FORTRA

WHITEPAPER (Email Security)

Die Rolle der E-Mail-Sicherheit

Schützen Sie Ihr Unternehmen vor versteckten E-Mail-Bedrohungen

Cyberkriminelle greifen häufig über E-Mails an. E-Mails sind in der Arbeitswelt ein weit verbreitetes und vertrauenswürdiges Kommunikationsmittel, sodass Ihre Nachrichten die gewünschten Empfänger in aller Regel erreichen. Phishing und andere E-Mail-basierte Angriffe sind einfach auszuführen, können in großem Umfang eingesetzt werden und dem Angreifer erhebliche Vorteile verschaffen.

E-Mail-Phishing ist auf dem Vormarsch

Phishing und Business Email Compromise (BEC) sind nach wie vor die häufigsten Angriffsvektoren, um sich Zugang zu Unternehmen zu verschaffen. Sie bieten Bedrohungsakteuren häufig die nötige Grundlage, um Unternehmen und ihren Kunden Schaden zuzufügen. Und das, obwohl in den vergangenen zwei Jahren Summen in Milliardenhöhe in die Perimeter- und Endpunktsicherheit investiert wurden. Allein im Jahr 2021 führten Phishing und andere Formen des ausgefeilten E-Mail-Betrugs zu Verlusten in Höhe von über 44 Millionen USD.[1]

Die Anzahl der Phishing- und E-Mail-Spoofing-Angriffe hat sich im Jahr 2021 verdoppelt.[2] Schädliche Datenlecks entstehen durch gestohlene Anmeldedaten, nicht durch installierte Malware. Die durchschnittliche Anzahl der Business Email Compromise (BEC)-Versuche in 2020 stieg zwischen dem 2. und dem 3. Quartal um dramatische 15 % an.[3]

Laut Untersuchungen von IBM waren im Jahr 2021 verlorene oder gestohlene Zugangsdaten für 19 % der schädlichen Datenlecks verantwortlich, Phishing-Angriffe machten 16 % aus.[4] Nach Informationen von Atlas VPN hat Google seit Anfang 2020 2,02 Millionen Phishing-Websites identifiziert.[5] Wie aus dem Transparenzbericht von Google hervorgeht, fand das Unternehmen im Jahr 2020 pro Woche durchschnittlich 46.000 neue Phishing-Websites.[6]

Fehlendes Bewusstsein für die Phishing-Gefahren

Phishing-Angriffe sind in modernen Unternehmen ein ernsthaftes Problem. Trotzdem schulen mehr als 20 % der Unternehmen nur einmal jährlich ihre Mitarbeiter.[7] Dieser Unwissenheit ist es geschuldet, dass Phishing noch immer die häufigste Form von Cyberangriffen ist, bei denen Informationen gestohlen werden. Fast 20 % aller Mitarbeiter klicken wahrscheinlich auf Links in Phishing-E-Mails. Davon geben unglaubliche 67,5 % ihre Anmeldedaten auf Phishing-Webseiten ein, was aus Daten des Berichts „2020 Gone Phishing Tournament“ von Terranova Security (aus dem Fortra-Portfolio) ersichtlich ist. Das heißt: Ungefähr jeder siebte Arbeitnehmer (13,4 %) würde seine Passwörter auf einer schädlichen Phishing-Website preisgeben.

Bedrohungen von innen sind möglich

Eine Untersuchung der Wirtschaftsprüfungsgesellschaft BDO kam zu einem sehr unerfreulichen Ergebnis: 34 % der Unternehmer gehen davon aus, dass „geheime Absprachen“ der Mitarbeiter Teil von betrügerischen Handlungen waren.[8] Etwa die Hälfte der von den Befragten aufgedeckten Scams resultierte aus externen Quellen. Noch besorgniserregender ist, dass 21 % meinen, eigene Mitarbeiter seien für Scams verantwortlich.

