mimecast®

E-MAIL-SICHERHEIT 2018 – EIN LAGEBERICHT

Informationen zur aktuellen Bedrohungslage, zu fehleranfälligen Schutzmechanismen und zu menschlichem Versagen –und wie eine Cyber Resilience Strategie Sie vor Cyber Angriffen schützt.

LAGEBERICHT 2018

INHALT

KAPITEL EINS

KAPITEL ZWEI

FAZIT

UNSERE FEHLER **BEIM THEMA CYBER SECURITY**

Wir schreiben und empfangen permanent E-mails. Das E-Mail-Programm ist die wichtigste Anwendung, die Ihr Unternehmen und Ihre Kommunikation am Laufen hält und für nahtlose Produktivität sorgt. Unternehmen brauchen E-Mails, um jederzeit über alles Wichtige informiert zu sein. Schließlich sollen die E-Mails einfach nur funktionieren, mehr erwartet man gar nicht, richtig?

Hier beginnen oft schon die Schwierigkeiten, denn auch Cyberkriminelle greifen viel zu gern auf E-Mails zurück. Sie sind die wichtigste Waffe, um Malware-Angriffe (denken Sie nur an Ransomware), Identitätsmissbrauch und den Diebstahl von Zugangsdaten zu starten. Genau genommen haben über 90 % der globalen Unternehmen* in den letzten 12 Monaten einen Anstieg an Phishing-Angriffen verzeichnet. Und auch interne Bedrohungen sind auf dem Vormarsch: Die meisten Unternehmen waren im letzten Jahr solchen internen Gefahren ausgesetzt, sei es durch unvorsichtige Mitarbeiter (88 %), kompromittierte Konten (80 %) oder böswillige Insider (70 %).

90%

der globalen Unternehmen haben in den letzten 12 Monaten einen Anstieg an Phishing-Angriffen verzeichnet.

ANGREIFER ÜBERNEHMEN DIE FÜHRUNG

Cyberkriminelle aus der ganzen Welt greifen Unternehmen wie Ihres an. Es finden bedeutende Veränderungen statt, wie beispielsweise der Wechsel in die Cloud – was insbesondere für Unternehmen gilt, die ihre E-Mails in Massen auf Plattformen wie Microsoft Office 365™ migrieren. Da Unternehmen gleichzeitig Kosten senken, den Verwaltungsaufwand reduzieren und sich vor immer komplexeren E-Mail-basierten Bedrohungen schützen möchten, hat dieser neue Trend zur Folge, dass führende Unternehmen eine viel zu simple, lediglich auf Verteidigung ausgerichtete Sicherheitsstrategie implementieren. Das kann negative Konsequenzen mit sich bringen, die im Laufe der Zeit immer weitreichender werden.

Angreifer nutzen diese Änderungen ebenfalls und suchen in Echtzeit nach Lücken in Ihrem Sicherheitsprogramm.

*Globale Studie von Vanson Bourne, im Auftrag von Mimecast.

59%

aller Unternehmen werden in diesem Jahr mit negativen geschäftlichen Folgen aus einem E-Mail-basierten Angriff zu kämpfen haben.

Was passiert, wenn Sie aufgrund eines unerwünschten Ereignisses, das auf böswillige Absicht, menschliches oder technisches Versagen zurückzuführen ist, nicht auf Ihre E-Mails zugreifen können? Ihre Organisation könnte Reputationsschäden, interne betriebliche Probleme und finanzielle Verluste erleiden Möchten Sie dieses Risiko wirklich eingehen?

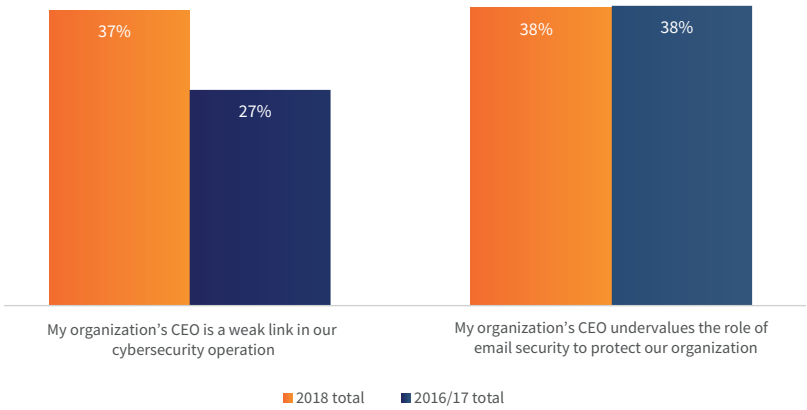
UNSERE FEHLER **BEIM THEMA CYBER SECURITY**

ES KOMMT AUF DIE RICHTIGE EINSTELLUNG AN. UND DIE BEGINNT AN DER SPITZE EINES UNTERNEHMENS.

