mimecast®

Der Stand des Markenschutzes 2021

Kampf um Markensicherheit – neue Cyber-Bedrohungen auf dem Vormarsch

Zusammenfassung: 2020 verändert die Markenschutz-Landschaft

Marketers zielen darauf ab, mit der richtigen Botschaft den richtigen Kunden zur richtigen Zeit zu erreichen. Das ist genau das, was Cyberkriminelle auch tun - nur dass sie Ihre Marke stehlen, um ihr "Produkt" zu verkaufen.

Im Jahr 2020 nutzten Cyberkriminelle die Angst und Unsicherheit der globalen Bevölkerung aus, die angesichts der COVID-19-Pandemie herrschte. Im Rahmen von E-Mail-Phishing-Kampagnen und anderen bösartigen Angriffen, bei denen sich Cyberkriminelle als Marken ausgeben, nutzten sie das Vertrauen der Kunden in diese Unternehmen für ihre Zwecke aus. Die Untersuchungen des Mimecast Threat Centers haben gezeigt, wie weit verbreitet Marken-Identitätsmissbrauch ist und welche Auswirkungen diese Bedrohung haben kann Basierend auf der Überwachung der Bedrohungsdaten durch Mimecast, kann auf folgende Erkenntnisse verwiesen werden:

Die Anzahl der Marken-Imitation-E-Mails pro Monat, die von Mimecast-Kunden **entdeckt wurden, stieg im Jahr 2020 gegenüber 2019 um 44 % auf durchschnittlich fast 27 Millionen.***

- **Unternehmen auf der Liste BrandZ™ mit den 100 wertvollsten globalen Marken 2020 erlebten in den beiden Monaten Mai und Juni 2020 einen 381%igen Anstieg von Brand Impersonation-Angriffen**
- Neue Domains, die unter dem Verdacht der Markenimitation stehen, stiegen ebenfalls sprunghaft an: **366% im Mai-Juni 2020.**
- Und das erschreckende Ergebnis: Die monatlichen unwissentlichen Klicks auf gefährliche Links stiegen **im Laufe des Jahres um 84,5%.**

In Übereinstimmung mit diesen Ergebnissen gaben 76% der in Mimecasts State of Email Security Report 2021 (SOES 2021) Befragten an, dass sie im Laufe des Jahres 2020 mindestens einen Web- oder E-Mail-Spoofing-Angriff unter Verwendung ihrer Domains oder ähnlicher Domains identifiziert haben oder darauf aufmerksam gemacht wurden; 25% sagten, sie hätten mehr als 10 identifiziert. Und das sind nur die, wovon denen sie wussten. In den Kundeninterviews für diesen Bericht hörten wir mehrere Geschichten darüber, wie überrascht Marketers und Cybersicherheitsexperten waren, als sie mit der proaktiven Überwachung von Identitätsmissbrauch begannen und herausfanden, wie viele ihrer Marken wirklich ausgenutzt wurden.

Die Herausforderung, wie Deloitte in seinem 2020 Global Marketing Trends Bericht darlegt, ist folgende: Unternehmen, denen es nicht gelingt, das Kundenvertrauen in digitalen Umgebungen zu sichern, werden wahrscheinlich existenzielle Bedrohungen für die Kundenloyalität und den Marktwert ihrer Marken erleben.

*Hinweis: Da diese Daten nur für Mimecast-Kunden gelten, wird die Anzahl der E-Mails zur Markenimpersonation, die alle Unternehmen angreifen, oft so hoch sein wie diese Zahl. Aber die Trends, die von den über 40.000 Mimecast-Kunden gesehen werden, gelten als illustrativ für die größere E-Mail-Nutzergemeinschaft.

Wichtigste Erkenntnisse

Jeder Klick von einer gefälschten E-Mail auf eine gefälschte Webseite kann den Lead eines Marketers stehlen.

.01 Alle Marken sind gefährdet.

Ob groß oder klein, B2C oder B2B, wenn Ihre Marke eine Online-Präsenz hat, ist sie gefährdet. Retail-Betrug, Compromise bei geschäftlichen E-Mails, Identitätsmissbrauch in der Lieferkette und Kampagnen zur Rekrutierung von Geldwäschern sind nur einige der Arten von Markenexploiting-Angriffen, die von Interviewern gemeldet wurden. Technologie- und Finanzunternehmen waren in unserer Analyse der 100 wertvollsten Marken die am meisten imitierten Marken, gefolgt von Telekommunikations-, Schifffahrts-, Einzelhandels-, Unterhaltungs- und Transportunternehmen.

.02 Marken sind sich des Ausmaßes des Problems nicht bewusst.

Marketers, Stakeholder und sogar Cybersicherheitsexperten erkennen oft nicht das volle Ausmaß, in dem ihre Marke genutzt wird, bis sie mit der proaktiven Überwachung beginnen – was immer noch selten ist. Zwei kleine Banken, eine in den USA und eine in Großbritannien, berichteten uns von ihrer Überraschung über durchschnittlich 10 bis 15 “Takedowns” von Marken-Imitaten pro Monat, nachdem sie proaktiv geworden waren.