Technologie zum Schutz vor E-Mail-Spoofing

Diese Gründe verdeutlichen, wie wichtig E-Mail-Sicherheit im Rahmen des gesamten Cybersicherheitsplans eines Unternehmens ist. Zum Glück gibt es technologische Schutzmaßnahmen gegen Spoofing, wie Domain-based Message Authentication, Reporting, and Conformance (DMARC) und Brand Indicators for Message Identification (BIMI), die zudem kostenlos und weithin verfügbar sind. Wenn Sie diese richtig einsetzen, erhöhen Sie die Sicherheit der ausgehenden und eingehenden E-Mail-Kommunikation in Ihrem Unternehmen erheblich.

Angriffe per E-Mail sind sehr effektiv. Es ist daher sehr unwahrscheinlich, dass Kriminelle in nächster Zeit damit aufhören werden. Unternehmen können sich nur dann effektiv gegen E-Mail-Bedrohungen schützen, wenn sie eine umfassende und individuelle E-Mail-Sicherheit einführen.

Arten von E-Mail-Risiken

Es gibt unterschiedliche Arten der Bedrohungen für die E-Mail-Sicherheit. Alle hängen allerdings eng mit Social-Engineering-Techniken zusammen. Social Engineering ist so effektiv, weil es unsere Emotionen manipuliert und somit unser Urteilsvermögen trübt. Entscheidend ist, wie wir Informationen verarbeiten.

Die Verhaltensökonomie besagt, dass Menschen zwei unterschiedliche Verarbeitungsgeschwindigkeiten haben: schnell und langsam.[9] Nehmen wir uns Zeit, Informationen zu verarbeiten, treffen wir Entscheidungen mit Bedacht und Logik. Cyberkriminellen wäre es anders natürlich lieber. Wir sind angreifbar, emotional und leicht zu manipulieren, und sie wollen unsere Fähigkeit testen, unter Druck schnell zu denken. Also versuchen Betrüger uns mit psychologischen Tricks dazu zu bringen, verdächtige E-Mails zu öffnen, schädliche Anhänge herunterzuladen und vertrauliche Informationen preiszugeben.

Einige der häufigsten E-Mail-Angriffe, die Social Engineering nutzen, sind:

Business Email Compromise (BEC)

BEC ist eine Scam-Masche, bei der der Empfänger dazu verleitet wird, auf eine E-Mail zu antworten, die scheinbar von einer Führungskraft des Unternehmens stammt. Die Kompromittierung durch E-Mails ist im Geschäftsalltag eine weit verbreitete und zunehmende Bedrohung für Unternehmen jeder Größe und in allen Branchen auf der ganzen Welt.

Unternehmen erleiden durch BEC-Scams Verluste, die in die Milliarden gehen können. Social Engineering ist eine der Haupttaktiken, mit denen BEC-Betrüger versuchen, unvorsichtige Mitarbeiter zu täuschen. Die häufigste Masche ist es, sich als CEO oder eine andere hochrangige Führungskraft auszugeben, um beispielsweise Überweisungen zu tätigen. Betrüger führen auch umfangreiche Hintergrundüberprüfungen und Überwachungen von Unternehmen und Personen durch, die sie angreifen wollen.

Nach Angaben des FBI gibt es 5 Arten von BEC-Scams[10]:

1. Beim „Supplier Swindle“ geben sich Betrüger als seriöse Unternehmen aus und bitten um die Überweisung von Geld auf ihr Konto, indem sie sich als die Lieferanten ausgeben, die die Rechnungen schicken.
2. Ein CEO-Betrug liegt vor, wenn Betrüger eine E-Mail an die Finanzabteilung eines Unternehmens senden und sich als CEO oder eine andere hochrangige Führungskraft ausgeben und sie auffordern, Geld auf ein von ihnen kontrolliertes Konto zu überweisen.
3. Das E-Mail-Konto des Geschäftsführers oder eines Mitarbeiters eines Unternehmens wird gehackt, um dann Zahlungsaufforderungen an die Lieferanten zu senden, die als Kontakte in dem kompromittierten Konto gespeichert sind. Im Anschluss werden die Gelder an fiktive Finanzinstitute überwiesen.
4. Mit „Attorney Check Scam“ werden Angriffe bezeichnet, bei denen sich der Täter als Anwalt oder Mitglied einer Anwaltskanzlei ausgibt, der für sensible und wichtige Themen zuständig ist. E-Mails oder Anrufe, die am Ende des Arbeitstages eingehen, haben oft einen betrügerischen Hintergrund.
5. Mitarbeiter der Personal- und Buchhaltungsabteilungen sind häufig das Ziel von Datendiebstählen. Hacker versuchen, sich Zugang zu vertraulichen Informationen wie Steuererklärungen oder sonstigen sensiblen Finanzdokumenten zu verschaffen, die zu anderen Mitarbeitern oder Führungskräften gehören. Solche Informationen dienen der Planung zukünftiger Angriffe.

Spear-Phishing
Spear-Phishing ist eine Form des Phishings mit dem Ziel, bestimmte Personen oder Abteilungen zur Herausgabe sensibler Informationen zu verleiten. Eine besonders gefährliche Form des Phishings ist die betrügerische Kommunikation mit Opfern auf elektronischem Wege (E-Mail, soziale Medien, Instant Messaging usw.). Dabei handelt es sich um eine fortschrittliche Taktik mit dem Ziel, sensible Informationen zu erlangen oder jemanden zu einer Aktion zu zwingen, durch die ein Netzwerk kompromittiert wird, Daten gestohlen werden oder anderweitig finanzieller Schaden verursacht wird. Herkömmliche Phishing-Techniken umfassen das Versenden von Massen-E-Mails an eine Vielzahl potenzieller Opfer. Spear-Phishing ist gezielter und erfordert viel Vorbereitung.

Eine E-Mail mit schädlichem Anhang ist ein häufiger Bestandteil von Spear-Phishing-Kampagnen. Der Name des Empfängers und seine Position in der Firma gehören zu den Details, die in hoch personalisierten E-Mails enthalten sind, um die Wahrscheinlichkeit zu erhöhen, dass die E-Mails geöffnet und der infizierte Anhang heruntergeladen wird.

Kontenübernahme
Kontenübernahme liegt vor, wenn ein unbefugter Dritter die Anmeldeinformationen eines Benutzers erlangt und dessen Online-Konto übernimmt. Cyberkriminelle können ein Unternehmen kompromittieren, indem sie sich als Mitarbeiter ausgeben und unbefugte Änderungen an Konten vornehmen, Phishing-E-Mails versenden, sensible Daten stehlen oder sich heimlich im Unternehmensnetzwerk bewegen. Daher ist es unerlässlich, dass Abteilungen wie IT, HR und Management die Bedrohungen kennen, denen sie in ihren jeweiligen Rollen ausgesetzt sind.

Cyberkriminelle verwenden auch regelmäßig betrügerische E-Mails, um Online-Kontoinhaber dazu zu bringen, Benutzernamen, Passwörter und andere sensible Daten auf Phishing-Websites einzugeben. Mit diesen Informationen können Betrüger auf echte Kundenkonten zugreifen und Betrug begehen.

Spam
„Spam“ ist mit Sicherheit jedem ein Begriff und trotzdem hat doch jeder sein eigenes Verständnis davon, was damit gemeint ist. Manche verstehen unter Spam jede Form von Werbenachrichten, die vom Empfänger nicht ausdrücklich angefordert wurde. Diese Art von E-Mails kann ziemlich lästig und aufdringlich sein. Daher sollten seriöse Unternehmen sie nur dann versenden, wenn der Empfänger sie ausdrücklich angefordert hat. Es ist wichtig zu wissen, dass diese Form von Spam völlig sicher ist.