E-Mails können ein leistungsstarkes Business-Tool sein. Doch wenn Ihre E-Mail-Lösung nicht Teil der grundlegenden Sicherheitsstrategie Ihres Unternehmens ist, können E-Mails schnell zur Sicherheitslücke werden. Wenn man Cyber Security zur Priorität macht, sollte man ganz oben anfangen. Das wird leider in vielen Fällen versäumt.

Fast 40 % der Befragten bestätigen, dass der CEO ein „schwaches Glied“ in der Kette der Cyber Security Strategie ihres Unternehmens ist. Dieser Eindruck hat sich seit dem vergangenen Jahr um fast 30 % verstärkt. Es ist sogar so, dass im letzten Jahr 31 % der Mitarbeiter aus Führungsebenen versehentlich sensible Daten an die falsche Person geschickt haben, wohingegen es bei den normalen Mitarbeitern nur 22 % waren. Und bei einem von fünf Unternehmen wurden in den letzten 12 Monaten sensible Daten per E-Mail von einem Mitglied aus der Führungsebene als Antwort auf eine Phishing-E-Mail geschickt.

Könnte es an der Spitze vieler Organisationen ein Einstellungsproblem geben? Vielleicht. Knapp 40 % der Befragten glauben, dass ihr CEO „die Bedeutung von E-Mail-Sicherheit als wichtigstes Element des Sicherheitsprogramms unterschätzt“.



Ist der CEO eine Schwachstelle in Ihrer Cyber Security Strategie?

UNSERE FEHLER **BEIM THEMA CYBER SECURITY**

SCHNELLE MASSNAHMEN:

MIT DIESEN SECHS SCHRITTEN KÖNNEN SIE DIE LÜCKE IN DER FÜHRUNGSEBENE SCHLIESSEN

1. Stellen Sie sicher, dass Personen mit Sicherheitskenntnissen im Vorstand vertreten sind.
2. Integrieren Sie die IT-Sicherheit in die Rolle, die dafür verantwortlich ist, die Risikominimierung im Unternehmen insgesamt zu verwalten.
3. Seien sie sich bewusst, dass die obere Führungsebene den Ton für die Unternehmenskultur vorgibt – und dass Sicherheitskultur ein Teil davon ist.
4. Vergleichen Sie Ihre Sicherheitskontrollen und Risikomanagementprogramme regelmäßig mit Peer-Organisationen.
5. Beteiligen Sie die zuständigen Aufsichtsbehörden konstruktiv an Ihrem Sicherheitsprogramm und halten Sie sich an deren spezifische Anforderungen.
6. Nutzen Sie Ihre Unternehmenskommunikation, um zu zeigen, dass IT-Sicherheit nicht nur ein IT-Problem ist.

UNSERE FEHLER **BEIM THEMA CYBER SECURITY**

FEHLENDE SCHULUNGEN MACHEN SIE ANGREIFBAR

Wann haben Sie zum letzten Mal eine Sicherheitsschulung für Ihre Mitarbeiter durchgeführt? Wenn Ihre Antwort „daran erinnere ich mich nicht mehr“ lautet, ist Ihr Unternehmen gefährdet. Doch das betrifft nicht nur Ihr Unternehmen Nur 11 % aller Unternehmen schulen Mitarbeiter regelmäßig, wie sie Cyber Angriffe erkennen können. 24 % geben an, monatliche Schulungen zu veranstalten, und 52 % führen Schulungen nur einmal jährlich durch.