.03 Marken verlieren Vertrauen - und Leads - an Cyberkriminelle.

So schädlich der Vertrauensverlust für den Ruf einer Marke auch sein kann (Frost & Sullivan-Studien zeigen, dass 48% der Befragten einen Online-Dienst nicht mehr nutzen, wenn dieser eine Datenschutzverletzung hatte), für Marketers sind verlorene Leads ein weitaus greifbarerer Schmerzpunkt. Jeder Klick von einer gefälschten E-Mail auf eine gefälschte Webseite kann einem Marketer einen Lead stehlen.

.04 Marketers und Sicherheitsteams müssen zusammenarbeiten.

Diese traditionell isolierten Geschäftsabteilungen müssen zusammenarbeiten, um Markensicherheit zu erreichen. Cybersecurity-Experten können nicht immer legitime Nutzungen der Marke von den bösen Akteuren unterscheiden, und Marketers können ohne ihre IT-Sicherheitspartner keinen Einblick in das Ausmaß des Problems erhalten. Ein IT-Experte erzählte uns, dass er ein Programm zur Überwachung von Markenimitationen gestartet hat, nur um den Marketers die Augen für das Problem zu öffnen und eine kollaborative Brücke zwischen ihrem und seinem Team zu bauen.

.05 Ein schneller Takedown des Angriffs ist entscheidend – aber schwer zu erreichen.

Unternehmen können spoofed Web-Domains entfernen, aber das kann eine Herausforderung darstellen. Selbst mit einer firmeninternen Markenschutzstrategie können manuelle Takedowns kostspielig und zeitaufwändig sein - wenn Sie sie überhaupt abschalten können.

.06 Markenüberwachungs-/-schutzdienste sind ein Muss.

Services, die Überwachung zur Identifikation von Identitätsmissbrauch der Marke bieten, einschließlich des Domain-basierten E-Mail-Authentifizierungsprotokolls. Reporting und Konformität (DMARC), sind ein Muss für die Sicherheit der Online-Marke. Zunächst beleuchten sie den Schweregrad des Problems, der sich für jede Marke unterscheidet. Dann kann Markenschutz Marken dabei unterstützen, das Problem zu mindern und die Websites mit Identitätsmissbrauch schneller zu beseitigen, als die meisten Unternehmen selbst tun können.

