mimecast®

State of RANSOMWARE Readiness 2022

Verringerung der persönlichen und geschäftlichen Kosten

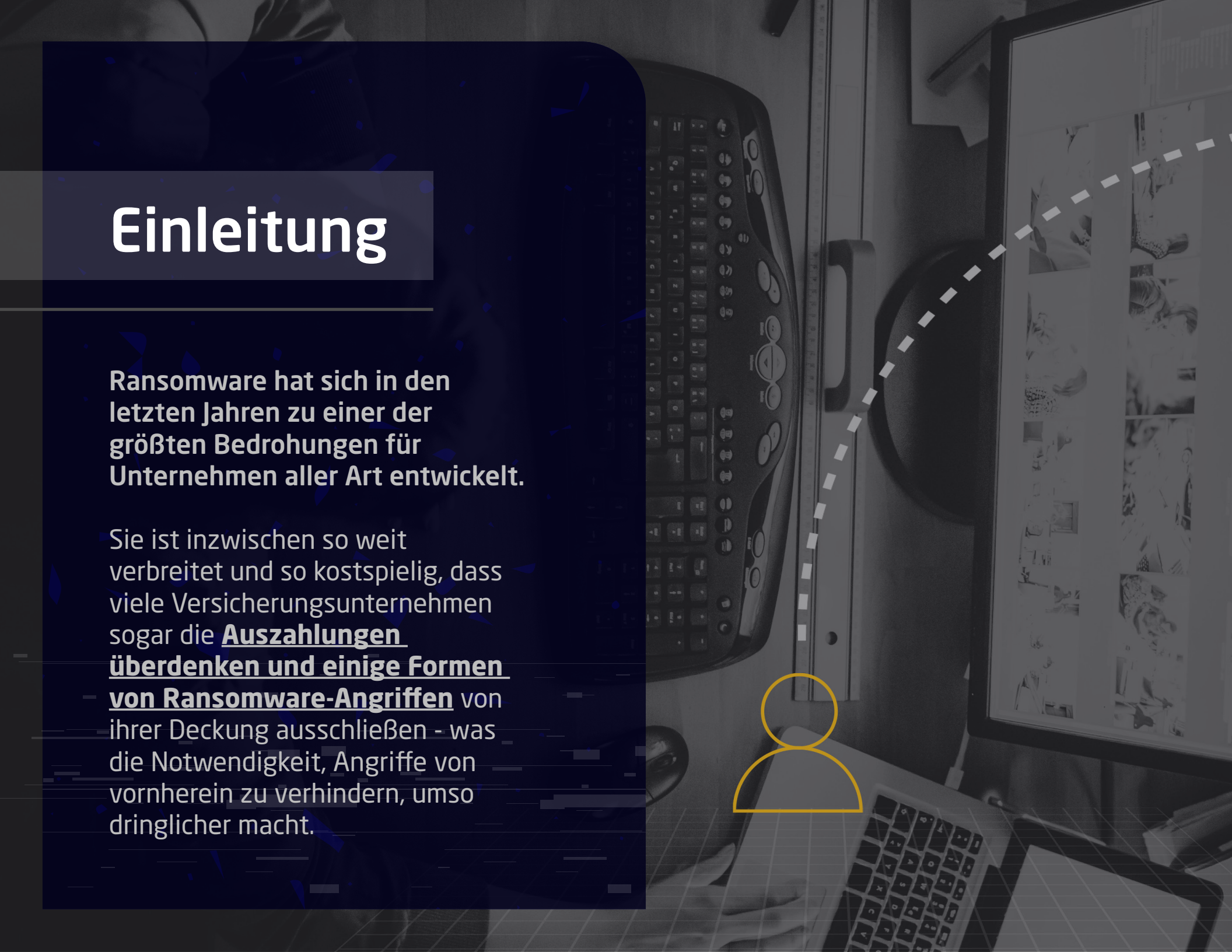
Inhaltsverzeichnis

Einleitung....3
Zusammenfassung....5
Kapitel Eins: Die Ransomware-Landschaft: Steigender Druck....7
Kapitel Zwei: Angriffsabwehr: Sich entwickelnde Bedrohung, statische Abwehrmaßnahmen....10
Kapitel Drei: Bereitschaft der Unternehmen: Unvermeidbarkeit begrenzt Proaktivität....13
Empfehlungen zum Thema....18

Einleitung

Ransomware hat sich in den letzten Jahren zu einer der größten Bedrohungen für Unternehmen aller Art entwickelt.

Sie ist inzwischen so weit verbreitet und so kostspielig, dass viele Versicherungsunternehmen sogar die **Auszahlungen überdenken und einige Formen von Ransomware-Angriffen** von ihrer Deckung ausschließen - was die Notwendigkeit, Angriffe von vornherein zu verhindern, umso dringlicher macht.



Seit der berüchtigte **WannaCry**-Angriff Ransomware 2017 in die Schlagzeilen brachte, haben zahlreiche Vorfälle, die auf Unternehmen und Infrastruktur abzielten, internationale Aufmerksamkeit erregt.

Der Angriff auf **Colonial Pipeline führte** im Jahr 2021 zur Abschaltung einer US-Ölpipeline und zur Zahlung eines Lösegelds in Höhe von 4,4 Millionen US-Dollar. Erst kürzlich hatten es Kriminelle auf einen **IT-Lieferanten des Gesundheitswesens in Großbritannien abgesehen,** wodurch der Zugang zu Patientenakten blockiert und ein dringender Gesundheitsdienst gefährdet wurde.

