mimecast®

Cyber-Risiko rückt in den FOKUS der Chefetage

Der “State of Email Security 2023”

Durchbrüche auf Vorstandsebene

Da die Unternehmen angesichts der zunehmenden wirtschaftlichen Volatilität und der sich verschärfenden geopolitischen Spannungen immer nervöser werden, hat sich in allen Geschäftsbereichen ein konservativerer Ansatz durchgesetzt. Dies gilt insbesondere für den digitalen Bereich, wo Risiken, die Führungskräfte vor einigen Jahren noch ertragen haben, heute als inakzeptabel gelten.

Deloitte drückt es folgendermaßen aus: “Die Risikolandschaft verändert sich schnell. Jeden Tag gibt es neue Schlagzeilen, die daran erinnern, dass die Zukunft vor der Tür steht, und manchmal hat man das Gefühl, dass an jeder Ecke neue Risiken und Reaktionsstrategien auftauchen.” Zu den wichtigsten Herausforderungen, die die Unternehmensberatung hervorhebt, gehören die Störungen, die sich aus neuen Technologien ergeben, und die Risiken, die mit der vernetzten Wirtschaft verbunden sind.

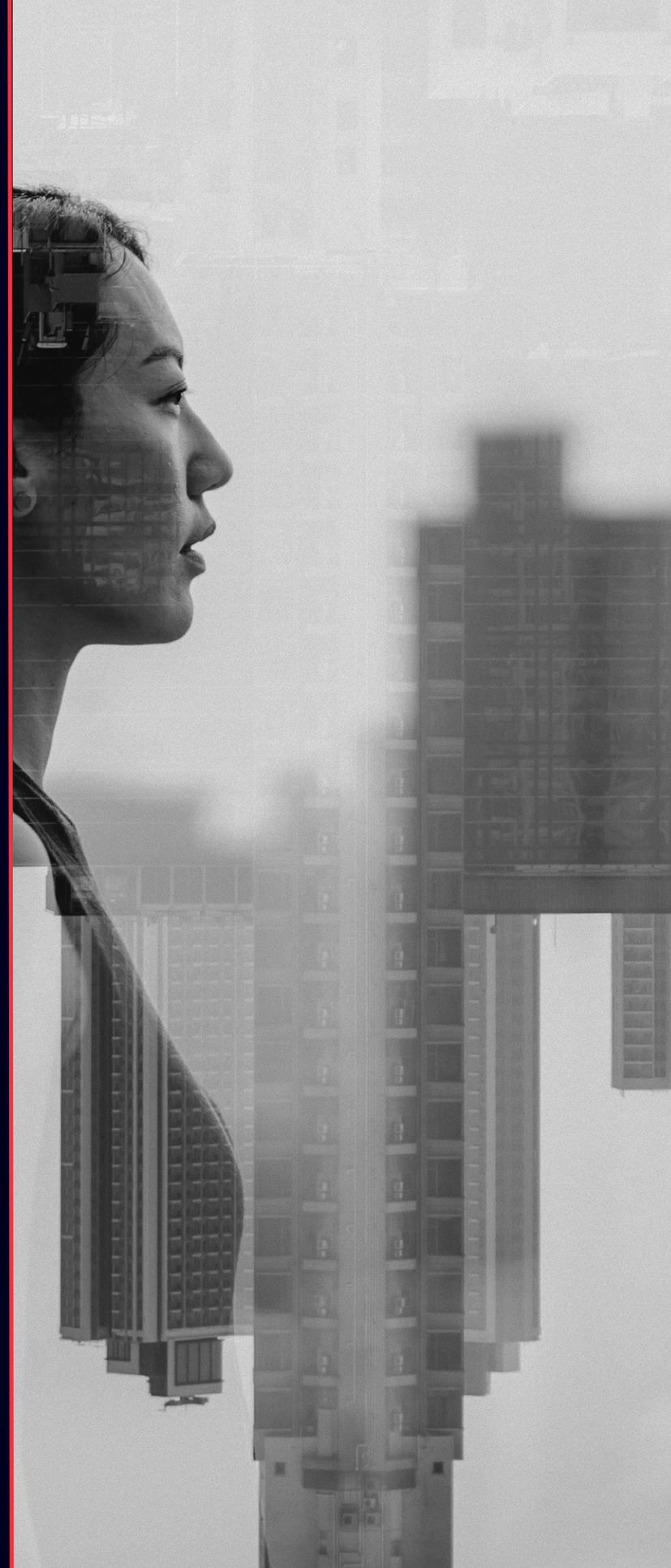
Da sich die Cyber-Bedrohungen vervielfacht haben, ist die globale Geschäftswelt zunehmend sensibler für die Gefahr geworden und zeigt eine größere Bereitschaft, sich ihr zu stellen - ein Trend, der im Mimecast-Bericht 2023 über den Stand der E-Mail-Sicherheit, der siebten jährlichen Studie dieser Art, laut und deutlich zum Ausdruck kommt.

Das wachsende Bewusstsein für die sprunghaft ansteigenden Cyberrisiken zeigt sich auch in anderen Studien. In einer informellen Umfrage von Forbes unter Führungskräften aus der Wirtschaft wurde versucht, die wichtigsten Risiken zu ermitteln, mit denen Unternehmensleitende im Jahr 2022 konfrontiert sein werden. Neben dem Klimawandel, der Inflation und der Möglichkeit einer weiteren Finanzkrise stand das Risiko einer Datenschutzverletzung ganz oben auf der Liste.[1]

Das Allianz Risk Barometer - eine jährliche Umfrage unter Versicherungsexperten in Unternehmen, darunter Makler, Underwriter und Risikoberater-, die vom Versicherungsriesen Allianz Global Corporate & Specialty (AGCS) veröffentlicht wird, ist ein weiterer Beleg dafür, dass die Besorgnis über Cyberrisiken in den Chefetagen einen neuen Stellenwert eingenommen hat. Für das Jahr 2022 ergab die Umfrage, dass die Bedrohung durch einen Cybervorfall das wichtigste globale Risiko für Unternehmen ist, weit vor dem Klimawandel, dem Arbeitskräftemangel und der Möglichkeit einer Rezession.[2]

In der folgenden Aufschlüsselung unseres Berichts zum Stand der E-Mail-Sicherheit machen die 1.700 befragten CISOs und andere IT-Experten die Art der Risiken deutlich, mit denen sie konfrontiert sind, und geben ein realistisches Bild von den Schritten, die sie zur Bewältigung dieser Risiken unternehmen.

Datenschutzverletzungen werden als ein noch größeres Risiko angesehen als Klimawandel, Inflation und eine weitere Finanzkrise.



Wichtige SOES-Ergebnisse 2023

Email

Die E-Mail-Nutzung nimmt in **8/10** Unternehmen weiter zu.

