mimecast®

Das Jahr der sozialen Distanzierung

Sicherheitsherausforderungen des neuen digitalen Arbeitsplatzes

März 2021

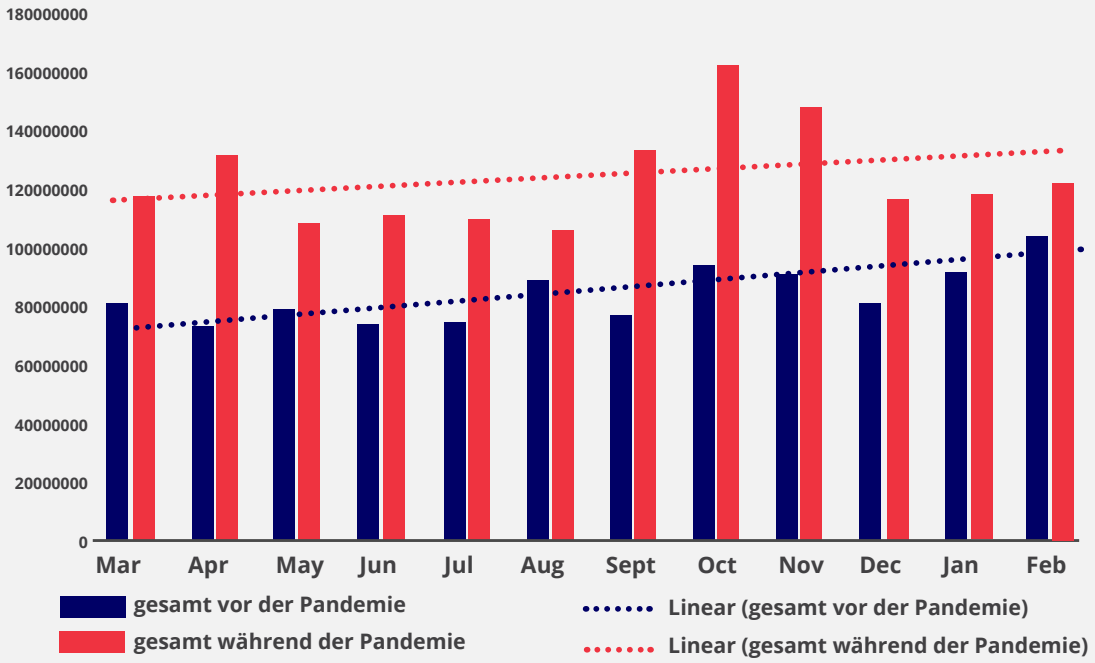
Im Laufe der Geschichte hat es Ereignisse gegeben, die einen grundlegenden Wandel der Gesellschaft auf globalem Maßstab bewirkt haben. Die Nutzbarmachung der Elektrizität, der Verbrennungsmotor, die beiden Weltkriege und das Internet kommen in den Sinn. Keines dieser Ereignisse hatte jedoch eine globale Transformation der Gesellschaft so schnell wie die COVID-19-Pandemie zur Folge.

COVID-19 wurde erstmals in der Silvesternacht 2019 gemeldet und wurde von der Weltgesundheitsorganisation im März 2020 zur Pandemie erklärt. Daraus folgte, das ein Großteil der Welt soziale Distanzierungsrichtlinien und andere Schutzmaßnahmen, einschließlich Abriegelungen, einführten. Arenen, Bahnhöfe, Bürogebäude und andere Orte, die normalerweise Menschenmassen anziehen, waren leer, da die Menschen sich in ihre Häuser zurückzogen, um sich und ihre Angehörigen vor der Pandemie zu schützen.

In dem Jahr, in dem die Abriegelungen begannen, gab es eine Explosion von Innovation und digitaler Transformation. Unternehmen gingen teilweise zu vollständig dezentraler Arbeit und digitalisierten Geschäftsprozessen über. Der sich langsam entwickelnde digitale Arbeitsplatz des Jahres 2019 war Mitte 2020 vollständig angekommen. (Der Running Gag lautete: “Wir haben das Jahr 2020 begonnen und beenden es im Jahre 2030.”)