Darüber hinaus bedeutet globales Chaos wie Pandemien, Naturkatastrophen oder politische Instabilität, dass die Häufigkeit von Ransomware-Angriffen - und Cyberkriminalität im Allgemeinen - zunimmt, ebenso wie die **Gesamtkosten für die Opfer.**

Dies alles kommt zu einem kritischen Zeitpunkt für Unternehmen und ihre IT-Abteilungen.

Die Pandemie bot versierten Cyberangreifern, die **Remote- und Hybridarbeit** sowie Schatten-IT nutzten, neue Möglichkeiten, um in Unternehmen einzudringen.

Nach einigen schädlichen Jahren stehen die Fachleute auch vor persönlichen Herausforderungen. Viele Cybersicherheitsteams haben mit Stress und sogar Burnout zu kämpfen, während in der Branche ein **Mangel an Talenten** herrscht, der noch lange nicht behoben ist.

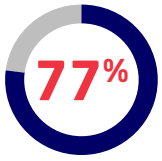
Positiv zu vermerken ist, dass die Bedrohung zwar zunimmt, es für Unternehmen jedoch Möglichkeiten gibt, ihre Cybersicherheitsstrategien weiterzuentwickeln und die Herausforderungen komplexer Unternehmensnetzwerke, begrenzter Ressourcen, überlasteter Teams und komplexer Bedrohungen zu bewältigen. Das bedeutet, dass sich Unternehmen nicht nur auf die Schadensbegrenzung, sondern auch auf die proaktive Prävention konzentrieren müssen, um ihre Fähigkeiten zur Erkennung von Bedrohungen und zur Reaktion auf Angriffe zu verbessern - und letztlich die persönlichen und geschäftlichen Kosten von Ransomware zu senken.

Um die Ransomware-Bedrohung genauer zu untersuchen und ihre Auswirkungen auf Cybersecurity-Teams und Unternehmen zu bewerten, haben wir mit 1.100 Cybersecurity-Entscheidungsträgern in Australien, Kanada, Frankreich, Deutschland, den Niederlanden, den nordischen Ländern, Singapur, Südafrika, den Vereinigten Arabischen Emiraten, Großbritannien und den USA gesprochen.

Dieser Bericht untersucht die geschäftlichen und persönlichen Auswirkungen von Ransomware und zeigt auf, wie sich Unternehmen heute gegen Angriffe wehren.

Wichtige Erkenntnisse

Cybersecurity-Fachleute stehen unter wachsendem Druck durch Ransomware-Angriffe



der Führungskräfte im Bereich Cybersicherheit geben an, dass die Zahl der Cyberangriffe auf ihr Unternehmen seit dem letzten Jahr zugenommen hat oder gleich geblieben ist

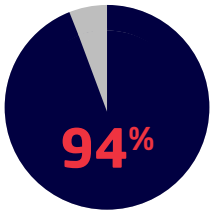
Zwei Fünftel der Unternehmen haben aufgrund von Ransomware-Angriffen erhebliche Ausfallzeiten erlebt

Viele Fachleute sind an ihrer Belastungsgrenze angelangt, denn **ein Drittel** zieht in Erwägung, in den nächsten zwei Jahren aufgrund von Stress oder Burnout aus dem Unternehmen auszuscheiden

der Angriffe kosten insgesamt mehr als 100 000 US-Dollar

Die Angriffe werden von Jahr zu Jahr schädlicher, aber die Abwehrmaßnahmen bleiben gleich

Ein Drittel der Teams verzeichnet nach einem Angriff eine erhöhte Anzahl von Abwesenheiten aufgrund von Burnout

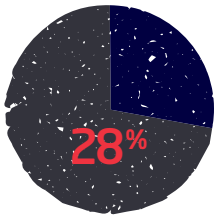


der Verantwortlichen für Cybersicherheit sind der Meinung, dass mehr Budget für die Bekämpfung von Ransomware erforderlich ist, wobei im Durchschnitt eine Erhöhung des Budgets um 28% festgestellt wurde.

der Unternehmen haben in den letzten zwölf Monaten Umsatzeinbußen aufgrund eines Ransomware-Angriffs erlitten.

Weitere Wichtige Erkenntnisse

Führungskräfte sehen Ransomware-Angriffe als praktisch unvermeidlich an, was dazu führt, dass der Schwerpunkt eher auf Schadensbegrenzung als auf Prävention liegt



Die Integration wird übersehen, da nur 28% ihre Sicherheitskontrollen in eine SIEM- oder SOAR-Plattform integrieren, um ihre Ransomware-Reaktion zu orchestrieren

Die Sicherung und Wiederherstellung von Dateien ist die wichtigste Technologie zur Verringerung des Risikos und des Schadens durch Ransomware-Angriffe

Weniger Führungskräfte im Bereich Cybersicherheit fühlen sich persönlich verantwortlich, wenn ein Angriff erfolgreich war: **57%** würden sich im Falle eines Ransomware-Angriffs sehr persönlich verantwortlich fühlen; im letzten Jahr **waren es noch 71%**.