●●●○

3/4 Unternehmen haben auch eine Zunahme von E-Mail-Bedrohungen festgestellt.

Cyberangriffe

59% der Umfrageteilnehmer geben an, dass Cyberangriffe immer raffinierter werden.

2/3 Unternehmen wurden durch einen Ransomware-Angriff geschädigt.

97% der Unternehmen sind Ziel von Phishing-Angriffen per E-Mail geworden.

97

Budget

2/3 Befragten sagen, dass ihre Unternehmen mehr für Cybersicherheit ausgeben müssen.

●●○

Überwachung

98% der Unternehmen haben entweder ein System zur Überwachung und zum Schutz vor E-Mail-Bedrohungen oder planen aktiv die Einführung eines solchen Systems.

92% der Unternehmen nutzen oder planen den Einsatz von KI und maschinellem Lernen, um ihre Cybersicherheit zu verbessern.

94% der Unternehmen sind der Meinung, dass sie einen stärkeren Schutz benötigen als den, der in ihren MS 365- und Google Workspace-Anwendungen enthalten ist.

94

99

Cyber-Bewusstsein

99% bieten ihren Mitarbeitern eine Form von Cyber-Sensibilisierungsschulung an.

97% der Unternehmen sind Ziel von Phishing-Angriffen per E-Mail geworden.

Werkzeuge zur Zusammenarbeit

●●●○

3/4 Befragten geben an, dass Collaboration-Tools erhebliche neue Sicherheitsrisiken mit sich bringen.

72% der Unternehmen gehen davon aus, dass sie im Jahr 2023 durch einen Angriff mit einem Collaboration-Tools geschädigt werden.

72

Die Erklärung ist einfach: Die Schnittstelle von Kommunikation, Menschen und Daten birgt ein enormes Risiko, da böswillige Akteure die Vernetzung der modernen Arbeitsoberfläche ausnutzen.

Neue und alte Bedrohungen bewältigen

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 ist einfach: Die Überschneidung von Kommunikation, Menschen und Daten birgt ein enormes Risiko, da böswillige Akteure die Vernetzung der modernen Arbeitswelt ausnutzen.

Mehrstufige Angriffe mit mehreren Vektoren sind zur Norm geworden, wobei Kriminelle einen Einstiegspunkt nutzen, um die Tür zu anderen zu öffnen. In der vernetzten Geschäftswelt von heute können selbst kleine Sicherheitsmängel und Fehler einen verheerenden Dominoeffekt haben.

2023

33 Milliarden

wird erwartet, dass etwa 33 Milliarden elektronische Datensätze gestohlen werden.[3]

$8 Billionen Dollar

wird erwartet, dass Cyberkriminalität die Welt 8 Billionen Dollar kosten wird. Wirtschaftlich gesehen ist dies mehr als das BIP aller Länder zusammen, außer den USA und China.[4]

$4.35 Millionen Dollar

belaufen sich weltweit die durchschnittlichen Kosten für eine Datenschutzverletzung auf 4,35 Millionen Dollar. Die durchschnittlichen Kosten in den USA sind mit 9,44 Millionen Dollar mehr als doppelt so hoch.[5]

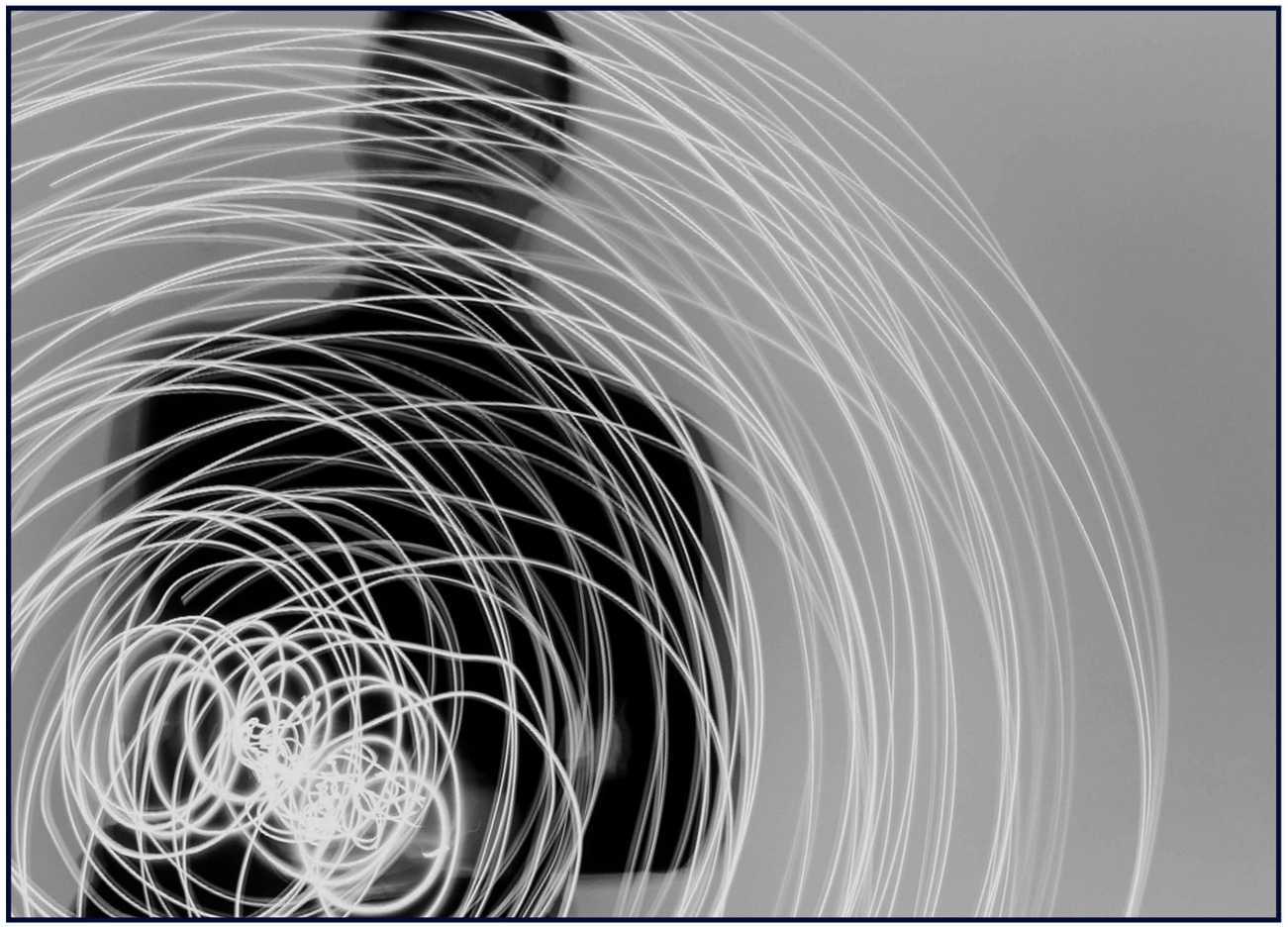
13%

Im Jahr 2022 gab es einen Anstieg von Ransomware um 13 % - ein Anstieg, der so groß war wie in den letzten fünf Jahren zusammen.[6]

212 Tage

Im Durchschnitt dauert es 212 Tage, bis eine Datenschutzverletzung entdeckt wird, und weitere 75 Tage, um sie einzudämmen.[7]

Es wird erwartet, dass Cyberkriminalität im Jahr 2023 weltweit 8 Billionen Dollar kosten wird - mehr als das BIP aller Länder außer den USA und China.