Warum werden Sicherheitsschulungen generell nur so selten durchgeführt, vor allem, wenn knapp 40 % der Befragten das Gefühl haben, dass Mitarbeiterschulungen der beste Schutz vor Angriffen per E-Mail sind? Vielleicht liegt das an den 33 %, die Bedrohungen durch höhere Investitionen in Technologie den Kampf ansagen möchten, oder an den 29 %, die sich für optimierte Geschäftsprozesse entscheiden.

61%:

so viele Unternehmen waren Ziel von Angriffen, in denen bösartige Aktivitäten von einem infizierten Benutzer an andere Mitarbeiter übertragen wurden.

Bösartige Aktivitäten, die sich von Mitarbeiter zu Mitarbeiter verbreiten, kommen häufiger vor als man denkt. Fast 50 % aller Unternehmen berichten, dass bei ihnen schon einmal böswillige Aktivitäten durch infizierte E-Mail-Anhänge aufgetreten sind, wobei intern verschickte, schädliche URLs bei mehr als einem Viertel der Angriffe die Ursache waren.

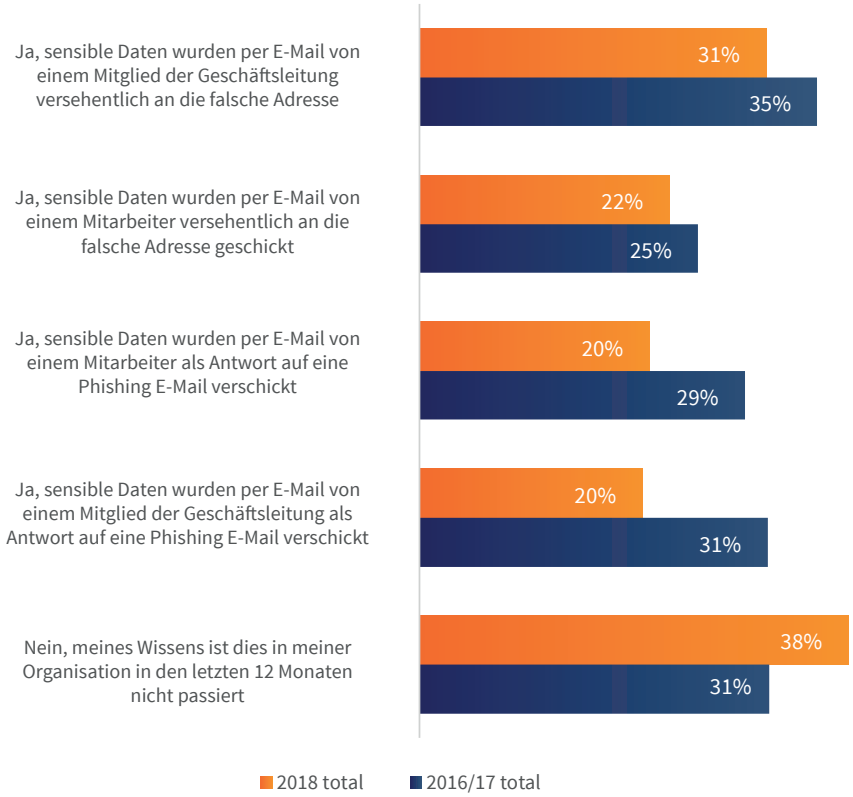
IM DETAIL: IDENTITÄTSDIEBSTAHL

Durch E-Mails verursachter Identitätsdiebstahl hat sich als großes Problem für Unternehmen und einzelne Mitarbeiter gleichermaßen erwiesen. **40 % der befragten Unternehmen haben in den letzten 12 Monaten einen Anstieg an Fällen von Identitätsmissbrauch festgestellt, wobei um die Überweisung von Geld gebeten wurde. Bei 39 % der Unternehmen haben unrechtmäßige Anfragen nach vertraulichen Daten zugenommen.**

JEDER KANN ZUM ZIEL WERDEN

Angreifer wenden Social-Engineering-Taktiken an und haben gelernt, sich auf bestimmte Personen in einem Unternehmen zu konzentrieren – und zwar auf diejenigen mit direktem Zugriff auf vertrauliche bzw. finanzielle Informationen. Fast 40 % aller Unternehmen verzeichneten im letzten Jahr Identitätsdiebstahl von Personen im Finanz-/Buchhaltungsbereich. 28 % geben an, dass die Führungsebene häufig Ziel von Identitätsdiebstahl ist und bei 25 % wurde die Identität von Mitarbeitern aus der Personalabteilung erschlichen.