Cybersecurity-Führungskräfte müssen sich darauf konzentrieren, die Wahrscheinlichkeit eines Ransomware-Angriffs, der Störungen verursacht, proaktiv zu verringern, indem sie:

01. Integration von Sicherheitstools zur Verbesserung der Fähigkeiten zur Erkennung von Bedrohungen und zur Reaktion darauf, um den Druck auf vielbeschäftigte Teams zu mindern

02. Sicherstellen, dass das Unternehmen über gute grundlegende Sicherheitspraktiken verfügt, um Schwachstellen zu verringern

03. Bewertung der Krisenplanung, um die tatsächlichen Folgen eines Angriffs zu verstehen

04. Sicherstellen, dass die Unternehmensleitung dies als ein größeres Vorrecht des Unternehmens betrachtet und die finanzielle und personelle Belastung nicht den IT-Teams überlässt

Methodik

Die Umfrage umfasst 1.100 Entscheidungsträger im Bereich Cybersicherheit in Australien, Kanada, Frankreich, Deutschland, den Niederlanden, den nordischen Ländern, Singapur, Südafrika, den Vereinigten Arabischen Emiraten, Großbritannien und den USA. Die Umfrage wurde im Juli 2022 von Vitreous World online durchgeführt und von Mimecast beauftragt.

01.

Die Ransomware-Landschaft: Wachsender Druck

Die COVID-19-Pandemie hat zu einem sprunghaften **Anstieg der Ransomware**-Angriffe geführt - und es ist klar, dass der Druck auf die Cybersicherheitsexperten noch lange nicht nachlässt. Drei Viertel der Führungskräfte im Bereich Cybersicherheit geben an, dass die Zahl der Cyberangriffe auf ihr Unternehmen seit dem letzten Jahr zugenommen hat oder gleich geblieben ist (**77%**).

Die meisten dieser Führungskräfte im Bereich Cybersicherheit haben in letzter Zeit einen Ransomware-Vorfall erlebt. Tatsächlich haben fast zwei **Drittel** (64%) im vergangenen Jahr mindestens einen Ransomware-Angriff erlebt, bei Unternehmen in den Vereinigten Arabischen Emiraten sind es sogar **75%**. Viele dieser Ransomware-Angriffe beeinträchtigen den täglichen Geschäftsbetrieb. Zwei **Fünftel** (40%) der Unternehmen haben aufgrund von Ransomware-Angriffen erhebliche Ausfallzeiten erlebt - wobei diese Zahl stark variiert, von 27% in den nordischen Ländern bis zu 49% in Großbritannien.

Es besteht auch das Potenzial für langfristige Folgen. Als Folge eines Ransomware-Angriffs mussten **22%** der Unternehmen einen Wechsel in der Führungsetage hinnehmen, während 20% rechtliche Schritte gegen das Unternehmen einleiten mussten.

Mehr als die Hälfte der Führungskräfte (**53%**) gibt an, dass die zunehmende Berichterstattung über Ransomware-Angriffe in den Medien den Druck erhöht, sich vorzubereiten.

Zusätzlich zu den Auswirkungen, die Ransomware auf den Ruf der Marke haben kann, können die Gesamtkosten eines Ransomware-Angriffs, einschließlich Lösegeldzahlungen, Systemwiederherstellung, zusätzliche Sicherheitsmaßnahmen und zusätzliches Personal, hoch sein - und einen beträchtlichen Teil des **Budgets für Cybersicherheit** verschlingen.

Eine genauere Untersuchung der Cybersicherheitsbudgets und der Kosten von Angriffen in den befragten Unternehmen ergab, dass **56% der Angriffe insgesamt mehr als 100,000 US-Dollar kosten.** In Anbetracht der Tatsache, dass die Hälfte der Entscheidungsträger jährlich weniger als 550 000 US-Dollar für ihr Cybersicherheitsbudget bereitstellt, könnte ein einziger Angriff 20 % des Gesamtbudgets kosten.

In Südafrika steigt der Anteil der Unternehmen, die jährlich weniger als 550,000 Dollar für ihr Cybersicherheitsbudget bereitstellen, auf 82%, was das Problem möglicherweise noch weiter verschärft.

Dies hat persönliche Konsequenzen für das **Wohlbefinden** der Führungskräfte im Bereich der Cybersicherheit. Mehr als die Hälfte (54%) geben an, dass sich Ransomware-Angriffe negativ auf ihre psychische Gesundheit auswirken, während 56% sagen, dass ihre Rolle von Jahr zu Jahr stressiger wird.

Angesichts des zunehmenden Drucks erreichen viele Fachleute ihre Belastungsgrenze: **Ein Drittel** (33%) der Entscheidungsträger im Bereich Cybersicherheit denkt darüber nach, ihre Position in den nächsten zwei Jahren aufgrund von Stress oder Burnout aufzugeben, in den Vereinigten Arabischen Emiraten sind es 46% und in Großbritannien 42%.

77% der Führungskräfte im Bereich Cybersicherheit sagen, dass die Zahl der der Cyberangriffe auf ihr Unternehmen seit letztem Jahr gestiegen oder gleich geblieben ist

Fast zwei Drittel (**64%**) der Führungskräfte im Bereich Cybersicherheit haben im vergangenen Jahr mindestens einen Ransomware-Angriff erlebt

Das Fazit

Die Folgen eines Cyberangriffs können verheerend sein, sowohl für Unternehmen als auch für einzelne Cybersicherheitsexperten. Das Ausmaß und die Intensität der Angriffe haben seit vielen Jahren nicht abgenommen, und Ransomware trägt wesentlich zu den Herausforderungen bei, denen sich die Verantwortlichen für Cybersicherheit und ihre Teams gegenübersehen.

Unternehmen erfahren aus erster Hand, dass Cyberkriminalität einen hohen finanziellen Tribut fordern kann, angefangen bei den betrieblichen Auswirkungen bis hin zur langfristigen Schädigung des Rufs und der rechtlichen Stellung des Unternehmens.