E-Mail-basierte Bedrohungen

Die Studie State of Email Security (SOES) hat ergeben, dass die Abhängigkeit der Unternehmen von E-Mails weiterhin stärker zunimmt als zu Beginn der COVID-19-Pandemie. 82% der Unternehmen geben an, dass das E-Mail-Aufkommen im Jahr 2022 steigen wird, verglichen mit 79% im Jahr 2021 und 81% im Jahr 2020. Mehr E-Mails haben zu mehr E-Mail-Bedrohungen geführt, und drei von vier (74%) der SOES-Befragten geben an, dass diese in den letzten 12 Monaten zugenommen haben.

Doch während die steigende Zahl der Bedrohungen ein Problem darstellt, ist ihre zunehmende Raffinesse eine noch größere Gefahr.

Cyberkriminelle verfeinern ihre Strategien immer weiter und passen sie an, und Malware-Kits im Dark Web ermöglichen es selbst gewöhnlichen Kriminellen ohne technologisches Wissen, hochentwickelte Angriffsmethoden anzuwenden. In der Tat ist es die immer ausgefeiltere Art der Angriffe, mit denen sie konfrontiert werden, die die Befragten von SOES 2023 als ihre größte Herausforderung bezeichneten (59%).

3VON4

3 von 4 Unternehmen befürchten ernsthafte Folgen eines E-Mail-Angriffs

Die zunehmende Komplexität der Angriffe führt bei den CISOs und anderen Cybersicherheitsexperten, die an der SOES-Umfrage teilgenommen haben, zu einem Gefühl der Befürchtung.

Drei von vier (76%) erwarten, dass ein E-Mail-Angriff im kommenden Jahr schwerwiegende Folgen für ihr Unternehmen haben wird.

Von diesen glauben 7%, dass ein solcher Angriff “unvermeidlich” ist, während weitere drei von 10 ihn für “extrem wahrscheinlich” halten.

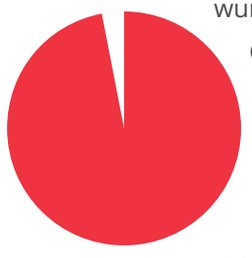
Aber während die zunehmend Anzahl der Bedrohungen ist a Problem, ihr Wachsen Raffinesse stellt eine noch größere Gefahr.

Ein tückisches Trio

Es gibt viele verschiedene Arten von E-Mail-Bedrohungen, mit denen Cybersecurity-Profis konfrontiert sind, aber die drei häufigsten sind Phishing, ransomware und Spoofing. Insgesamt haben 84% der Sicherheitsentscheider in den letzten 12 Monaten eine Zunahme von mindestens einer Art dieser Angriffe festgestellt, von denen Phishing am weitesten verbreitet ist:

Phishing

Im Jahr 2022 gab es schätzungsweise 255 Millionen phishing-Versuche, ein Anstieg von 61% gegenüber dem Vorjahr.[8]
Schlimmer noch: Mehr als 70% dieser E-Mails wurden vom Empfänger geöffnet.[9]



Gibt es irgendjemanden, der noch nie eine verdächtig aussehende E-Mail erhalten hat - oder schlimmer noch, eine E-Mail, die scheinbar von einer vertrauenswürdigen Partei stammt, es aber nicht ist? Aus diesem Grund fürchten sich Unternehmen vor phishing - denn es ist einfach, jemanden dazu zu verleiten, eine mit Malware verseuchte E-Mail zu öffnen und diese E-Mail dann an andere weiterzuleiten, wodurch die Bedrohung weiter verbreitet wird. Es ist daher kaum überraschend, dass 90 % der Sicherheitsverletzungen in Unternehmen auf Phishing zurückzuführen sind. [10]

Im vergangenen Jahr waren praktisch alle der diesjährigen SOES-Befragten (97%) das Ziel eines Phishing-Angriffs. Die Mehrheit (59%) hat mehr Angriffe erlebt als in den Vorjahren, und bei großen Unternehmen mit mehr als 10.000 Mitarbeitern ist dies sogar noch weiter verbreitet: 71% berichten von einem deutlichen Anstieg der Phishing-Versuche. Und von allen Befragten gaben 80% an, dass sie mindestens einen Angriff erlebt haben, bei dem sich die Bedrohung von einem infizierten Benutzer auf einen anderen ausgebreitet hat.

Ransomware

Zwei Drittel der diesjährigen SOES-Befragten (66%) gaben an, Opfer von Ransomware geworden zu sein, aber in diesem Fall waren kleinere Unternehmen stärker betroffen. Bei den Unternehmen mit 250 bis 500 Mitarbeitern gaben sieben von zehn Befragten (70%) zu, dass ein Ransomware-Angriff ihr Geschäft geschädigt hat, während 73% der Unternehmen mit 1.000 bis 5.000 Mitarbeitern dasselbe zugaben. Von den Großunternehmen mit 10.000 oder mehr Mitarbeitern wurde weniger als die Hälfte (46%) durch Ransomware geschädigt.

Auch Unternehmen in bestimmten Branchen wurden häufiger Opfer von Ransomware. Von den Unternehmen in den Branchen Verbraucherdienste (87%), Energie (83%), Gesundheitswesen (80%) und Medien und Unterhaltung (86%) wurden mehr als acht von zehn durch einen Ransomware-Angriff ernsthaft geschädigt.

7 von 10 Unternehmen wurden bereits durch einen Ransomware-Angriff geschädigt.

Spoofing

E-Mail-spoofing bleibt ein ernstes Risiko, insbesondere für den öffentlichen Sektor. Fast alle SOES-Befragten (91%) waren sich der Versuche bewusst, ihre E-Mail-Domäne zu missbrauchen, und fast die Hälfte (44%) sahen eine Zunahme dieser Art von Aktivitäten im Jahr 2022. Der Anstieg war bei Regierungsbehörden und anderen öffentlichen Einrichtungen sogar noch ausgeprägter: 54% berichteten von häufigerem E-Mail-Spoofing.

