mimecast

Human Risk & KI

TRANSFORMATION DER ZUKUNFT

Der Stand der E-Mail- und Collaboration-Sicherheit 2024

Teil I:

Wachsende Cyber-Bereitschaft

Im Jahr 2023 war die Welt voller Risiken, und die Bedrohungen der Cybersicherheit nahmen weiter zu. Wie könnten sie nicht? Angesichts der Bedrohung durch staatliche Akteure in vielen Ländern und der weit verbreiteten wirtschaftlichen und politischen Verwerfungen, die eine Flut krimineller Aktivitäten auslösten, war es unvermeidlich, dass auch die Internetkriminalität zunehmen würde.

Am bemerkenswertesten ist, dass laut den Ergebnissen des SOECS 2024 9 von 10 Unternehmen eine formelle Cybersicherheitsstrategie haben. Dazu gehören die 48% der Befragten, die eine formelle Cybersicherheitsstrategie haben, die auch alle wichtigen Geschäftsfunktionen umfasst, sowie 43%, die zwar eine formelle Strategie haben, diese aber in die alleinige Verantwortung ihrer IT-Abteilung legen.

Weitere 3 % führen derzeit eine formelle Strategie ein und 6 % haben Richtlinien und bewährte Verfahren für die Cybersicherheit eingeführt, allerdings keine formelle Strategie.

100%

der Unternehmen engagieren sich jetzt stark für die Cyber-Vorsorge.

Dieser Grad der Vorbereitung erstreckt sich über alle Branchen und Unternehmen jeder Größe.

Dieser Grad der Vorbereitung erstreckt sich über alle Branchen und Unternehmen jeder Größe. Der Finanzdienstleistungssektor beispielsweise hat den höchsten Prozentsatz an SOECS-Teilnehmern mit einer formellen Cybersicherheitsstrategie, die sich auf das gesamte Unternehmen erstreckt (60 %). In der Medien- und Unterhaltungsbranche sind es dagegen nur 33 % - der niedrigste Wert unter den an der Umfrage beteiligten Branchen. Dennoch haben alle befragten Unternehmen in beiden Sektoren entweder eine formelle Cybersicherheitsstrategie oder eine Reihe von Best Practices eingeführt.

Konsistente Vorbereitung über das gesamte Unternehmensspektrum hinweg

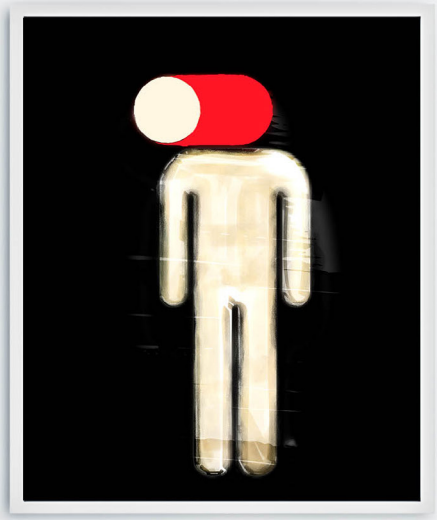
Auch bei Unternehmen verschiedener Größe ist der Unterschied in der Bereitschaft gering. Die größten Unternehmen mit mehr als 10.000 Mitarbeitern sind führend: 60% haben eine formelle Strategie für das gesamte Unternehmen eingeführt. Im Vergleich dazu waren es nur 43% der Unternehmen in der Größenordnung von 500 bis 1.000 Mitarbeitern. Aber die kleineren Unternehmen machten dies durch einen höheren Prozentsatz von Teilnehmern wett, die entweder eine IT-geführte Strategie oder Best Practices eingeführt haben.

Natürlich bedeutet dies nicht, dass die Cyberabwehr in Unternehmen vollständig ausgereift oder so robust ist, wie sie sein sollte. Wie im weiteren Verlauf dieses SOECS 2024-Berichts erläutert, weisen die Abwehrmaßnahmen vieler Unternehmen noch immer erhebliche und gefährliche Lücken auf, und viele Cybersicherheitsexperten sind nach wie vor frustriert über unzureichende finanzielle Mittel, mangelnde organisatorische Unterstützung und den Druck der Unternehmensleitung, die Ausgaben für Sicherheitstools auf die von Microsoft 365 bereitgestellten zu beschränken. Insbesondere viele menschliche Risikofaktoren - die heute die größte Lücke in der Cybersicherheit darstellen - bleiben unbehandelt und liegen außerhalb der Kontrolle von Cybersicherheitsexperten.

Doch trotz dieser Einschränkungen gibt es Grund zu beträchtlichem Optimismus, da ein Unternehmen nach dem anderen Schritte unternimmt, um die Cybersicherheit in seine täglichen Abläufe zu integrieren.

HUMAN RISK

Das menschliche Risiko ist heute die größte Lücke in der Cybersicherheit und wird oftmals zu wenig beachtet.

