Mai 2020

13 Arten von E-Mail-Bedrohungen, über die man aktuell Bescheid wissen sollte

Wie Posteingangsschutz vor immer komplexer werdenden Angriffen schützt

Barracuda
Your journey, secured.

Inhaltsverzeichnis

Einführung: Deutliche Senkung der Anfälligkeit für gezielte E-Mail-Angriffe

Cyberangriffe können, abhängig von ihrer Art, ihrem Umfang und ihrer Schwere, Ihrem Unternehmen in vielerlei Hinsicht schaden. Dem Crime Complaint Center (IC3) des FBI zufolge haben Cyberangriffe alleine im Jahr 2019 für ein Schadensausmaß in der Höhe von 3,5 Milliarden USD gesorgt. Die beträchtliche Anzahl an undokumentierten Schäden ist dabei nicht inkludiert. Beim IC3 gingen im vergangenen Jahr 467.361 Meldungen ein, was mehr als 1.300 Meldungen pro Tag entspricht. 93% aller E-Mail-Datenverluste gehen auf Phishing zurück. Aus diesen Angriffen resultieren verschiedene indirekte und immaterielle Folgeschäden wie rechtliche Gebühren, Bußgeld, betriebliche Störungen, ein geschädigtes Image und weitere, schwerwiegende Auswirkungen.

In einer Welt, die stetigem Wandel unterliegt, reichen klassische E-Mail-Security-Lösungen nicht mehr aus, um ein Unternehmen zu schützen. Zudem muss man sich effektiv vor komplexen E-Mail-Bedrohungen schützen, die oft mittels Backdoor-Techniken wie Spoofing, Social Engineering und Betrug, Abwehrmechanismen umgehen, um in Netzwerke einzudringen und für Chaos zu sorgen.

Während umfassende E-Mail-Gateway-Abwehrmechanismen eine solide Basis bilden, senkt eine mehrstufige Schutzstrategie die Anfälligkeit für Angriffe drastisch und hilft, Ihr Unternehmen, Ihre Daten und Ihre Mitarbeiter besser zu schützen.

Dieses eBook bietet einen detaillierten Einblick in die wichtigsten Arten von E-Mail-Bedrohungen, deren Risiken und Auswirkungen auf Unternehmen. Es zeigt, wie KI und API-basierter Posteingangsschutz Lücken im E-Mail-Gateway beseitigen und so Ihre E-Mails umfassend vor Angriffen schützen können.

"Bis 2023 werden sich Business Email Compromise Angriffe (BEC) weiterhin jedes Jahr auf bis zu 5 Milliarden USD verdoppeln und somit zu großen finanziellen Verlusten für Unternehmen führen."

Quelle: Gartner, März 2020

Barracuda

Abwehr von immer komplexer werdenden E-Mail-Angriffen

Die E-Mail- und Phishing-Bedrohungen, vor denen Unternehmen heutzutage stehen, unterscheiden sich sehr stark, was Komplexität, Ausmaß und Auswirkung auf das Unternehmen und dessen Mitarbeiter anbelangt. Es gibt unterschiedliche Kategorien von E-Mail-Bedrohungen:

- **Spam:** unerwünschte Massen-E-Mails, die meist kommerzieller Natur sind. Sie werden ohne Bezug auf die Identität des Empfängers versandt.

- **Malware:** Software die genutzt wird, um Geräte zu beschädigen, für betriebliche Störungen zu sorgen, Daten auszuschleusen oder Zugriff auf ein Remote-System zu erlangen. Malware wird für gewöhnlich über E-Mail-Anhänge oder URLs verteilt, die zu bösartigen Inhalten weiterleiten.

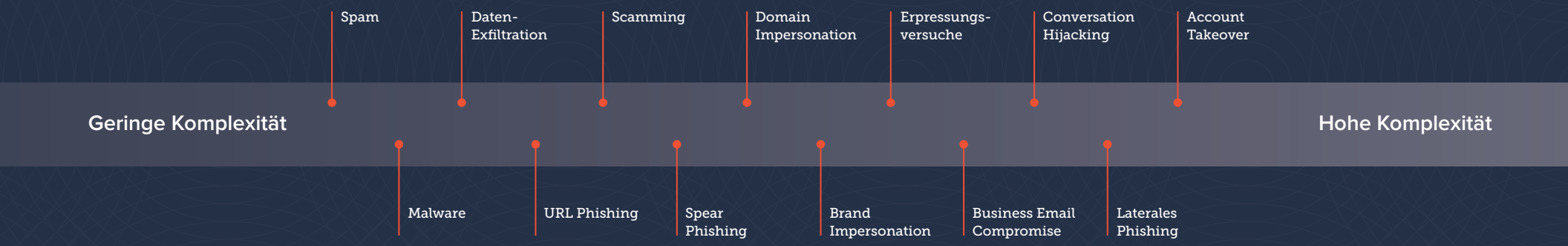
- **Data Exfiltration:** Diese Angriffe treten auf, wenn Daten ohne Zustimmung des Eigentümers kopiert oder von einem Remote-System abgerufen werden. Das kann versehentlich oder aus böswilliger Absicht geschehen.

- **Phishing:** Mittels dieser E-Mails soll dem Endanwender vorgetäuscht werden, dass diese von einer vertrauenswürdigen Person oder einem Unternehmen kämen. Dabei wird das Ziel verfolgt, dass der Endanwender Daten weitergibt, Geld überweist oder sich im Auftrag des Angreifers bei einem rechtmäßigen Konto einloggt.

- **Impersonation:** In diese Kategorie fallen sämtliche Angriffe, bei denen sich jemand als eine andere Person, ein Unternehmen oder ein Servicedienstleister ausgibt. Dabei handelt es sich um einen übergeordneten Begriff für verschiedene Angriffe, die für gewöhnlich Hand in Hand mit Phishing gehen.

13 Arten von E-Mail-Bedrohungen fallen unter diese Kategorien. Bei einigen dieser Angriffe kommen mehrere dieser Techniken gleichzeitig zum Einsatz, die Hacker oft miteinander kombinieren. Viele Spam E-Mails enthalten beispielsweise Phishing URLs und es ist nicht ungewöhnlich, dass ein kompromittiertes Konto für internen Betrug oder Überweisungsbetrug verwendet wird. Verständnis für das Wesen und die Merkmale dieser Angriffe hilft den bestmöglichen Schutz für Ihr Unternehmen, Ihre Daten und Ihre Mitarbeiter zu erstellen.

Da die Angriffe immer komplexer werden, wird es auch immer schwieriger, sich vor ihnen zu schützen.

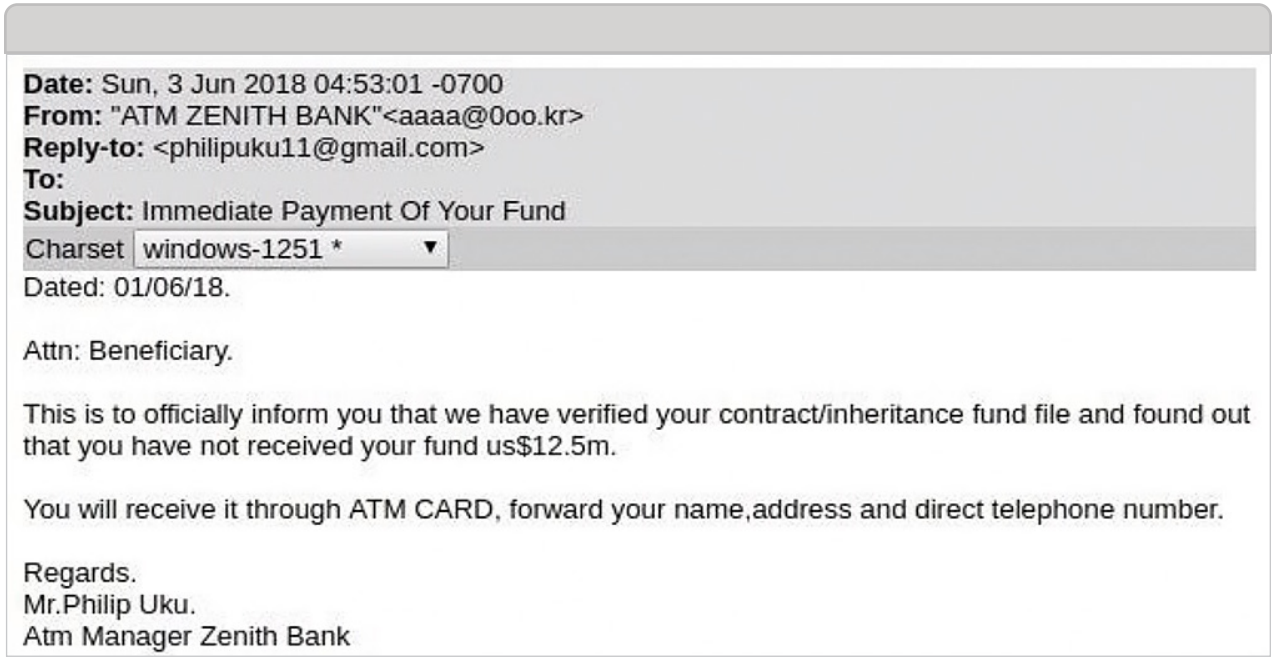


Spam

Barracuda

Spam E-Mails sind unerwünschte Massen-E-Mails, die auch Junk-E-Mails genannt werden. Spammer schicken für gewöhnlich ihre E-Mails an mehrere Millionen Empfänger mit der Erwartungshaltung, dass nur einige wenige auf die E-Mail antworten werden. Spammer sammeln E-Mail-Adressen von mehreren Quellen – u.a. verwenden sie Software, um sie aus Adressbüchern zu „ernten“. Die gesammelten E-Mail-Adressen werden oft auch an andere Spammer weiterverkauft.

Spam tritt in verschiedensten Formen auf. Manche Spam-E-Mails dienen Scam-Zwecken; andere haben E-Mail-Betrug als Ziel. Spam kann aber auch die Form einer Phishing-E-Mail annehmen, die mittels Brand Impersonation versucht, Benutzer zu täuschen, um an persönliche Informationen wie Anmelde- und Kreditkarteninformationen zu kommen.



Date: Sun, 3 Jun 2018 04:53:01 -0700
From: "ATM ZENITH BANK"<aaaa@0oo.kr>
Reply-to: <philipuku11@gmail.com>
To:
Subject: Immediate Payment Of Your Fund
Charset windows-1251 *

Dated: 01/06/18.

Attn: Beneficiary.

This is to officially inform you that we have verified your contract/inheritance fund file and found out that you have not received your fund us$12.5m.

You will receive it through ATM CARD, forward your name,address and direct telephone number.

Regards.
Mr.Philip Uku.
Atm Manager Zenith Bank

Beispiel für einen Angriff

Barracuda

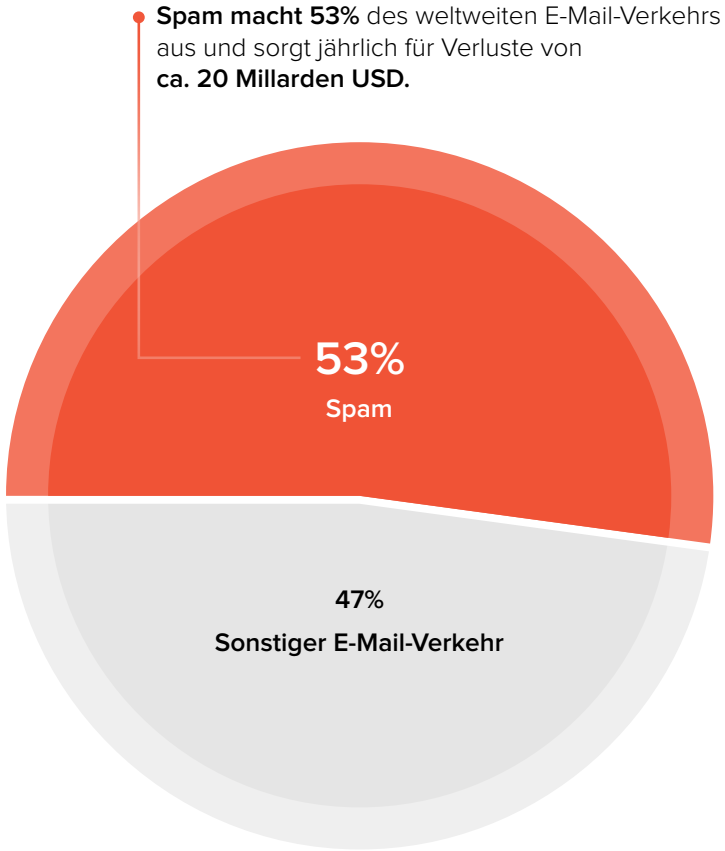
Auswirkungen von Spam

Spam verursacht bei Unternehmen Verluste von ca. 20 Milliarden USD pro Jahr. Durch die Flut an Junk-E-Mails im Posteingang wird die Produktivität gesenkt und dem Server erschwert, Nachrichten zu verarbeiten. Spam wird auch zur Verbreitung von Malware und in großflächigen Phishing-Angriffen verwendet.

Stärkung Ihrer E-Mail-Abwehr gegen Spam

Moderne Gateways wehren Spam erfolgreich ab; der Inline-Einsatz von Spam-Filtern sorgt dafür, dass Spam abgefangen wird, bevor er den Posteingang erreicht.

API basierter Posteingangsschutz ist bei solchen großflächigen Angriffen nicht so effektiv. Umfangreiche Angriffe wie Spam können E-Mail-Server überfordern und negative Auswirkungen auf die Performance des Posteingangs haben, da sie für eine große Last im Posteingang sorgen, bevor sie von APIs abgefangen werden.




Malware
Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover
Geringe Komplexität
Hohe Komplexität
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

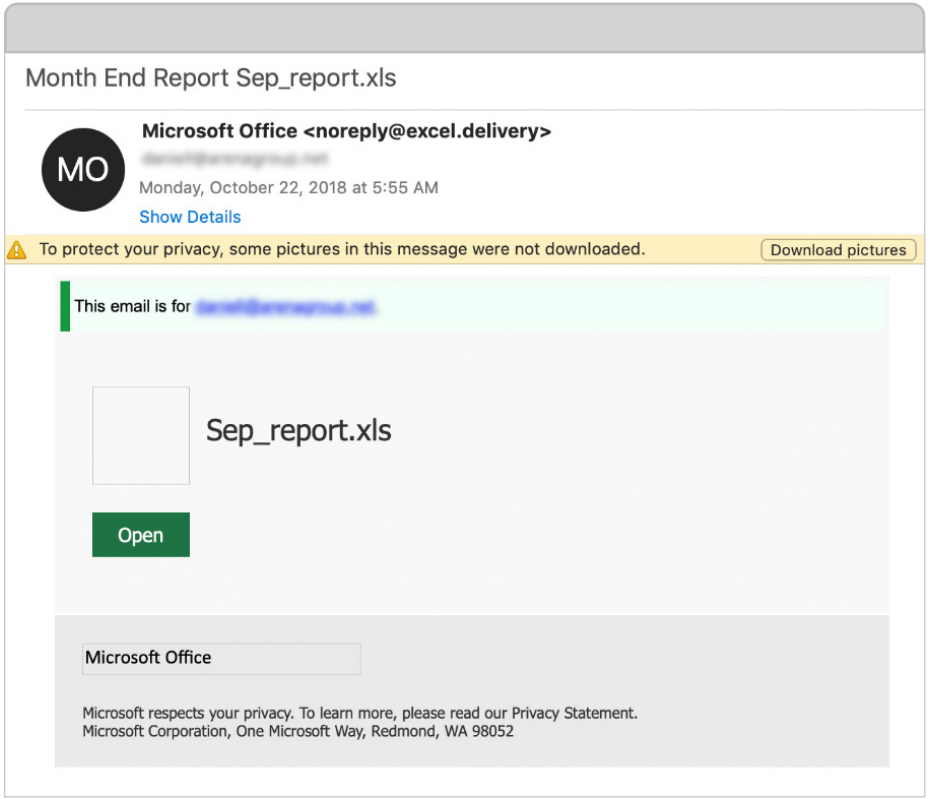
Cyberkriminelle nutzen E-Mails, um Dokumente, die bösartige Software – auch Malware genannt – beinhalten, zu versenden. Normalerweise ist die Malware direkt im Dokument integriert oder ein eingebettetes Script lädt sie von einer externen Webseite herunter. Zu den häufigsten Arten von Malware gehören Viren, Trojaner, Spyware, Würmer und Ransomware.

Häufigste Arten von Malware-Angriffen

Volumetrische Malware : Diese Art von Malware ist darauf ausgerichtet, sich rapide auszubreiten, indem sie gängige Schwachstellen alter, ungepatchter Systeme nutzt. Es werden bekannte Schwachstellen ausgenutzt und diese Art von Malware kann allgemein durch Signaturen und einfache Heuristiken identifiziert werden.
Volumetrische Malware ist auch unter folgenden Namen bekannt: Commodity Malware und Viren.

