Spear Phishing: Top-Bedrohungen und Trends

Vol. 7 März 2022

Wichtige Erkenntnisse über die neuesten Social-Engineering-Taktiken und die zunehmende Komplexität der Angriffe

Cyberkriminelle verfeinern ständig ihre Taktiken und sorgen dafür, dass ihre Angriffe immer komplizierter und schwieriger zu erkennen sind. Dieser fundierte Bericht behandelt die Entwicklungen und Trends in Sachen Social Engineering sowie die neuen Tricks, mit denen Angreifer ihre Opfer hinters Licht führen.»

Barracuda
Your journey, secured.

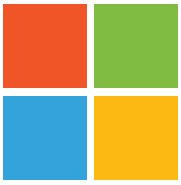
Inhaltsverzeichnis

Zentrale Ergebnisse

51 % von Social Engineering-Angriffen sind Phishing

Conversation Hijacking hat um annähernd **270 %** im Jahr 2021 zugenommen

Ein durchschnittlicher Angestellter eines kleinen Unternehmens mit weniger als 100 Mitarbeitern ist um **350 %** mehr Social Engineering-Angriffen ausgesetzt als ein Angestellter eines größeren Unternehmens



Microsoft ist die am häufigsten imitierte Unternehmensmarke, die bei **57 %** der Phishing-Angriffe verwendet wird

Bei 1 von 5 Unternehmen wurde 2021 ein Account kompromittiert

Cyberkriminelle kompromittierten 2021 etwa **500.000** Microsoft Office 365-Konten

1 von 3 bösartigen Logins in kompromittierte Accounts kamen aus Nigeria

Cyberkriminelle haben **3 Millionen** Nachrichten von 12.000 kompromittierten Accounts aus versendet

Die 13 E-Mail-Bedrohungsarten, die zunehmend komplexer werden

Jahrelang haben Security-Anbieter sich auf den Schutz vor E-Mail-Angriffen konzentriert, und der für ihre Kunden entwickelte Schutzumfang hat sich bei der Blockierung der meisten bösartigen oder unerwünschten E-Mail-Nachrichten als wirksam erwiesen. Doch dieser Ansatz allein reicht nicht mehr aus.

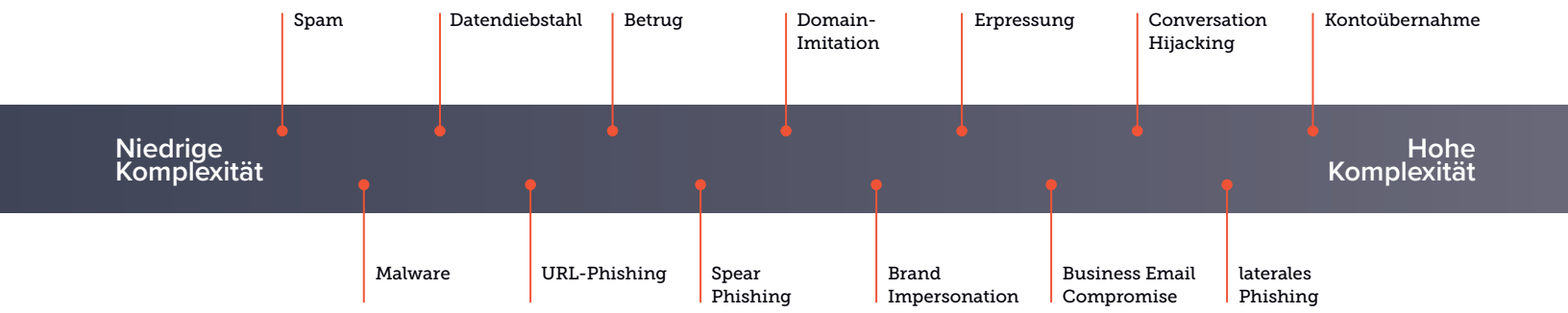
Selbst wenn Unternehmen Millionen Angriffe aufhalten können, sind E-Mail-Bedrohungen immer noch erfolgreich, weil sie zusehends komplexer und ausgeklügelter werden. Es vollzieht sich ein bedeutender Wechsel von volumetrischen zu gezielten Angriffen, von Malware zu Social Engineering, von einzelnen Hackern zu organisierten kriminellen Unternehmen, die von Angriffen profitieren, die mit einer einzigen Phishing-E-Mail beginnen.

E-Mail-Schutz, der sich auf Regeln, Richtlinien, Erlaubnis- oder Sperrlisten, Signaturen und andere Arten herkömmlicher E-Mail-Sicherheit stützt, ist gegen die sich ständig weiterentwickelnde Bedrohung durch Social Engineering-Angriffe nicht mehr wirksam.

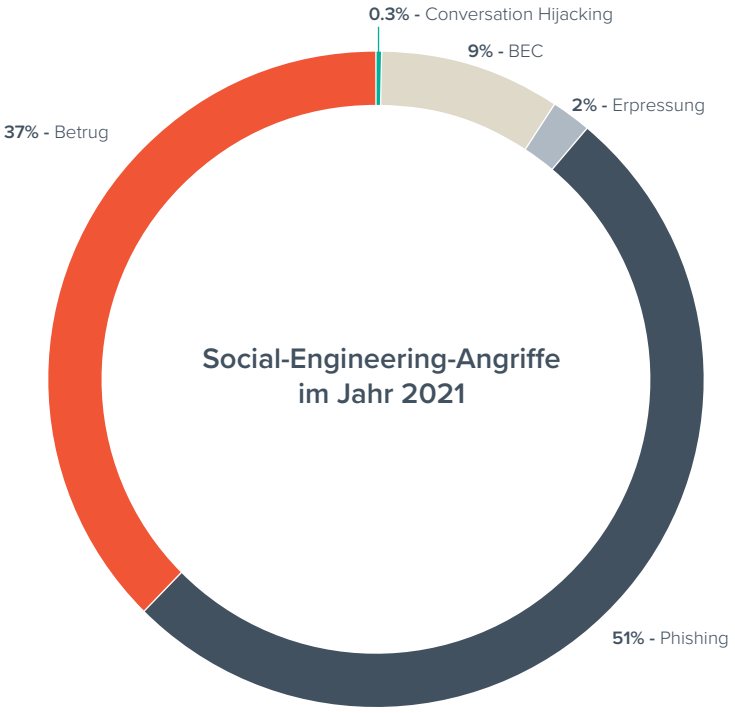
Hacker setzen eine Kombination von Taktiken ein, um die Benutzer zu einer Aktion zu verleiten, wie die Preisgabe ihrer Anmeldedaten, damit die Angreifer Zugriff auf die Unternehmensumgebung erhalten, die Weitergabe vertraulicher Informationen, die verkauft oder für weitere Angriffe verwendet werden könnten, oder einfach das Senden einer Zahlung, von Geschenkgutscheinen oder einer Geldüberweisung.