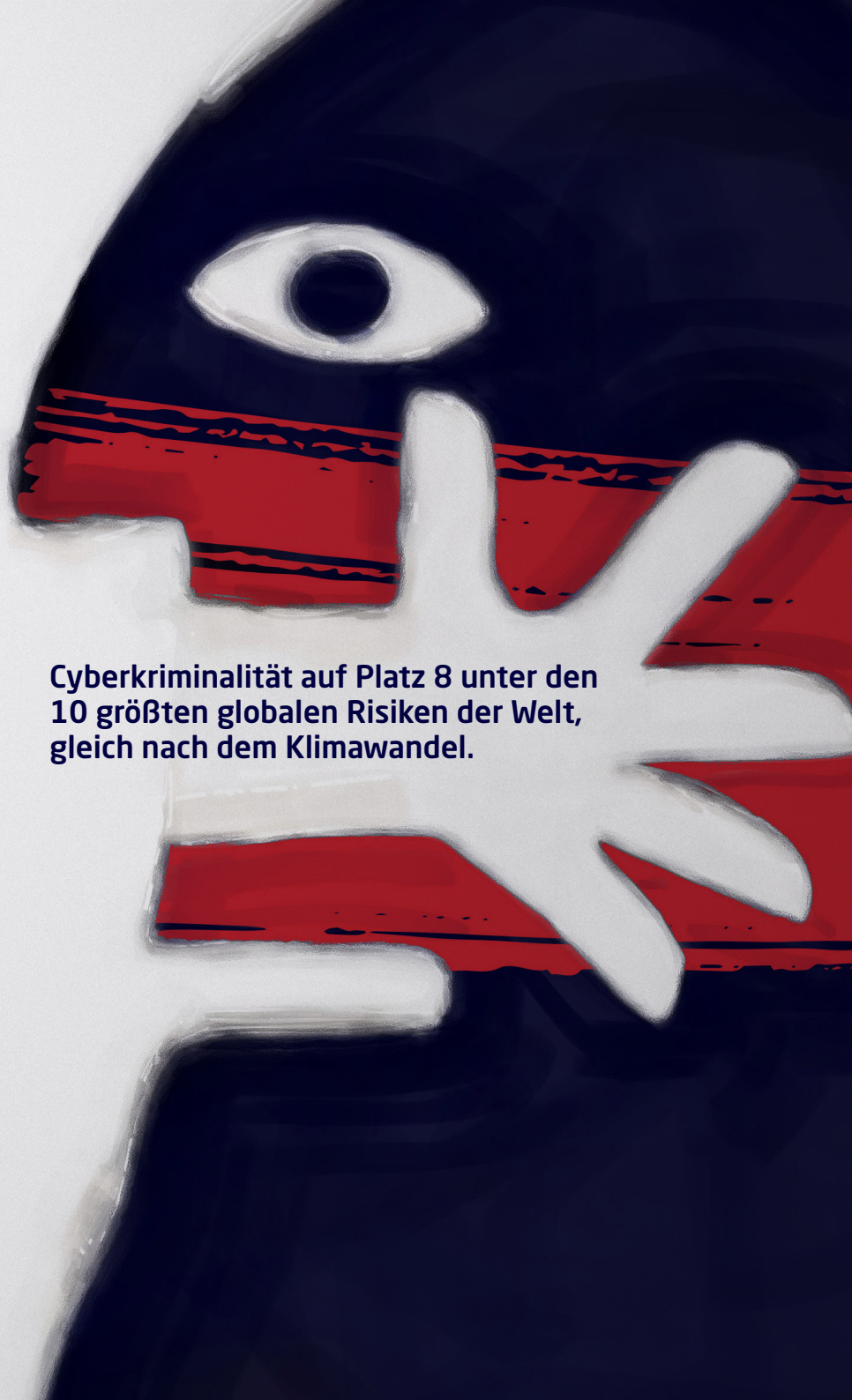


Teil II:

Cyber-Risiken an der Schnittstelle von Menschen, Kommunikation und Daten

Das Weltwirtschaftsforum (WEF) stuft die Cyberkriminalität jetzt auf Platz 8 der 10 größten globalen Risiken ein, gleich nach dem Klimawandel und vor der großen menschlichen Migration. Nach der Definition des WEF ist ein "globales Risiko... die Möglichkeit des Eintretens eines Ereignisses oder Zustands, das, wenn es eintritt, einen erheblichen Anteil des globalen BIP, der Bevölkerung oder der natürlichen Ressourcen negativ beeinflussen würde."

In der heutigen digitalen und stark vernetzten Wirtschaft muss sich jedes Unternehmen mit Cyberrisiken auseinandersetzen. Der Betrieb, der Ruf und die Einnahmen jedes Unternehmens, ob groß oder klein, sind durch eine Datenverletzung oder einen Systemeinbruch gefährdet - das ist inzwischen allgemein anerkannt. Laut einer Umfrage des Deloitte Center for Controllership erwartet fast die Hälfte (48,8 %) der Führungskräfte, dass die Anzahl und der Umfang von Cybervorfällen, die sich gegen die Buchhaltungs- und Finanzdaten ihres Unternehmens richten, im kommenden Jahr zunehmen werden."[2]



Cyberkriminalität auf Platz 8 unter den 10 größten globalen Risiken der Welt, gleich nach dem Klimawandel.

E-Mail [redacted]
[redacted]
bleibt [redacted]
der Angriffsvektor [redacted]
[redacted]
. Nummer 1 [redacted]
für Cyberkriminelle [redacted]
[redacted]

Das Ausmaß der Bedrohung durch das Internet ist erschreckend:

+15%

Es wird erwartet, dass die Cyberkriminalität in den nächsten zwei Jahren um 15% pro Jahr wachsen wird, von 7,3 Billionen Euro weltweit im Jahr 2023 auf 9,7 Billionen Euro im Jahr 2025. Das ist ein Anstieg von fast 3 Billionen Euro im Jahr 2025 und stellt den größten Vermögenstransfer in der Geschichte der Menschheit dar.[i][ii]

[i]"Cybersecurity Almanach 2023 ", Zeitschrift Cybercrime
[ii] "Cyberkriminalität wird die Welt bis 2025 jährlich 10,5 Billionen Dollar kosten", Cybercrime Magazine

1 MILLIARDE

Fast eine Milliarde E-Mails waren im Jahr 2023 Anrgiffen ausgesetzt,
damit ist einer von fünf Internetnutzern betroffen.
Im Jahr 2023 lag die Zahl der gestohlenen elektronischen Aufzeichnungen weltweit bei knapp sechs Milliarden.[i]

[i] "Liste der Datenschutzverletzungen und Cyberangriffe im Jahr 2023", IT Governance

4,1 MILLIONEN EURO

Weltweit belaufen sich die durchschnittlichen Kosten eines Datenschutzverstoßes jetzt auf 4,1 Millionen Euro, ein Anstieg um 15% in drei Jahren. Bei US-Unternehmen sind die durchschnittlichen Kosten mit 8,75 Millionen Euro pro Verstoß mehr als doppelt so hoch.[i]

[i] "Bericht über die Kosten einer Datenschutzverletzung 2023", IBM

PHISHING ANGRIFFE

Phishing-Angriffe bleiben die größte Bedrohung für E-Mail-Nutzer

E-Mail ist nach wie vor der wichtigste Angriffsvektor für Cyberkriminelle, und Phishing-Angriffe bleiben die größte Bedrohung für E-Mail-Nutzer.

