mimecast

Sicherheit bei der Zusammenarbeit

Risiken und Realitäten der modernen Arbeitsoberfläche

Globale Umfrage zeigt, dass die Komplexität der Sicherung von IT-Umgebungen angesichts der raschen Einführung von Collaboration-Tools gestiegen ist.

13:20 ✓✓

Einführung.

Der kontinuierliche Anstieg der Nutzung von Collaboration-Tools bietet Cyberkriminellen eine neue Angriffsfläche.

Da Cyber-Bedrohungen immer ausgefeilter und umfangreicher werden, konzentrieren sie sich auf Plattformen, die für Cyber-Kriminelle unwiderstehlich sind. Diese Plattformen, wie Microsoft 365, erhöhen die Anfälligkeit von Unternehmen für Angriffe. Der Grund - und weniger die Lösung - ist einfach: Die zunehmende Online-Zusammenarbeit zwischen Mitarbeitern und die Konsolidierung von E-Mail- und Collaboration-Tools haben ein Umfeld für Cyberkriminelle geschaffen, das nur einen einzigen Einstiegspunkt benötigt, um potenziell verheerende Auswirkungen zu haben.

In der modernen Arbeitswelt können nur wenige Organisationen ohne den Einsatz von E-Mail- und Collaboration-Tools funktionieren. Software-Suites und ihre Add-Ons wie Microsoft Teams, Google Workspace und Slack integrieren Kommunikation und Messaging mit Projektmanagementfunktionen. Die Software für die Zusammenarbeit wurde entwickelt, um eine zentrale Plattform für die gemeinsame Nutzung von Daten und Dokumenten zu bieten. Sie hilft Unternehmen, die virtuelle Teamarbeit zu fördern und die Arbeit in den heutigen Remote- und Hybrid-Arbeitsumgebungen effizienter zu gestalten.

Während E-Mails nach wie vor der Hauptangriffsweg für Cyberkriminelle sind, bietet die zunehmende Nutzung von Collaboration-Tools eine neue Angriffsfläche für Cyberkriminelle, die sie infiltrieren wollen. Der Gartner™ Market Guide for Email Security stellt fest, dass “obwohl E-Mail immer noch der häufigste Angriffsvektor ist, viele Angreifer E-Mails nutzen, um die Kommunikation zu beginnen und sie dann zu Slack, Teams oder anderen Kollaborationsplattformen weiterzuleiten.” Dadurch entstehen noch mehr Risiken, die die Sicherheitsverantwortlichen verwalten müssen, und noch mehr Sicherheitsbewusstsein von den Mitarbeitern verlangt wird.

Ein Ansturm von Angriffen, während sich die Angriffsfläche auf Collaboration-Tools und hybride Arbeitsumgebungen ausweitet, ist die neue Norm für Benutzer und Sicherheitsteams. Es ist geschäftskritisch geworden, Collaboration-Plattformen so schnell wie möglich zu sichern.

[1] Marktführer für E-Mail-Sicherheit, Ravisha Chugh, Peter Firstbrook, Franz Hinner, 13. Februar 2023

Tools für die Zusammenarbeit:

Ein gefährlicher Bedrohungsvektor

Mimecast hat eine Umfrage unter 600 Cybersecurity-Führungskräften und mehr als 3.000 Mitarbeitern in Auftrag gegeben, um deren Verständnis und Verhalten in Bezug auf die Sicherheit von Collaboration-Tools in ihren Unternehmen zu ermitteln. Die Umfrage ergab, dass die Bedrohung durch Angriffe über Collaboration-Tools trotz des Vertrauens der Verantwortlichen in ihre Cyber-Bereitschaft (74 %) nach wie vor immens ist und fast alle Unternehmen bereits Opfer einer Cyber-Bedrohung waren, die von diesen Tools ausging. Die Auswirkungen dieser Verstöße sind beträchtlich, einschließlich des Verlusts von Unternehmensdaten, Kunden, Reputation und erheblichen finanziellen Kosten, unabhängig von der Größe des Unternehmens, der Region oder der Branche.

94%

der befragten Unternehmen haben eine Bedrohung durch Collaboration-Tools erlebt.

Kleine Unternehmen sind im Vergleich zu Unternehmen anderer Größenordnungen am wenigsten zuversichtlich, was ihre Cyber-Bereitschaft anbelangt. Nur 66 Prozent der Befragten sind der Meinung, dass ihr Unternehmen sehr gut oder sehr gut vorbereitet ist, um mit Hilfe von Collaboration-Tools auf einen Verstoß gegen die Cybersicherheit zu reagieren.