Zero-Day-Malware : Bei komplexen Malware-Angriffen kommen Zero-Day-Bedrohungen zum Einsatz. Diese sind neuartig und passen nicht zu bekannten Malware-Signaturen Sie nutzen noch unbekannte Schwachstellen oder eine neue Malware-Variante über die üblichen Wege. Diese Zero-Day-Angriffe können von signaturbasierten Sicherheitslösungen nicht erkannt werden.
Zero-Day-Malware ist auch unter folgendem Namen bekannt: 0Day.

URL-Angriffe: URL-Angriffe, die zu bösartigen Webseiten oder Schadsoftware führen, haben meist das Ziel, Benutzer dazu zu bewegen, auf den Link zu klicken und somit Malware herunterzuladen.



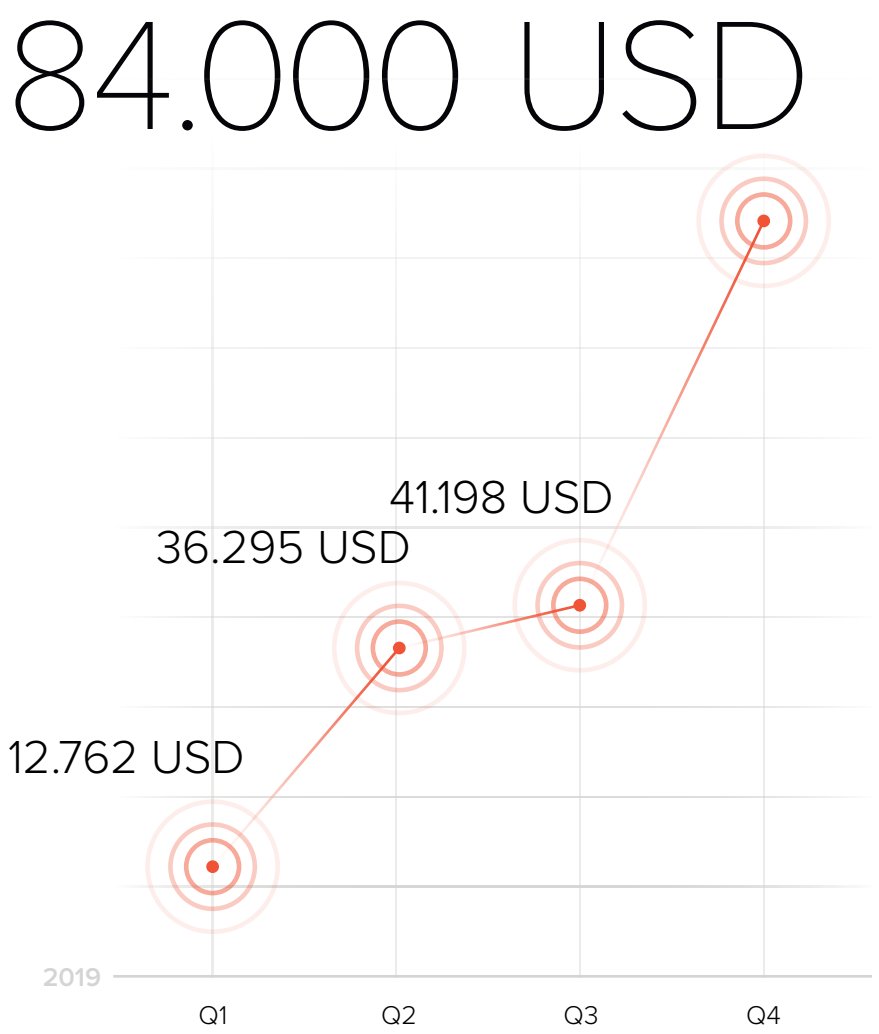
Beispiel für einen Angriff

Auswirkungen von Malware

94 % der Malware wird via E-Mail verbreitet. Mittels Ransomware – einer der beliebtesten Formen von Malware – infizieren Cyberkriminelle das Netzwerk und verschlüsseln E-Mails, Daten und andere kritische Dateien, bis Lösegeld ausbezahlt wird. Diese sich stets weiterentwickelnden und komplexen Angriffe verursachen Schäden und finanzielle Verluste. Sie können das tägliche Geschäft lähmen, für Chaos sorgen und zu finanziellen Einbußen durch Ausfälle, Lösegeldzahlungen, Schadensbehebungskosten und zu anderen unerwarteten, nicht budgetierten Ausgaben führen.

Im Jahr 2019 haben die durch Ransomware verursachten Kosten 170 Milliarden USD betragen. Diese Zahl umfasst nicht nur das ausbezahlte Lösegeld, sondern auch die Verluste durch Produktivitätsminderung, Datenbeschädigung und andere vom Angriff verursachte finanzielle Schäden. Das durchschnittliche Lösegeld hat sich mehr als verdoppelt. Von 41.198 USD im Q3 2019 auf 84.000 USD im Q4 2019.

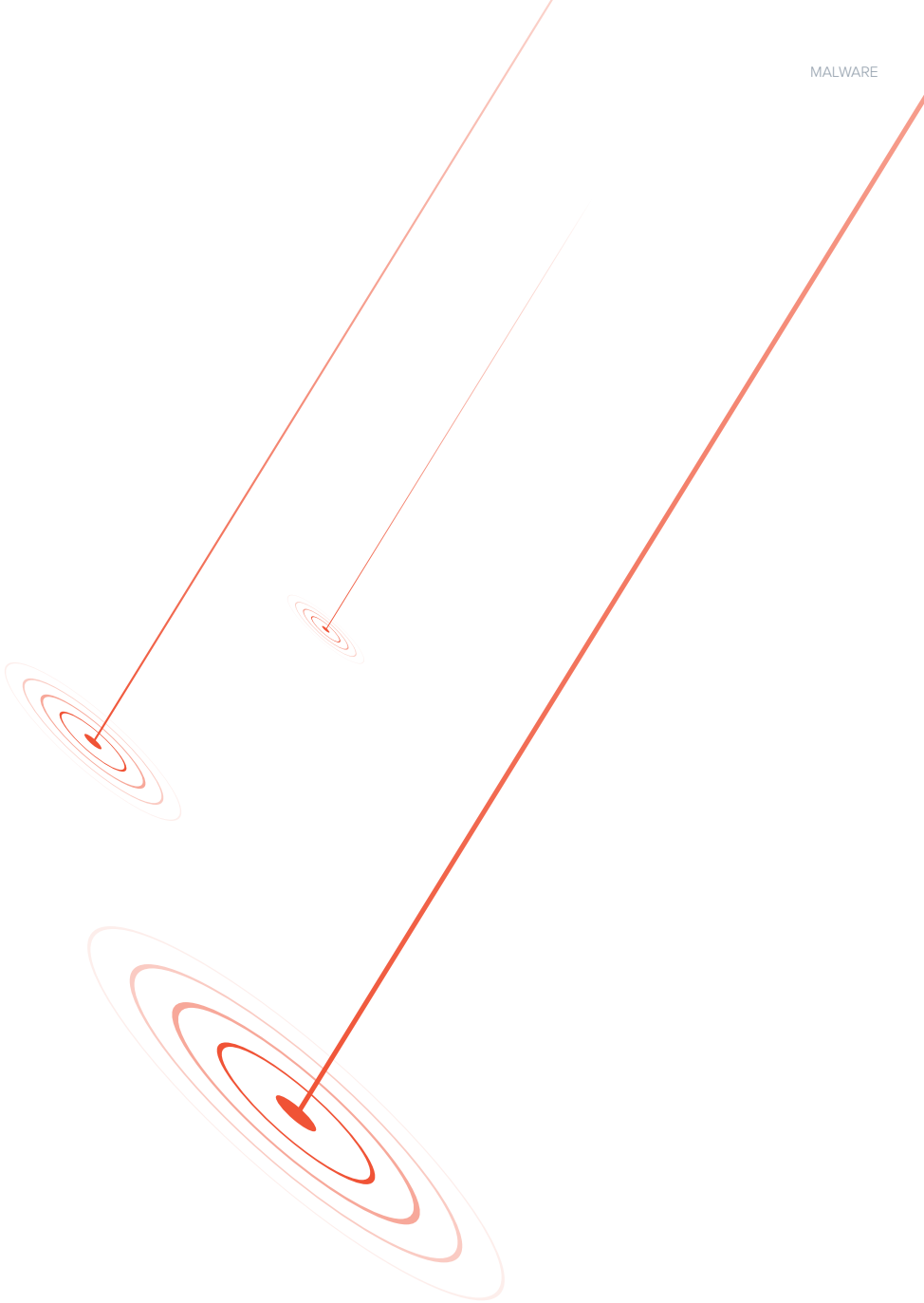
Im Jahr 2019 gab es zahlreiche, öffentlich bekannte Ransomware-Angriffe auf Unternehmen und Regierungseinrichtungen. Bei Regierungen zielten Ransomware Angriffe auf Landes-, Bezirks- und Staatsregierungen ab sowie auf Schulen, Gesundheitswesen, Büchereien, Gerichte und andere Institutionen.



Die durchschnittlichen Lösegelder sind explosionsartig angestiegen

E-Mail-Abwehr gegen Malware

Malware-Schutz wird am besten auf Gateway-Ebene umgesetzt, bevor die E-Mails in den Posteingang gelangen. Signature Matching bleibt weiterhin ein wichtiger Mechanismus zur Erkennung und Abwehr der meisten Malware-Arten. Doch gibt es fortschrittlichere Techniken zur Erkennung von Zero-Day-Bedrohungen. Sandboxing gehört zu diesen Techniken: Verdächtige Dateien und Links werden in einer isolierten Testumgebung analysiert, um sicherzustellen, dass sie unbedenklich sind, bevor sie im Posteingang landen. Neue Malware-Signaturen können basierend auf einer Sandbox-Analyse erstellt werden, um zukünftige Angriffe zu verhindern.



Barracuda

Daten-Exfiltration

Spam | **Daten-Exfiltration** | Scamming | Domain Impersonation | Erpressungs-versuche | Conversation Hijacking | Account Takeover

Geringe Komplexität — **Hohe Komplexität**

Malware | URL Phishing | Spear Phishing | Brand Impersonation | Business Email Compromise | Laterales Phishing

Barracuda

Daten-Exfiltration ist die unberechtigte Übertragung von Daten von einem Computer oder einem anderen Gerät. Dies kann manuell mittels direktem Zugriff auf einen Computer geschehen oder im Zuge eines automatisierten Prozesses, der bösartige Programme via Internet oder Netzwerk nutzt. Diese Angriffe sind meist gezielt und dienen dazu, Zugriff zu einem Netzwerk oder einem Gerät zu erhalten, um spezifische Daten zu finden und zu kopieren. Neben bösartigen Angriffen gehen Daten oft auch durch menschliches Versagen verloren.

Daten-Exfiltration ist auch unter folgenden Namen bekannt: Daten-Extrusion, Datenexport, Datenverlust und Datendiebstahl.

Auswirkungen von Daten-Exfiltration

Laut einem jährlichen IBM-Bericht, betrugen die durchschnittlichen Gesamtkosten eines Datendiebstahls im Jahr 2019 3,92 Millionen USD. In manchen Sparten, wie im Gesundheitswesen, kann sich diese Zahl fast verdoppeln. Datendiebstahl verursachte in den Vereinigten Staaten mit durchschnittlich 8,19 Millionen USD die höchsten Kosten. Das durchschnittliche Ausmaß eines Datendiebstahls betrug 25.575 Datensätze. Datenverlust kann auch zu finanziellen Einbußen führen und langfristige Auswirkungen auf den Ruf eines Unternehmens haben.

Durchschnittliche **Kosten** eines Datendiebstahls im Jahr 2019

3,92
Mio USD

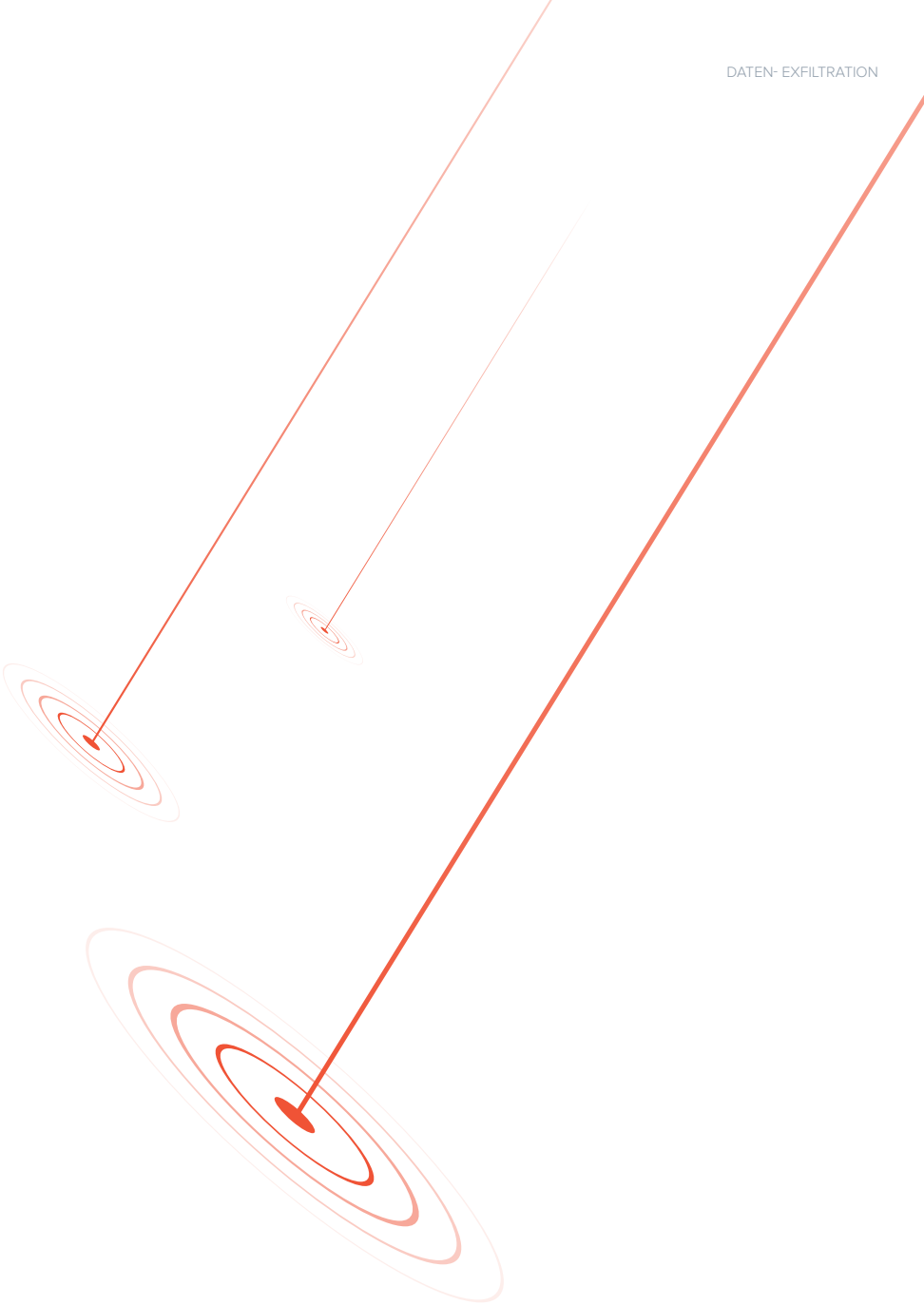
Durchschnittliches **Ausmaß** eines Datendiebstahls

25.575
Datensätze

Barracuda

E-Mail-Abwehr gegen Daten-Exfiltration

Sichere E-Mail-Gateways werden inline zum E-Mail-Fluss eingesetzt; sie filtern sowohl eingehende als auch ausgehende E-Mails. Data Loss Prevention (DLP) umfasst mehrere Technologien und Unternehmensrichtlinien, um sicherzustellen, dass Endanwender keine sensiblen oder vertraulichen Daten außerhalb des Unternehmens weitergeben. Ein DLP-System scannt sämtliche ausgehende E-Mails und sucht nach festgelegten Mustern, die auf sensible Daten wie Kreditkartennummer, Sozialversicherungsnummer und HIPAA-bezogene Informationen hinweisen könnten. E-Mails, die sensible Daten wie diese enthalten, werden automatisch verschlüsselt.