Die Ermittler von Barracuda haben 13 Arten von E-Mail-Bedrohungen identifiziert, denen Unternehmen heute gegenüberstehen. Das Spektrum reicht von breit gestreuten Angriffen wie Spam oder Malware bis hin zu gezielteren Bedrohungen, die Social Engineering wie Business Email Compromise und Impersonation nutzen.

13 Arten von E-Mail-Bedrohungen



Wir haben fünf unterschiedliche Kategorien von Social Engineering-Angriffen nachverfolgen können:



Business Email Compromise, abgekürzt BEC. Diese Angriffe beinhalten in der Regel den Identitätsmissbrauch einer Person entweder innerhalb oder außerhalb einer Organisation. 2021 machten diese Angriffe 9 % aller Social Engineering-Angriffe aus, die wir analysiert haben, ähnlich wie im Vorjahr. Aber sie sorgen für mehr Schlagzeilen. Das Bildungswesen, das Gesundheitswesen, der Handel, die Reisebranche – Organisationen aller Branchen wurden Opfer einer dieser Angriffe und haben dabei oft Millionen verloren. Bei einem typischen BEC-Angriff gibt sich ein Hacker als Mitarbeiter aus, in der Regel als eine Führungskraft, und fordert Überweisungen, Geschenkgutscheine oder die Überweisung von Geld an erfundene Wohltätigkeitsorganisationen.

Diese Angriffe richten sich nicht nur gegen Benutzer mit einem hohen Bekanntheitsgrad. Einem unserer früheren Berichte zufolge ist zum Beispiel der Finanzvorstand eines Unternehmens ebenso häufig das Ziel von Angriffen wie jeder andere Mitarbeiter seiner Abteilung.

Phishing Impersonation: Angriffe, die in der Regel als E-Mails einer bekannten Unternehmensmarke oder eines Service getarnt sind, um die Opfer dazu zu verleiten, auf einen Phishing-Link zu klicken. Diese Angriffe machen 51 % aller Social Engineering-Bedrohungen aus, die wir im vergangenen Jahr beobachtet haben. Fast alle Angriffe, die in diese Kategorie fallen, enthalten eine bösartige URL. Obwohl Phishing-E-Mails nichts Neues sind, haben Hacker mittlerweile raffinierte Methoden entwickelt, um die Erkennung durch Link Protection-Technologien zu umgehen und ihre bösartige Payloads in die Posteingänge der Benutzer zu liefern. Sie verkürzen URLs, verwenden zahlreiche Umleitungen und hosten bösartige Links auf Websites zur gemeinsamen Nutzung von Dokumenten, all dies um zu vermeiden, dass sie von E-Mail-Scan-Technologien blockiert werden.

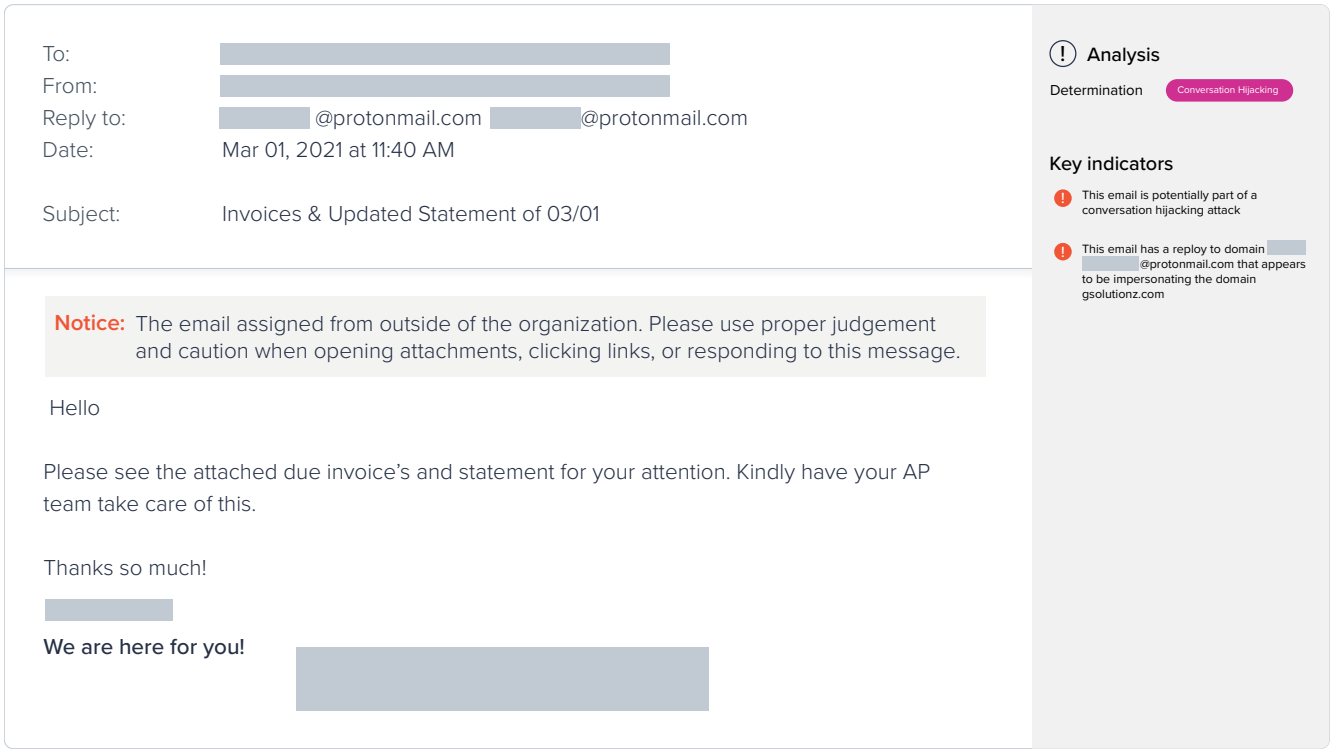
Hacker nutzen zunehmend Phishing als Teil ihrer Ransomware-Angriffe. Sie geben sich als bekannte Unternehmensmarken aus, um die Opfer auf Phishing-Seiten zu leiten und ihre Anmeldedaten zu stehlen. Sobald sie Zugang zu den Accounts eines Unternehmens haben, können sie die Ransomware von innen heraus verbreiten und so die Wahrscheinlichkeit verringern, entdeckt zu werden.