Vierundneunzig Prozent der befragten Unternehmen haben bereits eine Bedrohung durch Collaboration-Tools erlebt. Ein geschädigter Ruf des Unternehmens ist eine drohende Gefahr, über die sich die Verantwortlichen für Cybersicherheit angesichts der Kompromittierung der Sicherheit von Collaboration-Tools Sorgen machen, die finanziellen Kosten dieser Angriffe auf Unternehmen können hoch sein. Die durchschnittlichen Gesamtkosten von Angriffen auf Unternehmen, die auf Collaboration-Tools basieren, beliefen sich im vergangenen Jahr auf über 523.722 Euro - darin enthalten sind Kosten für zusätzliche Sicherheitsmaßnahmen, zusätzliches Personal und die Wiederherstellung von Systemen.

Username

****

Gesamtkosten von Angriffen auf Unternehmen durch Collaboration-Tools

574.783 €

1 Million Euro

Sechzehn Prozent der Befragten schätzen die Gesamtkosten von Angriffen über Collaboration-Tools im vergangenen Jahr auf über 1 Million Euro. Diese Zahl steigt auf 30 Prozent in den USA und 18 Prozent im Vereinigten Königreich.

Ein kleiner, aber bedingter Hoffnungsschimmer ist, dass kleinere Unternehmen geringere Kosten durch Collaboration-Tool-basierte Angriffe zu tragen haben als größere Unternehmen - ein kleines Unternehmen hatte im vergangenen Jahr im Durchschnitt Gesamtkosten in Höhe von 374.104 €. Dies liegt wahrscheinlich daran, dass KMUs weniger Geld für Gegenmaßnahmen ausgeben können und dass sie weniger ins Visier von Cyberkriminellen geraten, da sie weniger Geld zur Verfügung haben.

Alle Unternehmen können jedoch die Kosten von Angriffen auf Collaboration-Tools verringern, indem sie Schulungen zum Sicherheitsbewusstsein durchführen oder verstärken. Wenn sichergestellt wird, dass die Benutzer kontinuierlich und effektiv im sicheren Umgang mit Collaboration-Tools geschult werden, kann dies dazu beitragen, den Erfolg von Angriffen zu verringern, so dass weniger Zeit, Ressourcen und Geld für die Beseitigung erfolgreicher Cyberangriffe aufgewendet werden müssen, die über Collaboration-Tools in das Unternehmen eingedrungen sind.

Eine Lücke in der Wahrnehmung von Sensibilisierungs-schulungen:

Cybersecurity-Führungskräfte vs. Mitarbeiter

Angesichts der Geschwindigkeit, mit der Unternehmen begonnen haben, Collaboration-Plattformen als wichtige Geschäftsfunktion zu nutzen, sind spezielle Schulungen für Mitarbeiter auf der Strecke geblieben. Die Sicherheitsteams und die Verantwortlichen für Cybersicherheit in diesen Unternehmen glauben, dass sie ihre Mitarbeiter ausreichend Collaboration-Tools schulen.

85% **38%**

Ganze 85%t der Cybersecurity-Führungskräfte sind der Meinung, dass ihr Unternehmen seine Mitarbeiter effektiv über die Sicherheitsschwachstellen von Collaboration-Tools informiert hat, aber 38% der Mitarbeiter geben an, dass sie keinerlei Sicherheitsschulung für Collaboration-Tools erhalten haben.

Führungskräfte.

Cybersecurity-Führungskräfte geben an, Sicherheitsschulungen für Collaboration-Tools durchzuführen, wobei die überwiegende Mehrheit der Meinung ist, dass sie den Mitarbeitern die Risiken und die besten Praktiken effektiv vermitteln.

100%

Tatsächlich geben 100 Prozent der Befragten an, dass ihr Unternehmen in irgendeiner Form Cybersecurity-Schulungen für Collaboration-Tools durchführt, wobei 70 Prozent behaupten, dies monatlich oder vierteljährlich zu tun.

85%

85 Prozent der Befragten geben an, dass ihr Unternehmen seine Mitarbeiter effektiv über die Risiken und Möglichkeiten von Collaboration-Tools informiert hat.

Mitarbeiter.

Doch nur ein sehr kleiner Teil der Mitarbeiter ist der Meinung, dass sie eine spezielle Schulung zum Thema Collaboration Tools erhalten haben.