Ebenso zahlen die Cybersecurity-Teams oft mit ihrem Wohlbefinden, da sie darum kämpfen, das Unternehmen vor der zunehmenden Häufigkeit von Ransomware zu schützen - und den Schaden von Angriffen abzuwehren, wenn diese erfolgreich sind.

Angesichts des Drucks, dem die Branche durch ständige Angriffe, Störungen und Burnout ausgesetzt ist, ist es von entscheidender Bedeutung, dass Unternehmen die Sicherheitsteams unterstützen, indem sie Cyberangriffen die nötige Aufmerksamkeit und die erforderlichen Ressourcen zukommen lassen - sonst droht der Verlust wichtiger Mitarbeiter.

Die Zuweisung von Ressourcen für die Cybersicherheit, die dem Schweregrad der Bedrohung entspricht, hilft den Teams, Bedrohungen auf eine Weise zu bewältigen, die für sie und das Unternehmen nachhaltig ist.

> Laut **Kiri Addison, Senior Product Manager bei Mimecast,** "können Ransomware-Angriffe besonders verheerend sein, und sie werden nicht verschwinden. Sie sind mit einer Vielzahl von Auswirkungen und einem steigenden Maß an Unsicherheit verbunden, was sie für Unternehmen besonders stressig und schwierig macht. Zum Beispiel die Entscheidung zu zahlen oder nicht zu zahlen und nicht zu wissen, ob die Daten überhaupt wiederherstellbar sind, wenn man es tut. Der Übergang zu einer doppelten Erpressungstaktik, bei der der Bedrohungsakteur damit droht, exfiltrierte Daten zu verkaufen oder freizugeben, wenn die Forderungen nicht erfüllt werden, erhöht den Druck zusätzlich. Darüber hinaus kann die Wiederherstellung von Diensten auf der Grundlage von Backups und/oder Lösegeldverhandlungen als Teil der Angriffsreaktion und -wiederherstellung ein langwieriger Prozess sein, und die Sicherheitsteams stehen unter dem Druck, die Ausfallzeiten des Unternehmens zu begrenzen.

02.

Angriffsabwehr: Sich entwickelnde Bedrohung, statische Verteidigungsmaßnahmen

Die Ransomware-Bedrohung entwickelt sich ständig weiter, und es gibt Anzeichen dafür, dass die Angriffe von Jahr zu Jahr gefährlicher werden. **Zwei Fünftel** der Cybersecurity-Führungskräfte (40%) haben in diesem Jahr Ransomware-Angriffe erlebt, bei denen die Taktik der kompromittierten Anmeldeinformationen genutzt wurde, im Vergleich zu 33% im letzten Jahr. Während Ransomware-Angriffe in der Regel von Endpunkten ausgehen, ist diese Zunahme von Ransomware über kompromittierte Anmeldedaten alarmierend und sollte die Verantwortlichen für Cybersicherheit dazu veranlassen, die E-Mail-Sicherheit zu verdoppeln, um das Abgreifen von **Anmeldedaten** zu verhindern.

Mehr als ein Drittel der Unternehmen (36%) musste in den letzten zwölf Monaten Umsatzeinbußen aufgrund eines Ransomware-Angriffs hinnehmen, verglichen mit 28% im Vorjahr. **In Deutschland und den Vereinigten Arabischen Emiraten sind es sogar 44% der Unternehmen.**

Die Verantwortlichen für Cybersicherheit haben auch immer weniger Vertrauen in ihre Fähigkeit, den Schaden zu begrenzen, wenn es zu einem Vorfall kommt. Waren letztes Jahr noch 82% der Fachleute zuversichtlich, dass sie nach einem Ransomware-Angriff die **E-Mail-Kontinuität** ohne Unterbrechung aufrechterhalten können, so sind es dieses Jahr nur noch 73%. Und diese schwindende Zuversicht sollte für alle Unternehmen Anlass zur Sorge sein.

Unternehmen greifen zunehmend auf **Cybersecurity-Versicherungen** zurück, um Verluste bei erfolgreichen Angriffen zu decken, aber auch hier sinkt das Vertrauen der Fachleute in dieses Sicherheitsnetz. Während im letzten Jahr vier von fünf (79%) glaubten, dass ihr Cyber-Versicherungsanbieter jede von Angreifern geforderte Lösegeldzahlung abdecken würde, sind in diesem Jahr nur noch 64% dieser Meinung - in Kanada sogar nur noch 50%. Angesichts der Tatsache, **dass die Versicherer die Deckung für bestimmte Arten von Angriffen einschränken,** haben die Verantwortlichen Recht, dass es eine riskante Strategie sein kann, sich auf eine Cyberversicherung zu verlassen.

Außerdem gibt es Anzeichen dafür, dass es den Cybersicherheitsteams oft an den Grundlagen der Angriffsprävention mangelt. Bei der Frage nach den zusätzlichen Ressourcen, die zur Verhinderung von und zur Vorbereitung auf Angriffe benötigt werden, **gibt fast die Hälfte der Führungskräfte an, dass sie aktuelle Sicherheitssysteme benötigen** (46%).

Ebenso nennen 46% eine bessere Schulung des **Sicherheitsbewusstseins** der Endbenutzer als notwendige zusätzliche Ressource - in Singapur steigt diese Zahl auf 61%.

Fast alle Verantwortlichen für Cybersicherheit (**94%**) sind der Meinung, dass mehr Budget erforderlich ist, um dieser Bedrohung zu begegnen, und zwar sowohl im Hinblick auf die Prävention als auch auf die Schadensbegrenzung. Die Entscheidungsträger bräuchten im Durchschnitt eine Budgeterhöhung von 28%, um allein Ransomware zu bekämpfen.