Aber Spam, der in böswilliger Absicht verschickt wird, kann verheerend sein. Spyware und Ransomware sind zwei weit verbreitete Formen dieses Spams. Diese wird immer raffinierter und kann weitreichende Folgen für Unternehmen haben.

Vorschussbetrügereien, ähnlich dem E-Mail-Betrug des „nigerianischen Prinzen“, sind immer noch weit verbreitet, auch wenn die Leute heute misstrauischer sind und besser wissen, wie man sie erkennt und meldet. Gleichzeitig versuchen Cyberkriminelle mit realistischeren und ausgefeilteren (und daher gefährlichen) E-Mails, die Empfänger dazu zu bringen, auf einen Link zu klicken und das System des Nutzers zu beschädigen oder zu hacken.

Die vier Ziele der E-Mail-Sicherheit

Ein wichtiger Faktor, den wir bei der E-Mail-Sicherheit berücksichtigen müssen, ist, was wir mit dem Schutz von Unternehmens-E-Mails erreichen wollen.

Hohe Sicherheit für Ihr Unternehmen

Schutz der Email-Eingänge Ihrer Mitarbeiter

Stellen Sie den Schultz Ihrer Unternehmensdaten sicher

Sichern Sie Ihre Unternehmensmarke vor Reputationsverlust

1. Das Unternehmen schützen

E-Mail-Sicherheitslösungen geben Ihnen die Möglichkeit, Ihr Unternehmen vor externen Bedrohungen wie Malware, Spam oder immer raffinierteren Ransomware- und Spyware-Angriffen zu schützen, die in Ihr Unternehmen gelangen.

Unternehmen konzentrieren sich außerdem auch sehr darauf, gegen sie gerichtete Phishing-Angriffe abzuwehren. Die Schwierigkeit bei dieser Art von Angriffen ist jedoch, dass die Nachricht keinen schädlichen Inhalt enthält. Es sind im wahrsten Sinne des Wortes nur ein paar Worte, mit denen jemand versucht, z. B. die Finanzabteilung dazu zu bringen, eine falsche Rechnung auf die Bankkonten des Angreifers zu überweisen.

2. Datensicherheit erreichen

Mithilfe von E-Mail-Sicherheitslösungen können sowohl der ausgehende als auch der interne Datenfluss überwacht und gesichert werden, sodass die Daten geschützt sind. Mit integrierten DLP-Kontrollen (Data Loss Prevention) können Unternehmen sicherstellen, dass nur autorisierte Personen Zugang zu sensiblen Daten erhalten, oder sie können diese Daten automatisch verschlüsseln, um sie während der Übertragung zu schützen.

3. Posteingänge der Mitarbeiter schützen

Der wichtigste Teil des Schutzes des Datenflusses besteht darin, die Posteingänge Ihrer Mitarbeiter durch flexible Richtlinien zu schützen, die einen reibungslosen Datenaustausch ermöglichen, ohne die tägliche Kommunikation unnötig zu behindern. Das ist wichtig, wenn Sie vermeiden wollen, dass Sicherheitskontrollen die Produktivität Ihres Unternehmens und die Zufriedenheit Ihrer Mitarbeiter beeinträchtigen.

4. Den Ruf der Marke sichern

Kriminelle starten E-Mail-Phishing-Kampagnen, um zu versuchen, die Kunden einer Institution, z. B. einer Bank, dazu zu verleiten, freiwillig ihre Anmeldedaten anzugeben, auf einen Link zu klicken oder eine Datei zu öffnen, weil es so aussieht, als käme sie von einer vertrauenswürdigen Quelle.

Neben den offensichtlichen Folgen eines Verstoßes gegen die gesetzlichen Bestimmungen erkennen immer mehr Unternehmen die schädlichen Auswirkungen einer Phishing-Kampagne auf den Ruf ihrer Marke. Wenn ein Unternehmen auf aggressive Weise von Social Engineers missbraucht wird, wird die allgemeine Bereitschaft zur Kommunikation mit diesem Unternehmen sinken, genau wie die Interaktionsraten.