Dies wird durch die SOECS 2024 Umfrage bestätigt, die ergab, dass das Volumen der E-Mail-basierten Phishing-, Spoofing- und Ransomware-Angriffe weiter zunimmt.[i]

[i] "E-Mail bleibt der wichtigste Angriffsvektor für Cyberkriminelle", Cybernews

Phishing

Im Jahr 2023 hat sich die Zahl der kompromittierten geschäftlichen E-Mails (BEC), eine besonders gefährliche Form von Phishing, fast verdoppelt, und Phishing bleibt zusammen mit gestohlenen Zugangsdaten und der Ausnutzung von Netzwerkschwachstellen einer der drei Hauptwege, auf denen Unternehmen gehackt werden.[i]

[i]Bericht "2023 Data Breach Investigations Report", Verizon

Einige Arten von Unternehmen sind davon viel stärker betroffen als andere. Während 39% der SOECS 2024-Befragten von einem Anstieg der Phishing-Aktivitäten berichteten, war der Prozentsatz in sechs der 12 in der Umfrage vertretenen Branchen deutlich höher. Dazu gehörten mehr als die Hälfte (54%) der Unternehmen im öffentlichen Sektor und fast die Hälfte (49%) der Unternehmen und Dienstleister, zu denen unter anderem Anwalts- und Wirtschaftsprüfungsfirmen gehören.

Insgesamt haben 41% der Teilnehmer der SOECS 2024 in den letzten 12 Monaten mehr E-Mail-Bedrohungen erlebt, und 38% sehen die zunehmende Raffinesse dieser Angriffe als ihre größte Herausforderung für die E-Mail-Sicherheit im Jahr 2024.

Spoofing

E-Mail-Spoofing, bei dem ein Betrüger versucht, den Anschein zu erwecken, dass eine E-Mail von einer vertrauenswürdigen Quelle stammt, breitet sich ebenfalls weiter aus. Mehr als ein Drittel (35 %) der Befragten der SOECS 2024 gaben an, dass die Zahl dieser Angriffe im vergangenen Jahr erneut zugenommen hat. Aber wie beim Phishing waren einige Branchen viel stärker betroffen als andere: Der Sektor der Unternehmens- und Berufsdienstleistungen hatte die zweifelhafte Ehre, dass die meisten Befragten (52%) einen Anstieg dieser Art von Angriffen meldeten.

Auch das Web-Spoofing, bei dem der Täter versucht, Unternehmen und ihre Kunden zu betrügen, indem er eine Website erstellt, die sich als die des Unternehmens ausgibt, ist weiterhin weit verbreitet. Fast alle (98%) der Teilnehmer der SOECS 2024 haben im vergangenen Jahr eine gefälschte Web-Domain entdeckt, wobei mehr als 60% diese Art von Betrug mehrfach aufgedeckt haben.

Ransomware

Die Art von E-Mail-Bedrohung, die sich am schnellsten ausbreitet und ihre Opfer am meisten kostet, ist jedoch mit Abstand Ransomware.

Im Jahr 2023 nahmen Ransomware-Angriffe im Vergleich zum Vorjahr um 95 % zu.[i] Gleichzeitig stiegen die durchschnittlichen Lösegeldzahlungen von 196.000 Euro im Jahr 2022 auf 683.000 Euro im Jahr 2023 - ein Anstieg um 250%.[ii]

[i] "Q3 Ransomware-Bericht", Corvus Insurance
[ii] "Durchschnittliche Höhe der Lösegeldzahlungen im Internet", Statista

Acht von zehn Befragten der SOECS 2024 sind im vergangenen Jahr Opfer von Ransomware geworden, und 3 von 4 dieser Opfer sahen sich gezwungen, das Lösegeld zu zahlen. Und während zwei Drittel dieser Lösegeldzahler ihre Daten erfolgreich wiederherstellen konnten, gelang dies dem restlichen Drittel nicht.

Bezeichnenderweise haben jedoch 23% der Ransomware-Opfer das Lösegeld nicht gezahlt, konnten aber dennoch ihre Daten wiederherstellen.

Die wichtigsten Erkenntnisse.

Strategie

9 VON 10
haben eine formelle Cybersicherheits-stratgie.

96%
von ihnen schreiben der Strategie sie Reduktion des Cybersicherheits-Risikos für ihre Organisation zu.

37%
sagen M365 reicht ohne zusätzliche Sicherheits-Tools nicht aus, um Malware zu blockieren.

75%
Unternehmen nutzen bereits oder sind dabei DMARC zur Abwehr von Spoofing-Angriffen einzuführen.

KI

80%
sind über neue Bedrohungen durch KI besorgt.

Mitarbeiter

3 VON 4
Befragten sagen, dass ihr Unternehmen durch unbeabsichtigte Datenlecks durch fahrlässige Mitarbeiter gefährdet ist...

aber nur

15%
der Unternehmen bieten ihren Mitarbeitern regelmäßig Schulungen zum Cyber-Bewusstsein an.

Collaboration

70%
der Befragten sagen, dass Collaboration-Tools eine neue Gefahr darstellen.

7 VON 10
befürchten die Folgen eines Collaboration-Tool-basierten Angriffs.

E-Mail

4 VON 10
sehen weiterhin einen Anstieg von E-Mail-basierten Bedrohungen.

Ransom

8 VON 10
waren schon Opfer eines Ransomware-Angriffs.

3 VON 4
haben das Lösegeld bezahlt.

67%
der Befragten sehen eine Cyberversicherung nicht mehr als ausreichendes Sicherheitsnetz an.

Unterstützung

97%
der Befragten geben an, dass ihr Vorstand und Führungskräfte ihre Cybersicherheits-Maßnahmen unterstützen.

67%

der Organisationen sagen, dass KI-gestützte Angriffe in den nächsten Monaten unvermeidbar werden.

86%

glauben, dass sie in der Lage sind, auf einen KI-Angriff zu reagieren.

KI-basierte Bedrohungen

Ein Hauptgrund für die beschleunigte Verbreitung von Phishing- und Ransomware ist das Aufkommen generativer KI, die es den Tätern erleichtert, erfolgreiche Angriffe zu verüben. Ein Tool wie ChatGPT kann beispielsweise dazu verwendet werden, E-Mails an einzelne Mitarbeiter zu generieren, die den Anschein erwecken, von ihrem Chef zu stammen und sich auf Firmenveranstaltungen oder persönliche Informationen beziehen.