Barracuda

URL Phishing

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

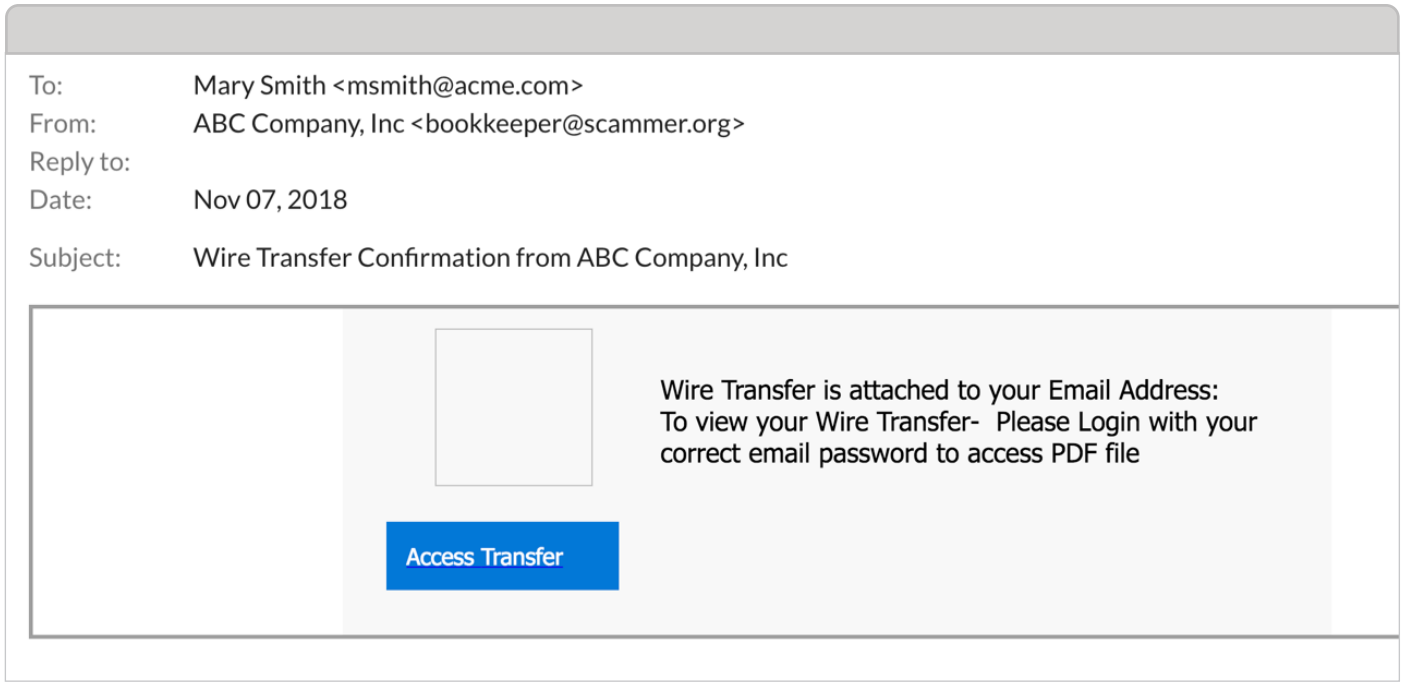
Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Bei Phishing-Angriffen versuchen Cyberkriminelle an sensible Daten wie Benutzernamen, Passwörter oder Bankdetails zu gelangen und diese für böswillige Zwecke zu nutzen. Bei URL-Phishing bewegen Cyberkriminelle ihre Opfer dazu, sensible Informationen in einer gefälschten Webseite, die wie eine echte Webseite aussieht, einzugeben.

URL-Phishing ist auch unter folgenden Namen bekannt: gefälschte Webseiten und Phishing-Webseiten



Beispiele für einen Angriff

Barracuda

Auswirkungen von URL-Phishing

Bei ca. 32 % aller Datendiebstähle kommt Phishing zum Einsatz und bei zahlreichen Phishing-Angriffen werden bösartige Links zu gefälschten Webseiten verwendet. Das Verwenden von URLs in Phishing-E-Mails ist beliebt und zugleich effektiv. Leider klicken 4 % aller Empfänger von Phishing-E-Mails auf den bösartigen Link und Hacker benötigen dann nur eine einzige Person, die ihnen Zugang gewährt.

Aufgrund der Erfolgsrate ist es nicht überraschend, dass die gemeldeten, Phishing-bedingten Verluste im Jahr 2019 fast 58 Millionen USD betrugen. Das sind, angesichts der Tatsache, dass einer Umfrage zufolge nur 57 % aller Unternehmen URL-Protection verwenden, schlechte Nachrichten.

E-Mail-Abwehr gegen URL-Phishing

Gateways bieten einen effektiven Schutz vor Massen URL-Phishing-Angriffen. Sie wenden URL-Filtering und URL-Re-write Technologien an, um den Zugriff zu bösartigen Webseiten, bekannter Malware und Phishing Seiten, die via E-Mail versendet werden, zu blockieren. Auch Sandboxing kann beim Blockieren bösartiger Links hilfreich sein.

API-basierter Posteingangsschutz ergänzt und komplettiert den Schutz, den Gateways bieten. Ein API kann einen Einblick in eine historische, interne Sicht auf URLs, die tatsächlich von einem Unternehmen verwendet werden, gewähren. Ungewöhnliche oder nachahmende URLs, die auf einen Phishing-Angriff hindeuten, werden blockiert. Auch wenn eine Phishing-Webseite noch nie zuvor für diese Zwecke verwendet wurde oder auf einer renommierten Domain gehostet wird, kann Posteingangsschutz dabei helfen, vor gezielten Spear Phishing Angriffen, die bösartige URLs verwenden, zu schützen.

Scamming

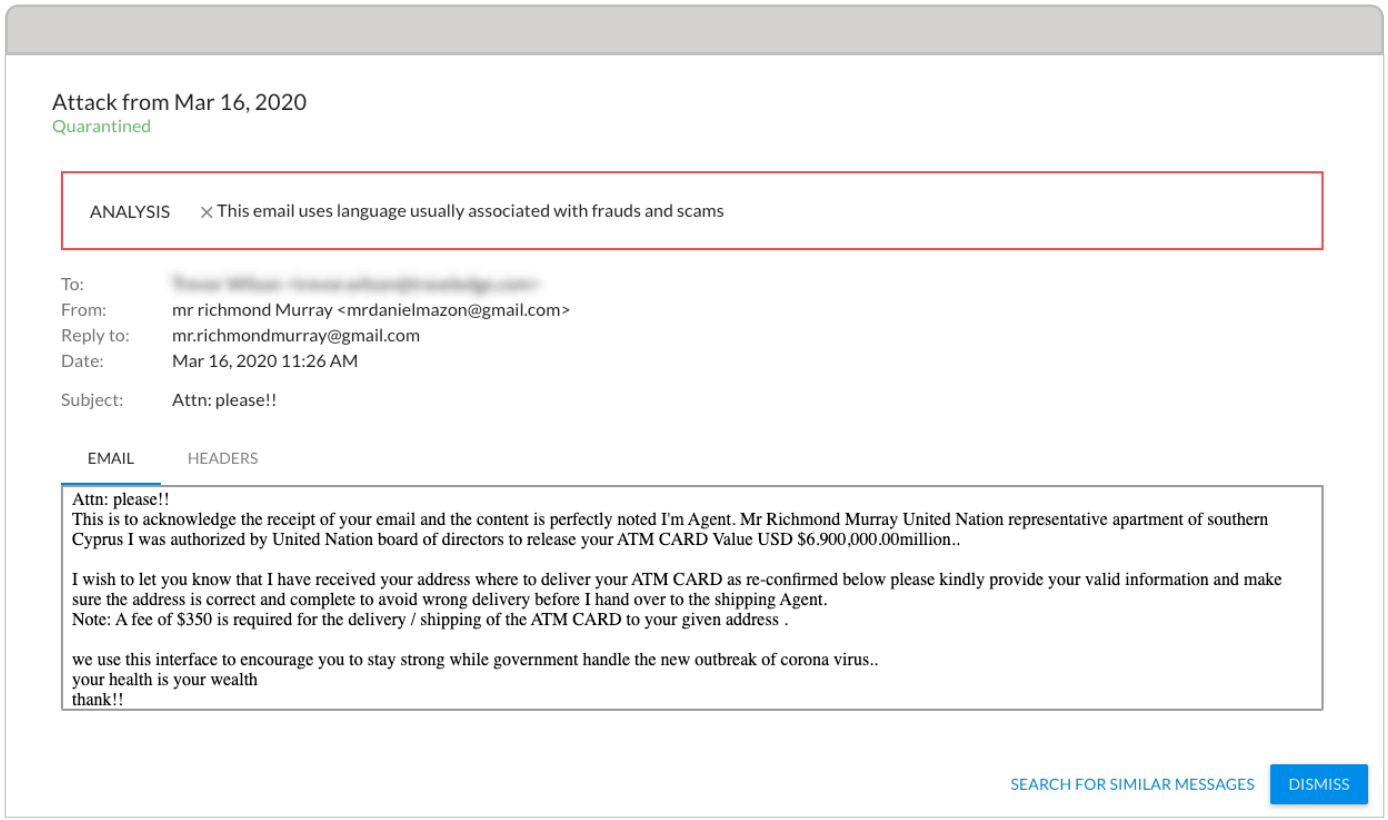
Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität — **Hohe Komplexität**

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

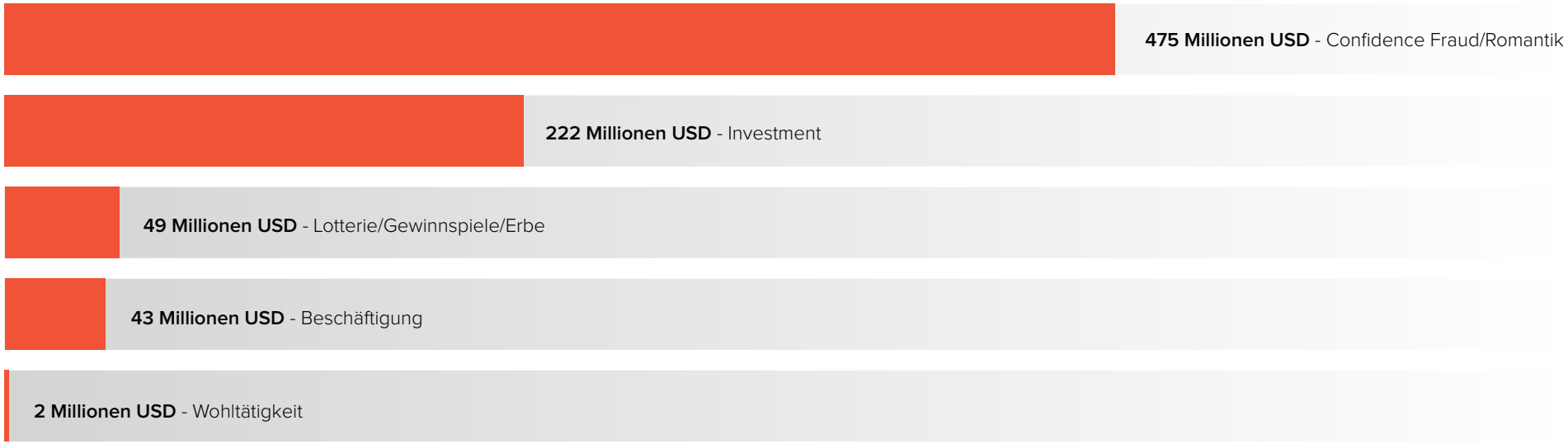
Bei E-Mail-Scamming nutzen Cyberkriminelle Betrugsmuster, um ihre Opfer zu betrügen oder deren Identität zu stehlen, indem sie sie dazu bewegen, persönliche Informationen zu teilen. Scamming tritt z.B. in Form von gefälschten Stellenanzeigen, Investmentmöglichkeiten, Erbbenachrichtigungen, Lotteriegewinnen und Geldtransfer auf.



Beispiele für einen Angriff

Auswirkungen von Scamming

39 % aller Spear Phishing-Angriffe sind Scamming. Scammer nutzen unterschiedlichste Techniken – von gefälschten Lotteriegewinnen bis zu Investment Scams. Es ist nicht ungewöhnlich, dass Scammer versuchen, aus Katastrophen wie Hurrikans, der COVID-19 Pandemie und anderen Ereignissen Geld zu machen. Scammer zielen in diesen Fällen darauf ab, in ihren Opfern Mitgefühl, Nächstenliebe oder Angst auszulösen. Leider lassen sich viele auf Scam-E-Mails ein und teilen unwissentlich sensible Informationen mit Scammern oder tätigen Zahlungen an sie. Infolge solcher Scamming-Angriffe kam es zu Folgeschäden in Höhe von mehreren Millionen USD, die vom FBI protokolliert wurden.



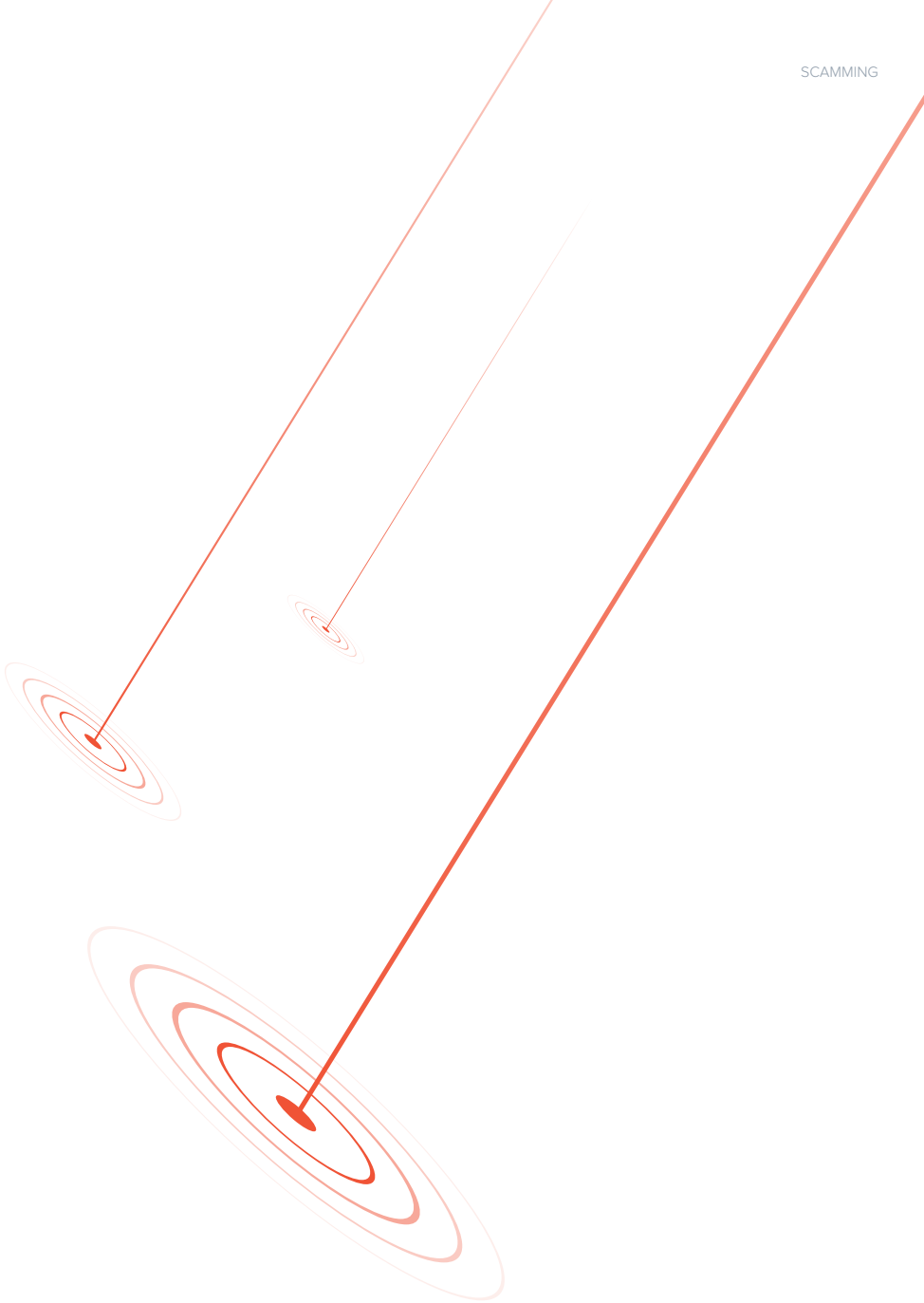
Scamming: Folgeschäden, die dem FBI 2019 gemeldet wurden

E-Mail-Abwehr gegen Scamming

API-basierter Posteingangsschutz nutzt historische E-Mail-Datensätze, um festzustellen, wie die normale E-Mail-Kommunikation für Mitarbeiter aussieht. Wenn Scamming E-Mails, die von der normalen oder erwarteten E-Mail-Kommunikation abweichen, versandt werden, markiert und blockiert sie der Posteingangsschutz.

Gateway-Lösungen arbeiten mit detaillierten Richtlinien und suchen nach bestimmten Keywords, die basierend auf dem Inhalt der E-Mail auf Scams hinweisen. In Verbindung mit Reputationsfilter und Blacklisten kann dieser Ansatz effektiv sein. Jedoch führt er oft zu Falschmeldungen und fängt wichtige Nachrichten vor dem Posteingang ab.

Viele Scam-E-Mails fallen auch in die Kategorie Spam. Unternehmen müssen sowohl Spamfilter im E-Mail-Gateway als auch API-basierten Posteingangsschutz verwenden, um effektiven Schutz vor Scamming zu gewährleisten.