E-Mail-Sicherheitsrisiken richtig einschätzen: Das Johari-Fenster der E-Mail-Sicherheit

Das Johari-Fenster ist ein Konzept, das 1955 von den beiden amerikanischen Psychologen Joseph Luft und Harrington Ingham entwickelt wurde und von den Analysten der amerikanischen Nachrichtendienste häufig verwendet wird.[11]

Das Johari-Fenster machte das Konzept des bekannten Bekannten, des bekannten Unbekannten und des unbekannten Unbekannten populär und wurde von den US-Geheimdiensten übernommen, um bei der Analyse von Daten blinde Flecken in Bezug auf das, was wir wissen und nicht wissen, zu identifizieren.

Es kann auch dafür eingesetzt, die für die E-Mail-Sicherheit relevanten Risiken zu identifizieren, wie in der folgenden Abbildung dargestellt.

	Ihnen bekannt	Ihnen nicht bekannt
Bekannt für andere	Bekannte E-Mail-Sicherheitsrisiken	Tote Winkel
Nicht bekannt für andere	Versteckte E-Mail-Sicherheitsrisiken	Der unbekannte Faktor

Die vier Quadranten der E-Mail-Sicherheit

Schauen wir uns diese vier Quadranten genauer an, um zu verstehen, was die echten Sicherheitsrisiken bei E-Mails sind.

Bekannte E-Mail-Sicherheitsrisiken

Da immer mehr Unternehmen ihre Infrastruktur in die Cloud verlagern, wird die Nutzung nativer E-Mail-Systeme für die offizielle Kommunikation zum Standard. Der Schutz vor gängigen E-Mail-Bedrohungen wie Phishing, gefährlichen Links und infizierten Anhängen scheint mit den integrierten E-Mail-Sicherheitsfunktionen von Microsoft 365 und Google Mail ein Kinderspiel zu sein.

Trotzdem müssen Sie sich darüber im Klaren sein, dass die integrierten Sicherheitsfunktionen nicht ausreichen, um die ausgeklügelten E-Mail-Sicherheitsbedrohungen abzuwehren, denen moderne Unternehmen ausgesetzt sind – das bekannte Unbekannte. Unabhängige Untersuchungen haben beispielsweise gezeigt, dass Microsoft Office 365 nicht sehr gut darin ist, Phishing-E-Mails zu unterbinden. Des Weiteren stellt die cloudbasierte Office 365-E-Mail-Lösung für Unternehmen diese vor ganz eigene Herausforderungen, die sich nicht durch den Einsatz von individuellen Punktlösungen von Drittanbietern auf den eigenen System lösen lassen.

Versteckte E-Mail-Sicherheitsrisiken

Zwar bieten Microsoft 365 und Google einen gewissen Schutz vor den alltäglichen E-Mail-Sicherheitsrisiken, aber es gibt einige Lücken, durch die Unternehmen neuen E-Mail-Sicherheitsbedrohungen ausgesetzt sind. Auch wenn durch diese Tools 80 % der bekannten Angriffe und Risiken abgewehrt werden können, gibt es immer noch weitere 20 % „versteckte" Risiken, die Ihre Infrastruktur lahmlegen können. Beispielsweise können gezielte Ransomware- und Spyware-Angriffe herkömmliche Abwehrmechanismen umgehen und in Ihrem Unternehmen Schaden anrichten.

E-Mail-Sicherheitslösungen wie Clearswift von Fortra können diese Lücken schließen. Die Deep Content Inspection von Clearswift bietet sogar noch mehr Schutz und scannt Inhalte in einem mehrstufigen Prozess, der jede andere strukturelle Verifizierungsstufe auf dem Markt weit übertrifft. Mit Sandboxing entdecken Sie eigentlich versteckte Mechanismen, die Ihr System infizieren können. Sie erkennen Zero-Hour-Bedrohungen, die einen Angriff auslösen könnten, und können diese Bedrohungen gleichzeitig auch entschärfen.