8 von 10 Befragten sind besorgt über neue Bedrohungen durch KI. Daher sind 8 von 10 Befragten der SOECS 2024 besorgt über den Einsatz von KI zur Durchführung von Angriffen auf ihr Unternehmen, wobei fast 7 von 10 (67%) zugeben, dass KI-gesponserte Angriffe in den nächsten Monaten unvermeidlich sein werden. Im Gegensatz dazu glaubt die große Mehrheit (86%), dass sie in der Lage sein wird, auf einen KI-Angriff genauso schnell zu reagieren wie auf andere Angriffe. [MD1] [MD2]

[MD1]This is interesting

[MD2]Business are more worried about human risk to their cyber preparedness than the risk AI imposes

Faktoren die außerhalb der Kontrolle von Cybersecurity liegen

Es gibt noch weitere Probleme die die Cyberbereitschaft der Unternehmen bedrohen. Die Befragten sind weniger zuversichtlich, dass sie in der Lage sein werden, diese zu bewältigen.

Human Risk

Es gibt jedoch noch andere Probleme, die die Cyberbereitschaft ihrer Unternehmen bedrohen und von denen die SOECS 2024-Befragten weniger überzeugt sind, dass sie sie bewältigen können. Dabei handelt es sich um Faktoren, die außerhalb ihrer Kontrolle liegen und oft mit dem menschlichen Risiko zusammenhängen, z. B. die Fähigkeit der Mitarbeiter, Cyberbedrohungen zu erkennen und darauf zu reagieren (von 36 % der Befragten genannt), und die Frage, ob die Sicherheitsprotokolle für externe Mitarbeiter strikt durchgesetzt werden (ebenfalls von 36 % der Befragten genannt).

Collaboration-Tools

Ein wichtiges Anliegen, das 69% der Befragten angaben, ist die breite Palette an Collaboration-Tools, die in ihren Unternehmen eingesetzt werden. Diese Tools und ihr weit verbreiteter Einsatz sind zu einem wichtigen Streitpunkt für die Verantwortlichen für die Cybersicherheit ihrer Organisation geworden.

Teil III:

Collaboration-Tools und die wachsende Angriffsfläche

Auch wenn E-Mails nach wie vor der Hauptangriffsweg sind, machen sich böswillige Akteure auch die Möglichkeiten zunutze, die der Einsatz von Collaboration-Tools bietet, um die Angriffsfläche eines Unternehmens zu vergrößern.

Kaum ein Unternehmen kommt heute noch ohne Collaboration-Tools aus, die Kommunikation und Messaging mit Projektmanagementfunktionen verbinden. Die Software für die Zusammenarbeit wurde entwickelt, um eine zentrale Plattform für die gemeinsame Nutzung von Daten und Dokumenten bereitzustellen, und ist zur unabdingbaren Voraussetzung für die heutigen Remote- und Hybrid-Arbeitsumgebungen geworden.

.

Diese Tools, zu denen virtuelle Kommunikationsplattformen wie Zoom und Apps für die Teamarbeit wie Google Workspace, Slack und Microsoft Teams gehören, erfreuen sich immer größerer Beliebtheit. Von den SOECS 2024-Befragten haben 84% festgestellt, dass diese Tools in den letzten 12 Monaten weiter zugenommen haben, und ein noch höherer Prozentsatz (90%) ist der Meinung, dass sie für ihr Unternehmen und dessen tägliche Arbeit unerlässlich geworden sind.

Unzureichende Sicherheitsvorkehrungen

Aber diese IT- und Cybersicherheitsexperten sind auch äußerst besorgt darüber, dass die schnelle Verbreitung und die wachsende Abhängigkeit von kollaborativer Software diese zu einem zunehmend attraktiven Ziel für Kriminelle macht. Sieben von zehn (70 %) sagen, dass sie eine dringende neue Bedrohung darstellen, während eine fast identische Anzahl (69 %) es für wahrscheinlich, sehr wahrscheinlich oder sogar unvermeidlich hält, dass ihr Unternehmen durch einen auf Collaboration-Tools basierenden Angriff geschädigt wird.

Die Befragten der SOECS 2024 weisen auf eine Reihe von Faktoren hin, die die Situation verschärfen:

59%

Ein großes Problem ist, dass die Mitarbeiter routinemäßig neue Collaboration-Tools herunterladen und nutzen, die nicht von der IT-Abteilung geprüft wurden (59 % der Befragten).

69%

Infolgedessen geben 69% der Befragten an, dass sie mit der Anzahl der in ihrem Unternehmen verwendeten Collaboration-Tools überfordert sind.

61%

Außerdem sagen 61%, dass die meisten der von diesen Tools gebotenen nativen Sicherheitsfunktionen unzureichend sind.

56%

Und mehr als die Hälfte (56%) macht sich Sorgen, dass die Cyberabwehr ihres Unternehmens mit diesen neuen Bedrohungen nicht Schritt halten kann.

Als Reaktion darauf drängen die Cybersicherheitsexperten Unternehmen zu robusteren Verteidigungsmaßnahmen.

48%

sagen, dass ihre Unternehmen bereits zusätzliche Schichten von Schutzsoftware vor Angriffen durch Collaboration-Tools implementiert haben.

47%

unternehmen Schritte um mehr Sichtbarkeit und Kontrolle darüber zu haben, welche Tools Mitarbeiter nutzen und auch wie sie genutzt werden.

47%

bieten Collaboration-Tool-spezifische Sicherheits-Sensibilisierungsschulungen an, um den Mitarbeitern zu helfen angemessen auf potenzielle Bedrohungen zu reagieren.

37%

sagen, ihre Unternehmen würden sich nur auf die systemeigenen Sicherheitsvorkehrungen, die in der Collaboration-Software integriert sind, verlassen.

1%

geben zu, dass sie nichts tun um einen Collaboration-Tool-basierten Angriff zu verhindern.

Die Besorgnis über Collaboration-Tools spiegelt das aktuelle Yin und Yang der Cybersicherheit in Unternehmen wider. Denn obwohl sich die Abwehrmaßnahmen der Unternehmen in den letzten Jahren deutlich verbessert haben, gibt es immer wieder neue Cyber-Risiken, und es bestehen nach wie vor erhebliche Lücken in der Cyber-Vorbereitung.

Teil IV:

Geschützt arbeiten und Cyber-Risiken managen

Die meisten Unternehmen verfügen inzwischen über eine formelle Cybersicherheitsstrategie, und fast alle (96 %) sind der Meinung, dass diese ihr Cyberrisiko verringert hat. Durch die Brille von Menschen, Prozessen und Technologie betrachtet, war ein strategischerer Ansatz ein durchschlagender Erfolg.