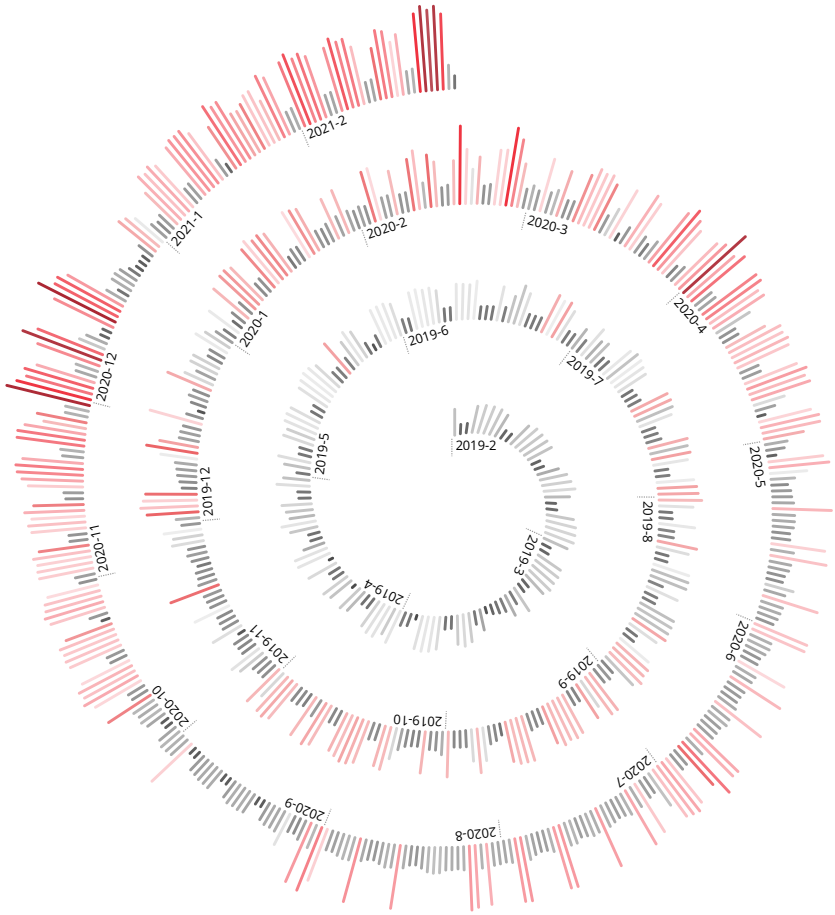
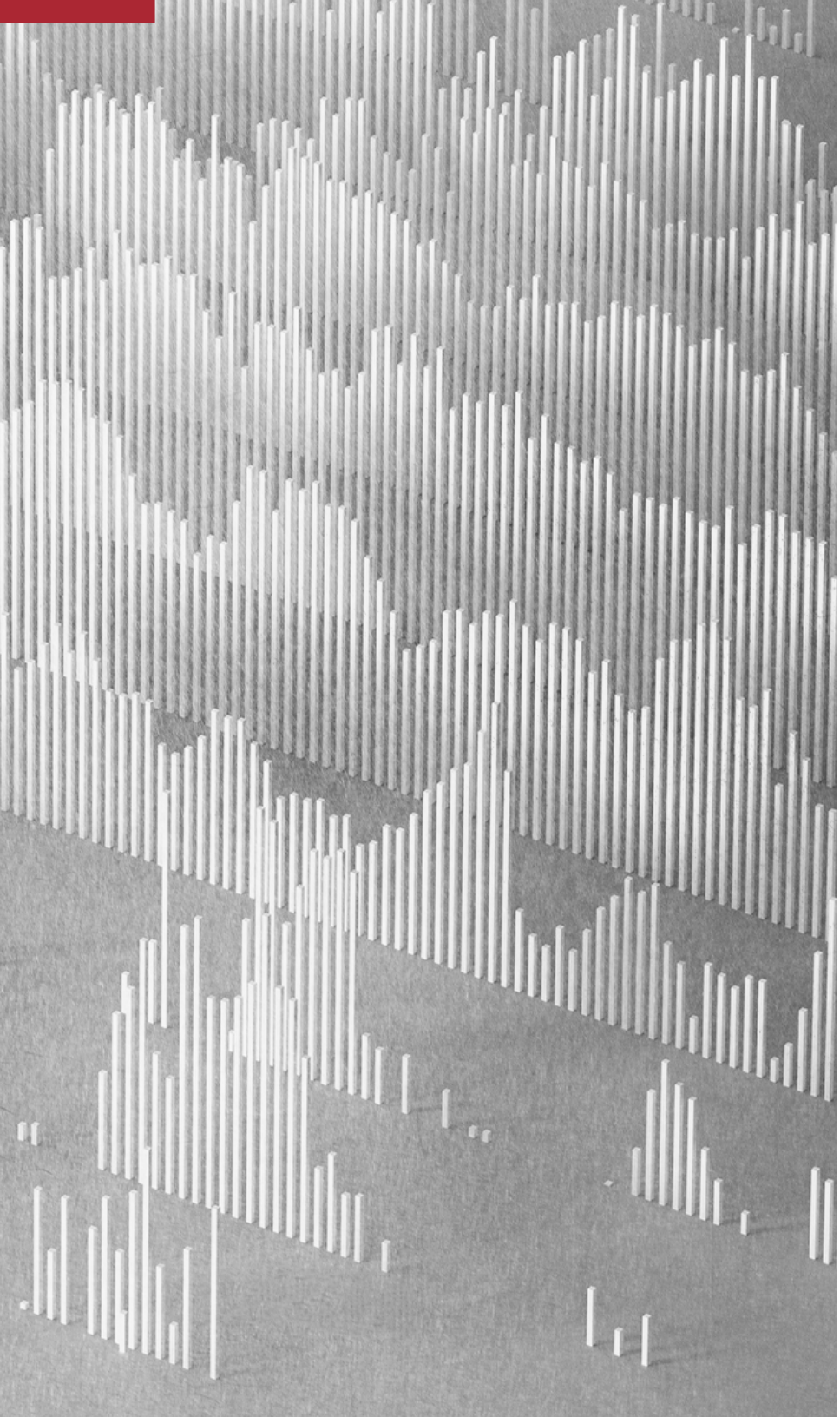


Abbildung 1: Tägliche Email Impersonations von Mimecast Daten, Feb. 2019-Feb. 2021

In diesem Spiraldiagramm der täglichen E-Mail-Marken-Impersonationsangriffe kennzeichnen graue und hellgraue Linien Tage mit leichten Marken-Impersonationen und rote und dunkelrote Linien Tage mit schweren Angriffen. Beachten Sie die Zunahme der Angriffsintensität von Markenimpersonationen im April und dann im November bis Dezember 2020 sowie im Februar 2021.



Methodik des Berichts

Die Daten in diesem Bericht stammen aus der Analyse von mehr als einer Milliarde E-Mails pro Tag, die von Mimecast im Auftrag seiner mehr als 40.000 globalen Kundenunternehmen überwacht und vom Mimecast Threat Intelligence Center zusammengestellt wurden.

Darüber hinaus befragten Berichtsautoren von November 2020 bis Februar 2021 Cybersicherheitsexperten in Organisationen, die Markenschutz, DMARC-Dienste oder beides verwendet haben. Die Mehrheit - aber nicht alle - waren Mimecast-Kunden.