Barracuda

Spear Phishing

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

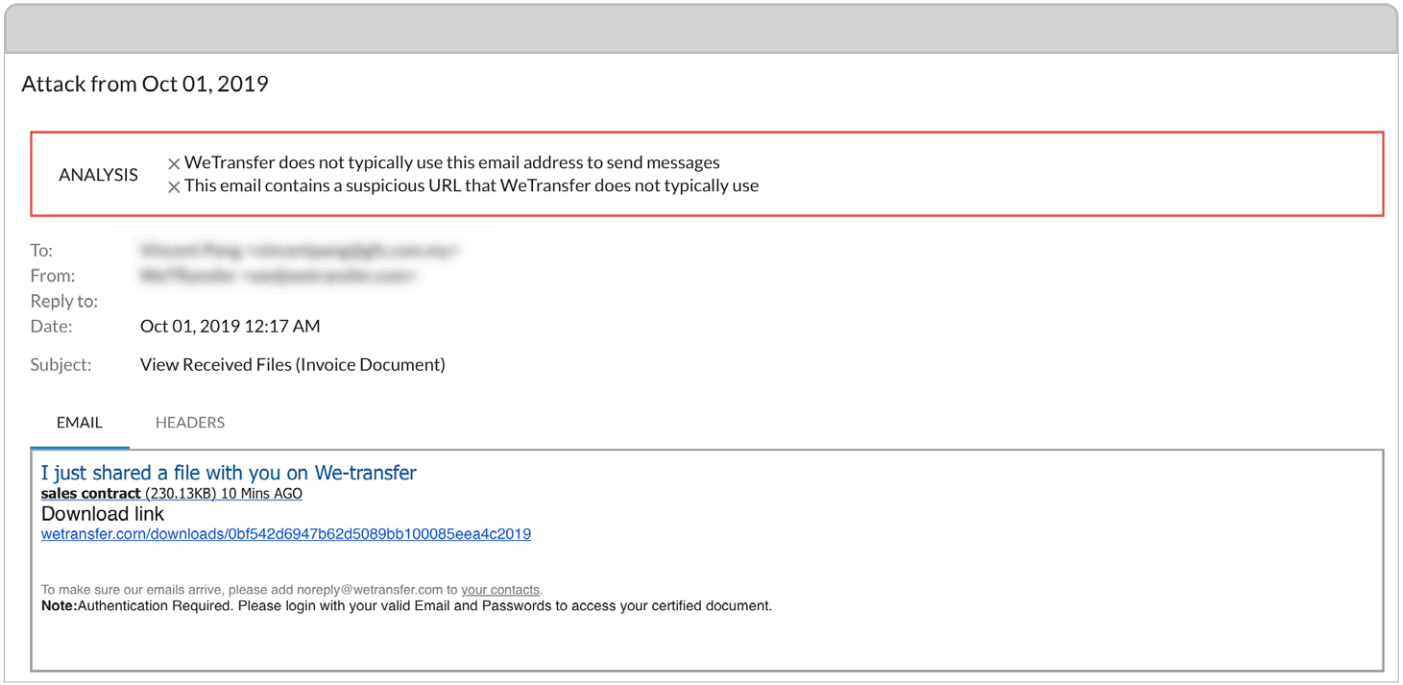
Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Spear Phishing ist eine stark personalisierte Art von E-Mail Phishing. Cyberkriminelle forschen ihre Ziele aus und erstellen personalisierte Nachrichten, in denen sie sich beispielsweise als ein vertrauenswürdiger Kollege, eine Webseite oder ein Unternehmen ausgeben. Das Ziel von Spear Phishing E-Mails ist es, sensible Informationen wie Anmeldeinformationen oder Bankdetails zu stehlen, die im Anschluss für Betrug, Identitätsdiebstahl und andere Verbrechen verwendet werden. Cyberkriminelle nutzen zudem bei Spear Phishing-Angriffen Social Engineering-Taktiken. Die Nachrichten sind knapp, dringlich und erzeugen Druck, um die Erfolgsaussichten zu erhöhen.

Spear phishing ist auch unter folgenden Namen bekannt: Whaling und Laser Phishing.



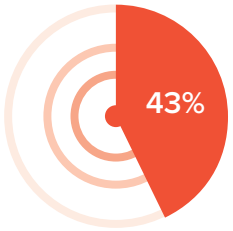
Beispiel für einen Angriff

Auswirkungen von Spear Phishing

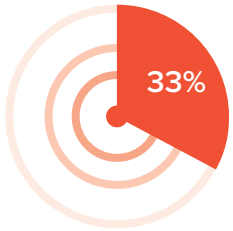
In einer aktuellen E-Mail Trend Umfrage von Barracuda gaben 43 % der Befragten an, in den vergangenen 12 Monaten Opfer von Spear Phishing-Angriffen gewesen zu sein. Jedoch gaben nur 23 % der Unternehmen an, einen speziellen Schutz vor Spear Phishing zu verwenden.

Wenn Unternehmen von Spear Phishing-Angriffen betroffen sind, dann wirken sich diese wie folgt aus: Geräte und Netzwerk sind mit Malware infiziert, es entstehen direkte finanzielle Verluste aufgrund von Überweisungen und der Ruf des Unternehmens wird geschädigt. In vielen Fällen kommt es bei Spear Phishing-Angriffen zum Diebstahl von Anmeldedaten und der Übernahme von E-Mail-Konten. Kompromittierte Konten werden oft genutzt, um weitere Spear Phishing-Angriffe zu starten. Unternehmen benötigen speziellen Schutz vor Spear Phishing, um aus diesem Teufelskreis auszubrechen.

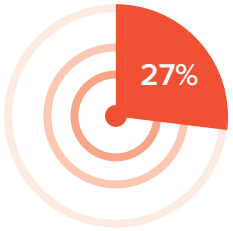
Wie Unternehmen 2019 von Spear Phishing-Angriffen betroffen waren[1]



Mit Malware oder Viren infizierte Geräte

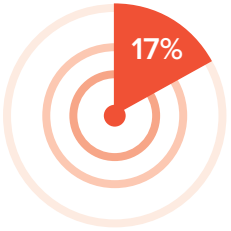


Gestohlene Login-Daten und/oder Account Takeover



Rufschaden

Direkter finanzieller Verlust (z.B. durch Überweisungen)



Diebstahl von sensiblen oder vertraulichen Daten

Keine Auswirkungen

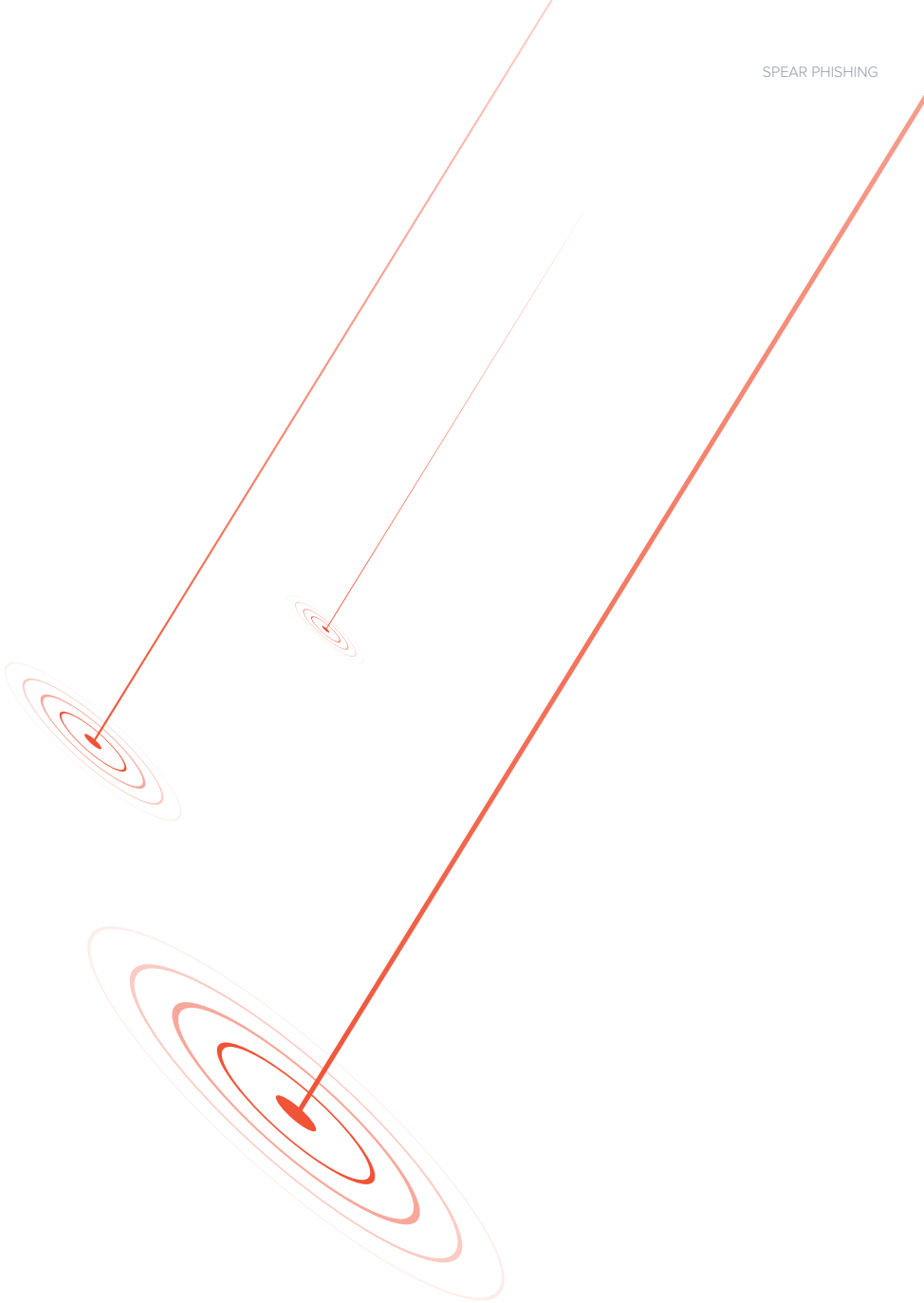
Andere **(3%)**

1 Email Security-Trends 2019

E-Mail-Abwehr gegen Spear Phishing

API-basierter Posteingangsschutz nutzt den Zugriff auf historische E-Mail-Datensätze, um einen Identity Graphen für die Kommunikation zu erstellen. Dabei handelt es sich um ein statistisches Modell, das für jeden Benutzer im Unternehmen spezifisch ist. Dieser Identity Graph wird verwendet, um ungewöhnliche Kommunikationsmuster zu erkennen, die vom statistischen Modell abweichen. Somit werden Spear Phishing-Angriffe, die am Gateway vorbeikommen, prognostiziert und blockiert.

Klassische E-Mail-Security-Gateways haben keine Einsicht in historische Daten. Sie evaluieren jede E-Mail basierend auf vorab festgelegten Richtlinien, Filtern und Signaturen und nicht basierend auf historischer Kommunikation und Kontext. Spear Phishing-Angriffe sind darauf ausgelegt, diese Filter und Richtlinien zu umgehen und landen somit oft im Posteingang.



Barracuda

Domain Impersonation

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Domain Impersonation wird oft von Hackern im Zuge eines Conversation Hijacking-Angriffs verwendet. Angreifer versuchen eine Domain nachzuahmen, indem sie Techniken wie Typosquatting verwenden. Sie ersetzen einen oder mehrere Buchstaben in einer echten Domain durch ähnliche Buchstaben oder fügen einen unauffälligen Buchstaben hinzu, damit die E-Mail Domain echt wirkt. Cyberkriminelle registrieren oder kaufen die nachahmende Domain vorab.

Domain Impersonation ist auch unter folgendem Namen bekannt: Typosquatting und lookalike Domains.

Domain Impersonation Angriffe sind schwerwiegend. Leicht übersieht man die subtilen Unterschiede zwischen einer legitimen E-Mail Domain und einer nachahmenden E-Mail Domain. Ein Angreifer, der z.B. versucht barracuda.com nachzuahmen, würde eine URL wie diese verwenden:

barraeuda.com

barracada.com

barracúda.com

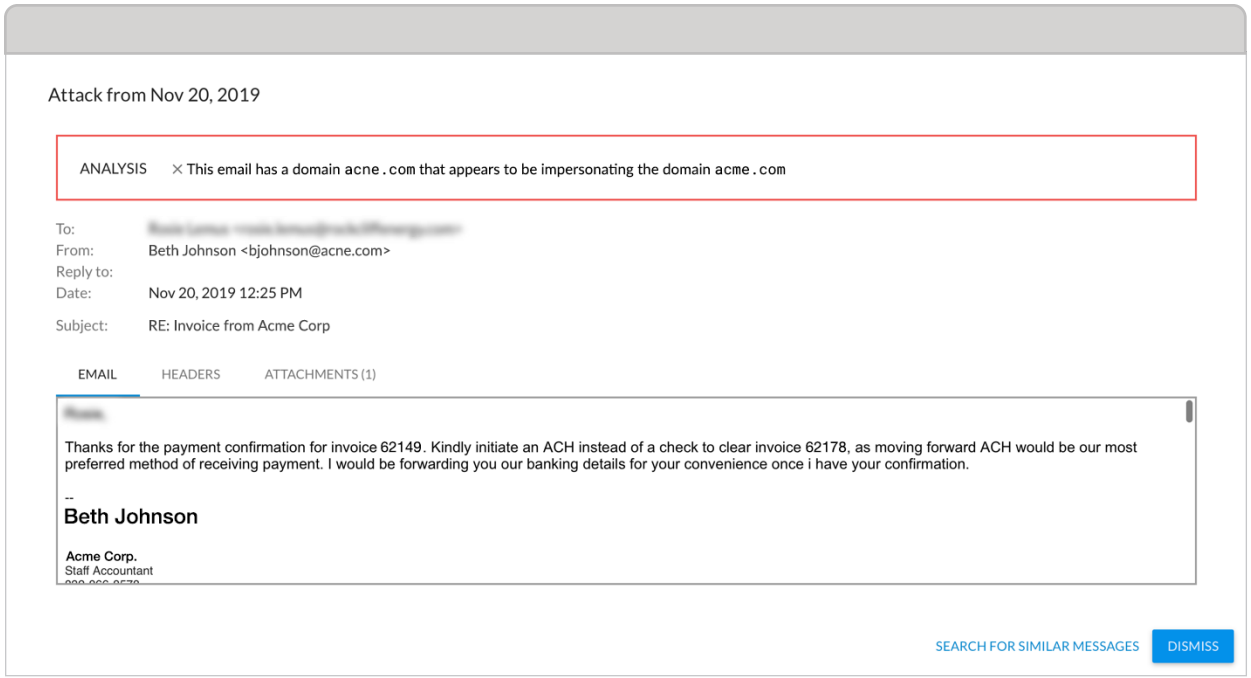
barrracud.com

Manchmal ändern Angreifer den Top-Level Domain (TLD), indem sie .net oder .co statt .com verwenden, um ihre Opfer zu täuschen:

barracuda.net

barracuda.co

Barracuda



Beispiele für einen Angriff

Auswirkungen von Domain Impersonation

In den letzten Monaten haben Sicherheitsexperten von Barracuda einen starken Anstieg bei Domain Impersonation-Angriffen zur Erleichterung von Conversation Hijacking bemerkt. Eine Analyse von ca. 500.000 monatlichen E-Mail-Angriffen zeigt einen Anstieg um 400 % bei den Domain Impersonation-Angriffen zu Conversation Hijacking Zwecken.