Menschen:

99%

Nahezu alle Befragten der SOECS 2024 (99%) geben an, dass die Cybersicherheitspraktiken ihres Unternehmens Kunden, Mitarbeiter und Geschäftspartner effektiv schützen.

Prozess:

99%

Die Befragten sind sich auch fast einig (99%), dass ihre Cybersicherheitsmaßnahmen die Geschäfts- und Betriebsprozesse ihres Unternehmens schützen.

Technologie:

100%

Und sie stimmen zu 100 % darin überein, dass dieselben Richtlinien funktionieren, um ihre E-Mails, Collaborations-Tools und andere technologiebasierte Ressourcen zu schützen.

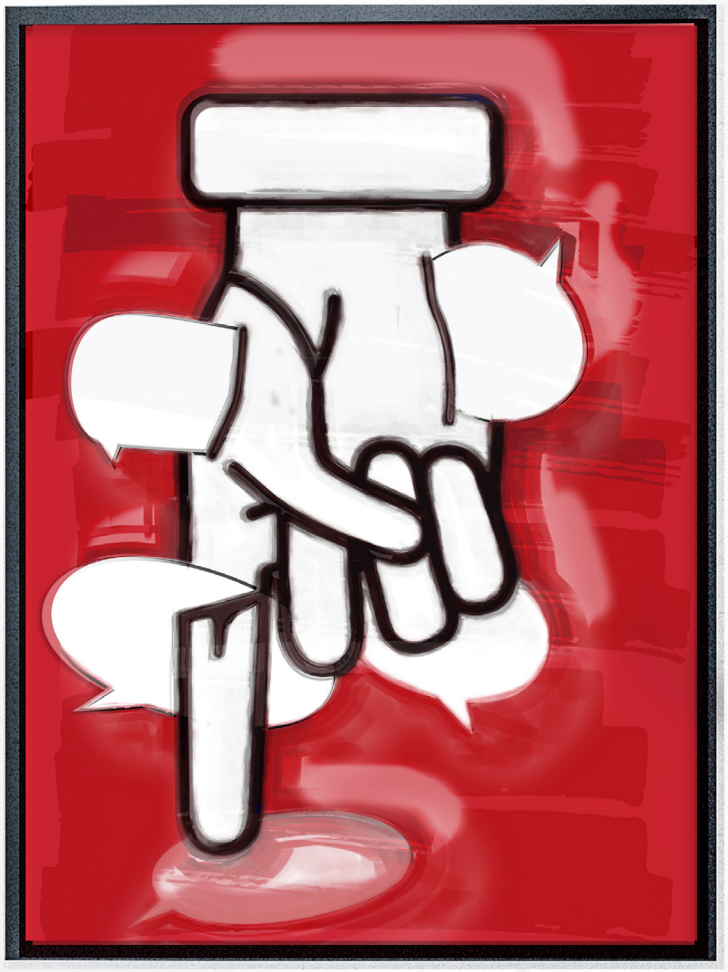
Diese Ergebnisse sind zwar erfreulich, werfen aber auch die Frage auf: Wenn die Cybersicherheitsstrategien all dieser Unternehmen so erfolgreich sind, warum wurden dann 2022 allein in den USA über 500 Millionen Phishing-Angriffe gemeldet?[i] Und warum haben Unternehmen weltweit in der ersten Hälfte des Jahres 2023 414 Millionen Euro Lösegeld für ihre Daten gezahlt?[ii]

[i] “Phishing-Statistiken nach Staat im Jahr 2024”, Forbes
[ii] “Krypto-Kriminalität Halbjahres-Update”, Chainalysis

Die Antwort ist natürlich, dass die Einführung umfassender Sicherheitsmaßnahmen das Cyberrisiko in vielen Unternehmen zwar gemindert, aber nicht annähernd beseitigt hat. Auf die Frage nach dem Grad des Schutzes, den die Cybersicherheitspraktiken ihrer Unternehmen bieten, gaben nur 7% der Befragten an, dass sie einen vollständigen Schutz bieten, während 92% zugaben, dass der Schutz unvollständig ist.

500 MIO.

Phishing-Angriffe in den USA gemeldet, allein im Jahr 2023.



Mehr Ressourcen erforderlich

97% der Befragten geben an, dass ihre Vorstände ihre Bemühungen um die Cybersicherheit unterstützen. Der Mangel an Ressourcen ist Teil des Problems. Positiv zu vermerken ist, dass die meisten Befragten (97%) angeben, dass ihre Vorstände und leitenden Angestellten ihre Bemühungen im Bereich der Cybersicherheit unterstützen, und die Mehrheit (57%) bezeichnet den Grad dieser Unterstützung als hoch. Gleichzeitig haben aber viele Befragte das Gefühl, dass ihre Bemühungen durch unzureichende Budgets und Einschränkungen bei der Verwendung dieser Gelder untergraben werden.

Die Befragten geben an, dass im Durchschnitt 9% des IT-Budgets ihres Unternehmens für die Cybersicherheit aufgewendet werden. In bestimmten Branchen wie dem Energiesektor, der nur 3% der IT-Ausgaben für die Sicherheit vorsieht, ist dieser Anteil noch viel geringer. Die Befragten hingegen glauben, dass der Durchschnitt von 9% um ein Drittel niedriger ist als er sein sollte. Sie wünschen sich, dass im Durchschnitt 12% des IT-Budgets ihres Unternehmens für die Vorbereitung auf Risiken aus dem Internet verwendet werden.

Zu den Folgen dieser unzureichenden Mittelverwendung gehören:

40%

Befragte sagen sie mussten Kompromisse eingehen, welche Sicherheits-Tools sie verwenden, um E-Mail- und Collaboration-Tool-basierte Bedrohungen überwachen zu können.

37%

sagen, sie seien nicht in der Lage auf Bedrohungen so schnell und effizient zu reagieren wie erforderlich wäre.

36%

sagen, dass die Nichtausschöpfung der Mittel zu erheblichen Löchern in der Verteidigung ihrer Organisationen geführt hat.