Auch das Spoofing von Web-Domains ist weit verbreitet, wobei Unternehmen wiederholt Versuche aufdeckten, ihre Websites zu klonen. Im Durchschnitt stellten die Unternehmen im vergangenen Jahr 10 solcher Versuche fest.

Während die meisten Unternehmen sagen, dass sie zumindest minimal auf Spoofing vorbereitet sind, sagen weniger als ein Drittel (29%), dass sie vollständig auf die unrechtmäßige Nutzung ihrer E-Mail-Domänen vorbereitet sind (obwohl diese Zahl bei Unternehmen mit mehr als 5.000 Mitarbeitern auf 35% ansteigt). Und obwohl fast neun von zehn (88%) der SOES-Befragten angaben, dass ihre Unternehmen daran interessiert sind, in den nächsten 12 Monaten DMARC (Domain-based Message Authentication, Reporting and Conformance) zu verwenden, um E-Mail-Spoofing zu vereiteln, hat es deutlich weniger als ein Drittel (27%) tatsächlich eingesetzt.

3 von 4 Unternehmen gehen davon aus, dass sie durch einen auf Collaboration-Tools basierenden Angriff geschädigt werden.

Collaboration ist ein zweischneidiges Schwert

In der Post-COVID-Ära bedeutet die moderne Arbeitsoberfläche, dass nur wenige Organisationen ohne den Einsatz von Collaboration-Tools funktionieren können. Software-Suites und ihre Add-ons, wie Microsoft Teams, Google Workspace und Slack, integrieren Kommunikation und Messaging mit Projektmanagementfunktionen. Die Kollaborationssoftware wurde entwickelt, um eine zentrale Plattform für die gemeinsame Nutzung von Daten und Dokumenten bereitzustellen. Sie hilft Unternehmen, die virtuelle Teamarbeit zu fördern und effizienter zu arbeiten, insbesondere im Zusammenhang mit den heutigen Remote- und Hybrid-Arbeitsumgebungen.

Doch während E-Mails nach wie vor der Hauptangriffsvektor für böswillige Akteure sind, bieten Collaboration-Tools eine neue Angriffsfläche für Cyberkriminelle, die sie infiltrieren können. Und das wiederum schafft noch mehr Risiken, die CISOs und ihre Teams bewältigen müssen.

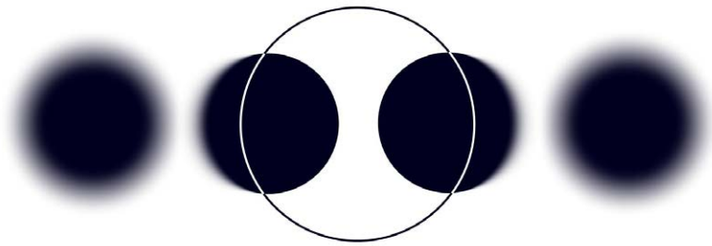
Collaboration-Tools sind wichtig, aber auch riskant

Die SOES-Teilnehmer von 2023 sind sich mit überwältigender Mehrheit einig (90%), dass Collaboration-Tools für das reibungslose Funktionieren ihrer Unternehmen unerlässlich sind. Aber zwei Drittel (67%) geben auch an, dass es eine große Herausforderung ist, mit der Anzahl der in ihrem Unternehmen verwendeten Collaborations-Tools Schritt zu halten, und mehr als die Hälfte (55%) beklagt, dass die Mitarbeiter routinemäßig neue Tools herunterladen und verwenden, die nicht von der IT-Abteilung geprüft oder genehmigt wurden.

In den meisten Unternehmen (82%) nimmt die Nutzung dieser Plattformen weiter zu, und mehr als ein Drittel der Befragten (38%) gibt an, dass die Zahl der auf Collaboration-Tools zurückzuführenden Angriffe im Steigen begriffen ist.

Noch aussagekräftiger ist, dass fast drei Viertel (72%) der SOES-Befragten sagen, dass es wahrscheinlich, sehr wahrscheinlich oder sogar unvermeidlich ist, dass ihr Unternehmen im Jahr 2023 von einem auf Collaboration-Tools basierenden Angriff negativ betroffen sein wird.

Dementsprechend sind drei Viertel (75%) der Befragten der Meinung, dass Tools für die Zusammenarbeit neue Bedrohungen darstellen und neue Sicherheitslücken schaffen, die dringend geschlossen werden müssen. Noch stärker war diese Meinung bei den Befragten in Unternehmen, in denen die Nutzung dieser Tools in den letzten 12 Monaten erheblich zugenommen hat (82%). Noch stärker war sie in den Sektoren Energie sowie Medien und Unterhaltung, wo 87% der Befragten ernste Besorgnis über die von Collaboration-Tools ausgehenden Risiken äußerten.



Unzureichende Sicherheitsmaßnahmen

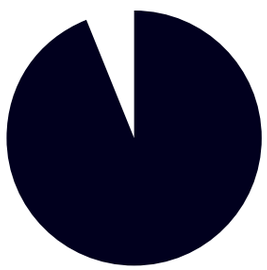
Die SOES-Befragten bezweifeln, dass die in den Kollaborationsplattformen enthaltenen Sicherheitsvorkehrungen einen angemessenen Schutz gegen die potenziellen Risiken bieten.

Fast zwei Drittel (62%) sind der Meinung, dass die Sicherheit der meisten nativen Collaboration-Tools nicht ausreicht, um ihre Bedürfnisse zu erfüllen. Fast ebenso viele (57%) wissen, dass die Cybersicherheitsvorkehrungen ihres Unternehmens nicht ausreichen, um die zusätzlichen Risiken zu bewältigen, die diese Plattformen mit sich bringen.

Bemerkenswert ist auch, dass in Bezug auf Google Workspace und Microsoft 365, tfast alle (94 %) der Meinung sind, dass zusätzliche Sicherheitsmaßnahmen erforderlich sind, um die nativen Sicherheitsfunktionen dieser Plattformen zu ergänzen.

Um ihren Schutz zu verbessern, sind viele Unternehmen der Meinung, dass sie mehr für die Sicherheit von Collaboration-Tools ausgeben müssen. Zwei Drittel (66 %) der Befragten sind der Meinung, dass ihr Unternehmen sein Budget für die Sicherung von Collaboration-Tools um durchschnittlich 8% aufstocken muss. Doch wie wir gleich sehen werden, sind dies nicht die einzigen Cyberschutzmaßnahmen, für die mehr Geld ausgegeben werden muss.

STÄ
RKER



94% der Unternehmen sind der Meinung, dass sie einen stärkeren Schutz für ihre MS 365- und Google Workspace-Anwendungen benötigen.

Bereitschaft für den Cyberspace

CISOs haben einen mächtigen neuen Verbündeten in ihren Bemühungen, die digitale Verteidigung ihrer Unternehmen zu stärken: den Unternehmensvorstand.