+400%

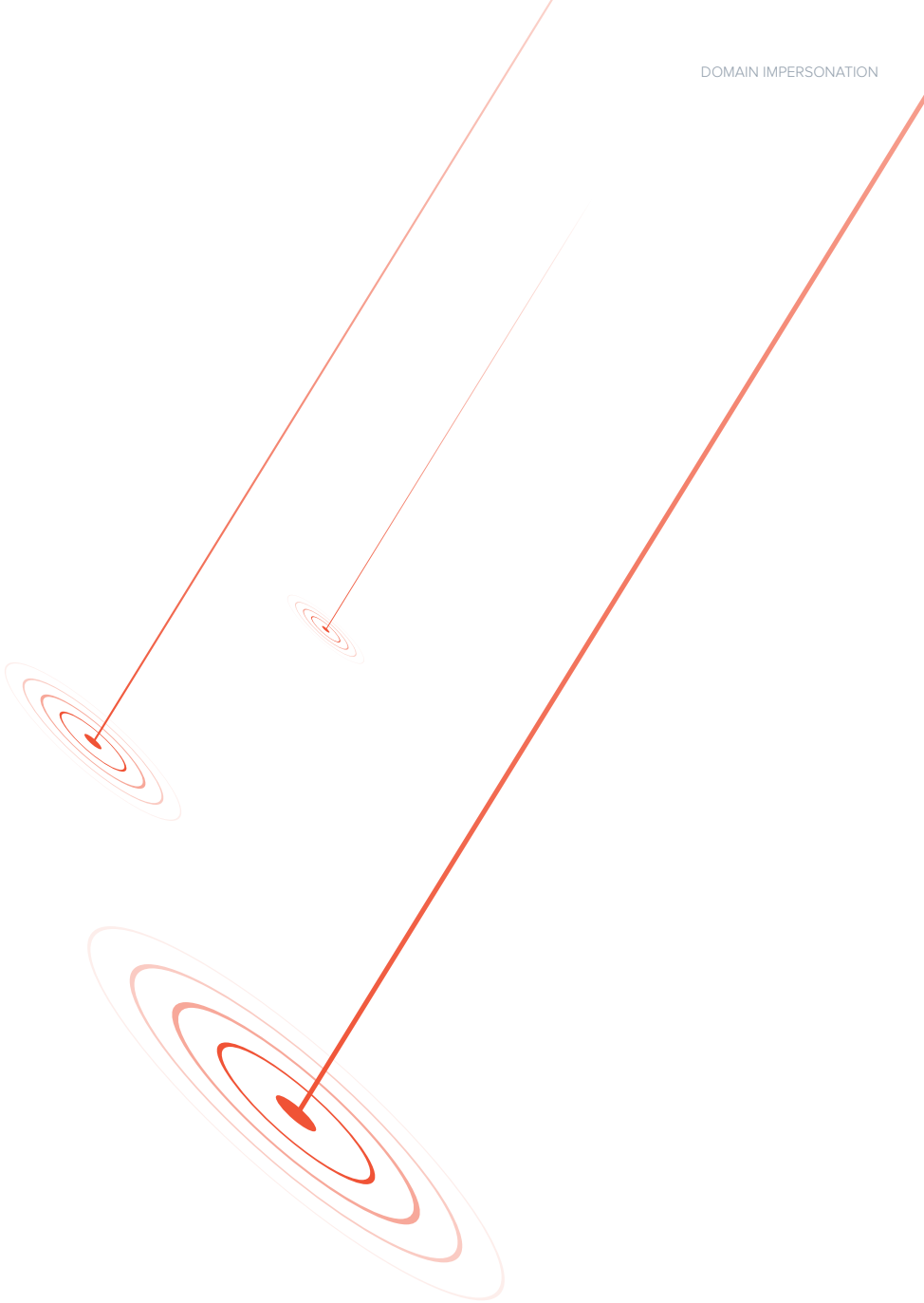
Anstieg von Domain Impersonation-Angriffen im 2. Halbjahr 2019

Barracuda

E-Mail-Abwehr gegen Domain Impersonation

Die größte Herausforderung bei Domain Impersonation ist das genaue Erkennen von Domains mit Tippfehlern und das Unterscheiden zwischen Spoofing-Versuchen und echten Webseiten. E-Mail-Gateways müssen Listen der Domains, die von dem Unternehmen und deren Partnern über längere Zeit verwendet werden, erstellen. Das ist ein langwieriger, fehleranfälliger Prozess, der kontinuierlich verwaltet und aktualisiert werden muss. Bei so vielen E-Mail Domains und Variationen führt die Verwendung von Gateways zur Erkennung von Domain Impersonation zu einer Vielzahl von Falschmeldungen und gleichzeitig werden Angriffe nicht abgewehrt.

Ein API basierter Posteingangsschutz verwendet historische E-Mails, um Daten über Domains, die von dem Unternehmen, deren Partnern und Kunden genutzt werden, zu erhalten. Der Posteingangsschutz assoziiert bestimmte Unterhaltungen, Anfragen und Personen mit bestimmten E-Mail-Domains. Wenn also ein Anbieter eine ungewöhnliche Anfrage von einer anderen Domain aus schickt, wird diese vom Posteingangsschutz erkannt und blockiert.



Barracuda

Brand Impersonation

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

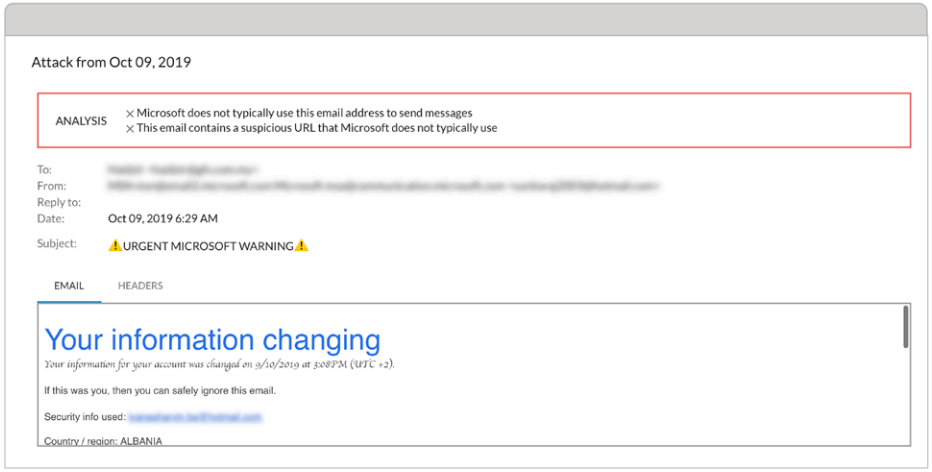
Barracuda

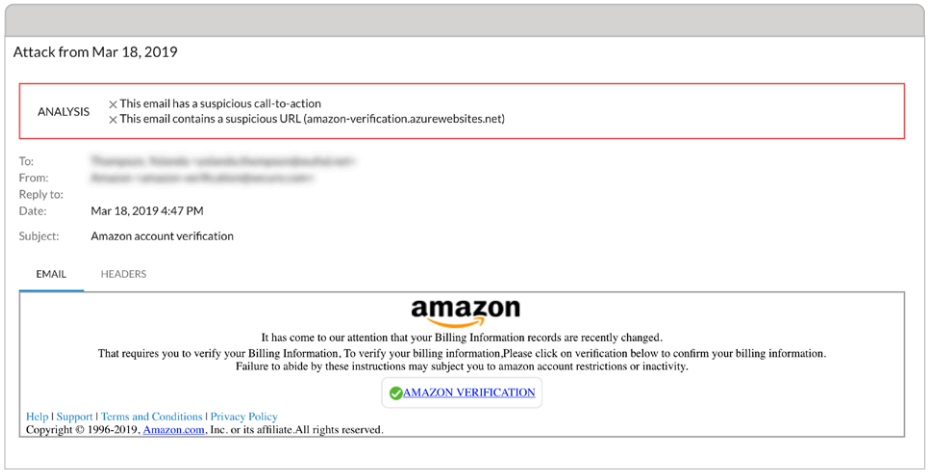
Brand Impersonation ist darauf ausgerichtet, ein Unternehmen oder eine Marke nachzuahmen und Personen dazu zu bewegen, persönliche oder andere sensible Informationen weiterzugeben.

Zu den häufigsten Arten von Brand Impersonation gehören:

Service Impersonation ist eine Art von Phishing-Angriff mit dem Ziel, ein bekanntes Unternehmen oder ein gängiges Programm nachzuahmen. Diese Angriffsmethode ist besonders beliebt, da die E-Mails so gestaltet sind, dass sie als Eintrittsstelle zum „Ernten" von Anmeldeinformationen und zur Ausführung eines Account Takeovers dienen. Service Impersonation Angriffe werden auch verwendet, um personenbezogene Daten wie Kreditkartennummern und Sozialversicherungsnummern zu stehlen. *Service Impersonation ist auch unter folgendem Namen bekannt: Vendor Email Compromise.*

Brand Hijacking ist eine weitere, gebräuchliche Art von Phishing. Dabei nutzt der Angreifer die Domain eines Unternehmens, um sich als dieses oder als ein Mitarbeiter auszugeben. Dies geschieht meist mittels E-Mails, die falsche oder abgewandelten Domain-Namen, die legitim wirken, beinhalten. *Brand Hijacking ist auch unter folgenden Namen bekannt: Brand Spoofing und Domain Spoofing.*





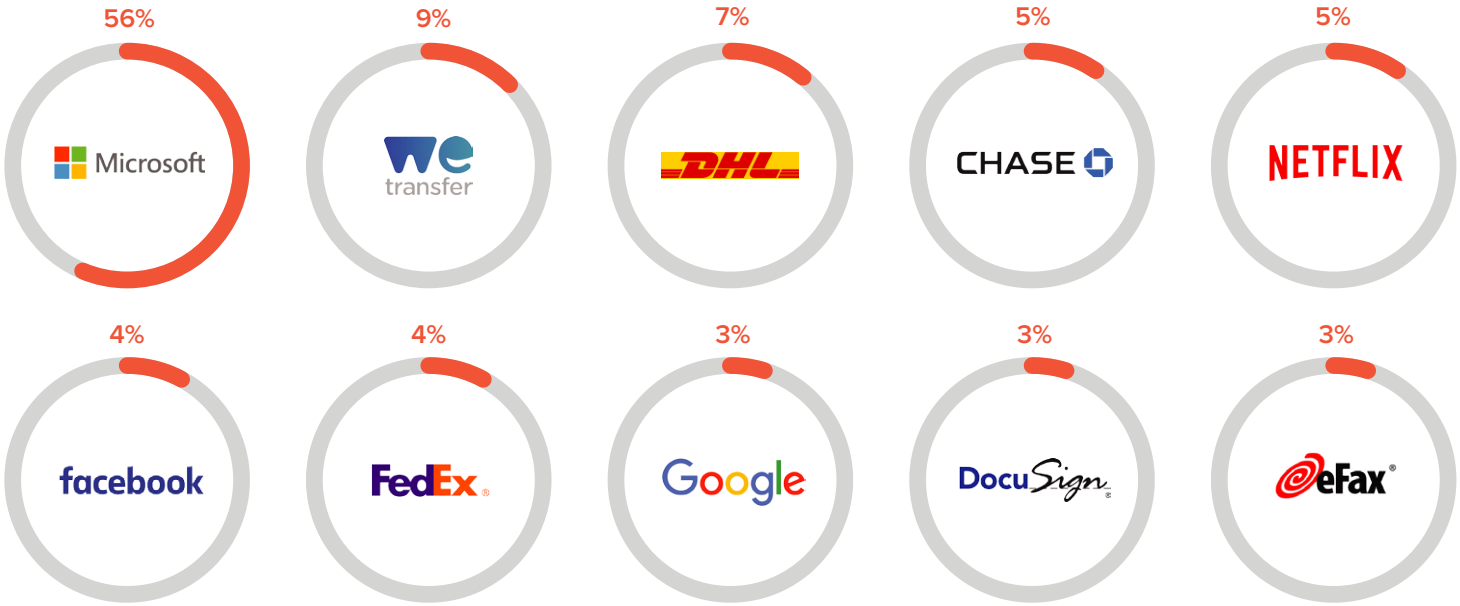
Beispiele für einen Angriff

Barracuda

Auswirkungen von Brand Impersonation

In 47 % aller Spear Phishing-Angriffe kommt Service Impersonation zum Einsatz. Microsoft ist bei Spear Phishing-Angriffen die am häufigsten nachgeahmte Marke. Microsoft nachzuahmen gehört zu den am häufigsten von Cyberkriminellen verwendeten Techniken, um ein Konto zu hacken. Microsoft und Office 365 Anmeldeinformationen sind besonders wertvoll, da sie es den Hackern ermöglichen, in Unternehmen einzudringen und weitere Angriffe zu starten.

Brand Hijacking oder Spoofing-Angriffe nutzen Schwachstellen im E-Mail RFC Standard, bei der eine vollständige Authentifizierung der sendenden Domains nicht notwendig ist. Standards wie DKIM, SPF und DMARC erschweren die Durchführung solcher Angriffe. Dennoch wird Domain-Spoofing häufig von Hackern bei Imitationsangriffen genutzt. Eine aktuelle Studie zeigt, dass es täglich fast 30.000 Spoofing-Angriffe gibt. Zudem verwenden 77 % der Fortune 500 Unternehmen keine DMARC-Richtlinien. Das macht es Scammern leicht, diese Marken bei Phishing-Angriffen nachzuahmen.



Unternehmen, die am häufigsten nachgeahmt werden

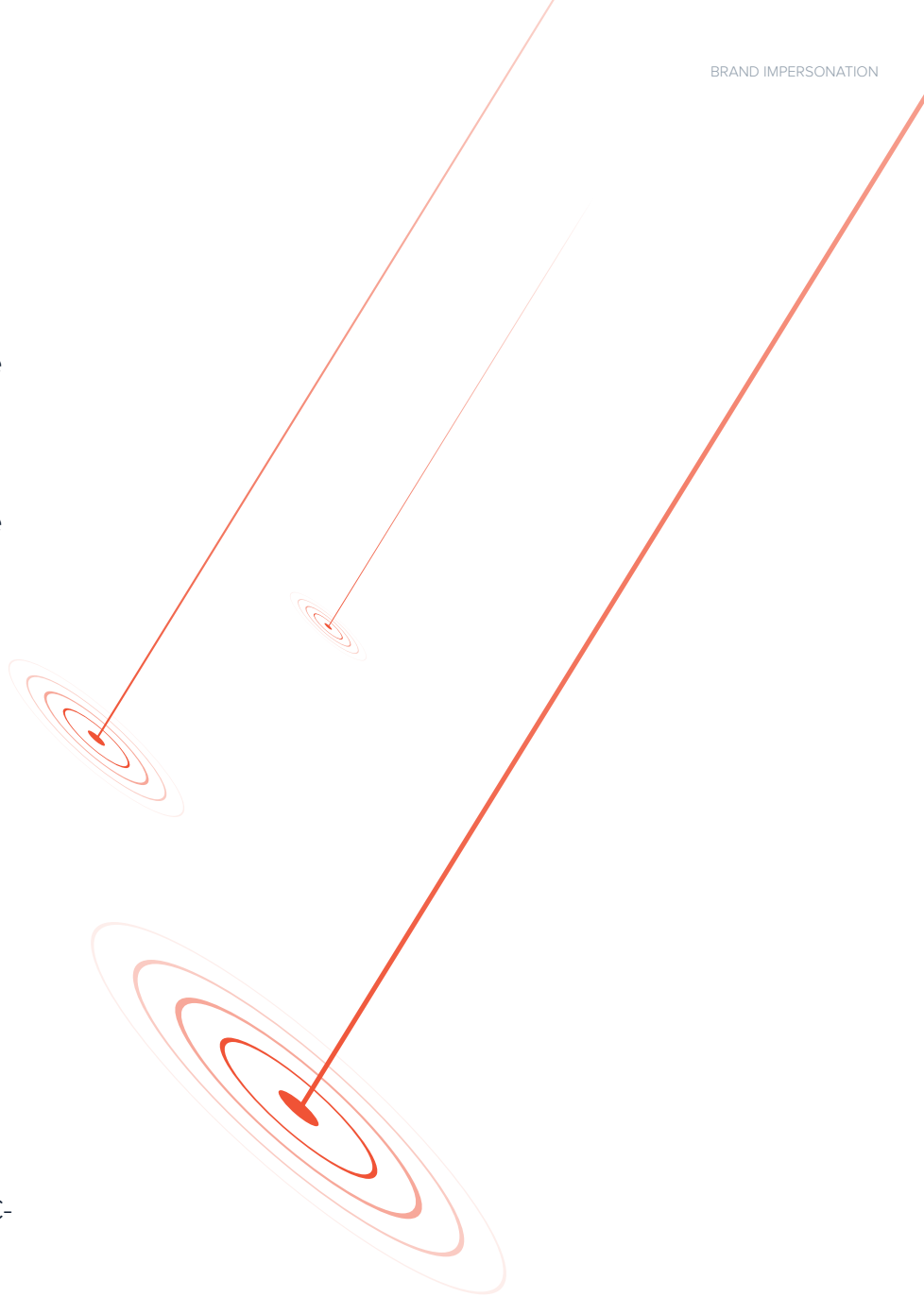
Barracuda

E-Mail-Abwehr gegen Brand Impersonation

API-basierter Posteingangsschutz zum Schutz vor Service Impersonation verwendet historische und interne E-Mail-Kommunikationen, um Einblick in die Servicedienstleistungen, die ein Unternehmen nutzt, zu bekommen. Die Daten werden in einem statistischen Erfassungsmodell verwendet, um den Unterschied zwischen legitimen und nicht legitimen E-Mails zu erkennen. Zudem enthält dieses Modell das Branding und das Bildmaterial, das für die Servicedienstleistungen eines Unternehmens verwendet wird.

Gateways haben keinen Einblick in die Servicedienstleistungen, die ein Unternehmen nutzt und können somit das Branding und Bildmaterial einer legitimen Marke nicht erkennen. Sie arbeiten mit festgelegten Richtlinien; jedoch reichen diese aufgrund der Vielfalt an Service Impersonation Angriffen nicht aus. API-basierter Posteingangsschutz ist ein effektiverer Weg zur Abwehr von Service Impersonation Angriffen.

Unternehmen können mittels DMARC-Authentifizierung Einblick in Domain-Betrug erhalten und sich somit vor Domain Impersonation und Brand Hijacking schützen. DMARC-Reporting zeigt, wie eine E-Mail-Domain verwendet wird. Das ermöglicht es einem Unternehmen wiederum, DMARC-Richtlinien einzusetzen, die vor Nachahmung der Domain schützen.