Gezwungenermaßen auf Microsoft 365 angewiesen

1 von 3 Befragten gibt an, dass die M365-Sicherheit allein keine Malware, Spam oder Phishing-Angriffe verhindern kann. Diese Ausgabenzwänge haben eine weitere gravierende Auswirkung. Um die Ausgaben einzudämmen, gibt mehr als ein Drittel der Befragten (35%) an, dass sie nicht in andere als die von Microsoft 365 angebotenen Cybersicherheitslösungen investieren können. Der Schutz, den die Microsoft-Software-Suite bietet, weist jedoch erhebliche Einschränkungen auf, was ihre Cyber-Vorbereitung untergraben hat.

Die Befragten weisen auf eine Reihe von Mängeln bei den Sicherheitsmaßnahmen von M365 hin. Der wichtigste von ihnen:

32%

begrenzte Fähigkeit über spezifische Vorfälle hinaus zu sehen und das Gesamtbild der Bedrohung zu erkennen.

30%

Versagen bei der Verhinderung, dass “zu viele Angriffe den Posteingang des Benutzers erreichen”.

30%

was es zu schwierig macht eine Zero-Trust-Politik umzusetzen.

Besonders bezeichnend ist, dass ein Drittel der Befragten angab, dass die systemeigenen Sicherheitsfunktionen von M365 allein, d.h. ohne den Einsatz zusätzlicher, nicht systemeigener Sicherheitstools, nicht in der Lage sind, Malware (37%), Spam (33%) oder Phishing-Angriffe (33%) zu verhindern. Fast ebenso viele (32%) gaben an, dass die M365-Sicherheitsanwendungen allein keine BEC- und Spoofing-Angriffe auf ihr Unternehmen abwehren können.

DMARC als Teil der Sicherheitsstrategie

Um Phishing-Angreifer und andere Betrüger daran zu hindern, ihre E-Mail-Domänen zu fälschen, machen Unternehmen DMARC zu einem Teil ihrer Cybersicherheitsstrategie.

Domain Message Authentication Reporting und Conformance ist ein Protokoll, mit dessen Hilfe festgestellt werden kann, ob eine E-Mail von der Domain gesendet wurde, mit der sie verknüpft ist. Dies macht es viel einfacher, E-Mails zu identifizieren und zu blockieren, die vorgeben, von einer Partei zu stammen, aber von einer anderen gesendet wurden. Die Implementierung von DMARC kann jedoch mühsam und zeitaufwändig sein, wes halb einige Unternehmen es nurzögerlich eingeführt haben.

Aber das war damals. Mittlerweile haben viele Unternehmen beschlossen, dass der größere Schutz, den DMARC bietet, die Mühe wert ist. So nutzen 94% der diesjährigen SOECS-Teilnehmer DMARC entweder bereits, sind dabei, es einzuführen oder planen, dies in den nächsten 12 Monaten zu tun - der höchste Prozentsatz, seit Mimecast die Umfrage 2016 erstmals durchgeführt hat.

Die wichtigsten Gründe für die Einführung von DMARC:

56%

um die E-Mail vertrauenswürdiger zu machen.

54%

Sicherstellung der Einhaltung der Industrie Vorschriften.

48%

der Schutz der Marke des Unternehmens (48%).

94%

der Teilnehmer nutzen DMARC entweder bereits, sind dabei, es einzuführen, oder planen dies in den nächsten 12 Monaten zu tun.

Die am häufigsten genannten Schwierigkeiten sind:

46%

Der Zeitaufwand für die Pflege und Verwaltung des Protokolls.

45%

Das Ausmaß, in dem es den Geschäftsbetrieb beeinträchtigen kann.

39%

Der Widerstand der Interessengruppen gegen die Verwendung des Protokolls.

Das menschliche Risiko ist heute die größte Lücke in der Cybersicherheit, und dies kommt im SOECS 2024 Bericht deutlich zum Ausdruck: Mehr als zwei Drittel der Befragten glauben, dass Mitarbeiter das Unternehmen durch den Missbrauch von E-Mails, die übermäßige Weitergabe von Unternehmensinformationen in sozialen Medien und unvorsichtiges Surfen im Internet gefährden.

In bestimmten Sektoren wie dem öffentlichen Sektor ist die Besorgnis sogar noch größer. Dort befürchten fast 9 von 10 Befragten (87%), dass der E-Mail- und Social-Media-Missbrauch ihrer Mitarbeiter ihrer Institution schadet.

74%

der Cybersicherheitslücken sind in menschlichem Versagen begründet.

Trotz dieser Befürchtungen gibt nur etwas mehr als die Hälfte der Befragten an, dass ihr Unternehmen monatliche oder fortlaufende Schulungen zum Thema Cybersicherheit anbietet. Dieser Anteil ist im Vergleich zum Vorjahr leicht rückläufig (52% gegenüber 54%).

Sicherheits-Experten sind seit langem der Meinung, dass Schulungen zum Sicherheitsbewusstsein nur dann effektiv sind, wenn sie konsequent, regelmäßig und in kleinen Dosen durchgeführt werden und auf die einzelnen Mitarbeiter zugeschnitten sind. Um die Lücke zu schließen und die Risikofaktoren, die von ihren Mitarbeitern ausgehen, signifikant zu reduzieren, wird jedoch zunehmend anerkannt, dass Unternehmen über eine Einheitsschulung hinausgehen müssen, die zwar die Einhaltung der Vorschriften überprüft, aber wenig zur Verringerung des Mitarbeiterrisikos beiträgt.

54%

sagen, dass ihre Organisation monatliche oder kontinuierliche Schulungen zum Thema Cybersicherheit anbieten.

Ausgehend von der Erkenntnis, dass 8% der Benutzer eines Unternehmens für 80 % der Sicherheitsvorfälle verantwortlich sind, entstehen immer effektivere Arten von adaptiven Schulungen.[i] Diese Trainingsprogramme beginnen mit der Bestimmung des Risikoniveaus, das die verschiedenen Mitarbeiter darstellen, und bieten dann - konzentriert auf die Mitarbeiter mit dem risikoreichsten Verhalten - ein individuelles Training, um diese Verhaltensweisen zu korrigieren.

[i] “8% Ihrer Benutzer verursachen 80% Ihrer Sicherheitsvorfälle”, Elevate Security

Die SOECS 2024 Befragten sind noch nicht so weit. Aber ihr ausgeprägtes Bewusstsein für menschliche Risiken und deren Auswirkungen auf Cyber-Risiken lässt vermuten, dass sie in Zukunft verstärkt darauf drängen werden, dass ihre Organisationen adaptive Schulungsmethoden einsetzen.