Wie bei jedem großen, chaotischen Ereignis nutzten Bedrohungsakteure die Unsicherheit der Welt sofort aus. Die Massenangst um die COVID-19-Pandemie schuf ein Umfeld, das reich an Möglichkeiten für Social Engineering-Angriffe ist. In der Tat verzeichnete Mimecast einen durchschnittlichen monatlichen Anstieg von 48% Bedrohungsvolumen im Jahr der sozialen Distanzierung (im Vergleich zum Vorjahr).

Mimecast Detection Camparator: Vor und nach der Pandemie



48%

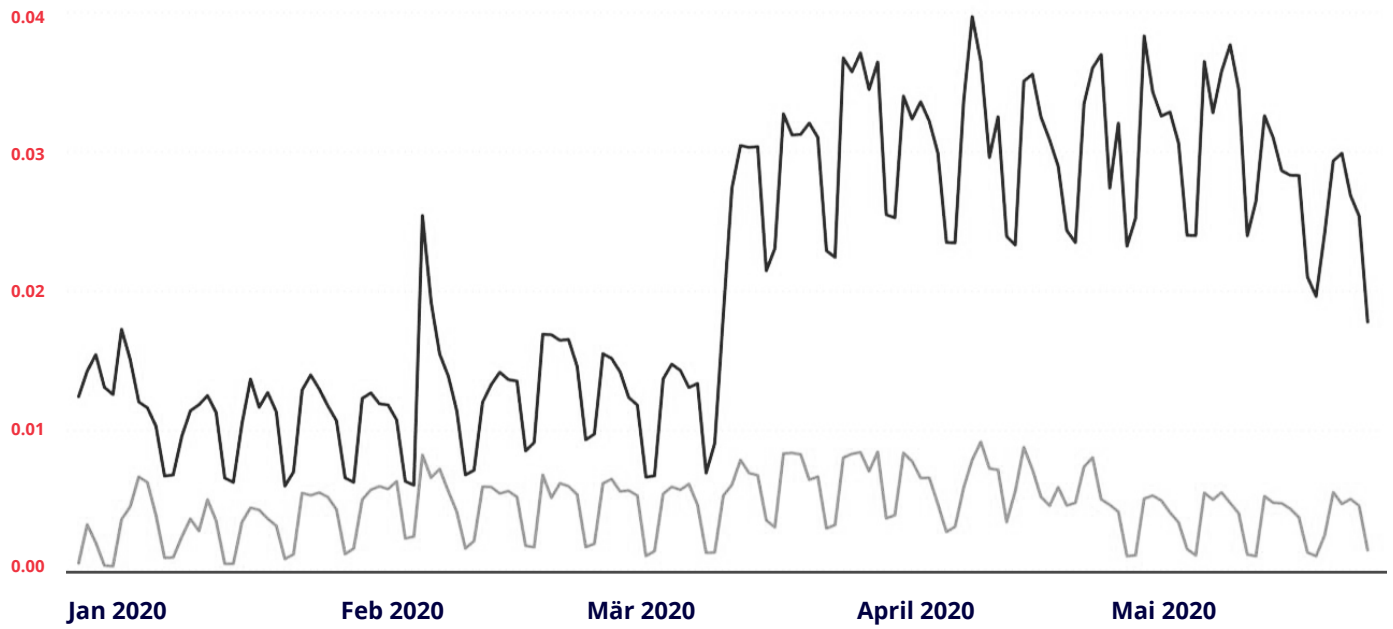
Mimecast verzeichnet einen 48%igen Anstieg des Bedrohungsvolumen im Zeitraum März 2020 bis Februar 2021 gegenüber dem Vorjahr, und der Anstieg fiel mit dem Ausbruch der COVID-19-Pandemie zusammen.