Erpresserische Angriffe machen nur 2 % der gesamten gezielten Phishing-Angriffe aus, die wir im vergangenen Jahr beobachtet haben. Bei diesen Angriffen handelte es sich meist um „Sextortion“ - E-Mail-Bedrohungen, bei denen Hacker damit drohen, sensible oder peinliche Inhalte an die Kontakte ihres Opfers weiterzugeben, wenn kein Lösegeld gezahlt wird. Die Forderungen belaufen sich in der Regel auf ein paar Hundert oder Tausend Dollar und müssen in Bitcoin gezahlt werden, die sich nur schwer zurückverfolgen lassen. Im Vereinigten Königreich ist die Zahl der an die National Crime Agency gemeldeten Fälle von Sextortion zwischen 2018 und 2020 um 88 % angestiegen und man geht davon aus, dass die Zahl weiter ansteigen wird.

Betrügerische Angriffe, sog. Scamming Attacks, können viele Formen annehmen und reichen von angeblichen Lotteriegewinnen und nicht beanspruchten Geldern oder Paketen bis hin zu gefälschten Geschäfts- und Stellenangeboten, Spenden und anderen Betrugsmaschen. Sie sind tendenziell etwas weniger zielgerichtet als die oben beschriebenen Angriffsarten, doch stellen betrügerische Angriffe 37 % aller Social Engineering-Angriffe dar, die wir im vergangenen Jahr entdeckt haben und sie sind immer noch erfolgreich. Da Hacker mit den verschiedenen von ihnen entwickelten Arten von Betrug ein weites Netz auswerfen, werden die Opfer durch diese Bedrohungen insgesamt um Hunderte Millionen von Dollar gebracht.

Hacker haben beispielsweise in den letzten Jahren COVID-19 in ihren Betrugsmaschen verwendet. Anfang 2021 haben wir eine Zunahme an Impfstoff-bezogenem Betrug mit gefälschten Angeboten für den frühzeitigen Zugriff auf Impfungen beobachtet. Gegen Ende 2021 stellten die Hacker ihre Taktik auf den Verkauf von COVID-19-Tests an ihre Opfer um.

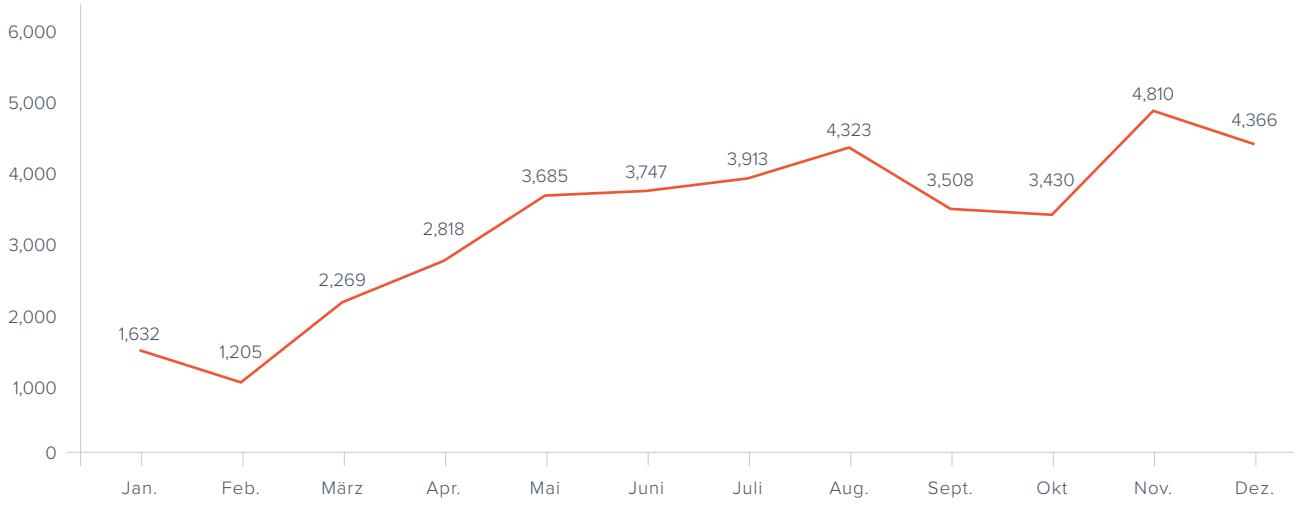
Conversation Hijacking, auch als Identitätsmissbrauch von Anbietern (Vendor Impersonation) bekannt, ist die Bezeichnung für einen gezielten E-Mail-Angriff, bei dem Cyberkriminelle sich in die bestehende Geschäftskommunikation einbringen oder neue Gespräche initiieren, basierend auf Informationen, die sie aus kompromittierten E-Mail-Konten oder anderen Quellen gesammelt haben.



Conversation Hijacking ist in der Regel, aber nicht immer, Teil eines Account Takeover-Angriffs. Angreifer nutzen Phishing-Angriffe, um Anmeldedaten zu stehlen und Geschäftskonten zu kompromittieren. Anschließend lesen Sie die E-Mails dieser kompromittierten Konten und überwachen diese, um die Geschäftsabläufe zu verstehen und etwas über laufende Geschäfte, Zahlungsverfahren und andere Details zu erfahren. Die Kriminellen nutzen diese Informationen, einschließlich interner und externer Gespräche zwischen Mitarbeitern, Partnern und Kunden, um authentische aussehende und überzeugende Nachrichten zu verfassen, sie von imitierten Domains aus zu versenden und ihre Opfer zur Überweisung von Geld oder zur Aktualisierung von Zahlungsinformationen zu verleiten.

Conversation Hijacking macht nur 0,3 % der Social Engineering-Angriffe aus, die wir im vergangenen Jahr beobachtet haben. Doch selbst in geringer Zahl können sie verheerende Folgen für Organisationen haben. Das Gesamtvolumen des Conversation Hijacking hat in den letzten Jahren zugenommen und die Beliebtheit dieser Methoden hat sich unter Hackern im Jahr 2021 verdoppelt. Das ist nicht überraschend, denn die Vorbereitung dieser Angriffe erfordert zwar einen hohen Aufwand für die Hacker, diese können aber erhebliche Gewinne abwerfen.