Teil V:

Cyber-Versicherung versus Cyber-Vorsorge

Da die Unternehmen ihre Bemühungen um Cyber-Vorsorge verstärkt haben, sind sie weniger abhängig von ihren Cyber-Versicherungspolicen.

Die Unternehmen lassen ihre Versicherungen keineswegs fallen: 95 % der SOECS 2024-Teilnehmer haben mindestens eine Police und 45% haben mehr als eine. Es wird jedoch immer unwahrscheinlicher, dass sie diese Policen als Ersatz für eine Kultur der Cyber-Resilienz betrachten.

2/3

sehen die Cyber-Versicherung nicht mehr als ein umfassendes Sicherheitsnetz.

2 von 3 Befragten sehen die Cyberversicherung nicht mehr als umfassendes Sicherheitsnetz an.
Auf die Frage, ob ihr Unternehmen eine Cyber-Versicherung als umfassendes Sicherheitsnetz zur Bewältigung von Cyber-Bedrohungen ansieht, antworteten beispielsweise knapp zwei Drittel der Befragten (65%), dass sie dies nicht tun. Im vergangenen Jahr waren nur 50% dieser Meinung.

Auch auf die Frage, ob ihr Unternehmen aufgrund der Einschränkungen, die die Versicherer diesen Policen auferlegen, weniger wahrscheinlich auf eine Cyberversicherung zurückgreifen wird, stimmten zwei Drittel (66%) zu, verglichen mit 52% im Jahr 2023.

Darüber hinaus gaben fast 9 von 10 Befragten (86%) an, dass sie der Meinung sind, dass ihr Unternehmen dies durch höhere Investitionen in die eigene Cyberabwehr kompensieren muss, da das Vertrauen in die Sicherheit sinkt.
Auf die Frage, wo diese Investitionen am ehesten getätigt werden sollten, nannten die Befragten als die drei wichtigsten Kategorien eine höhere E-Mail-Sicherheit (45%), eine höhere Sicherheit von Collaboration-Tools (44%) und eine stärkere Nutzung von KI für Cybersicherheitsanwendungen (41%).

Auch wenn der Versicherungsschutz gegen Cyberangriffe immer noch wichtig ist, erkennen Unternehmen aller Größen und Branchen, dass ihre eigene Cyberresilienz wichtiger ist.

Teil VI:

Die 10 wichtigsten Erkenntnisse

.01

Die meisten Cyberrisiken sind auf menschliches Versagen zurückzuführen.

Unabhängig davon, welche Prozesse und Technologien eingesetzt werden, hängt eine starke Cybersicherheit in erster Linie vom Verhalten der Menschen ab. Aber das menschliche Risiko stellt in den meisten Unternehmen eine große Sicherheitslücke dar. Um diese Lücke zu schließen, müssen Unternehmen adaptivere Formen der Cyber-Awareness-Schulung einführen, die es ihnen ermöglichen, zu erkennen, welche Mitarbeiter sich am risikoreichsten verhalten, und dann individuelles Training anbieten, um diese Verhaltensweisen zu verändern.

.02

Die Bedrohung steckt in der E-Mail.

E-Mail ist nach wie vor der Hauptangriffsvektor für die größten Cyber-Bedrohungen, denen die meisten Unternehmen ausgesetzt sind - Phishing, Spoofing und Ransomware. Mit anderen Worten: Es gibt keine Cybersicherheit ohne starke E-Mail-Sicherheit. Und robuste E-Mail-Sicherheit hängt von einem mehrschichtigen Schutz ab, der immer raffinierteren Angriffen standhalten kann.

.03

Phishing fängt Menschen ein.

Phishing-Angriffe sind allgegenwärtig und nehmen rapide zu. Das Problem beim Phishing ist, dass es nur funktioniert, wenn die Leute darauf hereinfallen. Der richtige E-Mail-Schutz ist ein wichtiges Hilfsmittel, um die Bedrohung einzudämmen - aber in erster Linie müssen die Mitarbeiter auf die Gefahr aufmerksam gemacht und geschult werden, sie zu vermeiden.

.04

Collaboration-Tools sind ein zweischneidiges Schwert.

Die E-Mail mag zwar der Hauptangriffsweg sein, aber die wachsende Zahl von Collaboration-Tools bietet Cyberkriminellen neue und gefährliche Möglichkeiten. Zwar können nur wenige Unternehmen in der heutigen globalen Arbeitsumgebung arbeiten, ohne sich auf diese Tools zu verlassen, aber sie müssen dringend die neuen Bedrohungen berücksichtigen, die sie darstellen.

.05

DMARC besiegt Spoofing.

DMARC ist nicht das am einfachsten zu verwaltende Protokoll, aber es ist äußerst wirksam gegen E-Mail-Spoofing, das sich immer weiter ausbreitet. Die wenigen Unternehmen, die sich noch nicht damit befasst haben, müssen sich dem Programm nun auch anschließen. Die Implementierung von DMARC ist zwar aufwändig, aber wenn ein Unternehmen wiederholt gespoofed wird, weil es dies versäumt hat, sind die Konsequenzen nicht unerheblich.

.06

Die Microsoft 365-Konsolidierung ist nicht alles.

Der Versuch, zu sparen, indem man die Ausgaben für Cybersicherheit auf die in M365 enthaltenen Tools beschränkt, ist eine Gradwanderung. Microsofts Schutzmaßnahmen sind für sich genommen einfach nicht effektiv genug. Sie müssen mit anderen Sicherheitstools ergänzt werden, um einen angemessenen Grad an Cyber-Vorsorge zu erreichen.

.07

Die KI-Bedrohung ist im Anmarsch.

Die Befragten des SOCES 2024 sehen die zunehmende Raffinesse der heutigen E-Mail-basierten Angriffe bereits als ihre größte Herausforderung für die Cybersicherheit an. Doch schon bald wird die weithin erwartete Verbreitung von KI-generierten Bedrohungen die Gefahr verstärken. Unternehmen müssen Feuer mit Feuer bekämpfen, indem sie ihre Investitionen in KI-gesteuerte Tools zur Erkennung und Abwehr von Bedrohungen erhöhen.

.08

Cyber-Bereitschaft reduziert Cyber-Risiken.