Da sich die Cyber-Risiken vervielfacht haben und die Unternehmensführung unter Druck steht, die Schlagzeilen über Cyber-Angriffe aus den Nachrichten herauszuhalten, sind die Vorstände und Führungskräfte in den Unternehmen sehr viel aufmerksamer gegenüber der Bedrohung geworden und zeigen eine neue Bereitschaft, sich ihr zu stellen.

Über den Wert von Cyber-Versicherungen sind die Befragten geteilter Meinung.

Unsicherheit über Cyberversicherungs-policen

Ein Thema, bei dem die SOES-Teilnehmer sehr geteilter Meinung sind, ist die Cyber-Versicherung, d. h. die Frage, ob solche Policen als Ersatz für die Entwicklung eines umfassenden Cyber-Vorsorgeprogramms dienen können. Viele Unternehmen sind skeptisch, was ihren Wert angeht (50 %), aber fast ebenso viele (48%) sehen sie als sinnvolle Ergänzung ihres Sicherheitsnetzes.

Die verschiedenen Branchen haben dazu sehr unterschiedliche Ansichten. Weniger geneigt, sich auf Cyber-Versicherungspolicen zu verlassen, sind die Befragten aus den Sektoren Unternehmensdienstleistungen (61%), Bauwesen (65%), Verbraucherdienstleistungen (65%) und insbesondere Energie (73%). In anderen Sektoren hingegen ist die Mehrheit der Befragten der Meinung, dass eine Versicherung ein gutes Maß an Schutz bietet, darunter die IT- und Telekommunikationsbranche (55%), das Gesundheitswesen (66%) und die Medien- und Unterhaltungsbranche (66%).

Diese Meinungsverschiedenheit gilt auch für Unternehmen unterschiedlicher Größe: Die Mehrheit der mittelständischen Unternehmen mit 500 bis 1.000 Mitarbeitern (59%) betrachtet die Cyberversicherung als integralen Bestandteil ihrer Cybervorsorge, während sechs von zehn Großunternehmen (60%) dies nicht tun. Unabhängig von ihrer Größe oder Branche sind sich die Unternehmen, die ihre Abhängigkeit von diesen Richtlinien verringern wollen, weitgehend einig (88%), dass sie dies durch höhere Investitionen in ihre eigene Cybersicherheitsabwehr ausgleichen müssen.

Unterfinanzierung bleibt ein Problem

Leider hat das wachsende Cyber-Bewusstsein noch nicht zu Budgets für die Cybersicherheit geführt, die mit der steigenden Bedrohungslage Schritt halten können. Die SOES-Befragten sind sich zwar einig, dass die Cybersicherheit mehr Beachtung findet als früher, aber das schlägt sich nicht immer in Geld nieder.

Genauer gesagt gaben zwei Drittel (66 %) der Befragten aus dem Jahr 2023 an, dass das Cybersicherheitsbudget ihrer Organisation geringer ist als es sein sollte - dies ist in etwa gleich geblieben wie im Vorjahr. Nach Angaben der diesjährigen Gruppe ist die Unterfinanzierung jedoch relativ bescheiden - im Durchschnitt etwas weniger als 8%. Betrachtet man die von den Unternehmen eingesetzten Cybersicherheitssysteme, so ergibt sich ein vielversprechenderes Bild. Nahezu alle SOES-Teilnehmer (98%) haben bereits Systeme zur Überwachung und zum Schutz vor E-Mail-Angriffen eingeführt, sind dabei, sie einzuführen oder planen dies aktiv.

Auch die Größe der Cybersicherheitsteams der meisten Unternehmen scheint zuzunehmen. So beschäftigt in Unternehmen mit 250 bis 500 Mitarbeitern fast die Hälfte (48%) zwischen sechs und zehn Mitarbeiter für Cybersicherheit, während ein Drittel (34%) zwischen 11 und 30 Vollzeit-Cybersicherheitsexperten beschäftigt. Und alle diese Unternehmen haben mindestens einen Mitarbeiter, der sich in Vollzeit mit Cybersicherheitsaufgaben beschäftigt.

Am anderen Ende des Spektrums haben mehr als die Hälfte der großen Unternehmen mit mehr als 10.000 Mitarbeitern (53%) mehr als 30 Mitarbeiter in ihren Cybersicherheitsteams.

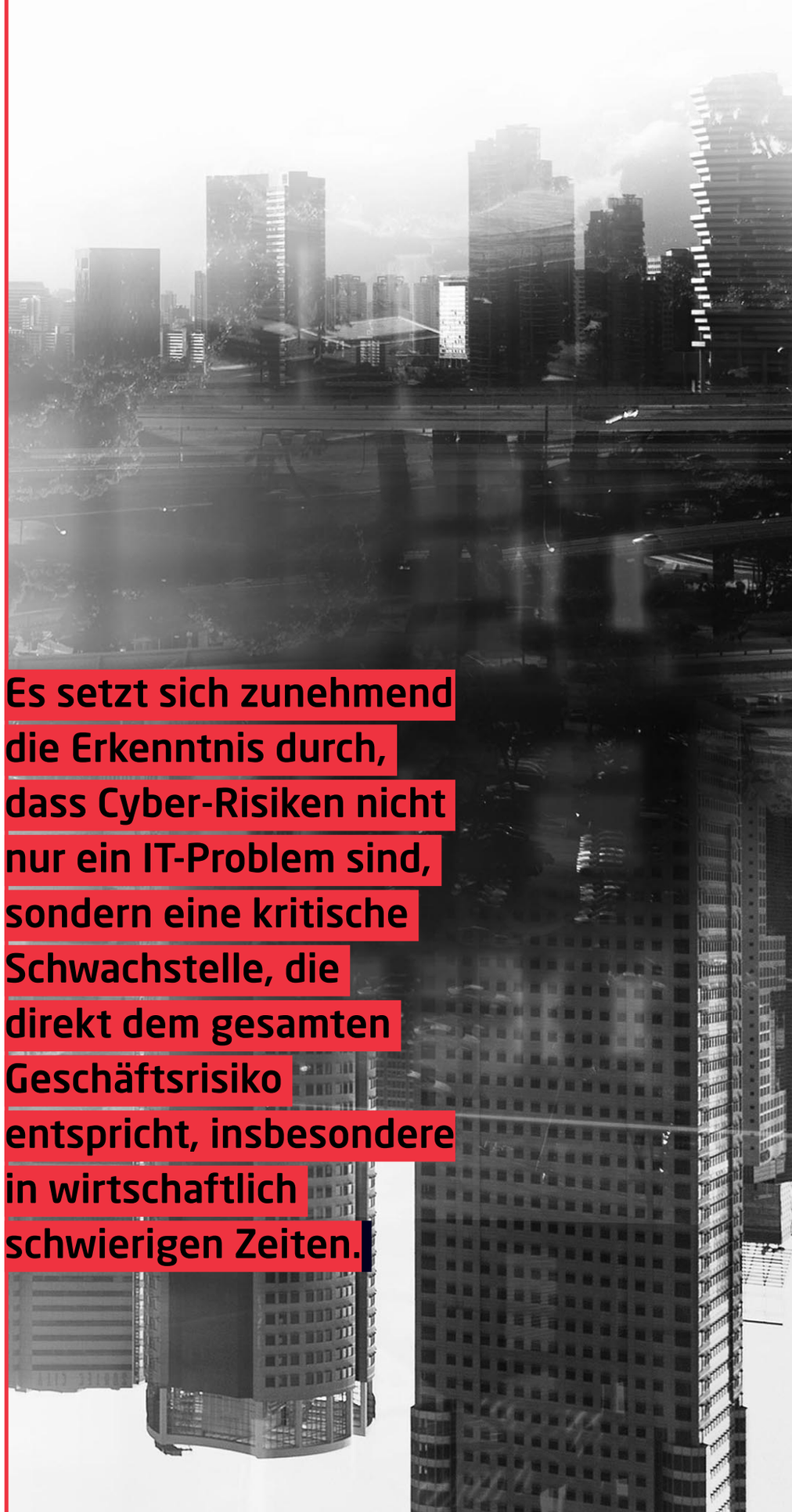
66% geben an, dass das Cybersicherheitsbudget ihres Unternehmens geringer ist, als es sein sollte