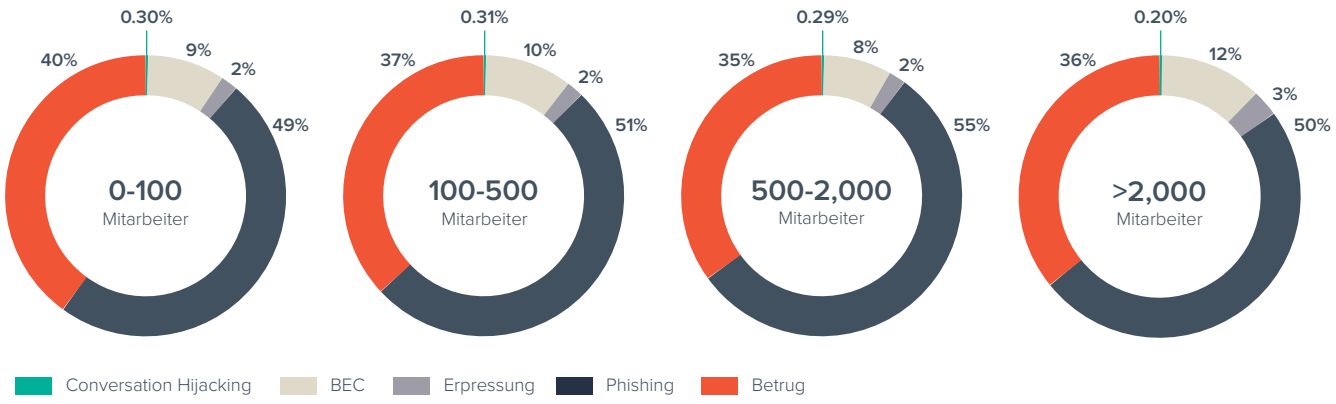
Conversation-Hijacking-Angriffe im Jahr 2021



Ziele von Social Engineering-Angriffen

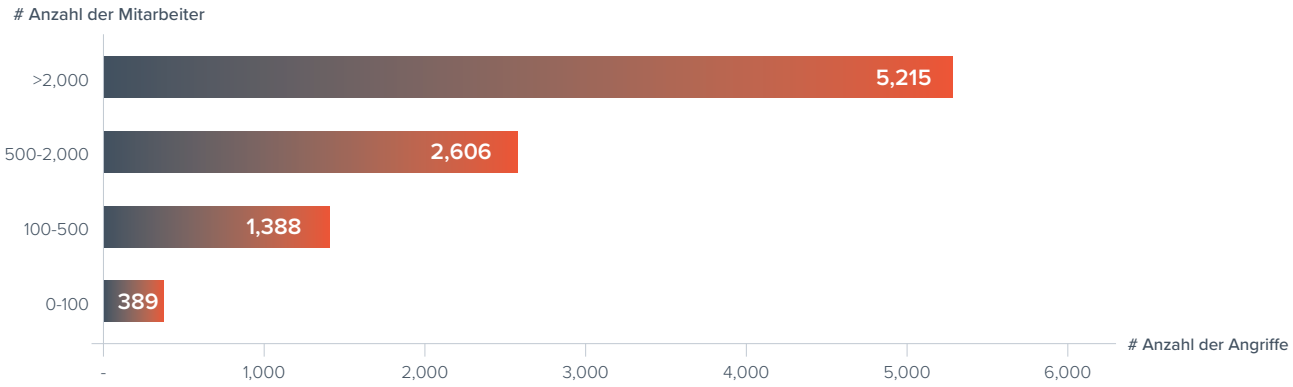
E-Mail-Angriffe unterscheiden sich nicht basierend auf der Größe einer Organisation. Größere Unternehmen mit mehr als 2.000 Mitarbeitern sind nur geringfügig häufiger von Business Email Compromise betroffen als kleine Unternehmen mit weniger als 100 Mitarbeitern. Die Wachsamkeit gegenüber allen Angriffsarten ist für jede Organisation wichtig, unabhängig von ihrer Größe.

Arten von Angriffen nach Unternehmensgröße



Es ist auch nicht verwunderlich, dass größere Organisationen allein aufgrund ihrer Größe mit einer größeren Anzahl von Angriffen konfrontiert sind. Ein Unternehmen mit über 2.000 Mitarbeitern ist beispielsweise jährlich mit über 5.000 Social Engineering E-Mail-Angriffen konfrontiert. Diese Zahl ist für Organisationen mit weniger Mitarbeitern viel kleiner.

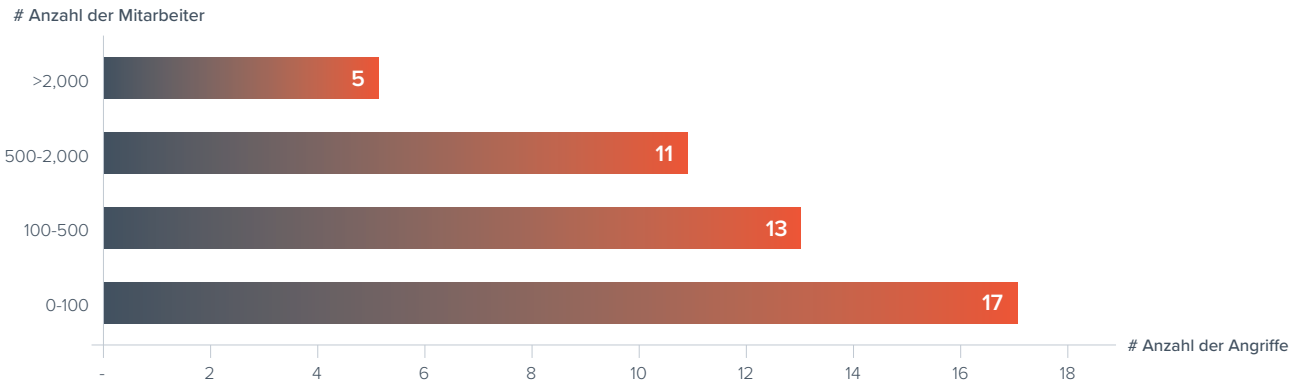
Durchschnittliche Anzahl von Social-Engineering-Angriffen pro Organisation



Wenn es jedoch um die Anzahl der Angriffe pro Posteingang geht, ist das Bild umgekehrt. Je kleiner das Unternehmen, desto wahrscheinlicher ist es, dass seine Mitarbeiter Ziele eines Angriffs werden. Tatsächlich ist ein durchschnittlicher Angestellter eines kleinen Unternehmens mit weniger als 100 Mitarbeitern zu 350 % häufiger von Social Engineering-Angriffen betroffen als ein Angestellter eines größeren Unternehmens. Kleine und mittelständische Unternehmen sind ein attraktives Ziel für Cyberkriminelle, da sie insgesamt einen erheblichen wirtschaftlichen Wert haben und es ihnen häufig an Ressourcen oder Fachwissen im Bereich Sicherheit fehlt.