Die Entscheidungsträger bräuchten im Durchschnitt eine Budgetaufstockung von **28%** zur Bekämpfung von Ransomware allein.

Mental vorbereitete Teams sind ebenfalls entscheidend um Cyberkriminalität zu verhindern und abzuschwächen - aber sobald ein Angriff stattfindet, haben die Mitarbeiter oft mit ihrem Wohlbefinden zu kämpfen. Ein Drittel der Teams (33%) verzeichnet eine erhöhte Anzahl von Abwesenheiten aufgrund von Burnout nach einem Angriff.

Darüber hinaus haben **34%** der Verantwortlichen für Cybersicherheit Probleme, nach einem Angriff wichtige IT-Mitarbeiter zu rekrutieren, was ihre Fähigkeit, zukünftige Vorfälle zu bekämpfen, weiter beeinträchtigt.

Das Fazit

Ransomware entwickelt sich ständig weiter, und die Verantwortlichen für Cybersicherheit sehen aus erster Hand, welchen Schaden diese Angriffe anrichten können. Und da das Sicherheitsnetz der Cyberversicherung im Falle eines Angriffs immer unzuverlässiger wird, ist die Gewährleistung, dass ein Angriff niemals erfolgreich ist, der einzig verbleibende sichere Weg.

Besorgniserregend ist jedoch, dass die Ransomware-Abwehr in den Unternehmen statisch geblieben zu sein scheint. Vielen Firmen fehlt es an den grundlegenden Dingen wie aktuellen Sicherheitsvorkehrungen und der Sensibilisierung der Mitarbeiter, was die Anfälligkeit und Gefährdung im Falle eines Angriffs potenziell erhöht.

Unternehmen können nach einem Angriff anfälliger für Angriffe werden, nicht zuletzt aufgrund von Stress, Burnout und Rekrutierungsproblemen, die die Teams nach einem Vorfall erleben.

Um diesen Kreislauf zu vermeiden, ist es wichtig, grundlegende Maßnahmen zu ergreifen, wie z. B. robuste E-Mail-Sicherheit und Mitarbeiterschulungen, die durch ein ausreichend großes Budget unterstützt werden.

Die Integration von Sicherheitssystemen ist eine weitere wirksame Methode, um die Transparenz zu erhöhen und den Druck, der auf vielbeschäftigten Teams lastet, zu verringern.

> Organisationen, die eine Cyberversicherung haben, sind immer noch sehr anfällig. Der Verlust von geistigem Eigentum und zukünftigen Gewinnen sind in der Regel nicht abgedeckt. Erhebliche Verluste an Marke und Ruf sind ebenfalls nicht abgedeckt. Schlimmer noch, die Deckung kann begrenzt sein, wenn es sich um Ransomware handelt oder überhaupt nicht anwendbar, wenn es sich um einen staatlich gesponserten Angriff handelt. Unternehmen müssen ihre modernisierte E-Mail Sicherheit aufrechterhalten, auch wenn sie eine Cyber-Versicherung haben."
>
> - **Andrew Williams,**
> **Principal Product Marketing Manager**

03.

Bereitschaft der Unternehmen: Unvermeidbarkeit begrenzt Proaktivität

Trotz des Mangels an Ressourcen und der psychischen Belastung, die sie feststellen, fühlen sich die Verantwortlichen für Cybersicherheit im Allgemeinen vorbereitet und vom Unternehmen unterstützt. Drei Viertel der Cybersecurity-Entscheidungsträger (**77%**) fühlen sich von ihrem Führungsteam oder Vorstand unterstützt.

Nach einem Cyberangriff glauben die Führungskräfte, dass es im Durchschnitt 3,5 Tage dauern würde, um zum normalen Betrieb zurückzukehren - 46% glauben, dass es höchstens zwei Tage dauern würde. Insgesamt geben sieben von zehn (**70%**) an, dass ihr Unternehmen sehr gut auf die Abwehr von Ransomware-Angriffen vorbereitet ist.

Diese optimistische Antwort könnte darauf zurückzuführen sein, dass Ransomware als unvermeidlich angesehen wird. Je häufiger und raffinierter die Angriffe werden, desto wahrscheinlicher ist es, dass sie erfolgreich sein werden.

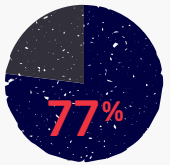
Infolgedessen fühlen sich Führungskräfte im Bereich Cybersicherheit weniger persönlich verantwortlich, wenn ein Angriff erfolgreich ist: **57%** würden sich im Falle eines Ransomware-Angriffs sehr persönlich verantwortlich fühlen; im letzten Jahr waren es noch 71%. In den Niederlanden sinkt dieser Anteil auf 36%.

Angesichts der Wahrnehmung, dass Angriffe unvermeidlich sind, legen viele Führungskräfte mehr Wert auf Schadensbegrenzung als auf Prävention. Während im letzten Jahr 46% der Führungskräfte angaben, dass sie sich vorbereitet fühlten, weil sie proaktiv Angriffe verhinderten, sind es in diesem Jahr nur noch **43%.**

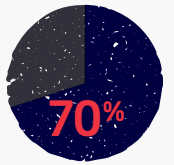
Stattdessen halten die Entscheidungsträger im Bereich Cybersicherheit die **Sicherung und Wiederherstellung von Dateien** für die wichtigste Technologie zur Verringerung des Risikos und des Schadens durch Ransomware-Angriffe - **49%** der Führungskräfte gaben dies an, im Vergleich zu 39% im letzten Jahr..