Wachsendes BEWUSSTSEIN für Cybersicherheit in der Vorstandsetage

Jahrelang haben CISOs und ihre Kollegen aus dem Bereich der Cybersicherheit einen oft einsamen Kampf geführt, um Strategien für die Widerstandsfähigkeit im Cyberspace zu entwickeln, die neue Bedrohungen erkennen und sich an sie anpassen können. Sie scheiterten jedoch oft am mangelnden Bewusstsein in den oberen Etagen ihrer Unternehmen und an der mangelnden Bereitschaft, mehr Geld für etwas auszugeben, das viele Führungskräfte als kostspielige Versicherung gegen eine Bedrohung betrachten, die möglicherweise nie eintritt.

Der Anstieg der Cyberkriminalität bei COVID, die moderne Arbeitsumgebung und die allgemein schwieriger gewordene Risikolandschaft haben viele Vorstände dazu veranlasst, diese Haltung zu überdenken. Es setzt sich zunehmend die Erkenntnis durch, dass Cyber-Risiken nicht nur ein IT-Problem sind, sondern eine kritische Schwachstelle, die sich direkt auf das allgemeine Geschäftsrisiko auswirkt, insbesondere in wirtschaftlich schwierigen Zeiten. Grundlegende Geschäftsentscheidungen - wie z. B. Fusionen und Übernahmen, Verträge mit Drittanbietern, Größenanpassungen und Partnerschaften in der Lieferkette - werden nun unter Berücksichtigung des Cyberrisikos getroffen.

CISOs haben in der Regel Schwierigkeiten, die Ressourcen zu erhalten, die sie für die Umsetzung einer robusteren Strategie zur Cyber-Resilienz benötigen. Nun aber, da ihre Vorstände regelmäßig die Risiken erörtern, die sich aus der Zunahme von Sicherheitsverletzungen und Cyber-Betrug ergeben, wächst das Gefühl, dass Anträge auf mehr Finanzmittel positiver aufgenommen werden.



92% der Unternehmen nutzen oder planen den Einsatz von KI und maschinellem Lernen, um ihre Cybersicherheit zu verbessern.

Verringerung des Cyber-Risikos mit Technologie der nächsten Generation

49% verbesserte Fähigkeit Bedrohungen zu blockieren

48% schnellere Behebung bei einem Angriff

50% genauerer Schutz vor Bedrohungen

Unterbudgetierung mag für die meisten CISOs immer noch eine Tatsache sein, aber da die Zahl und Komplexität von Cyberangriffen weiter zunimmt, helfen künstliche Intelligenz (KI) und maschinelles Lernen (ML) den unterfinanzierten Cybersecurity-Teams, der Kurve einen Schritt voraus zu sein.

Fast die Hälfte der befragten Unternehmen (49%) setzt bereits eine Kombination dieser Technologien ein (im Vergleich zu 46% im letzten Jahr und 38% im Jahr davor), und die meisten anderen (43% der Gesamtzahl) planen, dies zu tun.

Unter den Unternehmen, die derzeit KI/ML einsetzen, werden eine genauere Erkennung von Bedrohungen (50%), eine verbesserte Fähigkeit zur Abwehr von Bedrohungen (49%) und eine schnellere Behebung von Angriffen (48 %) als die drei größten Vorteile angesehen.

Die meisten SOES-Teilnehmer (81%) sind sich einig, dass KI-Systeme, die den Nutzern von E-Mail- und Kollaborationstools kontextbezogene Warnungen in Echtzeit liefern, ein großer Segen wären. Zwölf Prozent gingen sogar so weit zu sagen, dass die Vorteile eines solchen Systems die Art und Weise,

Über 95% aller Datenschutzverletzungen sind auf menschliches Versagen zurückzuführen

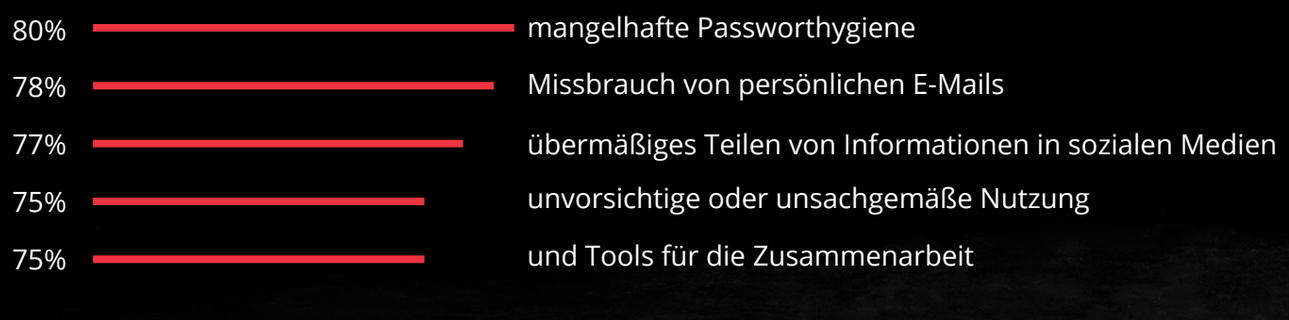
Fast die Hälfte (48%) gab an, dass ein unzureichendes Bewusstsein der Mitarbeiter für Cyber-Bedrohungen die größte Sicherheitsherausforderung ihres Unternehmens im Jahr 2023 sein würde

Verringerung des Cyber-Risikos durch Cyber-Bewusstsein

Eine erschreckende Tatsache: Über 95 % aller Datenschutzverletzungen sind auf menschliches Versagen zurückzuführen.[11] Und eine andere: Schätzungen zufolge können 97% der Nutzer nicht einmal eine einfache Phishing-E-Mail erkennen, wenn sie eine erhalten.[12] Dieser Umstand führt zu einer offensichtlichen Schlussfolgerung: Der wichtigste Schritt, den jedes Unternehmen zur Verbesserung seiner Cybersicherheit unternehmen kann, ist die Förderung einer Kultur des Cyber-Bewusstseins.