Da es weltweit Millionen von Unternehmen gibt, wird die tatsächliche Zahl der weltweiten Fälle von E-Mail-Phishing, Marken-Impersonation, verdächtigen Website-Domains und unsicheren URL-Klicks ein Vielfaches der in diesem Bericht beschriebenen Zahlen betragen. Aber die von Mimecast-Kunden erlebten Trends spiegeln wahrscheinlich die Trends in der Welt insgesamt wider und sollten daher als illustrativ betrachtet werden.

Marken sehen oft nicht das ganze Problem

Marken machen heute regen Gebrauch von digitaler Marketingtechnologie, um besser mit Kunden und Interessenten in Kontakt zu treten - hauptsächlich über E-Mails. Und das aus gutem Grund:

Schätzungen der Investitionsrendite (ROI) für E-Mail-Marketing liegen im Bereich von

$42 *für jeden ausgegebenen* **$1**

E-Mails haben jedoch eine inhärente Sicherheitslücke: Bis vor kurzem konnte jeder E-Mails von den Domains Ihrer Marke versenden – und 40% der Verbraucher zögern nicht, auf Links in E-Mails ihrer Lieblingsmarken zu klicken, laut einer neuen europäischen Umfrage zum Markenvertrauen, die später in diesem Jahr von Mimecast stammt.

40% **der Verbraucher zögern nicht, auf Links in E-Mails von ihren Lieblingsmarken zu klicken**

Jeder kann immer noch die Domain einer Marke in E-Mails fälschen, es sei denn, das Sicherheitsteam der Marke setzt relativ aktuelle E-Mail-Authentifizierungsprotokolle ein, vor allem DMARC. So geben sich Cyberkriminelle immer wieder als Marken und Domains im Web aus.

- B2C-Phishing-Angriffe, die darauf abzielen, Kunden zu betrügen oder ihre Anmeldedaten zu stehlen.
- Kompromittierende Angriffe auf Geschäfts-E-Mails, die das Konterfei Ihres CEOs und Ihrer Marke nutzen, um Mitarbeiter dazu zu verleiten, auf bösartige Inhalte zuzugreifen, was zu Datenverletzungen führen kann.
- B2B-Supply-Chain-Impersonation-Angriffe, die Ihre Marke nutzen, um mit Händlern und Lieferanten zu kommunizieren, oft mit der Absicht, Zahlungen abzufangen.

Der Identitätsmissbrauch einer Marke online ist unsichtbar, bis Sie proaktiv danach suchen.

Mimecasts SOES 2021-Bericht stellte fest, dass fast die Hälfte der Befragten (47%) im vergangenen Jahr eine Zunahme von Spoofing-E-Mails verzeichneten, die die Marke ihres Unternehmens missbrauchten, und 42% sahen eine Zunahme von gefälschte Web-Domains, die sich als ihre Marke ausgaben.

Viele andere schenken dem Problem vielleicht nicht genug Aufmerksamkeit. Denn während Markenimitation "im echten Leben" greifbar ist - gefälschte Waren, Warenzeichen und Urheberrechte, ist das für Marketers von Marken nicht so offensichtlich - da Markenimitation online unsichtbar ist, bis Sie proaktiv nach ihr suchen.

E-Mail-Phishing ist jedoch nur ein Teil der Gleichung. Cyberangreifer können jeden digitalen Touchpoint nutzen um die Beziehung zu den Stakeholdern der Marke auszunutzen und Betrug zu begehen, Malware ablegen, Zugangsdaten sammeln oder die Grundsteine für Datenpannen und Ransomware-Angriffe platzieren. Dazu gehören neben E-Mails auch Web-Domains, soziale Medien, mobile Apps und mehr - tatsächlich sind allein in Nordeuropa 55% der Verbraucher über die Suche und 52% über soziale Medien auf einer gefälschten Website gelandet. Angreifer verwenden sogar Verschlüsselung, um den Opfern vorzugaukeln, sie würden auf eine "sichere" Webseite zugreifen.

Im vierten Quartal 2020 klickten sich etwa 84% der E-Mail-Phishing-Angriffe zu bösartigen Websites durch, die durch das Verschlüsselungsprotokoll HTTPS "geschützt" waren, gegenüber nur 10% im ersten Quartal 2017, so die Anti-Phishing Working Group (APWG), ein internationales Konsortium von mehr als 1.700 Unternehmen.[4]

47%

sahen einen Anstieg des Volumens von Spoofing-E-Mails, die ihre Rechte missbrauchten

42%

sahen eine Zunahme von gefälschten Web-Domains, die sich als ihre Marke ausgaben

55%

über eine Suche auf einer gefälschten Website gelandet sind

52%

sind allein in Nordeuropa über soziale Medien auf einer gefälschten Website gelandet

Die vielen Möglichkeiten, wie Cyberkriminelle Ihre Marke ausnutzen

Link Manipulation

Was ist das?
Cyberkriminelle registrieren Domains mit Namen, die legitimen Markenwebsites sehr ähnlich sind. Diese manipulierten Links können Benutzer auf gefälschte Websites leiten, die bösartige Inhalte enthalten.