Für viele Unternehmen scheint es Raum für eine proaktivere Haltung zu geben, wenn es um die Verhinderung von Angriffen geht, insbesondere durch den Einsatz ausgefeilterer Tools und Integrationen.

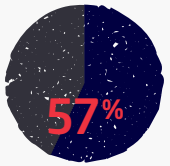
So ist beispielsweise die E-Mail ein wichtiger Vektor für Cyberangriffe. Mehr als die Hälfte der Cybersecurity-Verantwortlichen (53%) hat schon einmal eine **Phishing-E-Mail** mit Ransomware-Anhängen erhalten, in Deutschland sind es sogar 72%, während **43% schon einmal mit Phishing-E-Mails konfrontiert waren, die zu einem Drive-by-Download führten.**



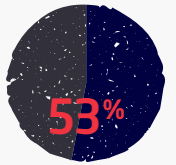
der Cybersicherheits-Entscheidungsträger fühlen sich durch ihre Führungsebene, das Team oder den Vorstand unterstützt



sagen, dass ihr Unternehmen sehr gut vorbereitet ist, um Ransomware-Angriffe zu verhindern



der cybersicherheits-beauftragten Führungskräfte würden sich im Fall eines Ransomware-Angriffs verantwortlich fühlen



der Führungskräfte hatten schon mal eine Phishing-E-Mail mit Ransomware Anhängen

Infolgedessen halten zwei Fünftel (39%) die Kennzeichnung verdächtiger E-Mail-Nachrichten mit **Warnbannern** für eine der wirksamsten Maßnahmen, die ihr Unternehmen zum Schutz vor Ransomware ergreift.

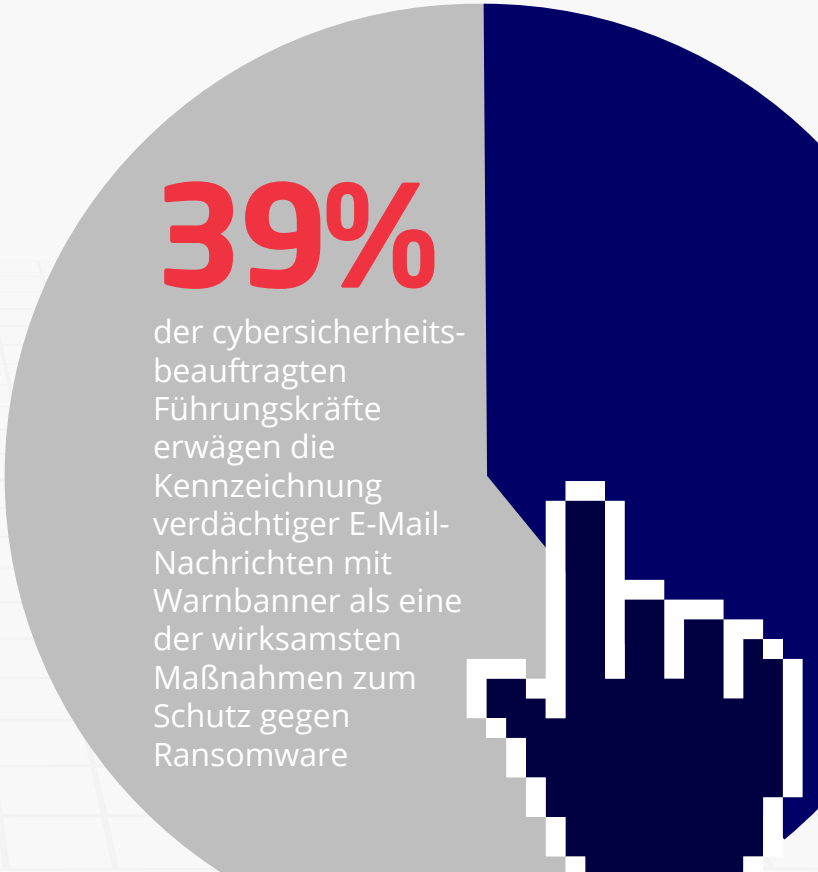
Dennoch werden nur 35% im nächsten Jahr zusätzliche Mittel in KI/ML investieren, z. B. in Form von Warnbannern, die in verdächtige E-Mails eingebettet werden, während nur 35% spezielle **sichere E-Mail-Gateways** einführen werden.

Wichtig ist, dass die Verantwortlichen für Cybersicherheit derzeit nicht die Möglichkeiten der Integration nutzen, um einen proaktiveren Ansatz für ihre Sicherheitslage zu verfolgen. Trotz der zunehmenden Komplexität von Unternehmensnetzwerken und der Vielzahl von **Sicherheitslösungen** sind weniger als drei von zehn Führungskräften (29%) der Meinung, dass sie auf Ransomware-Angriffe vorbereitet sind, indem sie mit Hilfe von **API-Integrationen Bedrohungsdaten über verschiedene Sicherheitskontrollen hinweg austauschen.**

Ebenso integrieren nur 28% ihre Sicherheitskontrollen in eine **SIEM**- oder **SOAR**-Plattform, so dass sie ihre Ransomware-Reaktion orchestrieren können.

Umgekehrt sagen 31% der Führungskräfte, dass ihr Unternehmen die Integration von Sicherheitskontrollen in eine SIEM- oder SOAR-Plattform benötigt, um Ransomware-Angriffe zu verhindern.