Der digitale Arbeitsplatz unter Beschuss

Mit dem Einzug der Mitarbeiter in das Work-from-Home-Modell wurde der digitale Arbeitsplatz für Unternehmen weltweit zur Realität. Büros und Konferenzräume wurden durch E-Mail, Instant Messaging und Zoom-Meetings ersetzt. Viele Unternehmen waren in der Lage, ihren Betrieb auf diese Weise mit nur minimalen Unterbrechungen aufrechtzuerhalten - das Cyber-Risiko stieg jedoch beträchtlich an. Aber eben auch die Notwendigkeit der digitalen Übertragung von sensiblen Inhalten. Themen, die früher in Konferenzräumen besprochen oder auf Whiteboards skizziert wurden, wurden nun über Collaboration-Tools besprochen und per E-Mail ausgetauscht.

Ein wesentlicher Eskalationsfaktor für Cyber-Risiken ist jedoch das Verhalten der Mitarbeiter im privaten Bereich. Die Leute sind einfach nicht so wachsam in Bezug auf die Cybersicherheit, wenn sie zu Hause sind. Mimecast stellte fest, dass die Zahl der unsicheren Klicks (Klicks auf bösartige URLs in E-Mails) von Mitarbeitern weltweit um das Dreifache anstieg, wenn sie zu Hause sind.

Durchschnittliche Anzahl von unsicheren Klicks pro Benutzer



3x

Es gab einen 3-fachen Anstieg an unsicheren Klicks, als die Arbeit von zu Hause aus begann.

Eine Untersuchung von Mimecast vom September 2020 ergab außerdem, dass die Gewohnheiten der Cyber-Hygiene von Land zu Land variieren. Zum Beispiel öffnen britische und deutsche Arbeitnehmer etwa halb so oft verdächtige E-Mails wie Arbeitnehmer aus den USA.

34% **Briten & Deutsche öffnen verdächtige Emails**

60% **Amerikaner öffnen verdächtige Emails**

61% **Emiratis öffnen verdächtige Emails**

Amerikaner und Emiratis öffnen fast doppelt so häufig verdächtige E-Mails wie Arbeitnehmer im Vereinigten Königreich und in Deutschland.

60%⇧

Die in Mimecasts Studie befragten Mitarbeiter gaben einen Anstieg von **60 % bei der Nutzung von Firmencomputern für private Zwecke** seit dem Beginn der COVID-19-Pandemie an.

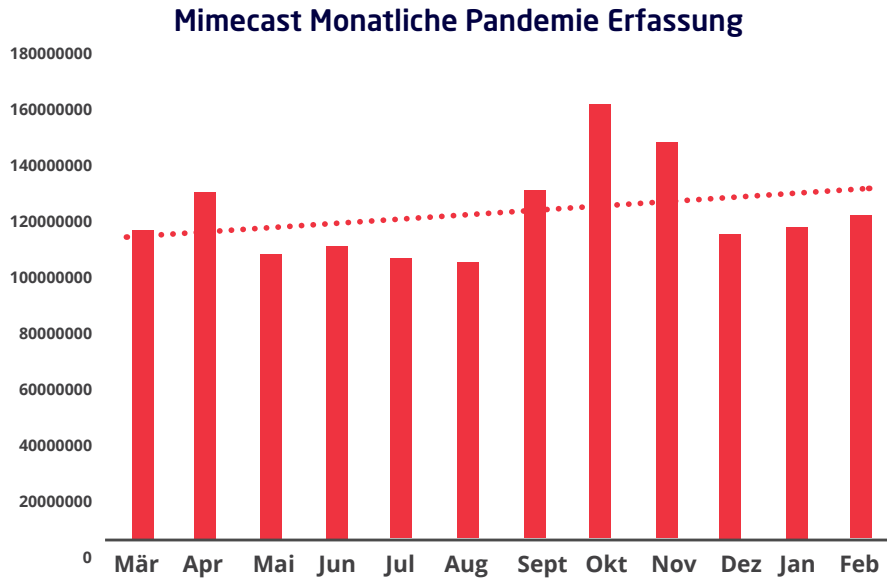
Persönliche Nutzung von Firmengeräten pro Tag

Die persönliche Nutzung von Firmencomputern hat während der Pandemie dramatisch zugenommen.