38%

Tatsächlich geben 38 Prozent an, dass sie keine Sicherheitsschulung für Collaboration-Tools erhalten haben, und nur 10 Prozent sagen, dass sie eine spezielle Sicherheitsschulung für Collaboration-Tools erhalten haben, die von der allgemeinen Cybersicherheitsschulung ihres Unternehmens getrennt ist.

31%

Einunddreißig Prozent haben eine Sicherheitsschulung für Kollaborationstools als Teil der allgemeinen Cybersicherheitsschulung ihres Unternehmens erhalten, und 21 Prozent haben diese als Teil des Einführungsprozesses erhalten.

+10%

Kleinere Unternehmen scheinen ihre Mitarbeiter viel weniger zu schulen als größere Organisationen, was ein viel größeres Cybersecurity-Risiko für diese Unternehmen darstellt. Ganze 48 Prozent der Mitarbeiter in kleinen Unternehmen geben an, keine Sicherheitsschulung für Collaboration-Tools erhalten zu haben, 10 Prozent mehr als in größeren Unternehmen.

Diese Ergebnisse zeigen, dass die Mitarbeiter in Bezug auf die Sicherheit von E-Mails viel umfassender geschult wurden als in Bezug auf die Sicherheit von Collaboration-Tools. Allerdings können die Sicherheitsverantwortlichen nicht davon ausgehen, dass die Mitarbeiter bei der Sicherheit von Collaboration-Tools die gleiche Strenge anwenden wie bei E-Mails.

Da die Nutzung von Collaboration-Tools immer weiter zunimmt, muss die Schulung zu Tools wie Microsoft Teams oder Slack ein klarer und gleichwertiger Teil der Sicherheitsschulung werden.

Mitarbeiter zeigen bei der Nutzung von Collaboration-Tools ein riskanteres Verhalten als bei der Nutzung von E-Mails. Es ist leicht anzunehmen, dass jede Person in einem Collaboration-Tool ein echtes Mitglied des Unternehmens ist, da es sich um eine geschlossene Umgebung zu handeln scheint, auch wenn sich Bedrohungsakteure, sobald sie über eine Plattform wie Microsoft 365 kompromittiert wurden, leicht als andere ausgeben können. So ist es zum Beispiel weniger wahrscheinlich, dass Mitarbeiter Dokumente, die über Collaboration-Tools versendet werden, überprüfen als solche, die per E-Mail verschickt werden. Und da Collaboration-Tools persönlicher erscheinen, ist die Wahrscheinlichkeit geringer, dass Mitarbeiter Anfragen, die sie über Collaboration-Tools erhalten, in Frage stellen, als Anfragen, die sie per E-Mail erhalten.

Ohne spezielle Schulung oder Überwachung von Collaboration-Tools ist es unwahrscheinlich, dass risikoreiches Verhalten von Mitarbeitern bei diesen Tools von den Sicherheitsteams bemerkt und verfolgt wird. Infolgedessen ist die Wahrscheinlichkeit geringer, dass Mitarbeiter für dieses riskante Verhalten gemaßregelt werden, was dazu führt, dass sie sich weniger verantwortlich für die Bedrohungen oder Verstöße fühlen, die in ihren Unternehmen stattfinden.

Da die Mitarbeiter nicht speziell geschult werden, sehen viele von ihnen Cybersecurity-Verstöße bei Collaboration-Tools nicht als etwas an, für das sie direkt verantwortlich sind. 30 %t sagen, dass sie sich nicht persönlich für einen Cyberangriff über ein Collaboration-Tool verantwortlich fühlen würden

Fast ein Drittel (30 %) gibt an, dass sie sich nicht persönlich verantwortlich fühlen würden, wenn ein Angriff über Collaboration-Tools erfolgen würde und ihr Gerät/Konto betroffen wäre - im Vergleich zu nur 18 Prozent der Führungskräfte im Bereich Cybersicherheit.

Mitarbeiter ...

30%

Führungskräfte ...

18%

Eine größere Gefahr:

Mitarbeiterverhalten bei Collaboration Tools vs. E-Mail

Die Mitarbeiter sind erstaunlich selbstbewusst, wenn es um die Nutzung von Tools für die geschäftliche Zusammenarbeit geht. Es besteht eine erhebliche Diskrepanz zwischen ihrem Verständnis der Sicherheit von Collaboration-Tools und ihrem spezifischen Verhalten bei der Nutzung von Collaboration-Tools. Während die meisten Mitarbeiter behaupten, die Bedrohung zu verstehen und ihr Verhalten in verschiedenen hybriden Umgebungen zu ändern, vergessen viele, selbst die grundlegendsten Sicherheitschecks durchzuführen.