Wie kann das aussehen?
Typosquatting, das auf der Wahrscheinlichkeit basiert, dass ein Benutzer einen Tippfehler oder einen ähnlichen Fehler macht, wenn er eine URL in seinen Webbrowser eingibt (“miemcast.com” anstelle von “mimecast.com”)

Internationalisierte Domain-Namen (IDNs), die internationale Zeichen anstelle von deutschen Zeichen verwenden, wie z. B. das lateinische Zeichen “ɱ” anstelle von “m”.

Missbrauch von Top-Level-Domains (TLD), die einen legitimen Domain-Namen verwenden und die falsche TLD verwenden, z. B. “.ca” oder “.jp” anstelle von “.com”.

Website-Spoofing

Was ist das?
Cyberkriminelle erstellen gefälschte Websites, die wie legitime Markenseiten aussehen. Die Benutzer werden in der Regel über manipulierte Links geleitet.

Wie kann das aussehen?
Phony-Websites mit Farben, Bildern und Codierung werden direkt von der Website einer echten Marke kopiert. Diese gefälschten Websites können erstaunlich echt aussehen und ahnungslose Benutzer leicht dazu verleiten, versehentlich Malware herunterzuladen oder ihre persönlichen Anmeldedaten in ein Anmeldeportal einzugeben.

Lieferketten-Imitation

Was ist das?
Cyberkriminelle geben sich als legitime Marke aus und schleusen sich in den Prozess der Lieferkette ein, meist per E-Mail.

Wie kann das aussehen?
Böswillige Akteure versuchen in der Regel, echte Zahlungen an Lieferanten abzufangen oder Mitarbeiter der Kreditorenbuchhaltung dazu zu bringen, doppelte oder gefälschte Zahlungen vorzunehmen. Eine E-Mail, die scheinbar von einem echten Verkäufer stammt, könnte dringend die Zahlung einer "unbezahlten Rechnung" verlangen, mit Überweisungsinformationen. Die Gelder gehen dann an ein kriminelles Bankkonto.

Gefälschte Stellenanzeigen

Was ist das?
Cyberkriminelle veröffentlichen gefälschte Stellenausschreibungen, die sich als legitimes Unternehmen ausgeben, entweder auf Job-Websites oder in Suchmaschinenanzeigen. Manchmal wenden Sie sich auch direkt an ahnungslose Verbraucher.

Wie kann das aussehen?
Bei vielen **Jobangebots-Scams** stellt der Betrüger ein Jobangebot ein und fordert das Opfer auf, eine Summe zu zahlen, um für eine nicht existierende Stelle "eingestellt" zu werden.

In **diesen Anwerbungskampagnen erhalten** Personen Jobangebote, zum Beispiel als Buchhalter, in der die Person unbewusst Geld für Betrüger abwickelt. Das Opfer weiß möglicherweise nicht, dass es an einer Geldwäsche beteiligt ist, weil die Betrüger ihnen ein scheinbar rechtmäßiges Gehalt zahlen.

Social Media Impersonation

Was ist das?
Cyberkriminelle erstellen gefälschte Social-Media-Konten unter Verwendung echter Markennamen, erstellen Beiträge und kommentieren Nachrichten, um legitim zu erscheinen.

Wie kann das aussehen?
Beiträge oder Kommentare können bösartige Links enthalten, die ahnungslose Opfer auf bösartige Websites leiten.

In anderen Fällen zielen Imitatoren vielleicht einfach darauf ab, eine Marke zu blamieren oder den Ruf zu ruinieren.

Business Email Compromise

Was ist das?
Cyberkriminelle verwenden E-Mail-Spoofing-Taktiken, um E-Mails zu versenden, die den Anschein erwecken, von legitimen Mitarbeitern oder Führungskräften des Unternehmens zu stammen.

Wie kann das aussehen?
Eine E-Mail, die scheinbar von einer Person in einer Führungsposition stammt und den Empfänger auffordert, auf einen Link zu klicken, der zu einer gefälschten Website führt, oder einen Anhang herunterzuladen, der Malware enthält.

In anderen Fällen bittet eine "Führungskraft" den Empfänger, die Überweisungsdaten für eine ansonsten rechtmäßige Zahlung zu ändern, damit der Kriminelle stattdessen das Geld erhält.

Search Ad Phishing

Was ist das?
Cyberkriminelle sorgen dafür, dass ihre bösartigen Webseiten in den Suchergebnissen erscheinen, meist durch Spoofing der Domain einer Marke.