Taktiken der Bedrohungsakteure

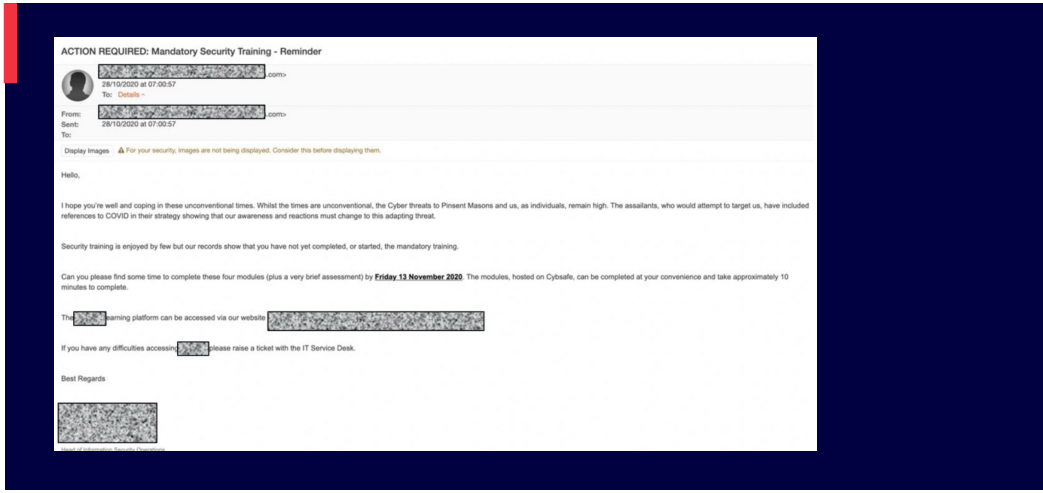
Bedrohungsakteure nutzen Krisen als Gelegenheit Social Engineering Angriffe zu starten. Wir sehen dies jedes Mal, wenn eine Naturkatastrophe oder ein anderes Ereignis geschieht, das die Menschen ablenkt und stresst. Während die meisten Katastrophen jedoch regionaler Natur sind und somit nur eine Teilmenge der Menschen in einem bestimmten Land oder einer Region betrifft, stellt die COVID-19-Pandemie eine perfekte Chance für Bedrohungsakteure dar, da es sich um eine Katastrophe handelt, die die ganze Welt betrifft. Bedrohungsakteure haben aus dem globalen menschlichen Elend Kapital geschlagen. Insgesamt ist das Bedrohungsvolumen im Vergleich zum Vorjahr um 48 % gestiegen. Die Abbildung unten zeigt, wie die Spitzen des Bedrohungsvolumens im April und Oktober mit den COVID-19 Infektionsspitzen im Jahr 2020 zusammenfallen.

Wie bereits erwähnt, ist ein Teil der Motivation für diesen dramatischen Anstieg der Angriffe die “Überflutung der Zone” mit Alarmen in SOCs, um die die Wahrscheinlichkeit zu erhöhen, dass überforderte Sicherheitsanalysten die Identifizierung von Angriffen verpassen.



COVID-bezogene Phishing-Angriffe nahmen viele Formen an. Einige versuchten Empfänger für die Notlage des Absenders zu sensibilisieren und Geld zu ergaunern. Andere gaben vor, wichtige COVID-bezogene Informationen für den Empfänger zu haben. Für Arbeitgeber waren diejenigen E-Mails am besorgniserregendsten, die darauf abzielten, die Zugangsdaten der Mitarbeiter zu stehlen. Die folgende E-Mail ist ein solcher Angriff, der versucht, Mitarbeiter dazu zu bringen, auf einen “Online-Kurs“ für „Obligatorisches Sicherheitstraining“ zu klicken.