Barracuda

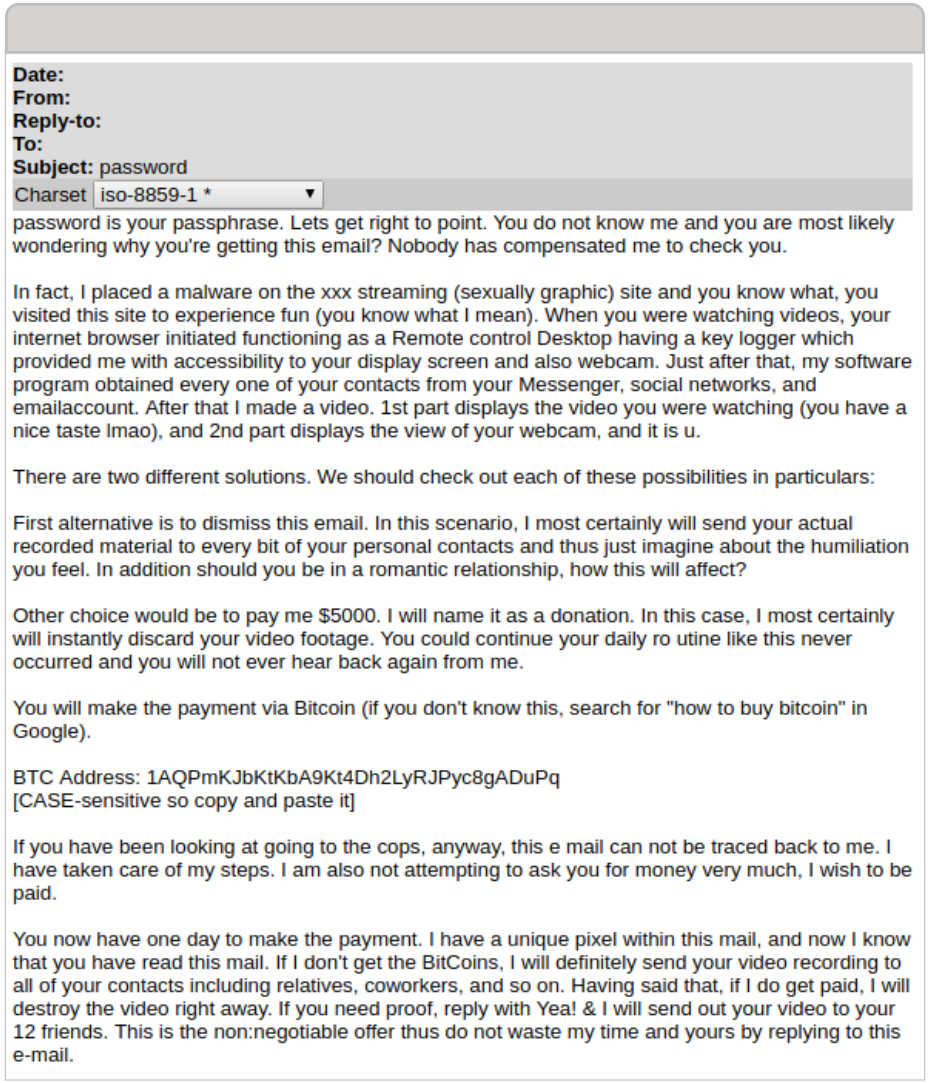

Erpressungsversuche
Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover
Geringe Komplexität
Hohe Komplexität
Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Erpressungs Scams – zu denen auch Sextortion gehört – treten immer häufiger auf, werden immer komplexer und umgehen E-Mail-Gateways.

Bei Sextortion-Angriffen nutzen Cyberkriminelle Benutzernamen und Passwörter, die sie im Zuge eines Datendiebstahls erlangt haben. Sie nutzen diese Informationen dann, um Personen zu kontaktieren und sie dazu zu bewegen, ihnen Geld zu überweisen. Scammer geben vor, über bloßstellendes Videomaterial zu verfügen, das angeblich auf dem Computer des Opfers aufgenommen wurde und drohen, das Video mit ihren Kontakten zu teilen, wenn der Betroffene nicht zahlt.

Erpressungsversuche sind auch unter folgendem Namen bekannt: Extortion und Sextortion.



Date:
From:
Reply-to:
To:
Subject: password
Charset iso-8859-1 *

password is your passphrase. Lets get right to point. You do not know me and you are most likely wondering why you're getting this email? Nobody has compensated me to check you.

In fact, I placed a malware on the xxx streaming (sexually graphic) site and you know what, you visited this site to experience fun (you know what I mean). When you were watching videos, your internet browser initiated functioning as a Remote control Desktop having a key logger which provided me with accessibility to your display screen and also webcam. Just after that, my software program obtained every one of your contacts from your Messenger, social networks, and emailaccount. After that I made a video. 1st part displays the video you were watching (you have a nice taste lmao), and 2nd part displays the view of your webcam, and it is u.

There are two different solutions. We should check out each of these possibilities in particulars:

First alternative is to dismiss this email. In this scenario, I most certainly will send your actual recorded material to every bit of your personal contacts and thus just imagine about the humiliation you feel. In addition should you be in a romantic relationship, how this will affect?

Other choice would be to pay me $5000. I will name it as a donation. In this case, I most certainly will instantly discard your video footage. You could continue your daily ro utine like this never occurred and you will not ever hear back again from me.

You will make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1AQPmKJbKtKbA9Kt4Dh2LyRJPyc8gADuPq
[CASE-sensitive so copy and paste it]

If you have been looking at going to the cops, anyway, this e mail can not be traced back to me. I have taken care of my steps. I am also not attempting to ask you for money very much, I wish to be paid.

You now have one day to make the payment. I have a unique pixel within this mail, and now I know that you have read this mail. If I don't get the BitCoins, I will definitely send your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I do get paid, I will destroy the video right away. If you need proof, reply with Yea! & I will send out your video to your 12 friends. This is the non:negotiable offer thus do not waste my time and yours by replying to this e-mail.

Beispiel für einen Angriff

Barracuda

Auswirkungen von Erpressungsversuchen

Ca. 7 % aller Spear Phishing-Angriffe sind Erpressungsversuche – das sind gleich viel wie bei Business Email Compromise. Es ist genauso wahrscheinlich, dass Mitarbeiterinnen und Mitarbeiter Ziel eines Erpressungs-Scams werden, wie auch eines Business-E-Mail-Compromise-Angriffs.

Laut dem FBI betrugen die durch Erpressungsversuche verursachten Kosten im Jahr 2019 mehr als 107 Millionen USD. Angreifer fordern durchschnittlich ein paar hundert oder tausend Dollar – ein Betrag, den eine Einzelperson zahlen könnte. Aufgrund der zahlreichen Angriffe summieren sich die kleinen Zahlungen an die Angreifer maßgeblich.

Erpressung-Scams werden aufgrund ihrer gewollt peinlichen und sensiblen Natur nur selten gemeldet. IT-Teams wissen oft nichts von solchen Angriffen, da die Mitarbeiter diese E-Mails nicht melden – egal ob sie das Lösegeld zahlen oder nicht.

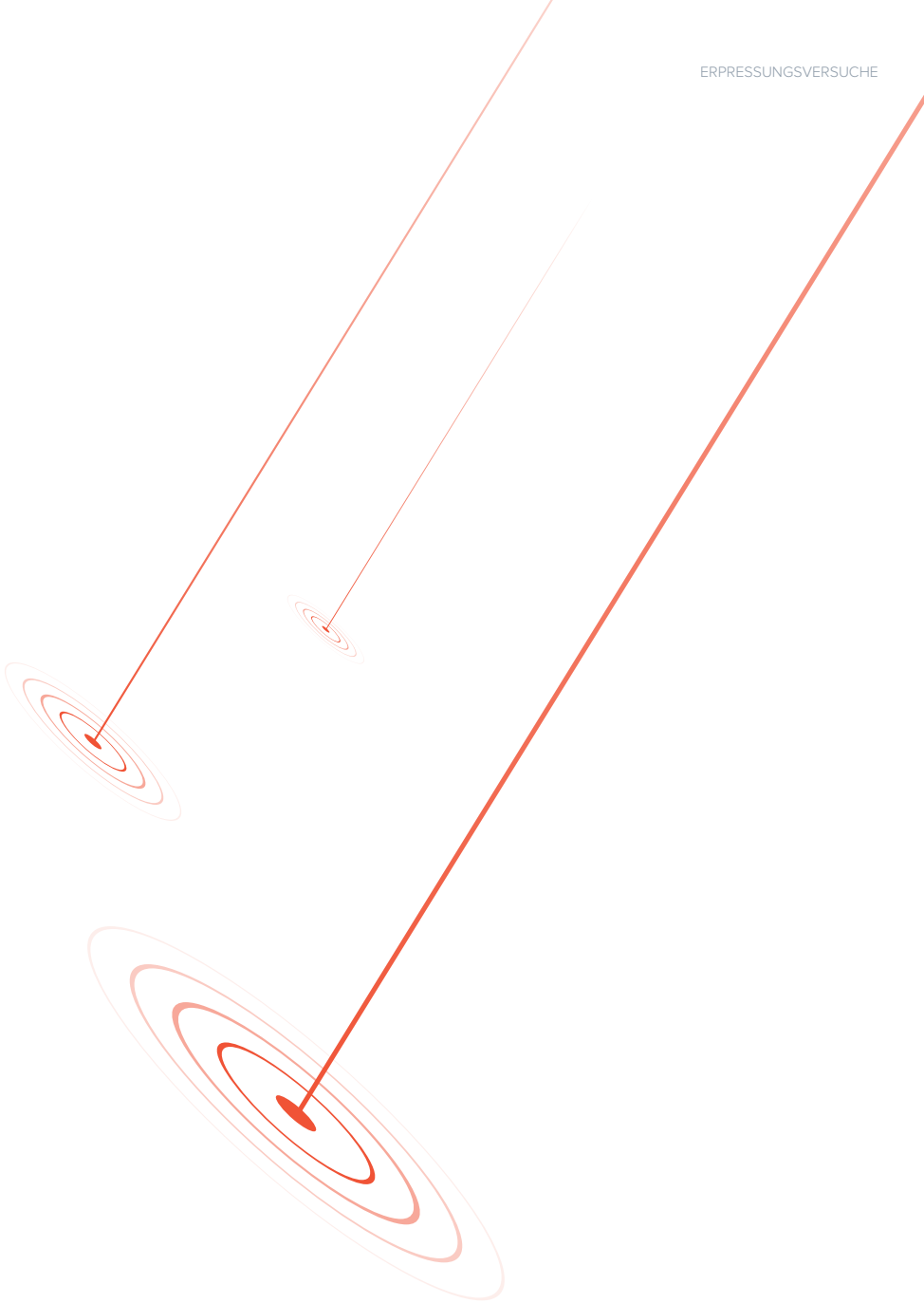
Die durch Erpressungsversuche verursachten Kosten wachsen stetig

Barracuda

Stärkung Ihrer E-Mail-Abwehr gegen Erpressungsversuche

Da der Posteingangsschutz via APIs auf historische E-Mails zurückgreifen kann, erstellt er ein statistisches Modell von Kommunikationsmustern, die auch den Tonfall des Absenders berücksichtigen. Das ermöglicht es dem Posteingangsschutz, einen ungewöhnlichen oder bedrohenden Tonfall in Erpressungs-E-Mails in Kombination mit anderen Signalen zu erkennen und diese als bösartig zu kennzeichnen.

Während Gateways nur auf ein paar Hinweise auf Erpressungsversuche, wie bestimmte Keywords, prüfen können, hält der fehlende Zugriff auf historische E-Mail-Daten und die Unfähigkeit, einen ungewöhnlichen Tonfall zu erkennen, das System davon ab, das Unternehmen vor Erpressungsversuchen zu schützen.



Barracuda

Business Email Compromise

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

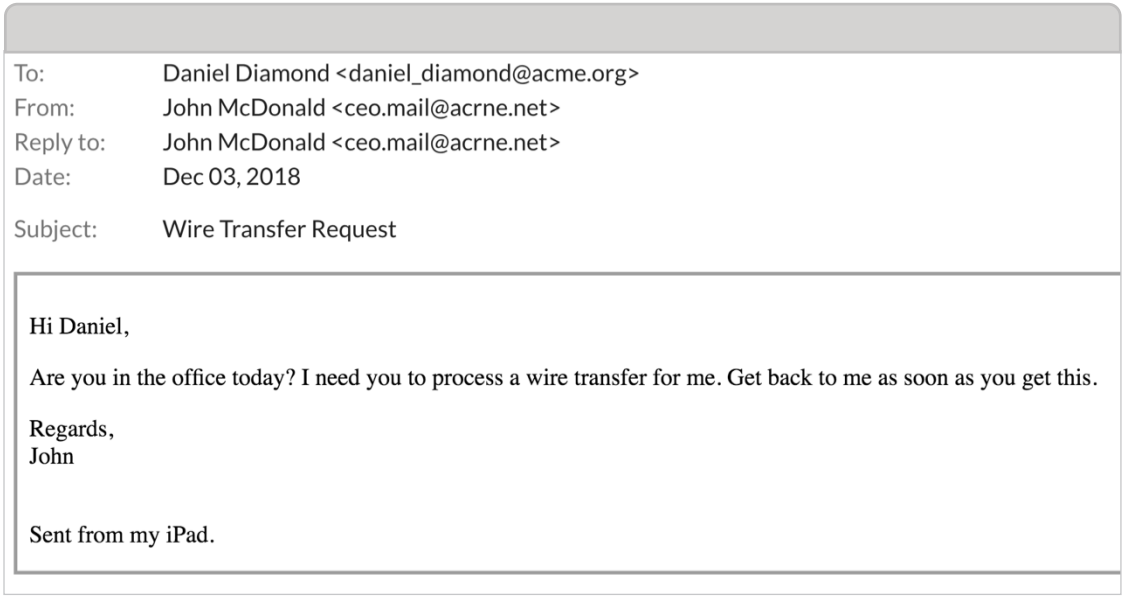
Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Bei Business Email Compromise (BEC) Angriffen geben sich Scammer als Mitarbeiter eines Unternehmens aus, und versuchen, das Unternehmen, Mitarbeiter, Kunden oder Partner zu betrügen. Meist zielen sie auf Mitarbeiter mit Zugriff zu Unternehmensfinanzen oder persönlichen Informationen ab. Sie bewegen die Mitarbeiter dazu, Überweisungen zu tätigen, oder sensible Informationen zu teilen. Bei diesen Angriffen werden Social Engineering Taktiken und kompromittierte Konten verwendet; oft beinhalten diese E-Mails keine Anhänge oder Links.

Weitere Bezeichnungen für BEC sind: CEO-Fraud, CFO-Fraud, Mitarbeiter Imitation, Whaling, Social Engineering und Überweisungsbetrug



To: Daniel Diamond <daniel_diamond@acme.org>
From: John McDonald <ceo.mail@acrne.net>
Reply to: John McDonald <ceo.mail@acrne.net>
Date: Dec 03, 2018
Subject: Wire Transfer Request

Hi Daniel,

Are you in the office today? I need you to process a wire transfer for me. Get back to me as soon as you get this.

Regards,
John

Sent from my iPad.