In jedem Unternehmen, unabhängig von seiner Größe, muss ein grundlegendes Verständnis der Risiken und der häufigsten Angriffsarten zum Allgemeinwissen werden. Mitarbeiter auf allen Ebenen müssen erkennen, dass Cybersicherheit nicht nur ein IT-Thema ist, sondern etwas, das sie persönlich betrifft und für das sie direkt verantwortlich sind.
All dies wird durch die SOES-Daten eindeutig bestätigt, aus denen hervorgeht, dass Angriffe, die sich schnell von einem infizierten Mitarbeiter auf andere ausbreiten, einen neuen Höchststand erreicht haben. Acht von zehn (80 %) der befragten Unternehmen waren von dieser Art von Angriffen betroffen. Dies ist der höchste Stand in allen sieben SOES-Umfragen mit Ausnahme des letzten Jahres, als 82% der Unternehmen berichteten, dass sie Opfer solcher Angriffe wurden.

Auf die Frage, welche Fehler Mitarbeiter machen, die zur Verbreitung beitragen



WACHSAMKEIT

im Cyberspace fördern

Das Gegenmittel gegen eine unzureichende Sensibilisierung der Mitarbeiter ist ein Cyber-Awareness-Training, das die Mitarbeiter über die Gefahren aufklärt und ihnen beibringt, die Bedrohungen, denen sie routinemäßig ausgesetzt sind, zu erkennen und sicher zu handhaben. Aus diesem Grund setzen sich viele Führungskräfte und Unternehmensvorstände für eine größere Cyber-Awareness ein, und praktisch alle diesjährigen SOES-Teilnehmer (99%) bieten ihren Mitarbeitern irgendeine Art von Sensibilisierungsschulung an.

Die wirksamsten Schulungen sind fortlaufend, fesselnd und basieren auf bewährten pädagogischen Verfahren, und auch hier scheint sich dies zunehmend in den Schulungsarten widerzuspiegeln, die die SOES-Teilnehmer anbieten. So führt mehr als die Hälfte (55%) Gruppenschulungen mit dem IT- oder Cybersicherheitsteam durch, und 41% bieten auch Einzelschulungen an.

Eine andere hochwirksame Form der Schulung - interaktive Videos - wird von fast der Hälfte (44%) der Teilnehmer angeboten und ist bei den größten Unternehmen mit mehr als 10.000 Beschäftigten (58%) noch beliebter. Es gibt jedoch auch Ausnahmen. Es scheint sich um einen Fall von “Schusters Rappen” zu handeln: Weniger als ein Drittel (32%) der Unternehmen der Medien- und Unterhaltungsbranche nutzen Schulungsvideos - die wenigsten von allen Branchen.

Was die Häufigkeit anbelangt, so bietet nur eine Minderheit der Unternehmen (18%) fortlaufende Schulungen an, aber mehr als ein Drittel (36%) bietet sie jeden Monat an, und fast ebenso viele (31%) bieten sie jedes Quartal an. Insgesamt bieten also 85% der SOES-Teilnehmer ihren Mitarbeitern mindestens einmal im Quartal eine Sensibilisierungsschulung an. Auch hier ist die Trendlinie positiv: Auch hier ist die Häufigkeit der von den SOES-Teilnehmern durchgeführten Schulungen in den letzten sieben Jahren stetig gestiegen, mit Ausnahme des letzten Jahres, als sie noch höher war (87% bieten mindestens einmal pro Quartal Schulungen an).

99% der Unternehmen schulen ihre Mitarbeiter in irgendeiner Form im Umgang mit dem Internet

Was sind die wichtigsten Lehren aus den diesjährigen SOES-Ergebnissen?

Die 10 wichtigsten Erkenntnisse

1

Es gibt kein höheres Risiko als das Cyber-Risiko.

Die Welt wird in diesem Jahr 8 Billionen Dollar durch Cyberkriminalität verlieren. Es dauert im Durchschnitt mehr als neun Monate, um eine Datenschutzverletzung zu entdecken und einzudämmen. Unternehmen fürchten Cyberangriffe mehr als die Inflation und den Klimawandel. Ist es da ein Wunder, dass viele CISOs das Gefühl haben, den Tiger am Schwanz zu haben?

2

Sichern Sie Ihre E-Mails, um die Cyber-Bedrohung zu bändigen.

Es gibt einen guten Grund, warum die E-Mail die Nr. 1 Angriffsvektor für Cyberkriminelle ist: Weil es dort die meisten digitalen Türen und Fenster gibt, durch die sie klettern können. So melden 82% der Unternehmen ein höheres E-Mail-Aufkommen, 74% sehen mehr E-Mail-basierte Bedrohungen, und drei von vier Unternehmen (76%) rechnen mit ernsthaften Folgen eines E-Mail-basierten Angriffs.

3

Collaboration Tools sind großartig, unerlässlich für die moderne Arbeit und riskant.

Die Nutzung von Collaboration-Tools hat explosionsartig zugenommen, und das macht sie zu einem weiteren attraktiven Ziel für Kriminelle. Mehr als ein Drittel der SOES-Befragten (38%) gibt an, dass die Zahl der Angriffe aufgrund von Collaboration-Tools zunimmt; fast drei Viertel (72%) glauben, dass ihr Unternehmen durch einen auf Collaboration-Tools basierenden Angriff geschädigt wird, und drei von vier (75%) sind der Meinung, dass die neuen Bedrohungen, die von Collaboration-Tools ausgehen, dringend angegangen werden müssen.

4

Um Phishing zu vermeiden, sollten Sie Ihre Benutzer besser schulen.

Phishing-Angriffe beruhen auf Vorspiegelung falscher Tatsachen und Social Engineering, um Mitarbeiter zu täuschen. Durch kontinuierliche und ansprechende Sensibilisierungsmaßnahmen können sie jedoch lernen, diese und andere Tricks zu erkennen und zu vermeiden. Man kann nie zu viel Cyber-Sensibilisierungstraining anbieten.

5

Spoofing ist ein Problem; DMARC die Lösung.