9 von 10 Unternehmen verfügen inzwischen über eine formelle Cybersicherheitsstrategie, und 96% von ihnen sind der Meinung, dass dies ihre Fähigkeit, ihre Mitarbeiter, Prozesse und Technologien zu schützen, erheblich verbessert hat. Die meisten leitenden Angestellten und Vorstandsmitglieder haben dies erkannt und setzen sich nun aktiv für eine bessere Vorbereitung auf Gefahren aus dem Internet ein.

.09

Eine Cyber-Versicherung ist nicht gleichbedeutend mit Cyber-Vorsorge.

Die meisten Unternehmen erkennen inzwischen diese grundlegende Wahrheit: Eine Cyber-Versicherungspolice ist kein Ersatz für den eigenen Cyber-Vorsorgeplan eines Unternehmens. Es mag zwar 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 die eigene Cybersicherheit eines Unternehmens leisten.

.10

Ressourcen für die Cybersicherheit.

Wo die heutigen Strategien für die Cybervorsorge versagen, ist die Art und Weise, wie sie umgesetzt werden. Zu viele Vorstände und leitende Angestellte unterstützen diese Bemühungen aktiv und versäumen es dann, sie mit ausreichenden Ressourcen zu unterstützen. Aber die Cybervorsorge ist wie ein Lebewesen: Um in einer immer tückischeren Umgebung zu überleben und zu gedeihen, muss sie ständig gepflegt und gefüttert werden.

Das Endergebnis

Der globale Sturm der Cyber-Bedrohungen nimmt weiter zu. Unternehmen aller Größen und Branchen sind sich der Gefahr dieser Cyber-Belagerung ihrer Mitarbeiter bewusster als je zuvor und unternehmen erhebliche Schritte, um ihr zu begegnen. Trotzdem müssen sie ihr Spiel in Zukunft verbessern. Neue Quellen von Bedrohungen und KI-gesteuerte Angriffe werden die ohnehin schon unruhigen Gewässer weiter aufwirbeln. Glücklicherweise gibt es auch neue Sicherheitstools und Schulungsmethoden, wie z.B. adaptives Training, die dazu beitragen, Menschen und ihre Arbeit zu schützen.

Über die in diesem Bericht enthaltenen Umfrageergebnisse

Der Bericht Stand der E-Mail-& Collaboration-Sicherheit 2024 basiert auf einer eingehenden globalen Umfrage unter 1.100 Fachleuten aus den Bereichen Informationstechnologie und Cybersicherheit. Mimecast beauftragte das in Großbritannien ansässige Forschungsunternehmen Vanson Bourne mit der Durchführung der Umfrage, die im Oktober und November 2023 stattfand. Die Umfrageteilnehmer kamen aus sechs Ländern, darunter die USA (27% der Gesamtteilnehmer), Großbritannien (18%), Frankreich (18%), Deutschland (9%), Südafrika (9%) und Australien (18%).

Die Teilnehmer an der Umfrage arbeiteten in Unternehmen mit 250 bis 500 Mitarbeitern (9% der Gesamtheit) bis zu mehr als 10.000 Mitarbeitern (8% der Gesamtheit). Diese Unternehmen verteilten sich auf 12 Branchen, darunter Informationstechnologie und Telekommunikation (15%), Einzelhandel (14%), verarbeitendes Gewerbe (12%), Unternehmens- und freiberufliche Dienstleistungen (12%), Finanzdienstleistungen (11%), Gesundheitswesen (10%), Energie (6%), Medien und Unterhaltung (5%), öffentlicher Sektor (5%), Baugewerbe und Immobilien (3%), Verbraucherdienstleistungen (2%) und sonstige gewerbliche Unternehmen (4%).

Unter den Teilnehmern waren 78% CIOs, CTOs, CISOs, IT-Direktoren und IT-Sicherheitsdirektoren. Der Rest waren IT- und SOC-Manager sowie Sicherheitsarchitekten und -analysten.

WORK PROTECTED.™

mimecast®

1. “The Global Risks Report 2023,” Weltwirtschaftsforum
2. “Fast die Hälfte der Führungskräfte erwartet für das kommende Jahr eine Zunahme von Cyber-Ereignissen, die auf Buchhaltungs- und Finanzdaten abzielen” Deloitte
3. “2023 Cybersecurity Almanac,” Zeitschrift Cybercrime
4. “Cybercrime to Cost the World $10.5 Trillion Annually by 2025,” Cybercrime Magazine
5. “Bericht über die Kosten einer Datenschutzverletzung 2023,” IBM
6. “Liste der Datenschutzverletzungen und Cyberangriffe im Jahr 2023,” IT Governance
7. “Globaler Bedrohungsbericht,” Mimecast
8. “Bericht “2023 Data Breach Investigations Report” Verizon
9. “E-Mail bleibt der wichtigste Angriffsvektor für Cyberkriminelle,” Cybernews
10. “Bericht “2023 Data Breach Investigations Report,” Verizon
11. “Q3 Ransomware-Bericht” Corvus Insurance
12. ”Durchschnittliche Höhe der Lösegeldzahlungen im Internet” Statista
13. “Phishing-Statistiken nach Staat im Jahr 2024” Forbes
14. ”Krypto-Kriminalität Halbjahres-Update” Chainalysis
15. “Bericht “2023 Data Breach Investigations Report” Verizon
16. “8% Ihrer Benutzer verursachen 80% Ihrer Sicherheitsvorfälle,” Elevate Security

Mimecast: Work Protected™

Seit 2003 unterstützen Mimecast-Lösungen Unternehmen dabei, ihre digitale Arbeitsumgebung zu sichern und vor Cyber-Bedrohungen zu schützen. Wir helfen mehr als 42.000 Kunden dabei, Cyberrisiken zu minimieren und eine zunehmend komplexe Bedrohungslandschaft zu bewältigen, die von immer professionelleren Cyberangriffen geprägt ist und keine menschlichen oder technologischen Fehler verzeiht. Unsere fortschrittlichen, KI-unterstützten Lösungen bieten die proaktive Erkennung und Priorisierung von Bedrohungen, E-Mail Archivierung, das Scannen von Links und QR-Codes, Lösungen für Markenschutz und Awareness Training und alles, was moderne Arbeitsplätze sonst benötigen. Mimecast bringt E-Mail- und Collaboration-Sicherheit auf das nächste Level.