Wie im E-Mail-Beispiel zu sehen ist, versuchten Bedrohungsakteure, die Beziehung zwischen Arbeitgeber und Arbeitnehmer auszunutzen, um Anmeldedaten zu stehlen und sich Zugang zu den Netzwerken und Systemen des Arbeitgebers zu verschaffen.


ACTION REQUIRED: Mandatory Security Training - Reminder

[redacted].com>
28/10/2020 at 07:00:57
To: Details -

From: [redacted].com>
Sent: 28/10/2020 at 07:00:57
To:

Display Images ⚠ For your security, images are not being displayed. Consider this before displaying them.

Hello,

I hope you're well and coping in these unconventional times. Whilst the times are unconventional, the Cyber threats to Pinsent Masons and us, as individuals, remain high. The assailants, who would attempt to target us, have included references to COVID in their strategy showing that our awareness and reactions must change to this adapting threat.

Security training is enjoyed by few but our records show that you have not yet completed, or started, the mandatory training.

Can you please find some time to complete these four modules (plus a very brief assessment) by **Friday 13 November 2020**. The modules, hosted on Cybsafe, can be completed at your convenience and take approximately 10 minutes to complete.

The [redacted] learning platform can be accessed via our website [redacted]

If you have any difficulties accessing [redacted] please raise a ticket with the IT Service Desk.

Best Regards

[redacted]

Diese Art von Taktik ist nur eine der Möglichkeiten, mit denen Bedrohungsakteure versuchen, den privaten Bereich zu nutzen, um Mitarbeiter zu kompromittieren und so unbefugten Zugriff auf Unternehmensnetzwerke und -systeme zu erhalten.

Während die COVID-19-Pandemie ein dominierendes Thema für Social-Engineering-Angriffe im Jahr der sozialen Distanzierung war, war es nicht das einzige. Im Laufe des Jahres gab es eine Reihe weiterer wichtiger Themen und Entwicklungen, darunter:

Angriffe auf den Gesundheitssektor. Eine weitere Möglichkeit, wie Bedrohungs -Akteure die COVID-19-Krise nutzen, sind Angriffe auf das überlastete Gesundheitssystem. Sowohl die U.K.'s National Cyber Security Center (NCSC) als auch das U.S.'s Federal Bureau of Investigation (FBI) habenWarnungen für den Gesundheits-Sektor im Mai 2020 herausgegeben.

Bedrohungsakteure versuchten vermehrt menschliche Fehler in Verbindung mit den stressigen Bedingungen zu nutzen, um Daten zu stehlen und Systeme mit Ransomware-Angriffen zu infizieren, in dem Glauben, dass Organisationen die unter dringenden Bedingungen arbeiten, eher bereit sind Lösegeld zu zahlen - in diesem Fall Krankenhäuser, die versuchen, die Gesundheit ihrer Patienten zu schützen.

Angriffe auf Impfstoff entwickler. Im Juli, haben das NCSC und die U.S. Cybersecurity und Infrastruktur-Sicherheit Agency (CISA) eine gemeinsame Warnung vor nationalstaatlichen Angriffen an Impfstoffentwickler geschickt. Die Angriffe zielten darauf ab geistiges Eigentum zu stehlen und die Reaktion der USA auf die COVID-19-Krise zu untergraben.

Angriffe auf Schulen. Da die Schulen daran arbeiten wieder zu öffnen, starteten Bedrohungsakteure lancierten Ransomware-Angriffe, da sie erkannten, dass Schulen oft schlecht geschützt sind. Da der Unterrichtsbeginn an Fristen geknüpft ist, und die Schulen auf operativen Budgets sitzen, die zur Lösegeldforderung angezapft werden können.