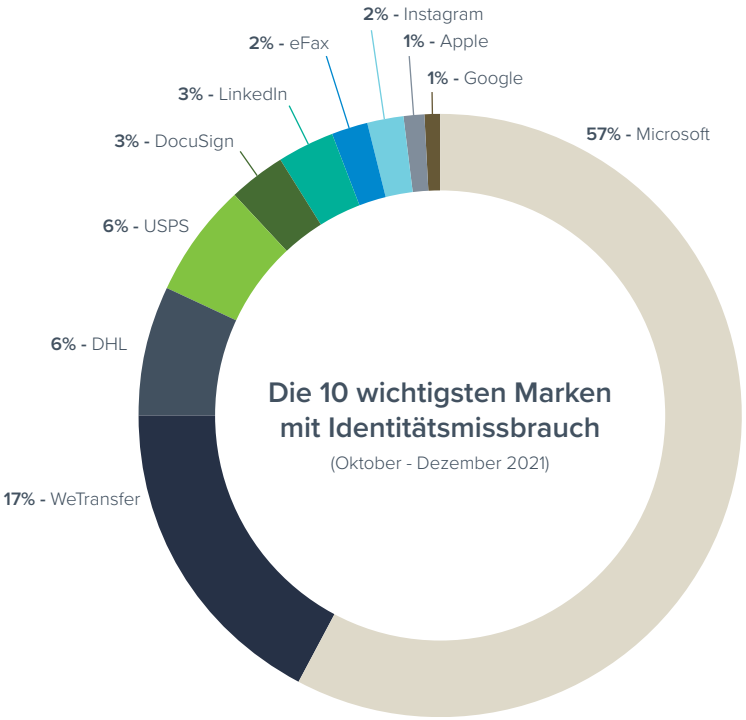
Kleinere Unternehmen sollten Investitionen in die Sicherheit nicht vernachlässigen – sowohl in Bezug auf die Technologie als auch auf die Aus- und Fortbildung der Benutzer. Die Kosten einer Sicherheitsverletzung können für kleinere Unternehmen verheerender sein. Einer Studie von Cybersecurity Ventures zufolge müssen 60 % der kleinen Unternehmen sechs Monate nach einem Sicherheitsverletzung ihre Türen schließen. Da 43 % von Online-Angriffen auf kleine Unternehmen abzielen, können die Kosten, wenn sie nichts unternehmen, zu hoch sein.

Durchschnittliche Anzahl von Social Engineering-Angriffen pro Mailbox



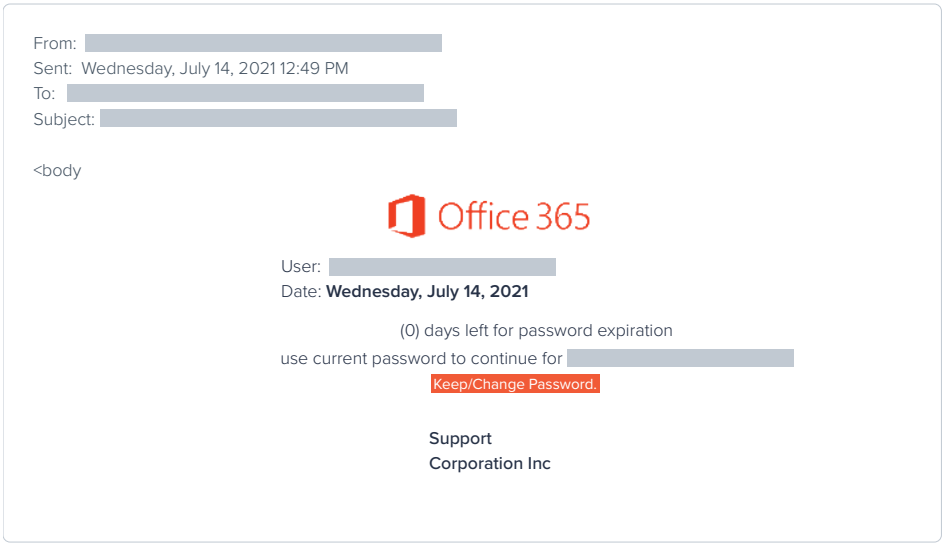
Die Top-10 der Brand Impersonation

Die Identität einer bekannten und vertrauenswürdigen Unternehmensmarke anzunehmen ist ein alter Trick vieler Hacker. Wir neigen dazu, Mitteilungen von unseren Lieblingsunternehmen zu erwarten und diesen zu vertrauen. Bei den Top-10-Unternehmensmarken, die bei Phishing-Impersonation-Angriffen verwendet werden, sind die drei Top-Unternehmensmarken – Microsoft, WeTransfer und DHL – seit 2019 dieselben geblieben.



Da 79 % der Organisationen zu Office 365 migriert haben und viele weitere planen, dies in naher Zukunft zu tun, überrascht es nicht, dass Microsoft-Marken nach wie vor ein Top-Ziel für Cyberkriminelle sind.

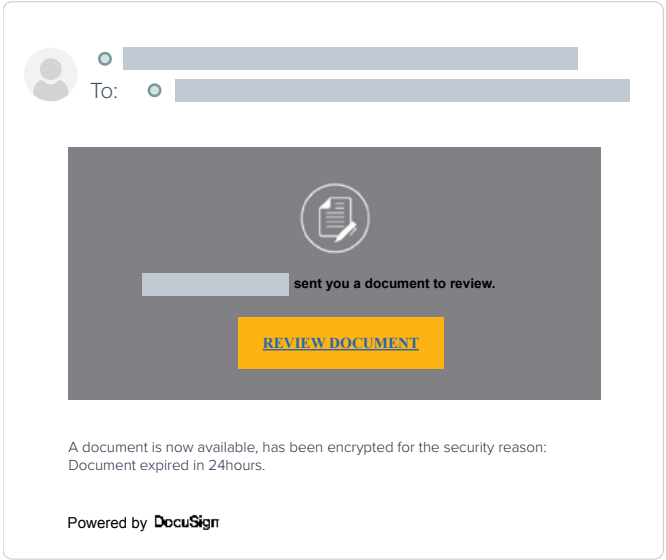
Betrachtet man die Top-10 der imitierten Unternehmensmarken, so wurde Microsoft bei 57 % der Phishing-Angriffe verwendet, ein erheblicher Anstieg im Vergleich zu 43 % im Juli 2021. Hacker machen sich die zunehmende Beliebtheit von Microsofts Cloud-basierten Diensten und das Arbeiten im Homeoffice in den letzten beiden Jahren zunutze. Cyberkriminelle senden gefälschte Sicherheitswarnungen oder Informationen zur Kontoaktualisierung an ihre Opfer, um sie zum Anklicken des Phishing-Links zu bringen. Das Ziel dieser Angriffe ist einfach: Anmeldedaten stehlen, um Zugang zu Unternehmensnetzwerken zu erhalten. Von dort aus können die Hacker andere Phishing-Angriffe einleiten, einschließlich Ransomware.