E-Mail ...

91%

Bei der Arbeit mit E-Mails geben 91% der befragten Mitarbeiter an, dass sie prüfen, bevor sie auf einen Link klicken oder eine angehängte Datei öffnen.

Collaboration-Tools ...

79%

Bei der Arbeit mit Collaboration-Tools sinkt diese Zahl jedoch auf 79%.

Im Vergleich zu E-Mails sind die Mitarbeiter bei der Nutzung von Collaboration-Tools eher unvorsichtig - sie klicken auf Links und öffnen Anhänge. Die meisten Mitarbeiter (81%) geben an, die Sicherheitsrisiken und bewährten Praktiken zu kennen, die in hybriden und dezentralen Arbeitsumgebungen erforderlich sind - und geben an, ihr Verhalten entsprechend zu ändern (78%).

Ein weiterer Beleg für diese Selbstüberschätzung ist, dass 61 Prozent der Mitarbeiter angeben, ihr Verhalten zu ändern, wenn sie in einer hybriden Umgebung arbeiten, um sicherer zu sein (z. B. bei der Nutzung eines öffentlichen Wi-Fi-Netzwerks nach verschlüsselten Verbindungen zu suchen), und 65 Prozent geben an, dass sie seit der Pandemie vorsichtiger darauf achten, welche Links sie bei der Nutzung von Collaboration-Tools anklicken.

In der Praxis zeigt das Verhalten dieser Mitarbeiter, dass sie bei der Verwendung von Collaboration-Tools viel eher unvorsichtig sind als bei der Verwendung von E-Mails. Bevor sie auf Links und/oder Anhänge klicken, die sie über ein Kollaborationstool erhalten haben, überprüfen sie weniger häufig die Rechtschreibung der Quelle und die Legitimität der Dateinamen im Anhang oder der URLs/Hyperlinks, als wenn sie diese per E-Mail erhalten haben. So geben 91 Prozent der Befragten an, dass sie innerhalb von E-Mail-Anwendungen wie Microsoft 365 die Rechtschreibung, Links oder die E-Mail-Adresse des Absenders überprüfen, aber innerhalb eines Tools wie Microsoft Teams sinkt diese Zahl auf 79 Prozent. Anders ausgedrückt: 1 von 5 Angestellten überspringt alle Cybersecurity-Prüfungen, bevor sie auf eine private Nachricht in einem Business Collaboration Tool mit einem Link oder einem Anhang antworten.

Anders ausgedrückt: 1 von 5 Mitarbeitern überspringt alle Cybersecurity Überprüfungen im Collaboration-Tool, bevor er auf eine private Nachricht mit einem Link oder einem Anhang antwortet.

Mitarbeiter sind am meisten gefährdet, wenn sie eine Nachricht von ihrem Vorgesetzten oder über einen Teamgruppen-Chat/Kanal erhalten. Von den Befragten klicken 65 Prozent wahrscheinlich auf einen Link zu einer unbekannten Website oder Quelle, wenn sie ihn von ihrem Vorgesetzten erhalten, und 24 Prozent überprüfen in der Regel nichts, bevor sie auf Links und/oder Anhänge in einer Nachricht in einem Teamgruppen-Chat/Kanal in einem Tool für die geschäftliche Zusammenarbeit klicken.

1 von 5 Mitarbeitern klickt bei einer privaten Nachricht im Collaboration-Tool auf einen Link oder öffnet einen Anhang ohne ihn vorher zu überprüfen.