Der Sommer der Ransomware. Mimecast berichtete über die Rückkehr von Emotet in die Bedrohungslandschaft im Juli 2020, nach einer fünfmonatigen Unterbrechung. Dieser Malware-Dropper wird häufig verwendet, um den Trojaner Trickbot als zweite Stufe der Infektion zu nutzen, der dann verwendet werden kann um Rechner mit Ransomware zu infizieren. Mimecast entdeckte zunehmende Volumen von Ransomware während des gesamten Sommers (auch wenn nicht alle Emotet zugeschrieben werden können).

Angriffe auf die Impfstoff-Lieferkette. Als sich 2020 dem Ende zuneigte und Impfstoff-Rollouts begannen, prognostizierte Mimecast mit einem hohem Grad der Wahrscheinlichkeit (80% - 90%), dass Bedrohungsakteure beginnen würden Unternehmen in der Impfstoff-Lieferkette ins Visier zu nehmen. Auch hier würden sie Unternehmen in einem Zustand der Dringlichkeit vorfinden und wesentlich anfälliger für Zahlungsaufforderungen.

Lehren aus dem Jahr der sozialen Distanzierung: Cyber-Täuschung ist das Problem

Mimecast hat die Wahrscheinlichkeit, dass Bedrohungsakteure weiterhin die unsichere Arbeitssituation ausnutzen, als nahezu sicher (95 %) identifiziert. Diese Angriffe werden sich sowohl an Remote-Mitarbeiter als auch auf diejenigen, die ins Büro zurückkehren, richten. Bedrohungsakteure nutzen Unruhen aus - ob sich diese nun durch unerwartete Naturkatastrophen, jährliche Ereignisse wie die Steuersaison oder eine Pandemie, die nur einmal in diesem Jahrhundert auftritt, ergeben. Wenn wir das also wissen, warum sind sie dann weiterhin erfolgreich?

Die Antwort liegt darin, was die Unternehmen in Bezug auf Sicherheit denken. Während Sicherheitsorganisationen in Begriffen denken wie: E-Mail-Sicherheit, Benutzerbewusstsein, Link-Scanning, Identitätsmanagement und so weiter, denken Bedrohungsakteure in Begriffen wie: Täuschungskampagnen. So wie ein Zauberer mehrere Werkzeuge einsetzt (Irreführung, Licht, spezielle Requisiten usw.), um das Publikum zu täuschen, damit es denkt, dass eine Sache passiert, nur damit eine andere Sache passiert, machen Bedrohungsakteure das Gleiche, indem sie mehrere orchestrierte Taktiken und Werkzeuge nutzen, um Menschen zu täuschen und ihre Angriffe ausführen zu können. Und genau wie Zauberer uneffektiv wären, wenn das Publikum einen vollständigen Einblick in ihre Aktivitäten hätte, ist der beste Weg, um die Bedrohungsakteure zu stoppen, mehr Einblick in ihre Vorgehensweisen zu erhalten.

Defense-in-Depth bleibt eine wichtige Grundlage der Sicherheitsstrategie, allerdings hat sie auch zum Problem der aufgeblähten Infrastruktur beigetragen, die viele Unternehmen plagt - zu viele Sicherheitstools für Mitarbeiter, um sie alle zu verwalten.

Ein Teil der Lösung für dieses Problem ist die Integration: Durch die Integration der besten Cybersicherheits-Tools können Unternehmen einen viel größeren und präziseren Einblick in Cyber-Täuschungskampagnen erhalten, um sie früher in ihrer Entwicklung zu stoppen. Diese Cyber-Täuschungskampagnen umfassen drei Komponenten: Vorbereitung, Ausführung und Ausnutzung. Allzu oft ist die Sicherheitsstrategie nur auf die Ausnutzung konzentriert. Sogar der Prozess des Vorfalls und Reaktionsprozess bedeutet, dass schon etwas stattgefunden hat und das Unternehmen im reaktiven Modus ist, um den Schaden zu minimieren.