Obwohl Identitätsdiebstahl in der Regel auf Menschen innerhalb desselben Unternehmens abzielt, hat sich das Problem mittlerweile auch auf andere Szenarien ausgedehnt: In 31 % der Unternehmen wurde im letzten Jahr Identitätsdiebstahl bei „vertrauenswürdigen“ Drittanbietern oder Partnern festgestellt. 19 % geben sogar an, dass Drittanbieter – im Gegensatz zu den Mitarbeitern ihres eigenen Unternehmens – innerhalb desselben Zeitraums häufiger Ziel von Identitätsdiebstahl waren.



Haben Sie schon mal sensible Daten per E-Mail an die falsche Person geschickt?

IM DETAIL: **IDENTITÄTSDIEBSTAHL**

SIND IHRE MITARBEITER IM STANDE BETRUGSVERSUCHE ZU ERKENNEN?

Um Identitätsdiebstahl zu verhindern, ist die Sensibilisierung und Schulung von Mitarbeitern das Wichtigste. Aber Unternehmen scheitern an diesem entscheidenden Schritt. **49 % der Unternehmen geben zu, dass ihre Management- und Finanzteams nicht über das notwendige Wissen verfügen, um einen Identitätsdiebstahlversuch zu erkennen und zu stoppen.** Und 40 % sind sich nicht sicher, ob ihr CEO vor Identitätsdiebstahl geschützt ist. Weniger als ein Viertel der Unternehmen vertrauen darauf, dass ihre Mitarbeiter eine E-Mail von jemandem, der sich als die falsche Person ausgibt und nach vertraulichen Daten oder Überweisungen fragt, erkennen können.

Ohne ständige, unternehmensweite Sicherheitsschulungen und Investitionen in die richtige Technologie wird Identitätsdiebstahl immer mehr zu Realität – und die Folgen werden teuer für Sie.

20%

haben durch Identitätsdiebstahl Verluste erlitten.

Bei einem Identitätsdiebstahl steht eine Menge auf dem Spiel. 32 % der Unternehmen, die im letzten Jahr von Identitätsdiebstahl per E-Mail betroffen waren, haben infolgedessen Datenverluste erlitten. Bei 25 % hat das Ansehen gelitten und eines von fünf Unternehmen hat Kunden verloren. 61 % berichten von Verlusten aufgrund von Identitätsdiebstahl in der Supply Chain. Was machen Sie, um Ihre Mitarbeiter besser zu schulen, den unüberlegten Umgang mit E-Mails zu verhindern und technische Kontrollen zum Schutz vor Identitätsdiebstahl in Ihrer Organisation zu optimieren?

IM DETAIL: **RANSOMWARE**

Ransomware-Angriffe sind in den letzten Jahren immer beliebter geworden. Warum? Einfach zu verwendende Ransomware-Kits sind problemlos über den Schwarzmarkt zu beziehen – jeder kann Ransomware lizensieren und die Software implementieren, um einen solchen Angriff zu starten. Und vielleicht der wichtigste Grund für die Zunahme von Ransomware-Angriffen: Die meisten Unternehmen konzentrieren sich nur auf die Prävention. Doch rein präventive Systeme, wie Anti-Virus-Lösungen, können die sich ständig ändernden Ransomware-Gefahren nicht erkennen und blockieren. Und die Zunahme von anonymen Kryptowährungen spielt ebenfalls eine wichtige Rolle.

IM DETAIL: **RANSOMWARE**

RANSOMWARE WIRD IMMER GEFÄHRLICHER

Es ist kein Geheimnis, dass diese gefährliche Art von Malware Daten verschlüsselt und Server sowie Endpunkte sperrt. So werden Unternehmen zu Geiseln und ihnen wird der Zugriff auf wichtige Dateien, Ordner und Produktivitäts-Tools verwehrt, einschließlich E-Mails. In fast 30 % aller Unternehmen hatte Ransomware in den letzten 12 Monaten Auswirkungen auf die geschäftlichen Abläufe. Doch warum sind Vorfälle mit Ransomware trotz der bekannten Folgen weiterhin auf dem Vormarsch?