Wie kann das aussehen?
Was wie eine legitime Suchanzeige für eine Einzelhandelsmarke aussieht, bietet Benutzern kostenlose oder vergünstigte Waren an. Stattdessen kann der Link den Benutzer zu einer geklonten Webseite führen, die Malware ablegt, Zugangsdaten sammelt oder den Benutzer zu einem betrügerischen Kauf verleitet.

Vishing & SMShing

Was ist das?
Cyberkriminelle senden Sprach- oder Textnachrichten, die so tun als wären sie von einer Marke.

Wie kann das aussehen?
Ein Mitarbeiter könnte eine Sprachnachricht von jemandem erhalten, der sich als Geschäftsführer ausgibt und darum bittet, Geld auf ein bestimmtes Bankkonto zu überweisen.

Ein Verbraucher erhält möglicherweise eine Textnachricht mit einem Link zu "Tracking-Informationen" eines bekannten Versandunternehmens, aber der Link leitet den Benutzer auf eine bösartige Webseite weiter.

Die Ausnutzung von Markennamen kann Unternehmen jeder Größe und in jeder Branche beeinflussen. Das Online-Banking z.B. gehörte in der europäischen Markenvertrauensstudie zu den vertrauenswürdigsten Branchen, aber ist paradoxerweise auch eine der Branchen, die am häufigsten Ziel von Marken-Imitation und Phishing-Angriffen sind. So berichtete uns ein CISO einer kleinen britischen Bank, dass er im vergangenen Jahr etwa 14 betrügerische Websites pro Monat gefunden - und entfernt - hat. Eine ähnlich kleine regionale US-Bank berichtete von durchschnittlich 10 oder 11 betrügerischen Websites pro Monat, die die Marke der Bank imitieren. SaaS-, Webmail-, Social-Media-, E-Commerce-, Einzelhandels-, Logistik-, Versand- und Telekommunikationsunternehmen sind ebenfalls einem hohen Risiko ausgesetzt.[5]

Nach Angaben der APWG haben sich die kriminellen Phishing-Aktivitäten im Jahr 2020 verdoppelt. [6] Eine Analyse der eigenen Threat Intelligence-Daten von Mimecast (Abbildung 2) gibt diesem Wachstum mehr Kontext und zeigt, wie Cyberangreifer opportunistisch zuschlagen und auf den richtigen Moment und die richtige Botschaft warten. Beim steilen Wachstum von Ende 2019 bis Ende 2020 konzentrierte sich der Spitzenwert rund um die frühen Monate der COVID-19 Pandemie, als Angst, Unsicherheit und Zweifel neue Schwachstellen eröffneten. Die bösen Akteure schienen eine Zeit lang eine Verschnaufpause einzulegen, bevor sie im Vorfeld der US-Präsidentschaftswahlen im November (der zweite Höhepunkt) erneut mit Nachdruck angriffen. Der Rückgang nach dem Wahlhoch war jedoch viel kürzer, da sowohl der Januar als auch der Februar 2021 dieses Hoch übertrafen.

Insgesamt stiegen die von Mimecast entdeckten E-Mail-Marken-Imitationen in dem von Abbildung 2 abgedeckten Zeitraum von 14,5 Millionen im Februar 2019 auf 39,2 Millionen im Februar 2021, was einem Anstieg von 170% entspricht - oder einer 2,7-fachen Steigerung. Der monatliche Durchschnitt für 2020 lag bei 26,95 Millionen, ein Anstieg von 44% gegenüber 18,73 Millionen im Jahr 2019.

Monatlich ansteigende E-Mail-Impersonations

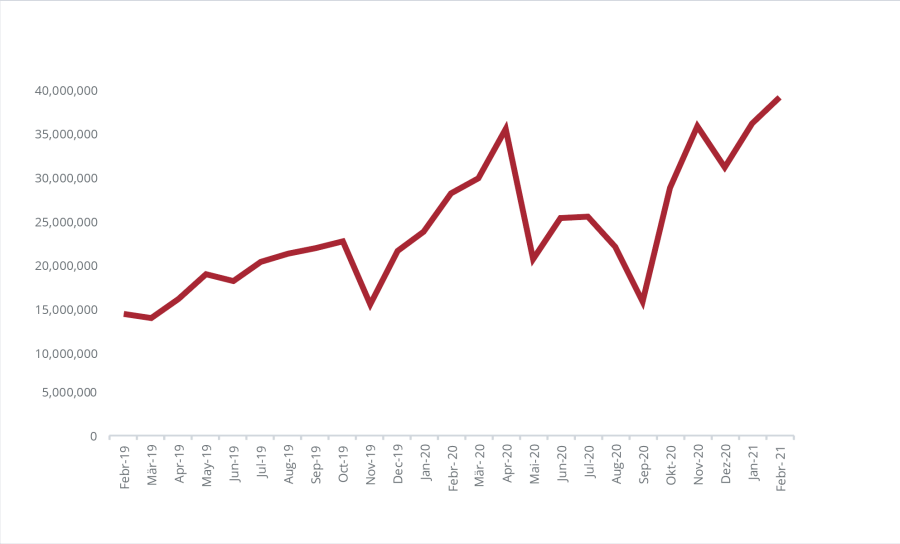


Abbildung 2: Steigende monatliche E-Mail-Impersonations, 2/2019 - 2/2021

Cyberangreifer sind opportunistisch in ihren Attacken und warten auf den richtigen Moment und die richtige Botschaft