WeTransfer bietet Online-Services zu Dateiübertragungen an, die es den Nutzern ermöglichen, große Dateien zu teilen, die sie möglicherweise nicht direkt per E-Mail versenden können. Die Unternehmensmarke wurde bei 17 % der Phishing-Angriffe verwendet. Das Unternehmen ist sich bewusst, dass sein Name bei dieser Art von Angriffen verwendet wird, und warnt seine Benutzer, wachsam zu sein. Unternehmen sollten Betrug, wie das Imitieren von WeTransfer, in ihre Bewusstseinsschulungen einbeziehen.

DocuSign machte nur 3 % der Phishing-Angriffe aus, aber auch diese Angriffe können verheerende Folgen für Unternehmen haben. Da so viele Geschäftspraktiken online und in die Cloud verlagert werden, ist es nichts Ungewöhnliches, ein DocuSign zur Überprüfung zu erhalten, so dass viele Mitarbeiter nicht weiter darüber nachdenken, bevor sie darauf klicken. Cyberkriminelle registrieren gefälschte DocuSign-Konten oder kompromittieren bereits bestehende Konten und erstellen und versenden dann Dateien an ihre Opfer.

Andere Unternehmensmarken, die es in die Top-10 geschafft haben, waren Google, DHL und LinkedIn. Wenn eines dieser Konten kompromittiert wird, erhalten Hacker eine Fülle von persönlichen Informationen, die sie für weitere Angriffe nutzen können.



Account Takeover auf dem Vormarsch

Die Akzeptanz von Office 365 wurde in den letzten Jahren beschleunigt, angetrieben durch die Auswirkungen der Pandemie auf die Arbeit vom Homeoffice aus und die Cloud-Migration. Heute meldet Microsoft über 200 Millionen monatlich aktive Nutzer. Diese Beliebtheit ist nicht überraschend, da Office 365 die Produktivität und Kommunikation in Unternehmen verbessert. Mitarbeiter können nun von überall aus auf ihre E-Mail-Konten und Daten zugreifen. Aber das können auch Hacker. Der Zugang zu Office 365-Konten ist unglaublich wertvoll, da sie als Tor zu Einrichtungen und Unternehmen und deren Daten dienen.

Account Takeover ist eine Form von Identitätsdiebstahl und Betrug, bei dem sich ein böswilliger Dritter erfolgreich die Anmeldedaten eines Benutzerkontos beschafft. Indem sie sich als der echte Benutzer ausgeben, können Cyberkriminelle Benutzerkontodaten ändern, Phishing-E-Mails versenden, Finanzinformationen oder sensible Daten stehlen oder gestohlene Informationen verwenden, um auf weitere Accounts innerhalb der Organisation zuzugreifen.

Account Takeover ist eine der am schnellsten wachsenden Bedrohungen. Im Jahr 2021 war bei etwa 1 von 5 Unternehmen (20 %) mindestens eines ihrer Office 365-Konten kompromittiert. Das bedeutet, dass es Hackern 2021 gelang, etwa 500.000 Office 365-Konten weltweit zu kompromittieren. Ohne das richtige Schutzniveau kann der Account Takeover unentdeckt bleiben und der Organisation, ihren Geschäftspartnern und ihren Kunden wirklichen Schaden zufügen.

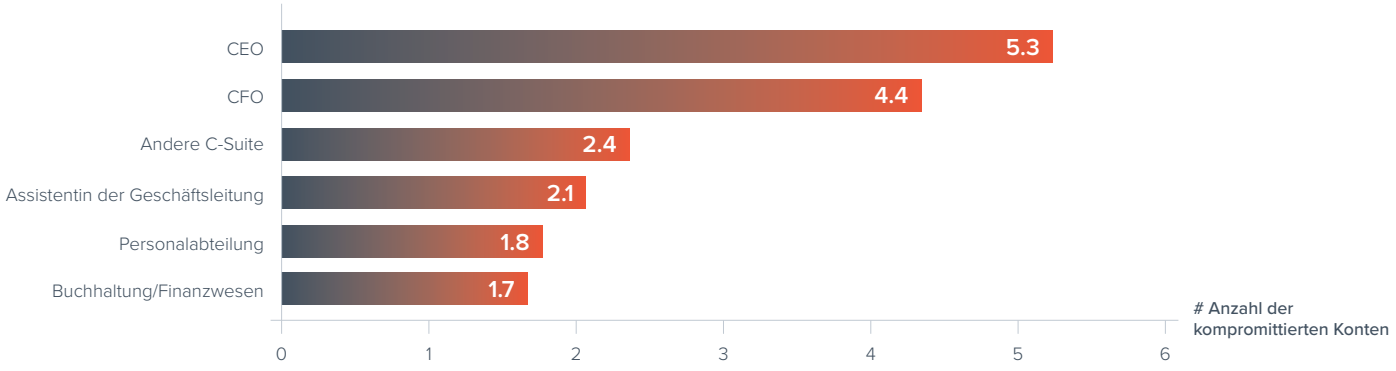
Bei 1 von 5 Unternehmen wurde 2021 ein Account kompromittiert

Führungskräfte der höchsten Ebene sind das Hauptziel von Account Takeover

Hacker haben es vor allem auf hochrangige Accounts von Führungskräften abgesehen. Die Wahrscheinlichkeit, dass Konten eines CEO und CFO übernommen werden, ist fast doppelt so hoch wie bei durchschnittlichen Angestellten. Sobald die Hacker Zugang haben, nutzen Cyberkriminelle diese Accounts zum Sammeln von Informationen oder um Angriffe innerhalb einer Organisation einzuleiten.