92 % geben an, dass im letzten Jahr Ransomware per E-Mail-Anhang an ihr Unternehmen geschickt wurde. 49 % wurden Opfer von bösartigen Aktivitäten, nachdem diese von einem Benutzer über infizierte E-Mail-Anhänge an andere Mitarbeiter weitergeleitet wurden. Und 52 % sagen, dass solche Angriffe seit dem letzten Jahr häufiger geworden sind.

WIE KÖNNEN SIE IHRE GESCHÄFTSKONTINUITÄT GEWÄHRLEISTEN?

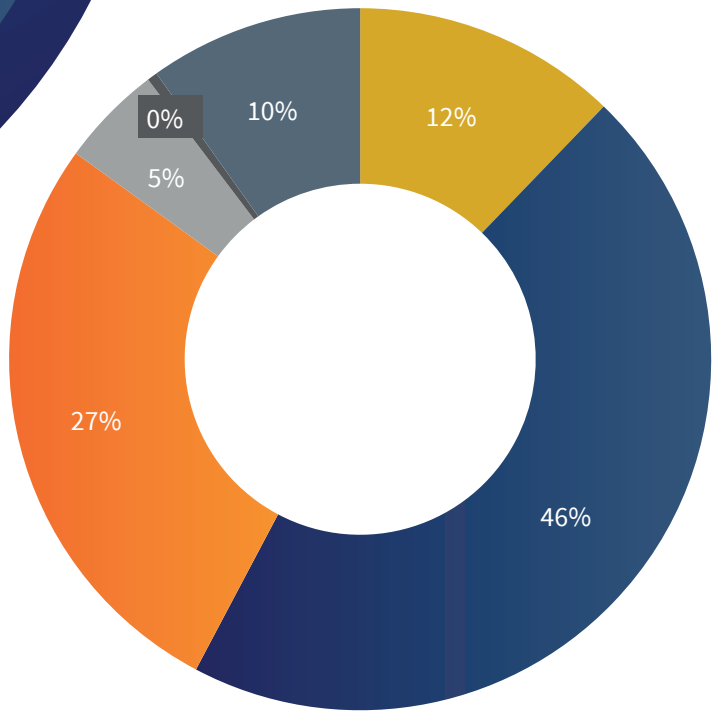
Die Folgen eines Ransomware-Angriffs können verheerend sein. Ausfälle können die Produktivität senken, Ihren Ruf schädigen und Ihre Daten gefährden. **Es ist nicht überraschend, dass 46 % der Unternehmen der Meinung sind, E-Mail-Verfügbarkeit sei nach einem Cyber Angriff entscheidend für Geschäftskontinuität.** Aber die meisten Organisationen schaffen es nicht, diese Kontinuität zu gewährleisten.

Wissenswert: 80 % der Unternehmen bezweifeln, dass ihre Mitarbeiter Ransomware in einem E-Mail-Anhang erkennen würden und dagegen vorgehen können.

Drei Tage:

durchschnittliche Ausfallzeit nach einem Ransomware-Angriff.

Wie viel Ausfallzeit kann Ihr Unternehmen verkraften? 78 % aller Unternehmen, die im letzten Jahr einem Ransomware-Angriff ausgesetzt waren, geben an, der Ausfall habe mindestens einen Tag gedauert. Im Durchschnitt wurden drei Tage genannt.



Wie lange hatten Sie infolge eines Ransomware-Angriffs mit Ausfallzeiten zu kämpfen?

CYBER RESILIENCE FÜR E-MAILS

ES IST ZEIT FÜR EINEN NEUEN ANSATZ

E-Mail-Sicherheit in der Cloud muss nicht kompliziert sein. Natürlich gibt es eine Menge Variablen: die Bekämpfung von neuen, bisher nicht bekannten E-Mail-Bedrohungen, die Entwicklung eines Wiederherstellungsplans für den Katastrophenfall, die Sicherstellung von ständiger Verfügbarkeit und die Gewährleistung, dass Daten geschützt und sofort wiederherstellbar sind. Aber einem einzelnen Anbieter wie Microsoft zu vertrauen oder Zeit und Ressourcen für Sicherheitsanbieter zu investieren, die unterschiedliche, oft zugekaufte Technologien anbieten, ist nicht die Antwort.