In der Zwischenzeit zeigt Abbildung 3, dass die Anzahl verdächtiger Domains mit Live-Inhalten der Marken, die den Brand Exploit Protect-Service von Mimecast nutzen, von Mai bis Juni 2020 um 366% gestiegen ist, im Vergleich zu Januar und Februrar 2020. 4,7 Mal so viele wie in den ersten zwei Monaten des Jahres, bevor die Auswirkungen der COVID-19 Pandemie spürbar wurden. Und obwohl die Anzahl der neuen verdächtigen Domains von diesem Höchststand Mitte 2020 zurückgegangen ist, ist sie auf einem "neuen normalen" höheren Niveau geblieben: In den letzten beiden Monaten des Jahres 2020 wurden 73% mehr verdächtige Domains registriert als in den ersten beiden Monaten des Jahres.

Abbildung 4 zeigt das erschreckende Ergebnis. Die zunehmenden Angriffe auf Marken-Identitäten zu einem Zeitpunkt, an dem große Teile der Weltbevölkerung psychologisch am anfälligsten waren, führten zu einem dramatischen Anstieg der Klicks von Benutzern auf unsichere URLs, die per E-Mail zugestellt wurden; tatsächlich verdoppelten sich die unsicheren Klicks, wenn man die Daten des Threat Intelligence Center für Mimecast-Kunden (+99,8 %) von Januar bis Mai 2020 betrachtet. Wieder gibt es eine Atempause von Mai bis September 2020 und dann ein erneutes Wachstum, so dass im Januar 2021 8,1 Millionen unsichere Klicks zu verzeichnen waren, 84,5% mehr als im Januar 2020.

Wie ein Befragter es ausdrückt: "Die Bedrohung ist allgegenwärtig, aber gleichzeitig scheint sie zu kommen und zu gehen." Ein anderer sagt: "In einem Monat haben wir gesehen, dass etwa 300.000 missbräuchliche E-Mails verschickt wurden, die vorgaben, unsere Marke zu sein. Einige gaben vor, Teil unseres Beschaffungsprozesses zu sein, um uns oder eine andere Person in unserer Beschaffungskette zu betrügen. Wir hatten sogar Personen der Öffentlichkeit, die gesagt haben, dass sie einen Job mit unserem Unternehmen erhalten haben, aber es stellt sich heraus, dass es sich bei den gefälschten Jobangeboten um Geldwäscher handelt, die Teil von Kriminalgeldwäschekampagnen sind."