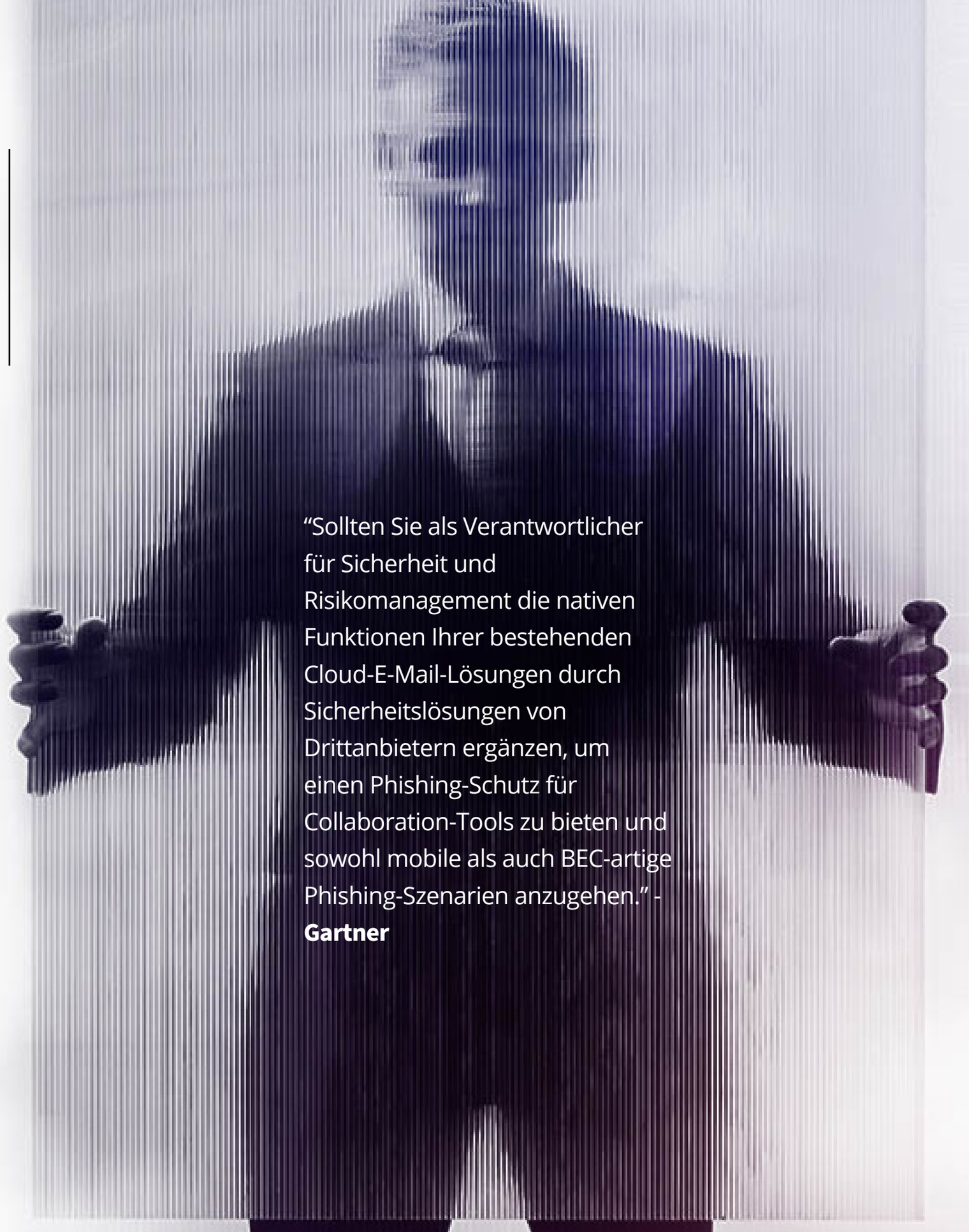
65 Prozent der Befragten klicken wahrscheinlich auf einen Link zu einer unbekannten Website oder Quelle, wenn sie ihn von ihrem Vorgesetzten erhalten

24% überprüfen in der Regel nichts, bevor sie auf Links und/oder Anhänge in einer Nachricht in einem Teamgruppen-Chat/Kanal klicken

Wichtige Erkenntnisse für Cyber-Führungskräfte

Collaboration-Tools können ein fruchtbarer Nährboden für Cyberkriminalität sein. Sie stellen eine enorme Bedrohung für Unternehmen auf der ganzen Welt dar - und die Auswirkungen der Angriffe gehen weit über die finanziellen Kosten hinaus.

Die von Mimecast durchgeführte Umfrage hat gezeigt, dass die Komplexität der Sicherung von IT-Umgebungen angesichts der raschen Einführung von Collaboration-Tools gestiegen ist. Es ist nicht nur eine technische Herausforderung, die benötigte Plattform so zu sichern, dass Cyberkriminelle nicht eindringen können, sondern auch eine kulturelle Herausforderung, das Bewusstsein und die Verantwortlichkeit im gesamten Unternehmen zu schaffen. Laut Gartners Market Guide für E-Mail Security.



“Sollten Sie als Verantwortlicher für Sicherheit und Risikomanagement die nativen Funktionen Ihrer bestehenden Cloud-E-Mail-Lösungen durch Sicherheitslösungen von Drittanbietern ergänzen, um einen Phishing-Schutz für Collaboration-Tools zu bieten und sowohl mobile als auch BEC-artige Phishing-Szenarien anzugehen.” - **Gartner**

Weitere wichtige Erkenntnisse sind:

Fehlende Schulungen sind eine der größten Hürden für Cyber-Führungskräfte.