Viele Unternehmen scheinen die Möglichkeit zu verpassen, die Integration zu nutzen, um eine bessere Sichtbarkeit und eine frühere Erkennung von Bedrohungen zu erreichen: Letztendlich werden Angriffe nicht nur früher erkannt, wenn sie auftreten, sondern auch die Wahrscheinlichkeit eines Erfolgs verringert.



Die Quintessenz

Die Häufigkeit der Angriffe scheint ein Gefühl der Unvermeidbarkeit von Angriffen zu erzeugen. Die Verantwortlichen für Cybersicherheit scheinen sich mit einem Angriff fast abgefunden zu haben - im Gegenzug fühlen sie sich weniger persönlich verantwortlich, wenn Kriminelle Erfolg haben, solange Strategien zur Schadensbegrenzung vorhanden sind.

Dies ist jedoch eine gefährliche Strategie, die davon abhängt, dass die Unternehmen über die besten Verfahren verfügen. Nicht alle Strategien zur Datensicherung und -wiederherstellung sind gleich: Es ist eine Sache, eine Woche Daten zu verlieren, aber was ist mit sechs Monaten? Gibt es einen soliden Plan für die Bewältigung eines Angriffs und die Bewältigung der Nachwirkungen? Wären die Mitarbeiter in der Lage, auf wichtige Informationen zuzugreifen und ihren Betrieb aufrechtzuerhalten?

Angesichts der zunehmenden Ransomware-Bedrohung muss die Sicherheit über die Überprüfung der Einhaltung von Vorschriften und die Schadensbegrenzung hinausgehen. Proaktive Prävention verringert nicht nur die Wahrscheinlichkeit von Angriffen, sondern auch deren Auswirkungen, wenn sie erfolgreich sind.

Angesichts der Komplexität der meisten Unternehmensnetzwerke profitieren Unternehmen oft von einem integrierten Ansatz - einer Cybersecurity-Mesh-Architektur, die den Sicherheitsschutz an jede Anlage im Netzwerk anpasst. Dies erhöht die Transparenz, minimiert die **Verweildauer** und hilft vielbeschäftigten Teams, Angriffe schneller zu erkennen und zu bekämpfen.

Brian Pinnock, VP of Sales Engineering bei Mimecast, ist der Meinung, dass die oft wiederholte Phrase "Es ist keine Frage des Ob, sondern des Wann eines Cybervorfalls" zwar wahr ist, aber keine sehr nützliche Anleitung für ein proaktives Cyber-Risikomanagement darstellt.

Brian erklärt: "Die Phrase bietet nur begrenzte handlungsrelevante Erkenntnisse, mit denen sich Investitionen in Mitarbeiter, Prozesse oder Kontrollen steuern lassen. Der Satz suggeriert Unvermeidbarkeit mit einem unendlichen Zeithorizont, was unsere Aufmerksamkeit davon ablenkt, heute umsetzbare risikobasierte Entscheidungen zu treffen, die auf einer quantitativen Bewertung des Risikos zukünftiger Ransomware-Vorfälle für das Unternehmen basieren.

"Bei der Untersuchung von Kennzahlen wie der Häufigkeit von Verlustereignissen, die in den meisten Regionen zunimmt, und dem Ausmaß der Verluste, das ebenfalls zunimmt, ist es wichtig zu fragen: 'Um wie viel?' und 'Welche Präventivmaßnahmen können diese Statistiken reduzieren?'" Brian fährt fort. "Proaktive Maßnahmen wie der Einsatz von KI/ML, der Austausch von Bedrohungen und die Integration von Sicherheitstools werden offenbar nicht ausreichend genutzt, was darauf hindeutet, dass es mehr Möglichkeiten gibt, die Anfälligkeit zu verringern und die Häufigkeit erfolgreicher Ransomware-Angriffe zu senken. Schadensbegrenzung ist ebenfalls wichtig, aber 56 % der Befragten gehen implizit davon aus, dass dies der einzige Hebel ist, den sie ziehen können."

Der Mimecast-Bericht "State of Ransomware" ermöglicht es Unternehmen, ihre Risikobewertungen auf der Grundlage quantitativer Veränderungen zu aktualisieren, die in verschiedenen Regionen in Bezug auf Kennzahlen wie die Häufigkeit von Bedrohungsereignissen, das Ausmaß der Anfälligkeit und das potenzielle Schadensausmaß sowohl in Bezug auf primäre Verluste (in der Regel monetäre Verluste auf der Grundlage von Lösegeldzahlungen, Datenverlusten und Produktivitätseinbußen) als auch auf sekundäre Verluste wie Reputationsverluste und Geldstrafen zu beobachten sind. Diese Bewertungen können dann dazu beitragen, die Investitionsentscheidungen eines Unternehmens in angemessenere Bahnen zu lenken.

Empfehlungen

Cybersicherheitsteams leiden heute unter erheblicher persönlicher Belastung, auch diejenigen in Führungspositionen. Cyberkriminelle haben ihre Bemühungen seit der Pandemie nur noch verstärkt und lassen die Teams mit der Verteidigung komplexer Netzwerke gegen ausgeklügelte Angriffe kämpfen. Die persönlichen Folgen reichen von Stress und Burnout für den Einzelnen bis hin zum Mangel an Talenten in der gesamten Branche.

Ransomware ist ein großer Teil des Problems, da sich die Bedrohung weiterentwickelt und sich als zunehmend schädlich erweist - sei es auf betrieblicher Ebene oder aus der Sicht der Unternehmen in Bezug auf Finanzen und Reputation.

