, Cyberrisiken zu mindern.

2 Die Schaffung einer Sicherheitskultur, die den Vorstand, die Geschäftsleitung und alle Organisationen innerhalb des Unternehmens durchdringt, ist eine grundlegende Praxis zur Verringerung von Cyberrisiken. Damit diese Grundlagen wirksam sind, muss jeder Mitarbeiter für die Cybersicherheit verantwortlich gemacht werden.

TEIL V

Das Fazit:

Die Führungsrolle im Bereich der Cybersicherheit war noch nie so komplex wie heute: Immer raffiniertere und umfangreichere Angriffe dringen aufgrund der modernen Arbeitsumgebung in Unternehmen ein, während die Einstellung von Cyberexperten weiterhin eine Herausforderung darstellt. Und doch war die Chance für CISOs, ihre Unternehmen zu schützen, noch nie so groß wie heute: Die Verbindung zwischen Cyber-Risiko und Geschäftsrisiko sollte bei Gesprächen mit dem Vorstand immer im Vordergrund stehen. Vermeiden Sie die Falle eines monolithischen Sicherheitsanbieters, indem Sie mehrschichtige, erstklassige Cyber-Sicherheits-Tools implementieren, und schützen Sie sich mit E-Mail-Schutz und Sensibilisierungsschulungen für Mitarbeiter vor uralten Bedrohungen wie Phishing. Sicherheitsverantwortliche müssen ihre Risikoprofile verstehen und gut kommunizieren, um gleichzeitig die Angriffsfläche zu reduzieren und die Kontrollen zu maximieren.

Die Unternehmensvorstände schenken der Cybersicherheit endlich Aufmerksamkeit, aber sie haben immer noch viele andere wichtige Prioritäten, wie z. B. eine wahrscheinliche Rezession, den Klimawandel und geopolitische Unsicherheit. Mehr Aufmerksamkeit bedeutet also nicht automatisch mehr Geld oder Vorteile für die Cyberabwehr. Mehr Aufmerksamkeit bedeutet mehr Prüfung - aber die Gelegenheit, Cyberrisiken als Geschäftsrisiken zu betrachten, ist da.

Sicherheitsverantwortliche müssen ihr Risikoprofil verstehen und den Zusammenhang zwischen Cyber- und Geschäftsrisiken im Auge behalten, wenn sie mit dem Vorstand sprechen.

PART VI

Methodik

Über die in diesem Bericht enthaltenen Ergebnisse

Die Umfrageteilnehmer arbeiteten in Unternehmen mit weniger als 500 Mitarbeitern (35 %), 501 bis 1.000 Mitarbeitern (33 %) und Unternehmen mit mehr als 1.000 Mitarbeitern (32 %).

Diese Unternehmen verteilten sich auf **fünf Branchen**, darunter Finanzdienstleistungen (29 %), Gesundheitswesen (21 %), öffentlicher Sektor (15 %), Einzelhandel (15 %) und Unterhaltung (19 %).

Die Umfrageteilnehmer kamen aus Unternehmen in Australien, Singapur, Frankreich, **Deutschland**, den Niederlanden, Schweden, Dänemark, den Vereinigten Arabischen Emiraten, Saudi-Arabien, Kanada, den USA und dem Vereinigten Königreich.

Work Protected.

Advanced Email & Collaboration Security

mimecast

Mimecast: Work Protected™ Since 2003, Mimecast has stopped bad things from happening to good organizations by enabling them to work protected. We empower more than 40,000 customers to help mitigate risk and manage complexities across a threat landscape driven by malicious cyberattacks, human error, and technology fallibility. Our advanced solutions provide the proactive threat detection, brand protection, awareness training, and data retention capabilities that evolving workplaces need today. Mimecast solutions are designed to transform email and collaboration security into the eyes and ears of organizations worldwide.