Beispiele für einen Angriff

Barracuda

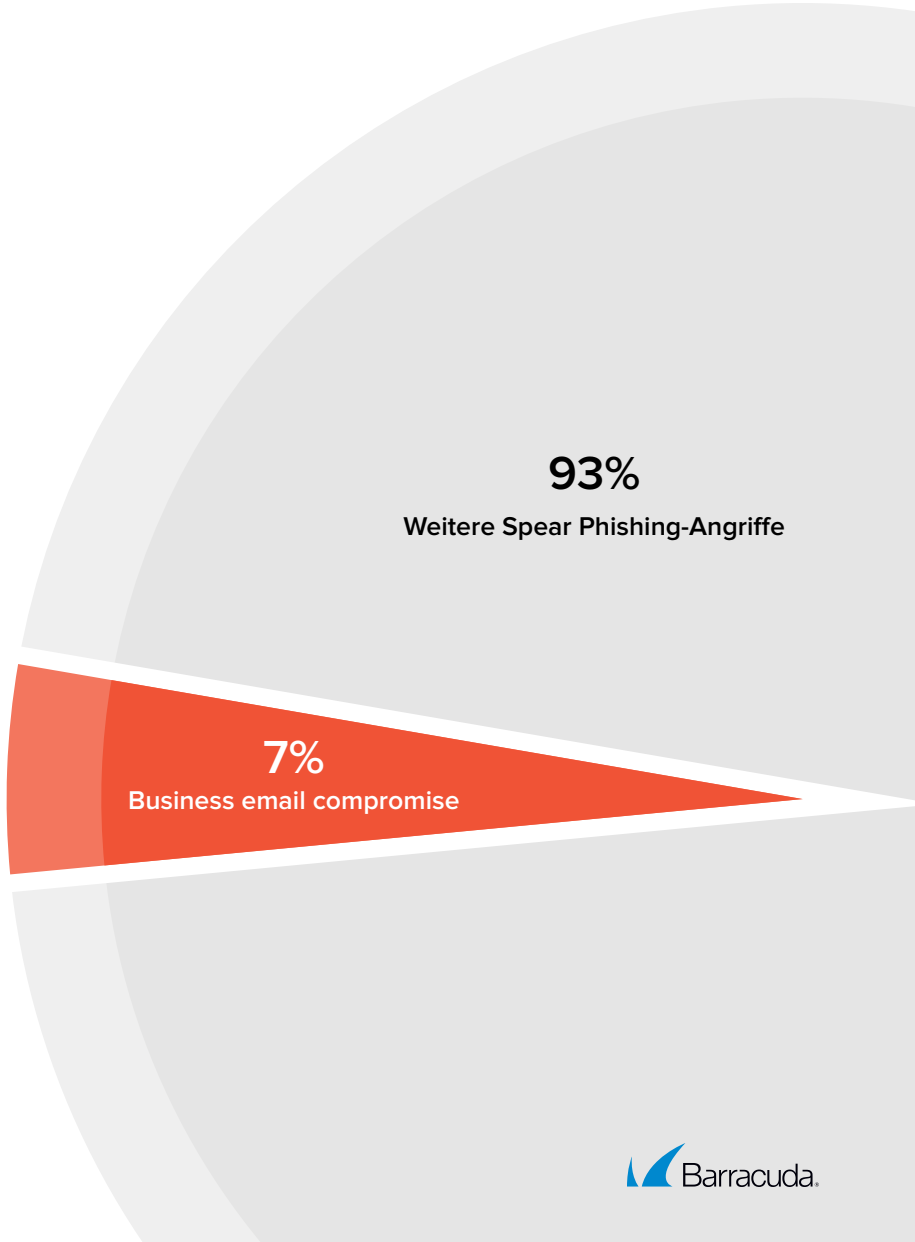
Auswirkungen von Business Email Compromise

Während Business Email Compromise nur 7 % aller Spear Phishing-Angriffe ausmacht, verursachte es laut dem FBI alleine im Jahr 2019 finanzielle Verluste von mehr als 1,7 Milliarden USD. 47 % aller Business Email Compromise Angriffe werden von Gmail Konten aus gestartet.

Gehaltsbetrug ist eine beliebte Form von BEC-Angriffen. Dabei werden Personal- und Lohnverrechnungsabteilungen mit dem Ziel, das Gehalt an ein anderes Bankkonto zu überweisen, angegriffen. Hacker geben sich als Mitarbeiter aus und übermitteln neue Kontodaten für die Gehaltsüberweisung. Gehaltsbetrug macht 8 % aller BEC-Angriffe aus. Jedoch nimmt die Zahl dieser Angriffe stetig zu und ist vor Kurzem um mehr als 800 % angestiegen.

1,7 Mrd. USD

1,7 Mrd. USD finanzielle Verluste im Jahr **2019**



Barracuda

E-Mail-Abwehr gegen Business Email Compromise

API-basierter Posteingangsschutz nutzt historische E-Mail-Daten, um ein statistisches Modell oder einen Identity Graphen zu erstellen. Dieser zeigt, wer für gewöhnlich miteinander kommuniziert und welche Namen und Identitäten verwendet werden. Zudem werden mittels Sentiment-Analyse typische Anfragen unter Mitarbeitern des Unternehmens analysiert. Wenn eine ungewöhnliche Anfrage geschickt wird, erkennt der API-basierte Posteingangsschutz einen Imitationsversuch anhand von historischen Kommunikationsdaten und nicht anhand von Regeln und Richtlinien, die klassischen E-Mail-Gateways nutzen.

E-Mail-Gateways haben keinen Einblick in Beziehungen und Kommunikationsmuster basierend auf historischen Daten. Gateways arbeiten mit individuellen, detaillierten Richtlinien und DMARC, um Schutz vor Spoofing und Imitationsangriffen zu gewährleisten. Diese Techniken reichen bei BEC jedoch nicht aus. Sich auf vorab festgelegte Richtlinien zu verlassen, führt zu zahlreichen Falschmeldungen oder falschen Negativmeldungen. API-basierter Posteingangsschutz bietet weitaus mehr Schutz vor BEC-Angriffen.

"Mittels fortschrittlichster Lösungsansätze werden historische Kommunikationsmuster analysiert und basierend auf diesen potenziellen Imitationen erkannt."

Quelle: Gartner, März 2020

Barracuda

Conversation Hijacking

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

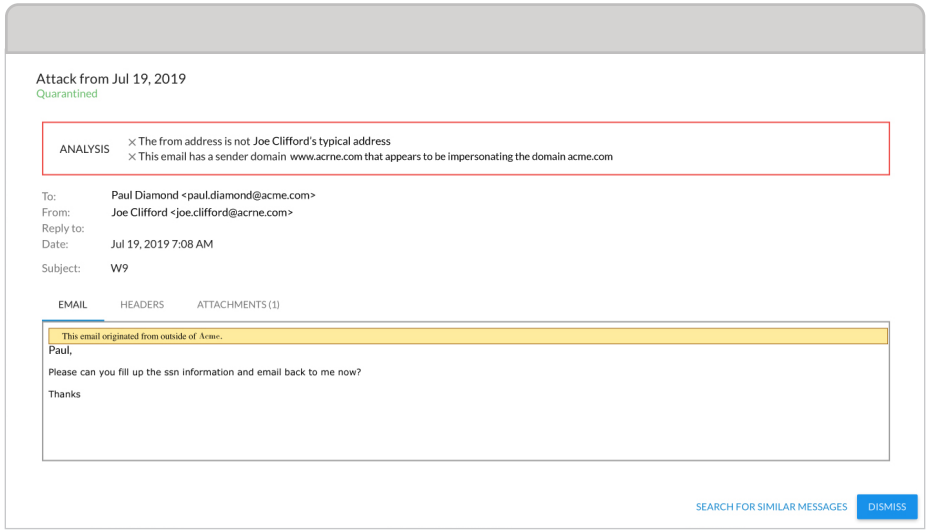
Barracuda

Bei Conversation Hijacking Angriffen klinken sich Cyberkriminelle in bestehende Unterhaltungen ein oder beginnen neue Unterhaltungen anhand der Informationen, die sie von kompromittierten E-Mail-Konten gesammelt haben und zielen darauf ab, an Geld oder persönliche Informationen zu gelangen.

Conversation Hijacking kann Teil eines Account Takeover Angriffs sein. Die Angreifer lesen E-Mails durch und überwachen das kompromittierte Konto, um die Geschäftsabläufe zu kennen und sich über laufende Geschäfte, Zahlungsabläufe und andere Details zu informieren.

Cyberkriminelle nutzen nur selten kompromittierte Konten, um einen Conversation Hijacking-Angriff anzustoßen. Stattdessen nutzen sie E-Mail Domain Impersonation.

Die folgende E-Mail zeigt, wie Cyberkriminelle während eines versuchten Conversation Hijacking Angriffs probieren, eine interne E-Mail Domain nachzuahmen.



Beispiele für einen Angriff

Auswirkungen von Conversation Hijacking

In den vergangenen Monaten kam es bei Domain Impersonation-Angriffen, die als Methode Conversation Hijacking nutzten, zu einem starken Anstieg von mehr als 400 %. Obwohl Conversation Hijacking bei Domain Impersonation-Angriffen im Vergleich zu anderen Arten von Phishing-Angriffen recht selten vorkommt, sind diese komplexen Angriffe sehr personalisiert, was sie effektiv, schwer zu erkennen und kostspielig macht.

Ein bekannter Fall ist jener von Barbara Corcoran, bekannt aus Shark Tank, die durch einen Phishing-Angriff fast 400.000 USD verlor. Scammer täuschten ihren Buchhalter, indem sie E-Mail Domain Impersonation verwendeten und eine Rechnung schickten, die von ihrem Assistenten zu kommen schien. Jedoch hatte Corcoran's Assistent nie eine Rechnung geschickt; die Rechnung kam von einer E-Mail-Adresse, die der des Assistenten stark ähnelte. Als das Team von Corcoran den Fehler bemerkte, war das Geld bereits an die Scammer überwiesen worden.

400K USD

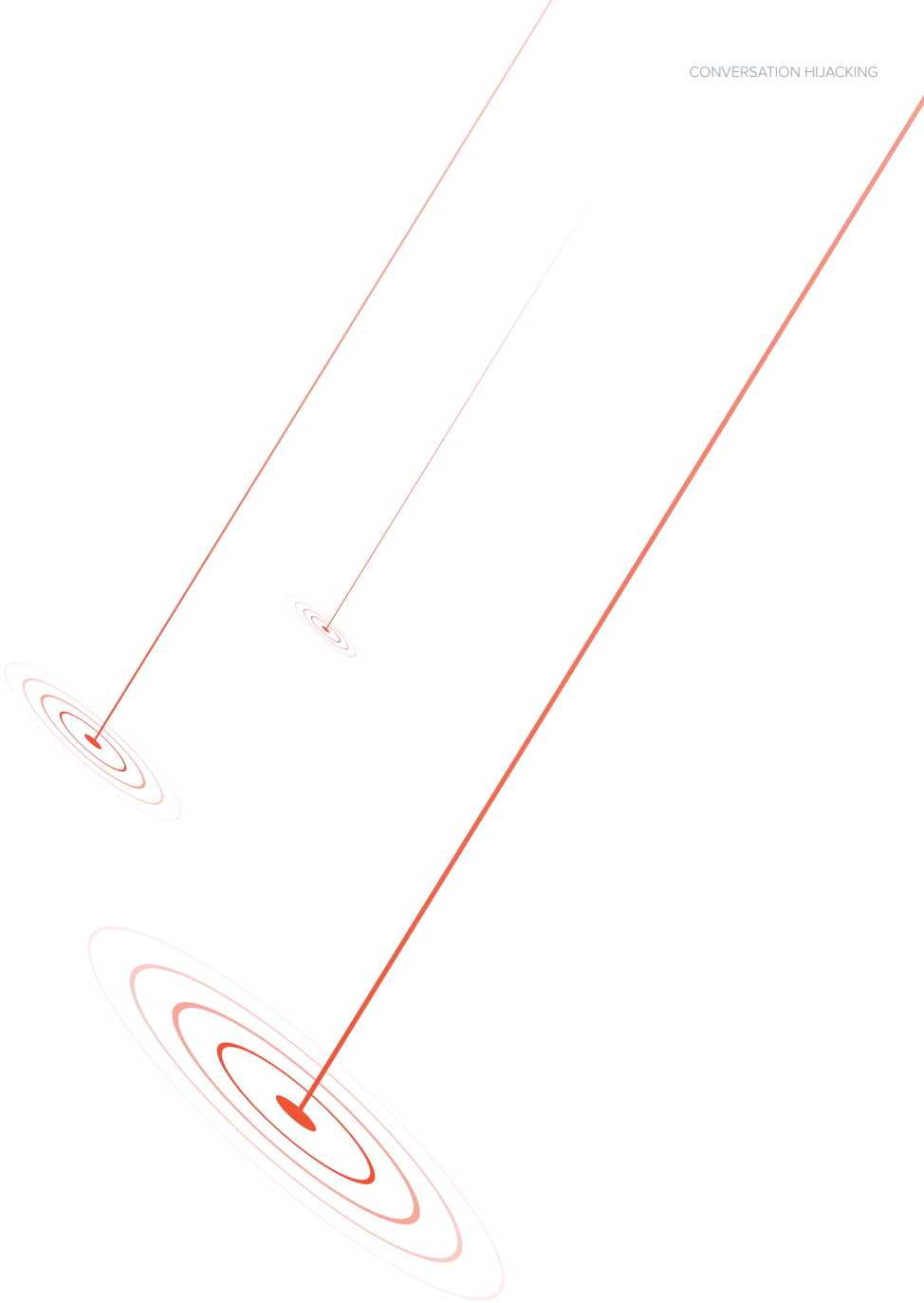
Verlor Barbara Corcoran aus Shark Tank
bei einem Conversation Hijacking-Angriff

Barracuda

Stärkung Ihrer E-Mail-Abwehr gegen Conversation Hijacking

Ein Posteingangsschutz hat durch API-Integration Zugriff auf historische E-Mail- Kommunikationen und nutzt diese im maschinellen Lernen, um zu verstehen, wer wahrscheinlich mit wem kommuniziert sowie wer die externen Kontakte sind und wie mit ihnen interagiert wird. Wenn eine E-Mail-Unterhaltung gekapert wird und sich Cyberkriminelle als Partner ausgeben, dann wehrt der Posteingangsschutz diesen Angriff ab.

Gateways können diese Informationen nicht einsehen. Es können zwar Richtlinien und Whitelists erstellt werden, jedoch ist dieser Ansatz schwer zu skalieren und kann zu Falschmeldungen führen. Wenn eine Unterhaltung gekapert wird, dann stellt das Gateway die E-Mail zu. Deshalb können Gateways vor dieser Angriffsart nicht schützen.



Barracuda

Laterales Phishing

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

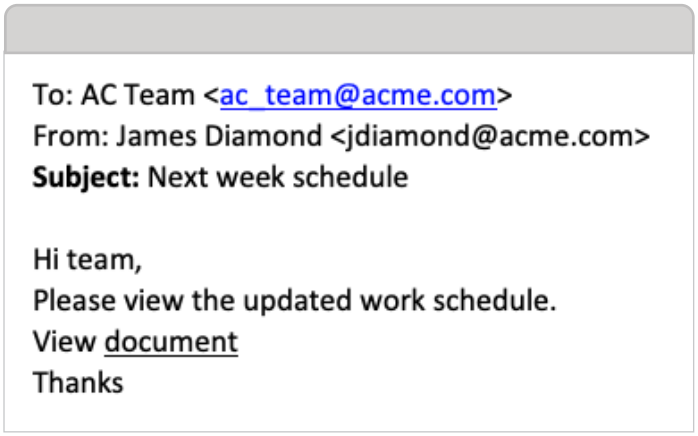
Geringe Komplexität

Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

Bei lateralen Phishing-Angriffen nutzen Angreifer kürzlich kompromittierte Konten, um Phishing-E-Mails an nichts ahnende Empfänger, wie Kontakte im Unternehmen und Partner von externen Organisationen zu senden und somit den Angriff auszuweiten. Da diese Angriffe von legitimen E-Mail-Konten kommen und der Sender ein scheinbar vertrauenswürdiger Kollege oder Partner ist, haben diese eine hohe Erfolgsrate.


To: AC Team <ac_team@acme.com>
From: James Diamond <jdiamond@acme.com>
Subject: Next week schedule

Hi team,
Please view the updated work schedule.
View document
Thanks


Dear user,
We noticed an error on your account, kindly rectify click here. Sorry for the inconvenience.

Beispiele für einen Angriff

Auswirkungen von lateralem Phishing

Im Zuge einer aktuellen Studie haben Forscher herausgefunden, dass jedes siebte Unternehmen in der Vergangenheit von einem lateralen Phishing-Angriff betroffen war. Diese Angriffe zielen auf eine große Bandbreite an Personen und Unternehmen ab und können den Ruf eines Unternehmens stark schädigen. Insbesondere wenn diese Angriffe zu weiteren Folgeangriffen auf andere Unternehmen führen.

Mehr als 55 % dieser Angriffe zielen auf Personen ab, die in irgendeiner Weise in Verbindung zu dem kompromittierten Konto stehen. Es überrascht nicht, dass es bei ungefähr 11 % dieser Angriffe gelingt, weitere Konten zu kompromittieren, was zu noch mehr lateralen Phishing-Angriffen führt.

Jedes siebte Unternehmen war in der Vergangenheit von lateralen Phishing-Angriffen betroffen.

Stärkung Ihrer E-Mail-Abwehr gegen laterales Phishing

In den meisten Fällen handelt es sich bei lateralen Phishing-Angriffen um interne Angriffe. E-Mail-Gateways haben keine Einsicht in diese Kommunikation und können interne Angriffe nicht aufhalten, da diese nie durch das Gateway kommen. Gateways können Angriffe auch nicht nach deren Eindringen beseitigen. Sobald eine E-Mail an den Posteingang versandt wurde, bleibt sie dort. APIs für Posteingangsschutz ermöglichen die Einsicht in interne Kommunikationen. Sie können interne Bedrohungen, wie laterales Phishing, erkennen und diese auch nach deren Versand beseitigen.