Der einzige Weg, um Angreifern einen Schritt voraus zu sein und sein Geschäft ganzheitlich zu schützen, ist eine neue Strategie für die E-Mail-Sicherheit, die Schutz, Anpassungsfähigkeit, Langfristigkeit und Wiederherstellbarkeit miteinander kombiniert.

Es wird Zeit für eine Cyber-Resilience-Strategie für E-Mails.

Wissenswert: 50 % denken, dass die Implementierung einer Cyber Resilience Strategie „wichtig“ ist, während 40 % dieses Thema als „entscheidend“ betrachten. Leider verfügen nur 27 % über eine komplette Cyber Resilience Strategie.

CYBER RESILIENCE FÜR E-MAILS

CYBER RESILIENCE IST EIN THEMA FÜR JEDEN IM UNTERNEHMEN

Einer der größten Fehler, den Unternehmen bei der Planung ihrer Cyber Resilience Strategie begehen, ist es, diese Aufgabe an nur einen Mitarbeiter oder an ein Team zu übertragen. **So glauben beispielsweise 78 %, dass die IT-Abteilung die Führung bei der Planung, Implementierung und Verwaltung der Cyber Resilience Strategie eines Unternehmens übernehmen sollte. Doch dieser Ansatz funktioniert nicht.** Da diese Strategie so wichtig ist, sollte sie zur unternehmensweiten Aufgabe werden, die viele Beteiligte mit unterschiedlichen Verantwortungs- und Zuständigkeitsbereichen einbezieht.

80%

der Unternehmen mit einem Cyber Resilience Plan sind bereit, Ransomware den Kampf anzusagen.

80 % der Unternehmen mit einer vollständigen Cyber Resilience Strategie vertrauen darauf, dass wichtige Dateien oder Systeme aus Backups wiederhergestellt werden können, sollte Ransomware sie verschlüsseln. Im Gegensatz dazu sind lediglich 35 % der Organisationen, bei denen die Cyber-Resilience-Strategie noch in den Kinderschuhen steckt, ebenso zuversichtlich.

Mehr als **nur Verteidigung**

Wenn Sie zu den 44 % der Unternehmen gehören, die derzeit die Einführung einer Cyber Resilience Strategie noch nicht geplant haben, ist Ihr Geschäftsbetrieb gefährdet. Der Schutz vor Bedrohungen sollte zwar Teil Ihrer Strategie sein, aber das allein reicht nicht aus. Sie müssen jede Phase eines Angriffs in Erwägung ziehen. Deshalb brauchen Sie:

1 Die richtigen Sicherheitslösungen, **bevor** ein Angriff geschieht.

2 Einen Kontinuitäts-Plan, damit Ihre E-Mails und geschäftlichen Abläufe **während** eines Angriffs oder eines Ausfalls weiter funktionieren.

3 Die Möglichkeit, Daten und anderes geistiges Firmeneigentum **nach** einem Vorfall oder einem Angriff wiederherzustellen.

DIE VIER DIMENSIONEN **DER CYBER RESILIENCE**

Cyber Angreifer entwickeln ihre Strategien immer weiter und passen sie kontinuierlich an. Aus diesem Grund steigt das Risiko Tag für Tag. Sie brauchen einen Plan, damit Ihre E-Mails und geschäftlichen Abläufe auch nach einem Angriff weiter funktionieren und Sie verloren gegangene oder gesperrte Daten schnell wiederherstellen können.
Sie benötigen diese vier Funktionen:

1 THREAT PROTECTION

Die Kombination von intern entwickelten Technologien und Technologien von Drittanbietern gepaart mit Dutzenden von internen und externen Bedrohungsdatenquellen bietet ein vielschichtiges Inspektionssystem. Damit sind Sie vor weit verbreiteten und gezielt auf Sie gerichteten Angriffen geschützt.

2 ADAPTABILITY

Sie müssen schnell handeln und sich rasch anpassen können, um den neuesten Angriffen stets einen Schritt voraus zu bleiben. Technologie sollte dabei nur einer der Faktoren einer erfolgreichen Herangehensweise sein. Ihre Mitarbeiter müssen sich der permanenten Bedrohungen bewusster werden, damit Ihr Unternehmen besser geschützt bleibt. Deshalb sollten Sie Ihre Mitarbeiter intern schulen, permanent führende Technologien prüfen und implementieren, laufende Bedrohungsanalysen durchführen und Dienste zur Beseitigung von Bedrohungen automatisieren.