Mit einer integrierten Anti-Täuschungsstrategie können Unternehmen Kampagnen unterbrechen, bevor sie passieren. Durch proaktive Maßnahmen in den ersten beiden Phasen einer Kampagne:

Erste Phase: Vorbereitungsphase
Bedrohungsakteure führen eigene Erkundungen durch, recherchieren Mitarbeiter und Unternehmen in sozialen Medien, um die Effektivität von Social Engineering-Angriffen zu verbessern. Möglicherweise fälschen sie auch vertrauenswürdige Domains - wie die Website des Arbeitgebers oder die Website der Bank des Mitarbeiters - als Vorbereitung für die Stufe.

Schutz: Eine effektive Strategie zur Betrugsbekämpfung ist die Anwendung unterstützender Tools um diese Aktivitäten früh im Kampagnenzyklus zu identifizieren und Gegenmaßnahmen anzuwenden.

Zweite Phase: Ausführungsphase
Während einmalige Angriffe wahrscheinlich ein Werkzeug im Arsenal der Bedrohungsakteure bleiben werden, erfordern die schädlichsten Angriffe mehr Geduld und Planung. Raffinierte Bedrohungsakteure verwenden Multi-Vektor-Sequenzen, die Elemente enthalten wie aufwendige Kommunikationsketten, um zum Opfer Vertrauen aufzubauen (Verwendung ähnlicher Domains, gefälschte LinkedIn-Profile und gescrapte Webseiten). All dies ist darauf ausgelegt, den Eindruck der Authentizität zu erwecken.

Schutz: Eine Kombination aus Schulungen zum Thema Cybersicherheit für Endanwender und guten internen Prozessen, kombiniert mit Technologie, die, verdächtiges Verhalten erkennt, kann helfen, diese Ausführungsphase zu unterbrechen, bevor größerer Schaden entsteht. Zum Beispiel, indem man die Kreditorenbuchhaltung warnt, dass eine Zahlungsanforderung von jemandem stammt, der ein Logo in betrügerischer Absicht verwendet, kann verhindern, dass die Kompromittierung einer Geschäfts-E-Mail erfolgreich ist.

Wie andere historische Großereignisse warf auch das Jahr der sozialen Distanzierung ein Licht auf Schwachstellen in den Modellen der organisatorischen Resilienz. Mit Cybersecurity haben wir die Unzulänglichkeiten bereits bestehender Sicherheitsstrategien gesehen. Indem die Sicherheitsstrategie zu einem Modell weiterentwickelt und implementiert wird, können Organisationen Täuschungskampagnen früher in ihrem Entwicklungszyklus aufdecken. Und dabei helfen, beunruhigende Entwicklungen zu verhindern, wie z. B. den 3-fachen Anstieg der falschen Klicks, den Mimecast im März 2020 beobachtete. Wenn das Programm auf solch eine Weise aufgebaut ist, ist es viel widerstandsfähiger gegenüber massiven Ereignissen - sogar einer Pandemie, die nur einmal in einem Jahrhundert auftritt.

mimecast®

Relentless protection. Resilient world.™

Mimecast (NASDAQ: MIME) entstand 2003 mit dem Fokus Unternehmen vor Cyber-Bedrohungen zu schützen. Dabei stehen unsere zehntausende Kunden täglich im Mittelpunkt und wir geben niemals auf Sicherheitsrisiken gemeinsam zu bewältigen. Unser skalierbarer Entwicklungsansatz schützt den Hauptangriffspunkt für Cyberattacken – E-Mail. Wir investieren kontinuierlich, um Markenschutz, Security Awareness Training, Web Security, Compliance und andere wichtige Funktionalitäten zu integrieren. Mimecast hilft, große und kleine Unternehmen vor bösartigen Attacken sowie menschlichem und technischem Versagen zu schützen. Darin ist Mimecast führend und trägt so dazu bei, eine widerstandsfähige Welt zu schaffen.

Weitere Informationen finden Sie hier: www.mimecast.com/de