Barracuda

Account Takeover

Spam
Daten-Exfiltration
Scamming
Domain Impersonation
Erpressungs-versuche
Conversation Hijacking
Account Takeover

Geringe Komplexität

Hohe Komplexität

Malware
URL Phishing
Spear Phishing
Brand Impersonation
Business Email Compromise
Laterales Phishing

Barracuda

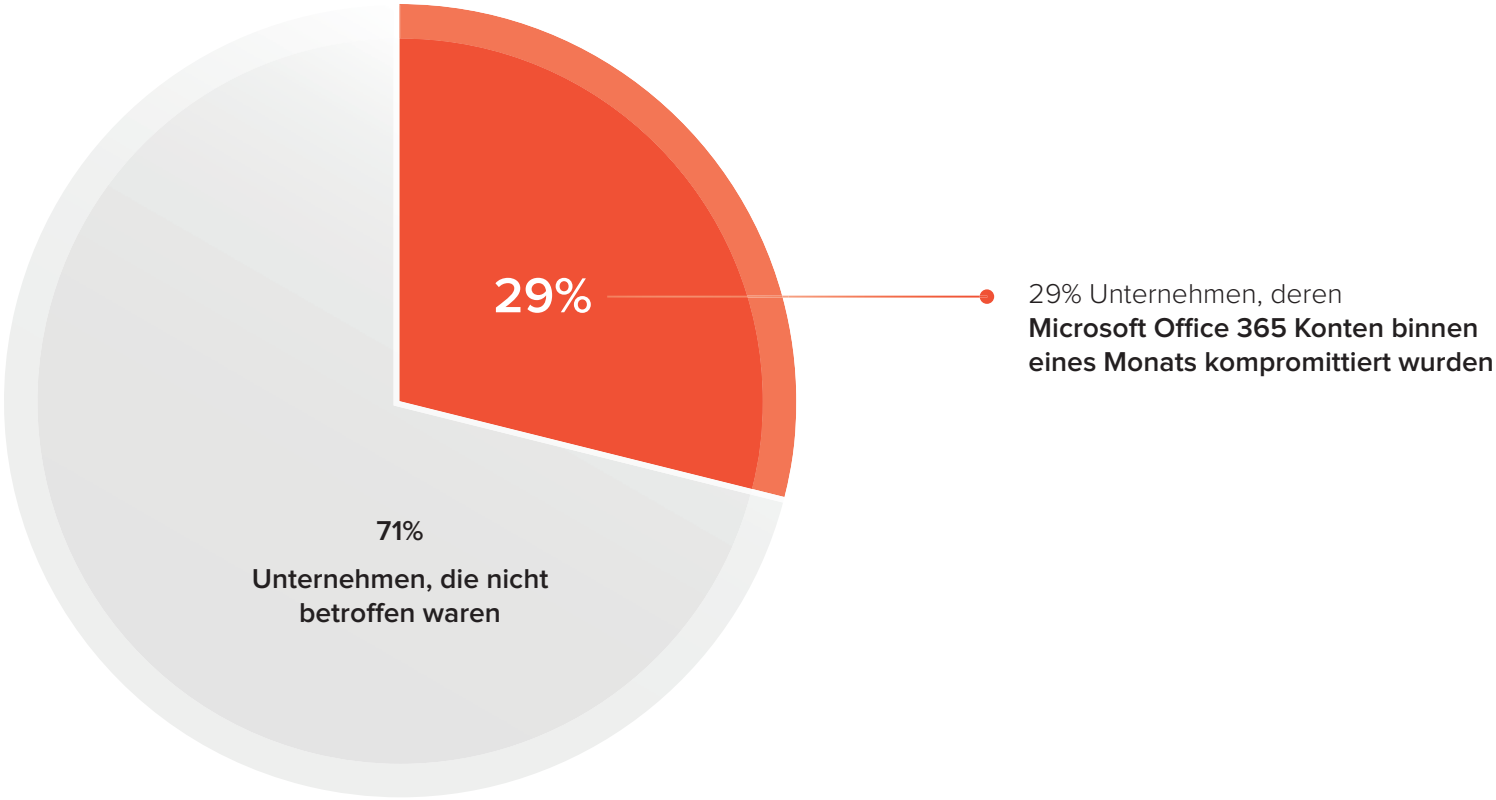
Account Takeover ist eine Art von Identitätsdiebstahl und Betrug, bei dem ein Dritter mit böswilligen Absichten erfolgreich Zugriff auf die Anmeldedaten eines Benutzers erhält. Cyberkriminelle nutzen Brand Impersonation, Social Engineering und Phishing, um Anmeldeinformationen zu stehlen und auf E-Mail-Konten zuzugreifen. Sobald das Konto kompromittiert ist, überwachen und tracken Hacker Aktivitäten, um zu erfahren, wie das Unternehmen seine Geschäfte führt, welche Signaturen verwendet werden und wie Überweisungen gehandhabt werden. Das hilft ihnen dabei, erfolgreiche Angriffe durchzuführen und zusätzliche Anmeldedaten für andere Konten zu sammeln.

Account takeover ist auch unter folgendem Namen bekannt: Account Kompromittierung.

Was bei einem Account Takeover Angriff passiert

Auswirkungen eines Account Takeovers

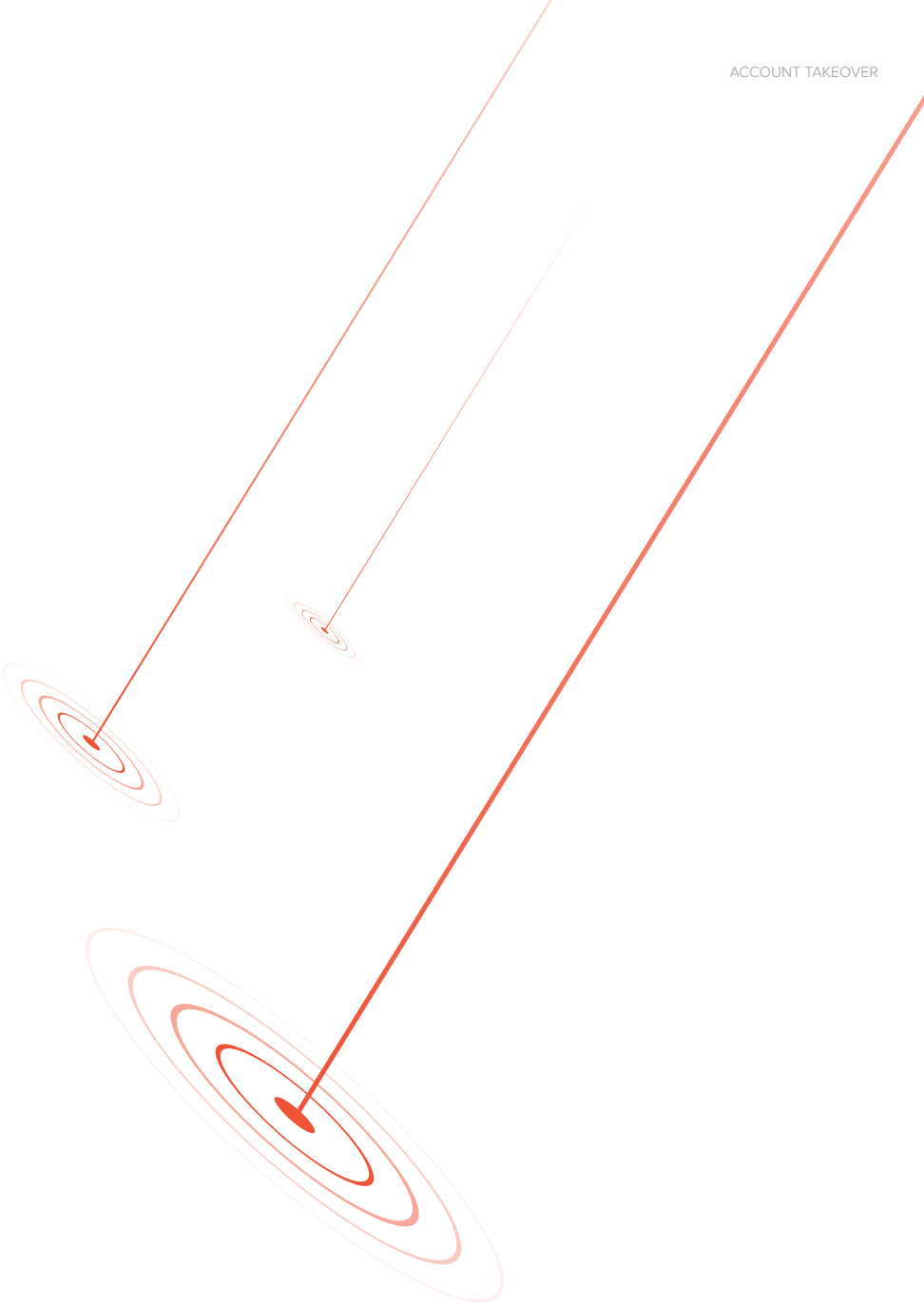
Eine aktuelle Untersuchung von Account Takeover Angriffen ergab, dass bei 29 % der befragten Unternehmen innerhalb eines Monats ihre Microsoft Office 365 Konten von Hackern kompromittiert wurden. Mehr als 1,5 Millionen Spam-E-Mails wurden von den gehackten Office 365 Konten im Zeitraum von 30 Tagen versandt.



E-Mail-Abwehr gegen Account Takeover

Gateways befinden sich am Perimeter außerhalb eines Unternehmens und sind somit nicht mit E-Mail-Posteingängen und Benutzern verbunden. Sie können verdächtiges Verhalten wie Logins von ungewöhnlichen Standorten oder intern versandte E-Mails nicht überwachen.

Ein API-basierter Posteingangsschutz verbindet sich direkt mit dem Posteingang eines Benutzers und überwacht diesen auf verdächtige Änderungen bei Posteingangsregeln, ungewöhnliche Login-Aktivitäten und bösartige Nachrichten, die von bereits kompromittierten Konten versandt wurden. Der Posteingangsschutz erkennt einen Account Takeover, bevor ein betrügerischer Angriff vorgenommen werden kann und mindert die Bedrohung, indem das kompromittierte Konto für böswillige Benutzer gesperrt wird.



Barracuda

Stärkung des Sicherheitsstatus Ihrer E-Mails mittels API-basiertem Posteingangsschutz

Klassische E-Mail-Gateway Security

Das E-Mail-Gateway ist ein Sicherheitsperimeter, das sich direkt vor dem E-Mail-Server befindet und darauf ausgelegt ist, ein- und ausgehende E-Mails auf bösartige Inhalte zu prüfen. E-Mail-Gateways nutzen Technologien wie Reputationsfilter, um IPs mit niedriger Reputation ausfindig zu machen. Sie durchsuchen E-Mail-Inhalte auf Anzeichen für bösartige Intentionen, suchen nach Viren und Malware und authentifizieren den Absender. Zudem analysieren sie URLs und blockieren jene, die zu Phishing-Seiten oder Seiten, die Malware verbreiten, führen. E-Mail-Gateways erkennen und blockieren Zero-Day-Angriffe und Ransomware effektiv. Diese Sicherheitsebene beinhaltet Advanced Threat Protection-Technologien wie Sandboxing. Mittels dieser Technik werden neue, gänzlich unbekannte Malware Arten in einer kontrollierten Umgebung geprüft.

Gateways bilden die notwendige Grundlage für E-Mail-Security. Sie wehren die meisten bösartigen Nachrichten, inklusive Spam, große Phishing-Angriffe, Malware, Viren und Zero-Day-Angriffe ab. Da Gateways jedoch hauptsächlich auf Filtern, Regeln und Richtlinien basieren, gelingt es ihnen nicht, Ihr Unternehmen vor gezielten E-Mail Angriffen, die Social Engineering Taktiken wie Spear Phishing und Business Email Compromise nutzen, zu schützen. Gateways suchen nach Anzeichen für bösartige Inhalte oder Absender, lassen jedoch Angriffe durch, bei denen die voreingestellten Richtlinien, Filter oder Authentifizierungsregeln nicht greifen.

API-basierter Posteingangsschutz

E-Mail-Gateways sind zwar immer noch notwendig, bieten jedoch nicht ausreichend Schutz vor den sich weiterentwickelnden Cybersicherheitsbedrohungen. Um Ihr Unternehmen vor „socially engineered“ Angriffen zu schützen, sollten Sie eine weitere Sicherheitsebene integrieren – außerhalb des Gateways und auf Posteingangslevel.

Posteingangsschutz basiert auf APIs, um sich direkt mit der E-Mail-Umgebung und einzelnen Posteingängen zu verbinden. API-Integration sorgt für Einsicht in historische und interne E-Mail-

> "Erweitern Sie sichere E-Mail-Gateway Lösungen, damit diese über einen modernen Phishing-Schutz, Betrugserkennung und internen E-Mail-Schutz verfügen."
>
> *Gartner: How to build an effective email security architecture, März 2020*

Barracuda

Kommunikation jeder Person im Unternehmen. Im Anschluss werden diese Daten sowie KI genutzt, um einen Identity Graph für jeden Benutzer zu erstellen, der die Kommunikationsmuster widerspiegelt.

Der Identity Graph setzt sich aus mehreren Klassifikatoren zusammen, die bestimmen, wie die normale E-Mail-Kommunikation bei jedem Mitarbeiter aussieht. Das System erfasst beispielsweise (basierend auf historischen Daten) von welchen Standorten aus sich Mitarbeiter für gewöhnlich einloggen, welche E-Mail-Adressen sie verwenden, mit wem sie kommunizieren, welche Anfragen sie stellen und hunderte weitere Signale. Wenn etwas Ungewöhnliches passiert, dass nicht in den Identity Graph einer Person passt, markiert der Posteingangsschutz gemeinsam mit KI dies als potentiell bösartig und entfernt es aus dem Posteingang, bevor der Benutzer damit interagieren kann.

Man kann E-Mail-Gateways zwar so einstellen, dass sie ähnlich funktionieren, jedoch ist diese Lösung nicht skalierbar. Zahlreiche der heutigen E-Mail-Gateways ermöglichen eine detaillierte Anpassung und die Erstellung von Richtlinien, um gezielte Angriffe abzuwehren. Aus jedem Klassifikator kann eine Regel oder Richtlinie für das Gateway gemacht werden, doch mit hunderten Richtlinien, die für tausende Mitarbeiter definiert werden müssen, ist diese Lösung nicht skalierbar. Sie passt sich nicht an Veränderungen an und ist anfällig für eine Vielzahl von Falschmeldungen und falschen Negativmeldungen.

Unternehmen, die sich auf angepasste Gateways zum Schutz ihrer Benutzer vor Spear Phishing-Angriffen verlassen, können nur eine bestimmte Anzahl an Mitarbeitern schützen, bei denen ein hohes Risiko festgestellt wurde. Spear Phishing-Angriffe werden so zwangsläufig die Gateways umgehen und den Posteingang von Benutzern erreichen.

Klassifizierung von E-Mail-Bedrohungen - 13 Arten

BEDROHUNGSARTEN	E-MAIL GATEWAY	API-BASIERTER POSTEINGANGSSCHUTZ
Spam	●	○
Malware	●	○
Daten-Exfiltration	●	○
URL Phishing	◑	●
Scamming	◑	●
Spear Phishing	○	●
Domain Impersonation	○	●
Service Impersonation	○	●
Erpressungsversuche	◑	◑
Business Email Compromise	○	●
Conversation Hijacking	○	●
Laterales Phishing	○	●
Account Takeover	○	●

○ bietet unzureichenden Schutz ◑ bietet angemessenen Schutz ● bietet besten Schutz

Barracuda

Fazit: Effektiver Schutz vor sich weiterentwickelnden E-Mail-Bedrohungen

E-Mail-Angriffe haben sich so entwickelt, das sie klassische Abwehrmechanismen umgehen können. Somit müssen Unternehmen nicht nur für Schutz am Gateway, sondern auch darüber hinaus sorgen. Jedes Unternehmen sollte die richtigen Technologien und Personen einsetzen, um effektiven E-Mail-Schutz zu gewährleisten.

Abwehren von Großangriffen am Gateway

Gateways bilden die notwendige Grundlage für E-Mail-Security. Sie wehren die meisten böswilligen Nachrichten wie Spam, großflächige Phishing-Angriffe, Malware, Viren und Zero-Day-Angriffe ab. Wenn diese Angriffe ungehemmt eindringen, sorgen sie für infizierte Geräte und Chaos innerhalb des Unternehmens, was sich auf die Produktivität auswirkt.

Benutzer auf Posteingangs-Level schützen

Obwohl Gateways wichtig sind, bieten sie alleine keinen ausreichenden Schutz mehr. Durch API basierten Posteingangsschutz erhält man Einblick in historische und interne E-Mail-Kommunikation, die für den Schutz vor gezielten Angriffen, die Gateways umgehen, notwendig sind.

Benutzer über die neuesten Bedrohungen informieren

Einige sich rasch entwickelnde und komplexe Phishing-Angriffe, inklusive jene, bei denen Social Engineering Taktiken zum Einsatz kommen, können das Secure E-Mail Gateway umgehen. Schulungen des Sicherheitsbewusstseins für Mitarbeiter helfen, das Unternehmen vor diesen Bedrohungen zu schützen. Durch Simulation und Training lernen Mitarbeiter, wie man bösartige Inhalte erkennt und meldet und werden so zu einer weiteren Schutzebene.

Barracuda
Your journey, secured.

Scannen Sie Ihre Microsoft 365-Umgebung. Schnell, kostenlos und sicher mit dem **Barracuda Email Threat Scanner**.