Unternehmen bieten ihren Mitarbeitern nicht die speziellen Sicherheitsschulungen für Collaboration-Tools an, die sie zum Schutz ihres Unternehmens benötigen.

Organisationen brauchen ganzheitlichen Schutzmaßnahmen.

Schädliche URLs und Anhänge können Unternehmen den gleichen Schaden zufügen, unabhängig vom Kommunikationsmedium. Anstelle von unzusammenhängenden Sicherheitsrichtlinien für E-Mail und Collaboration-Tools wie Teams, müssen Führungskräfte ihre Organisationen mit ganzheitlichem Cybersecurity-Schutz für die gesamte Umgebung ausstatten.

Die Benutzer müssen bei Collaboration-Tools die gleichen guten Sicherheitsgewohnheiten an den Tag legen wie bei E-Mails.

Die Mitarbeiter sind sich der Auswirkungen von Collaboration-Tools auf die Sicherheit nicht vollständig bewusst: Sie sind nicht vorsichtig bei dem, was sie teilen oder anklicken, obwohl sie behaupten, die Cyber-Risiken und die besten Praktiken bei der Verwendung dieser Tools zu kennen, und obwohl sie die E-Mail-Sicherheit viel ernster nehmen.

Unternehmen überschätzen ihre Bereitschaft.

Die Verantwortlichen für Cybersicherheit überschätzen die Bereitschaft ihrer Unternehmen, Cyberkriminalität über Collaboration-Tools zu bekämpfen. Sie glauben, dass ihre Mitarbeiter gut geschult sind, um mit einer solchen Verletzung umzugehen, während die Mitarbeiter das Gefühl haben, dass sie keine spezielle Schulung erhalten haben.

Mitarbeiter fühlen sich nicht persönlich für die Sicherheit von Collaboration-Tools verantwortlich.

Fast ein Drittel (30%) der Mitarbeiter gibt an, dass sie sich nicht persönlich verantwortlich fühlen würden, wenn ein Angriff über Collaboration-Tools erfolgen würde und ihr Gerät/Konto betroffen wäre.

Mangelnde Überwachung kann gefährlich sein.

Die Verantwortlichen für Cybersicherheit überwachen die Nutzung dieser Tools durch ihre Mitarbeiter nicht und behandeln diesen Kommunikationskanal nicht als den Angriffsvektor, zu dem er werden kann.

collaboration ✕ tool ✕
security ✕ ist ✕ noch ✕
wichtiger ✕ als ✕
je zuvor ✕

Der Bedarf an gezielter und umfassender Sicherheit für Collaboration-Tools ist wichtiger denn je.

Hier kommt der fortschrittlichen E-Mail-Sicherheit eine entscheidende Rolle zu, denn sie bietet die Vorteile einer mehrschichtigen Sicherheit und schützt Unternehmen vor einem einzigen Angriffspunkt. Unternehmen müssen fortschrittliche E-Mail-Sicherheitslösungen suchen und implementieren, die erstklassigen Schutz vor den raffiniertesten Angriffen bieten und dazu beitragen können, dass Nachrichten und Anhänge nicht nur in E-Mails, sondern auch in Collaboration-Tools sicher sind, was bei Microsoft 365 nicht der Fall ist.

Über diese Umfrageergebnisse

Diese quantitative Studie konzentriert sich darauf, wie Mitarbeiter und Cybersecurity-Führungskräfte auf die zunehmende Nutzung von Collaboration-Tools am Arbeitsplatz reagieren. Sie analysiert die Gewohnheiten und das Verständnis für die Nutzung von E-Mail und Collaboration-Tools in einer hybriden Welt. Wir haben mit mehr als 3.000 Mitarbeitern und 600 Führungskräften im Bereich Cybersicherheit gesprochen, von denen 53% CISOs, CIOs und CTOs und 47% IT-Direktoren sind. Die Teilnehmer der Umfrage kommen aus Australien, Frankreich, Deutschland, Südafrika, Großbritannien und den USA. Die Befragten repräsentieren Branchen wie Finanzdienstleistungen, Unterhaltung, Gesundheitswesen, öffentlicher Sektor und Einzelhandel.

WORK PROTECTED.™
Advanced Email & Collaboration Security

mimecast