Mit Optical Character Recognition (OCR) können Sie sogar schädliche Dateien erkennen, die auf den ersten Blick vertrauenswürdig aussehen, und diese bereinigen. Clearswift kann außerdem dank der Anti-Steganografie-Funktion versteckte Daten in Bildern entfernen. Ob es sich dabei um empfangene oder versendete Bilder handelt, spielt keine Rolle.

Darüber hinaus kann die Lösung Links zu schädlichen Websites entfernen, die im E-Mail-Text oder in den Anhängen versteckt sind. Und schließlich können Sie sensible Daten wie Kontonummern oder Steuer-IDs aus Ihren Dokumenten löschen und so Datenschutz- und Sicherheitsvorgaben einhalten.

Dabei werden weder die vertrauenswürdige Geschäftskommunikation behindert oder das Tagesgeschäft beeinträchtigt noch kommt es zu Verzögerungen.

Blinde Flecken

Neben den versteckten Risiken gibt es auch E-Mail-Risiken, die als blinde Flecken bezeichnet werden. Dabei handelt es sich um ausgeklügelte Phishing-Angriffe, bei denen die Nachricht vollkommen authentisch aussieht. Der Wortlaut in der E-Mail entspricht genau dem Wortlaut, den die Finanzabteilung oder das HR-Team jeden Tag sieht und liest. Die E-Mails sind allerdings so ausgelegt, dass sie Ihre Mitarbeiter dazu verleiten, freiwillig sensible Informationen über das Unternehmen preiszugeben oder sogar ihre Zugangsdaten weiterzugeben.

Diese Arten von Nachrichten erfordern einen anderen Einsatz von Bedrohungsdaten und -einblicken. Hier kommen Lösungen wie Agari von Fortra ins Spiel. Agari erkennt erweiterte Formen von Phishing und Social Engineering, die auf andere Art vielleicht nicht entdeckt werden. Mithilfe von Agari können auch ausgehende E-Mail-Inhalte gesichert werden. Ihre Mitarbeiter werden somit davor bewahrt, unabsichtlich Geschäftskunden und Partnern Probleme zu verursachen oder den Ruf Ihrer Marke zu schädigen.

Agari nutzt fortschrittlichste ML- und KI-Techniken, um die Muster vertraulicher Kommunikation und Inhalte zu modellieren und nicht vertrauenswürdige E-Mail-Kommunikation präventiv zu erkennen und sie automatisch aus den Posteingängen der Mitarbeiter herauszuhalten. Agari nutzt Bedrohungsdaten aus verschiedenen Quellen, um Unternehmensrichtlinien durchzusetzen und Schutzmaßnahmen für die Kommunikation der Mitarbeiter aufzubauen.

Der unbekannte Faktor

Doch trotz all der Schutzmaßnahmen, die wir um die Postfächer von Unternehmen herum aufbauen, tauchen täglich neue E-Mail-Bedrohungen und Social-Engineering-Taktiken auf. Daher ist es an dieser Stelle wichtig, dass Sie Ihre Mitarbeiter in die Lage versetzen, eine vorgeschaltete Verteidigungslinie zu bilden. Die Endnutzer in einem Unternehmen können der stärkste Verbündete sein und frühzeitig Anomalien erkennen.