Fast jedes Unternehmen ist von Spoofing betroffen (91%), und viele stellen eine Zunahme dieser Art von Betrug fest (44%). Was sie nicht tun, ist, die Vorteile von DMARC zu nutzen, einem robusten und kosteneffektiven Protokoll zum Aufspüren gefälschter E-Mails. Eine Marke zu schützen ist schwierig, und eine geschädigte Marke zu reparieren ist noch schwieriger. Das macht eine bewährte Lösung wie DMARC zu einem unbedingten Muss.

6

Microsoft 365 und Google Workspace bieten gute Sicherheit. Unternehmen brauchen aber mehr Sicherheit.

Die von MS 365 und Google Workspace gebotene

Sicherheitsebene ist zu dünn - zumindest nach Ansicht von 94% der SOES-Befragten. In einer Welt, in der fast die Hälfte der bösartigen E-Mail-Anhänge MS 365-Dateien sind, sind zusätzliche Schutzschichten erforderlich.

7

Eine Versicherungspolice kann Ihren eigenen Cyber-Vorsorgeplan nicht ersetzen.

Es mag finanziell sinnvoll sein, sich gegen Cyber-Risiken zu versichern, aber selbst die beste Cyber-Versicherung kann nur Schäden ausgleichen, die bereits entstanden sind; sie kann nicht verhindern, dass der Schaden überhaupt erst entsteht. Das kann nur Ihr eigener Cyber-Vorsorgeplan leisten.

8

Cyberkriminelle nutzen Künstliche Intelligenz und Sie sollten das auch.

Fast die Hälfte der SOES-Teilnehmer

(49 %) setzt bereits eine Art von KI/ML ein, um ihren Schutz zu verbessern. Sie berichten von einer langen Liste von Vorteilen, darunter eine genauere Erkennung von Bedrohungen (50%), eine bessere Abwehr von Bedrohungen (49%) und eine schnellere Beseitigung von Angriffen (48%). Die Zeichen der Zeit stehen auf Sturm: Angesichts der Tatsache, dass Cyberkriminelle KI einsetzen, um Ransomware, E-Mail-Phishing-Betrug und andere Angriffe zu verstärken, müssen die Verantwortlichen für Cybersicherheit KI mit KI bekämpfen.

9

Es ist ein erster Schritt, die Aufmerksamkeit des Vorstands zu haben. Das bedeutet aber noch nicht, dass sie ein größeres Budget zur Verfügung stellen werden.

Die Unternehmensvorstände schenken der Cybersicherheit endlich Aufmerksamkeit, aber sie haben immer noch viele andere Prioritäten, wie zum Beispiel eine wahrscheinliche Rezession. Mehr Aufmerksamkeit führt also nicht automatisch zu mehr Geld für die Cyberabwehr. Dennoch sind die Defizite in den einstelligen Bereich gesunken, und Anträge auf höhere Budgets werden ernsthaft geprüft.

10

Es geht aufwärts. Haben wir erwähnt, dass Sie jetzt die Aufmerksamkeit des Vorstands haben?

Jahrelang haben CISOs dafür gekämpft, dass ihre Vorstände die Cybersicherheit ernster nehmen. Jetzt haben sie es geschafft, und der Ball liegt jetzt bei ihnen. Sicher, es gibt Risiken. Mehr Aufmerksamkeit bedeutet mehr Kontrolle - aber die Chance, Cyberrisiken als Geschäftsrisiken zu verdeutlichen, war noch nie so groß. Sie haben den Zugang, nutzen Sie ihn jetzt, um für eine größere Cyber-Resilienz zu werben.

Rund um den Globus rüsten sich die Unternehmen gegen einen Cybersturm inmitten der Rezession. Ihre Bemühungen haben ihre Grenzen, aber was noch wichtiger ist, ihre Vorstände und Führungskräfte haben begonnen, das Risiko anzuerkennen. Dies ist von entscheidender Bedeutung, denn wenn die Vorbereitung auf den Cyberangriff erst einmal zu einer Geschäftspriorität geworden ist, ist es nur eine Frage der Zeit, bis die Unternehmen die Mittel und Wege zu seiner Umsetzung finden.

Der diesjährige SOES-Bericht beleuchtet ihre Bemühungen. Die eigentliche Erkenntnis ist jedoch, dass Unternehmen auf der ganzen Welt damit begonnen haben, die Cyber-Bedrohung einzudämmen, indem sie ihr eine höhere Priorität einräumen - auch wenn ihre völlige Beseitigung noch ein fernes Ziel ist.

Die Bilanz

Über die in diesem Bericht enthaltenen Umfrageergebnisse

Dies ist das siebte Jahr in Folge, in dem Mimecast eine eingehende globale Umfrage zum aktuellen Stand der E-Mail-Sicherheit durchgeführt hat. Für unseren Bericht 2023 beauftragten wir das Forschungsunternehmen Vanson Bourne mit der Befragung von 1.700 Fachleuten aus den Bereichen Informationstechnologie und Cybersicherheit - die größte Stichprobe seit Beginn der Studie im Jahr 2016. Die Befragung fand im Oktober und November 2022 statt. Die Teilnehmer kamen aus 13 Ländern: den USA, Kanada, dem Vereinigten Königreich, Frankreich, Deutschland, den Niederlanden, Schweden, Dänemark, Saudi-Arabien, den Vereinigten Arabischen Emiraten, Südafrika, Singapur und Australien..

Die Umfrageteilnehmer arbeiteten in Unternehmen mit 250 bis 500 Mitarbeitern (15%) und mit mehr als 10.000 Mitarbeitern (9%). Die Unternehmen verteilten sich auf 12 Branchen, darunter Finanzdienstleistungen (14%), Technologie und Telekommunikation (13%), Einzelhandel (13%), Gesundheitswesen (11%), Fertigung (9 %) und der öffentliche Sektor (7%).

Von den Teilnehmern waren 62 % CIOs, CTOs, CISOs, IT-Direktoren und IT-Sicherheitsdirektoren. Der Rest bestand aus IT- und SOC-Managern sowie Sicherheitsarchitekten und -analysten.

mimecast®

Advanced Email & Collaboration Security

1. "The 10 Biggest Risks and Threats for Businesses in 2022," Forbes
2. "The 3 Most Important Global Corporate Risks in 2022: Part I," Censinet
3. "Cybersecurity Breaches to Result in Over 146 Billion Records Being Stolen by 2023," Juniper Research
4. "Cybercrime to Cost the World 8 Trillion Annually in 2023," Cybercrime Magazine
5. "Cost of a data breach 2022," IBM
6. "Data Breach Investigations Report 2022," Verizon
7. "Blumira's 2022 State of Detection and Response," Blumira
8. "The State of Phishing 2022," SlashNext
9. "Phishing Statistics & How to Avoid Taking the Bait," DataProt
10. Ibid
11. "Top 21 Cybersecurity Stats You Should Know about in 2023," Simplilearn
12. "8 Cybersecurity trends to be aware of in 2022/2023," AT&T Business

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.