Unter den Entscheidungsträgern im Bereich Cybersicherheit herrscht jedoch Unklarheit über ihre Bereitschaft zur Bekämpfung dieser Bedrohung. Nur 6 % fühlen sich einigermaßen vorbereitet, um die Auswirkungen eines Ransomware-Angriffs abzumildern, gleichzeitig wünschen sie sich aber mehr Ressourcen, um der Bedrohung durch proaktive Prävention zuvorzukommen.

Es herrscht ein Gefühl der Unvermeidbarkeit, das sogar an Fatalismus grenzt, wenn es um Ransomware-Angriffe geht. Viele Unternehmen verlassen sich daher zu sehr auf Schutzmaßnahmen wie die Sicherung und Wiederherstellung von Dateien - was keine ausfallsichere Strategie ist.

Sobald ein Angriff stattgefunden hat, ist ein weiterer sehr viel wahrscheinlicher, nicht zuletzt, weil es für Cybersicherheitsteams schwierig ist, Mitarbeiter zu halten und zu rekrutieren. Es ist von entscheidender Bedeutung, dass Unternehmen vorausschauend handeln, um zu vermeiden, dass sie in einen Kreislauf von Zwischenfällen geraten.

Die Verantwortlichen für Cybersicherheit sollten sich darauf konzentrieren, ihre Verteidigungsfähigkeit zu verbessern: Sie sollten ihre Haltung proaktiver gestalten, um die Wahrscheinlichkeit zu verringern, dass ein Ransomware-Angriff Störungen verursacht.

01.

Integrieren Sie Sicherheitstools, um die Fähigkeiten zur Erkennung von Bedrohungen und zur Reaktion darauf zu verbessern und den Druck auf vielbeschäftigte Teams zu mindern

Da Bedrohungsakteure raffinierte Angriffe starten, die sich über Netzwerke hinweg bewegen, bieten fragmentierte Sicherheitssysteme nur begrenzten Schutz. Durch die Implementierung einer **Cybersecurity-Mesh-Architektur** (CSMA) können separate Sicherheitstools miteinander verbunden werden, um den Schutz an jede Ressource im Netzwerk anzupassen und so eine Null-Vertrauensumgebung zu schaffen. Eine **erweiterte Erkennungs- und Reaktionsarchitektur** (Extended Detection and Response, XDR) wiederum kann die Erkennung, Untersuchung und Reaktion vereinheitlichen, indem sie Echtzeitdaten von mehreren Sicherheitssystemen nutzt - und dann die Sicherheitssysteme automatisch anweist zu reagieren. Auf diese Weise werden E-Mail-Systeme zu den Augen und Ohren eines Unternehmens und ermöglichen eine bessere Erkennung von Bedrohungen.

02.

Sicherstellen, dass das Unternehmen über gute grundlegende Sicherheitspraktiken verfügt, um Schwachstellen zu verringern

Einfache Schritte können die Wahrscheinlichkeit von Angriffen deutlich verringern. Es ist von entscheidender Bedeutung, dass Cyber-Risiken auf Vorstandsebene als Priorität betrachtet werden und die Führungskräfte einen engagierteren Ansatz verfolgen. Da die Angreifer oft direkt auf die Mitarbeiter abzielen, können **Schulungen zum Sicherheitsbewusstsein** die Situation im gesamten Unternehmen verbessern. E-Mail ist ein besonders bedrohlicher Angriffsvektor, so dass robuste, aktuelle **E-Mail-Sicherheitslösungen** ebenfalls eine wertvolle Investition sind.

03.

Bewerten Sie Ihre Geschäftskontinuitätsplanung, um die tatsächlichen Folgen eines Angriffs zu verstehen

Angesichts der zunehmenden Zahl von Ransomware-Vorfällen ist es für Teams wichtig, über die **besten Strategien** zur Wiederherstellung des Betriebs im Falle eines Angriffs zu verfügen - aber das hängt von den Details ab. Stellen Sie sicher, dass in Ihrem gesamten Unternehmen bewährte Verfahren befolgt werden, z. B. indem Sie sicherstellen, **dass Datensicherungen** so regelmäßig wie möglich durchgeführt werden. Die Modellierung Ihrer Angriffsreaktion kann dazu beitragen, etwaige Lücken in Ihrer **Geschäftskontinuitätsplanung** aufzuzeigen.

Ransomware und alle Formen der Cyberkriminalität bleiben nicht untätig. Es ist von entscheidender Bedeutung, dass Cybersicherheitsteams ihre Ressourcen optimal nutzen können - und dass Unternehmen sicherstellen, dass sie die erforderliche Unterstützung erhalten.

Auf diese Weise können wir die Gesamtkosten von Ransomware für Unternehmen und Einzelpersonen senken und sicherstellen, dass Cybersicherheit eine nachhaltige, erfüllende Karriere ist.

Work Protected.

Advanced Email & Collaboration Security

mimecast

www.mimecast.com I ©2022 mimecast I All Rights Reserved I GL-4316

Mimecast: Work Protected™ Seit 2003 verhindert Mimecast, dass guten Unternehmen Schlimmes widerfährt, indem es ihnen ermöglicht, geschützt zu arbeiten. Wir ermöglichen es über 40.000 Kund:innen, Risiken zu minimieren und die Komplexität einer Bedrohungslandschaft zu bewältigen, die von bösartigen Cyberangriffen, menschlichem Versagen und technologischen Fehlern geprägt ist. Mimecast macht E-Mail- und Collaboration-Sicherheit zu den Augen und Ohren von Unternehmen weltweit.