3 DURABILITY

Es kann vorkommen, dass das E-Mail-System durch einen Cyber Angriff offline geht oder von der IT aktiv abgeschaltet wird, um einer aktuellen Bedrohung Einhalt zu gebieten. Dies kann sich direkt auf den Geschäftsbetrieb auswirken, indem die Kommunikationsfähigkeit verhindert oder eingeschränkt wird. Auch der Zugriff auf im System gespeicherte Dateien kann beeinträchtigt werden. Um solche Ausfälle zu verhindern, brauchen Sie ein E-Mail-System, das stets zu 100 % verfügbar ist und dafür sorgt, dass die darin gespeicherten Daten unversehrt bleiben.

4 RECOVERABILITY

Sie sollten dafür sorgen, dass Ihre Daten geschützt bleiben und Nutzer gleichzeitig darauf zugreifen können. Viele Unternehmen sind sich jedoch der Herausforderungen im Zusammenhang mit schädlichen Angriffen und einer Point-in-Time-Wiederherstellung nicht bewusst. Nutzen Sie einen für diese Zwecke entwickelten Archivierungsdienst und automatisieren und vereinfachen Sie den Wiederherstellungsprozess für Ihre E-Mails und weitere Exchange-Daten.

Wissenswert: Die Anpassung kann schwierig sein. Bis 2022 wird es weltweit 3,5 Millionen unbesetzte Stellen in der Sicherheitsbranche geben.*

FAZIT

Es ist klar, dass Sie gegen eine Reihe bösartiger E-Mail-Angriffe kämpfen – sowohl von externen als auch internen Quellen. Und die Lage wird immer bedrohlicher. E-Mails sind ein Kanal mit einem massiven Risiko. Wenn Sie den Schutz vor diesen Bedrohungen nicht zur Priorität machen, werden immer wieder auf Sie gerichtete Cyber Angriffe stattfinden – und Ihre Datenschutzbemühungen und Ihre persönliche Privatsphäre werden in Gefahr sein.

Sie wissen, welche Konsequenzen es hat, sich in puncto Sicherheit nur auf die Verteidigung, mehrere Anbieter und punktuelle Lösungen zu verlassen. Dieser Ansatz reicht nicht aus, um sich vor den schnelllebigen Bedrohungen zu schützen, die Unternehmen wie Ihres dem Risiko von Datenverletzungen, Ausfällen, Reputationsschäden, finanziellen Verlusten, blockierten Zugriffen oder Problemen bei der Wiederherstellung wichtiger Unternehmensinformationen aussetzen.

Es ist an der Zeit, Ihre veraltete Legacy-Sicherheitstechnologie in eine leistungsstarke, reine Cloud-Plattform zu verwandeln, die jede Dimension der Cyber Resilience ermöglicht.

DREI SCHRITTE FÜR DEN EINSTIEG:

1. **PRÜFEN SIE** (ehrlich) die vier Dimensionen der Cyber Resilience für Ihr Unternehmen.

2. **BESTIMMEN SIE** die direkten und indirekten Kosten, die Ihrem Unternehmen durch solche Lücken entstehen.

3. **ENTWICKELN SIE** Pläne für drei, sechs und 12 Monate und priorisieren Sie diese, um Lücken zu schließen.

Sind Sie bereit, Ihre Verteidigung zu stärken?

Erfahren Sie mehr

Mimecast Limited (NASDAQ: MIME) setzt sich dafür ein, geschäftliche E-Mails und Daten für Zehntausende von Kunden mit Millionen Mitarbeitern auf der ganzen Welt sicherer zu gestalten. Die hochmodernen und wegweisenden Cloud-basierten E-Mail-Sicherheits-, Archivierungs- und Kontinuitäts-dienste des 2003 gegründeten Unternehmens gewährleisten einen zuverlässigen E-Mail-Schutz sowie umfassendes Risikomanagement über einen einzigen, vollständig integrierten Subscription Service.