Dafür benötigen Sie eine Schulungs- und Sensibilisierungslösung, die sich in Ihre vorhandene Technologie integrieren lässt. Terranova ist dabei Ihr stärkster Verbündeter. Terranova bietet Ihnen eine Bibliothek mit Schulungsmaterial, mit dem Sie individuelle Kurse für Ihre Mitarbeiter erstellen können. Die Lösung kann in Ihr Unternehmensverzeichnis integriert werden, ganz gleich, ob sich dieses vor Ort oder in der Cloud befindet, und generiert sowohl allgemeine Schulungsinhalte (z. B. DSGVO-Anforderungen) als auch spezifisches Material, z. B. für die Finanzabteilung, um sie bei der Erkennung von E-Mails mit Finanzbetrug zu unterstützen.

Dank der Modularität von Terranova können Sie ein Programm erstellen, das sowohl leicht verständlich als auch sehr komplex ist. Beispielsweise können jährliche Schulungsveranstaltungen um kleine monatlich stattfindende Module zu spezifischen Themen ergänzt werden, damit Ihre Mitarbeiter bestens informiert sind, aber im Tagesgeschäft nicht ausgebremst werden. Darüber hinaus können Sie mit vorgefertigten Vorlagen ganz einfach simulierte Phishing-Angriffe erstellen, damit Ihre Mitarbeiter schädliche Inhalte besser erkennen können.

Einblicke gewinnen und für starken Schutz sorgen

Diese ganzen technologischen Instrumente wären allerdings nutzlos, wenn sie nicht den Rahmen für eine umsetzbare Bedrohungsanalyse bilden würden. Markenmissbrauch, Kontenübernahmen, Betrug in sozialen Medien, Datenlecks und erweiterte E-Mail-Angriffe sind nur einige der vielen Online-Risiken, die die wertvollsten digitalen Werte und Informationen eines Unternehmens kompromittieren können.

Mit PhishLabs von Fortra können riesige Datenmengen aus dem offenen Web und dem Darknet, von Client-Feeds, aus sozialen Medien, von Mobilgeräten und aus E-Mails kontinuierlich analysiert und überwacht werden, um verwertbare Informationen zu erhalten. Durch die Kombination hochmoderner automatischer Analyse und menschlicher Kuratierung können wir unwichtige Daten eliminieren und Bedrohungen zuverlässig erkennen. Indem Sie dieses gesammelte Know-how in Clearswift, Agari und Terranova von Fortra einspeisen, kann Ihr Unternehmen seine Anfälligkeit für E-Mail-Angriffe verringern, ohne den Aufwand für das Sicherheitsteam zu erhöhen.

Abschließende Gedanken

Die Lösungen von Microsoft 365 und andere Anbieter sind vielleicht eine erste wichtige Maßnahme, um die Posteingänge der Nutzer vor Spam und Malware zu schützen, aber sie können keine soliden Funktionen zur Verhinderung von Datenverlusten und Bedrohungsinformationen bereitstellen, die für Unternehmen jeder Größe inzwischen unerlässlich sind. Das könnte Unternehmen davon abhalten, eine Microsoft 365-Implementierung in Erwägung zu ziehen, aber die Einschränkungen können mithilfe einer unternehmensgerechten Lösung überwunden werden.

Fortra bietet eine breite Palette an granularen E-Mail-Sicherheits-Tools, mit denen Sie Ihr Unternehmen sicher halten, die Postfächer Ihrer Mitarbeiter schützen und den Ruf Ihrer Marke wahren können.

SELBSTBEURTEILUNG DURCHFÜHREN

Quellen

[1] https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[2] https://glockapps.com/blog/email-spoofing/
[3] https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_Q3_2020.pdf
[4] https://www.ibm.com/reports/data-breach
[5] https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/?sh=66f129bf1662
[6] https://transparencyreport.google.com/
[7] https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/
[8] https://www.bdo.co.uk/en-gb/rethink/business-issues/strategy-operations/has-covid-19-made-your-business-more-vulnerable-to-corporate-fraud
[9] https://www.youtube.com/watch?v=YN6pijC-Kec
[10] https://www.ic3.gov/media/2015/150122.aspx
[11] https://www.communicationtheory.org/the-johari-window-model/

FORTRA

Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.