Auch Assistenten der Geschäftsleitung sind ein beliebtes Ziel, da sie häufig Zugang zu Accounts und Kalendern der Geschäftsleitung haben und in der Regel Nachrichten im Namen der Geschäftsleitung versenden können.

Account Takeover über Geschäftsfunktionen hinweg (pro 1.000 Postfächer)



Die vier Phasen eines Account Takeovers

Infiltration

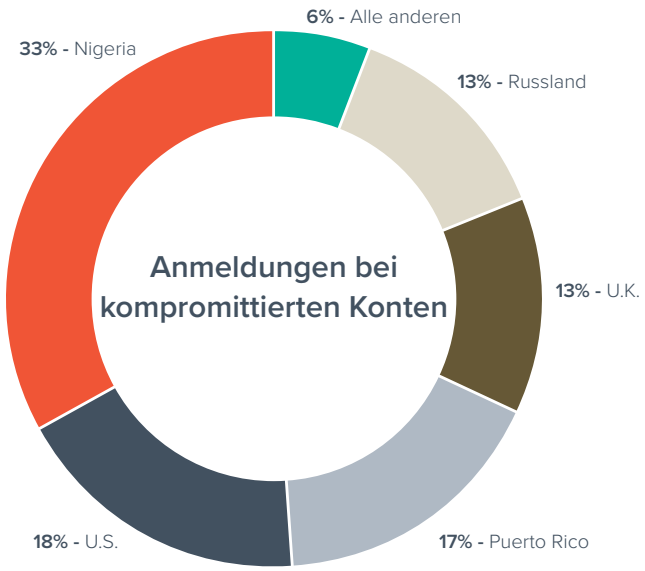
Microsoft ist eine der am häufigst imitierten Unternehmensmarken. Rund 57 % der Phishing-Angriffe geben sich als eine der Marken von Microsoft aus, wie Office 365, OneDrive, SharePoint oder andere. Hacker verwenden Social Engineering-Taktiken, um Benutzer dazu zu verleiten, eine Phishing-Website zu besuchen und ihre Zugangsdaten bekanntzugeben, was den Hackern ermöglicht, das System zu infiltrieren.

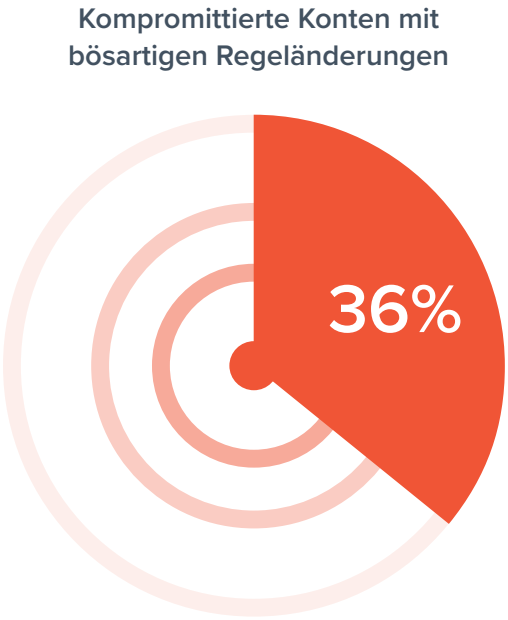
Reconnaissance

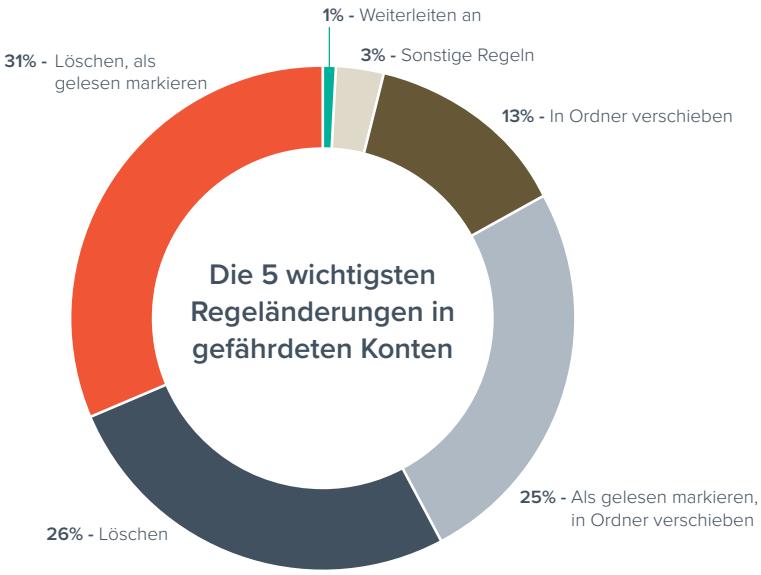
Sobald die Hacker Zugang zum Netzwerk einer Organisation haben, leiten sie ihre Angriffe selten sofort ein. Sie verwenden das kompromittierte Benutzerkonto, um die Aktivitäten des Unternehmens zu beobachten und zu verfolgen. Dann nutzen sie diese Informationen zu ihrem Vorteil. Die meisten Hacker bei den von uns analysierten Angriffen melden sich aus nur wenigen Ländern rund um den Globus an, wobei Nigeria an der Spitze der Liste steht. Eine von drei missbräuchlichen Anmeldungen bei kompromittierten Accounts kam aus Nigeria.

Sobald Hacker in einem Account sind, erstellen sie Weiterleitungsregeln oder Skripte, um alle E-Mails zu verbergen und zu löschen, die sie aus dem kompromittierten Posteingang senden. Verdächtige Posteingangsregeln sind häufig eines der Anzeichen für einen Account Takeover. Bei insgesamt 36 % der Organisationen, die einen kompromittierten Account hatten, wurde von den Hackern bösartige Posteingangsregeln eingerichtet, um ihre Aktivitäten zu verbergen. Genauer gesagt erstellen Hacker durchschnittlich zwei Regeln für jeden kompromittierten Account.

In mehr als 50 % der Fälle, in denen Hacker bösartige Regeln einrichten, legen sie Regeln zum Löschen von Nachrichten aus Accounts fest, damit Kontoinhaber keinerlei verdächtigen E-Mail-Aktivitäten bemerken. Eine weitere beliebte Aktion ist Nachrichten in einen bestimmten Ordner zu verschieben und diese häufig als gelesen zu markieren. Hacker kommen später zum Account zurück und überprüfen die Nachrichten im Ordner.







Sammeln von Zugangsdaten und Monetarisierung

Hacker nutzen kompromittierte Accounts als Startrampe für ihre Angriffe. Sie zielen auf hochwertige Accounts ab, versuchen, deren Zugangsdaten zu stehlen und bewegen sich dann lateral innerhalb einer Organisation weiter. Alles in allem werden kompromittierte Accounts für eine breite Palette von Angriffen genutzt, von Spam bis hin zu Business Email Compromise. Unsere Recherche zu fast 12.000 kompromittierten Accounts hat ergeben, dass sie im Jahr 2021 zum Versenden von über 3 Millionen bösartigen Nachrichten und Spam verwendet wurden.

Best Practices zum Schutz vor Spear-Phishing-Angriffen

Unternehmen sind heute zunehmenden Bedrohungen durch gezielte Phishing-Angriffe ausgesetzt. Um Ihr Geschäft und Ihre Benutzer zu schützen, müssen Sie in Technologien investieren, die Angriffe abwehren und in Schulungen, die den Mitarbeitern helfen, als letzte Verteidigungslinie zu agieren.

Technologie

- **Nutzen Sie die Vorteile künstlicher Intelligenz.** Betrüger passen ihre ihre E-Mail-Taktiken an, um Gateways und Spam-Filter zu umgehen. Daher ist es unerlässlich, eine Lösung einzusetzen, die Spear-Phishing-Angriffe, einschließlich Business Email Compromise, Impersonation und Erpressung, zuverlässig erkennt und abwehrt. Setzen Sie speziell entwickelte Technologie ein, die nicht nur auf der Suche nach schädlichen Links oder Anhängen beruht. Mithilfe von maschinellem Lernen zur Analyse normaler Kommunikationsmuster innerhalb Ihres Unternehmens kann die Lösung Anomalien erkennen, die einen Angriff anzeigen können.

- **Setzen Sie Account Takeover Protection ein.** Viele Spear-Phishing-Angriffe gehen von kompromittierten Accounts aus. Stellen Sie also sicher, dass Betrüger Ihre Organisation nicht als Basislager für diese Angriffe nutzen. Setzen Sie eine Technologie ein, die künstliche Intelligenz nutzt und erkennt, wenn Benutzerkonten kompromittiert wurden und die in Echtzeit Abhilfe schafft, indem sie Benutzer warnt und bösartige E-Mails entfernt, die von kompromittierten Accounts gesendet wurden.

- **Überwachen Sie Posteingangsregeln und verdächtige Anmeldungen.** Nutzen Sie Technologie, um verdächtige Aktivitäten zu identifizieren, einschließlich Anmeldungen von ungewöhnlichen Orten und IP-Adressen, ein mögliches Anzeichen für einen kompromittierten Account. Überwachen Sie E-Mail-Konten auch auf bösartige Posteingangsregeln, da diese häufig für die Übernahme von Accounts verwendet werden. Kriminelle loggen sich in das Konto ein, erstellen Weiterleitungsregeln und verbergen oder löschen alle E-Mails, die sie von dem Konto senden, um ihre Spuren zu verwischen.

- **Nutzen Sie die Multi-Faktor-Authentifizierung.** Die Multi-Faktor-Authentifizierung, auch MFA, Zwei-Faktor-Authentifizierung oder Zwei-Schritt-Verifizierung genannt, bietet neben dem Benutzernamen und dem Passwort eine zusätzliche Sicherheitsebene, wie einen Authentifizierungscode, einen Daumenabdruck oder einen Netzhaut-Scan.

- **Implementieren Sie DMARC-Authentifizierung und -Berichterstattung**. Domain-Spoofing ist eine der häufigsten Techniken, die für Impersonation-Angriffe verwendet werden. Die Authentifizierung und Durchsetzung mit DMARC kann Domain-Spoofing und das Kapern von Unternehmensmarken verhindern, während die DMARC-Berichterstattung und -Analyse Unternehmen bei der genauen Festsetzung für die Durchsetzung unterstützen kann.

- **Automatisieren Sie Incident Response.** Eine automatisierte Incident Response-Lösung hilft Ihnen, Bedrohungen, die in den Posteingängen der Benutzer gefunden wurden, schnell zu beseitigen. Dadurch wird die Schadensbehebung aller Nachrichten in Zukunft effizienter.

Mitarbeiter

- **Schulen Sie Mitarbeiter im Erkennen und Melden von Angriffen.** Klären Sie die Benutzer über Spear-Phishing-Angriffe im Rahmen von Schulungen zur Stärkung des Risikobewusstseins auf. Stellen Sie sicher, dass die Mitarbeiter diese Angriffe erkennen, ihren betrügerischen Charakter verstehen und wissen, wie sie die Angriffe melden können. Verwenden Sie Phishing-Simulationen für E-Mails, Voicemail und SMS, um Benutzer darin zu schulen, Cyberangriffe zu erkennen, die Wirksamkeit Ihrer Schulungen zu testen und die Benutzer zu bewerten, die am anfälligsten für Angriffe sind.

- **Überprüfen Sie interne Richtlinien.** Unterstützen Sie Ihre Mitarbeiter dabei, kostspielige Fehler zu vermeiden, indem Sie Richtlinien erstellen, die Verfahren für die Bestätigung von Anfragen festlegen, die per E-Mail eingehen, einschließlich Überweisungen und Kauf von Geschenkkarten.

- **Optimieren Sie den Schutz vor Datenverlust.** Verwenden Sie die richtige Kombination aus Technologien und Unternehmensrichtlinien, um sicherzustellen, dass E-Mails mit vertraulichen, persönlich identifizierbaren und anderen sensiblen Informationen blockiert werden und das Unternehmen nicht verlassen.

Über Barracuda

Wir von Barracuda wollen die Welt sicherer machen.

Wir sind der Meinung, dass jedes Unternehmen Zugang zu Cloud-basierten Sicherheitslösungen auf Unternehmensebene verdient, die einfach zu erwerben, bereitzustellen und zu nutzen sind. Wir schützen E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die mit der Entwicklung unserer Kunden wachsen und sich anpassen.

Über 200.000 Unternehmen weltweit vertrauen auf den Schutz durch Barracuda – auf eine Art und Weise, von der sie vielleicht nicht einmal wissen, dass sie gefährdet sind. Daher können Sie sich darauf konzentrieren, Ihr Unternehmen auf die nächste Stufe zu heben.

Weitere Informationen finden Sie unter barracuda.com.

Barracuda
Your journey, secured.