Verdächtige Domain-Registrierungen, 2020

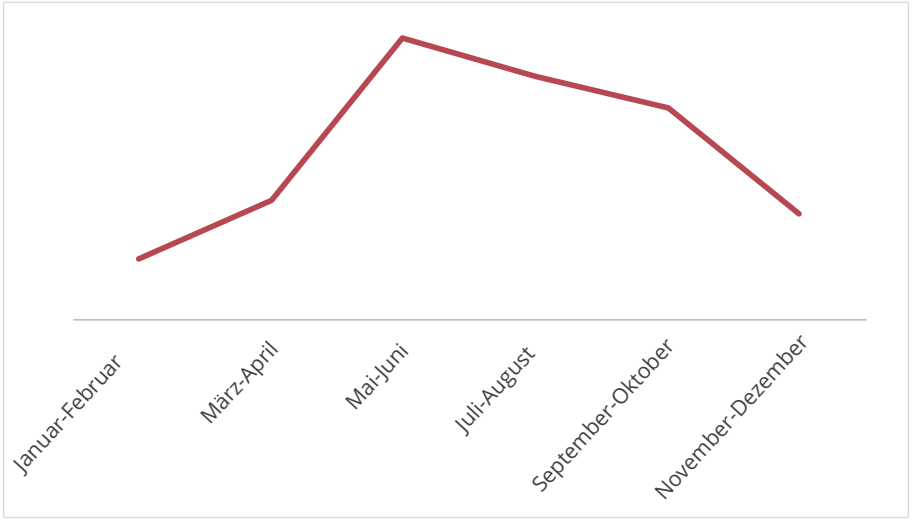


Abbildung 3: Verdächtige Domainregistrierungen, 2020

Monatliche Klicks auf unsichere URLs

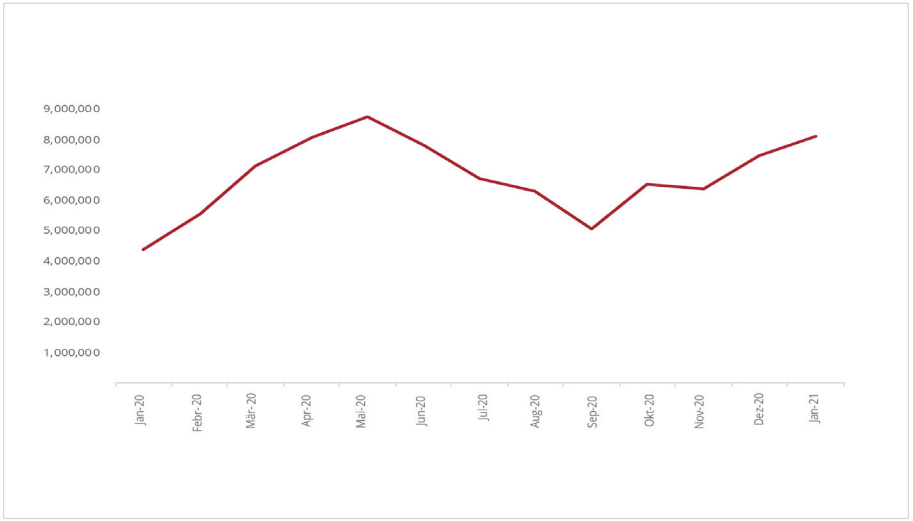


Abbildung 4: Monatliche Klicks auf unsichere URLs, 1/20 - 1/21

Je größer Ihre Marke ist, desto häufiger wird sie kopiert

Auch wenn selbst relativ kleine Unternehmen Opfer von Markenimpersonation sein können – vor allem, wenn sie eine Website mit Kundenanmeldung haben – gilt trotzdem, je größer die Marke ist, desto größer der potenzielle Wert den Cyberkriminelle stehlen können. Aus diesem Grund ist es entscheidend, vor allem Angriffe auf Marken, die auf der Liste BrandZ™ Top 100 der wertvollsten globalen Marken 2020 stehen, zu überwachen.

Die Kantar Group, das Londoner Datenanalyse- und Markenberatungsunternehmen, berechnet seit 2006, welche 100 Marken den größten Dollarwertbeitrag zum Gesamtwert ihrer Muttergesellschaften leisten und veröffentlicht jährlich die Top-100-Rangliste. Für 2020 stellte Kantar fest, dass der Gesamtwert dieser 100 Marken – beginnend mit Amazon und Apple auf Platz eins und zwei und endend mit den Marken Pepsi und Commonwealth Bank auf Platz 99 und 100 – $5 Billionen erreicht hatte. Und diese Zahl steht nur für den Wert der Marken, nicht für die gesamte Marktkapitalisierung der Unternehmen.

Je größer die Marke, desto mehr potenziellen Wert können Cyberkriminelle abschöpfen

Gesamtzahl der Angriffe auf Top-100-Marken

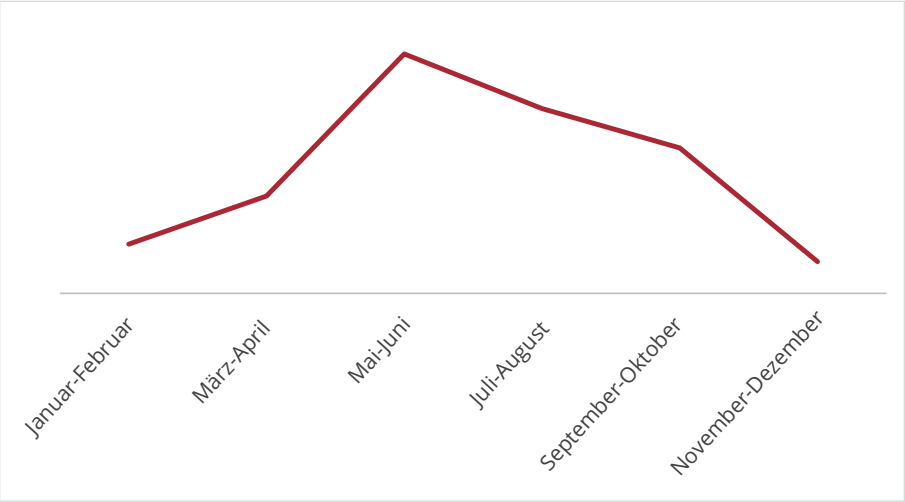


Abbildung 5: Angriffe auf die Top 100 der wertvollsten Marken

Mithilfe des Web-Scanning-Tools von Mimecast Brand Exploit Protect (BEP) konnte verzeichnet werden, wie die Angriffe auf die Top-100-Marken von Kantar [Abbildung 5] in der gleichen, inzwischen bekannten Kurve für das Jahr 2020, stiegen und fielen. Ein Anstieg um 381% Angriffs-Volumen im Januar/Februar bis zum Höchststand von Mai bis Juni, gefolgt von einem allmählichen Abfall. Hier gab es jedoch keinen anschließenden zweiten Anstieg.

Die 20 am häufigsten kopierten Marken der Top-100

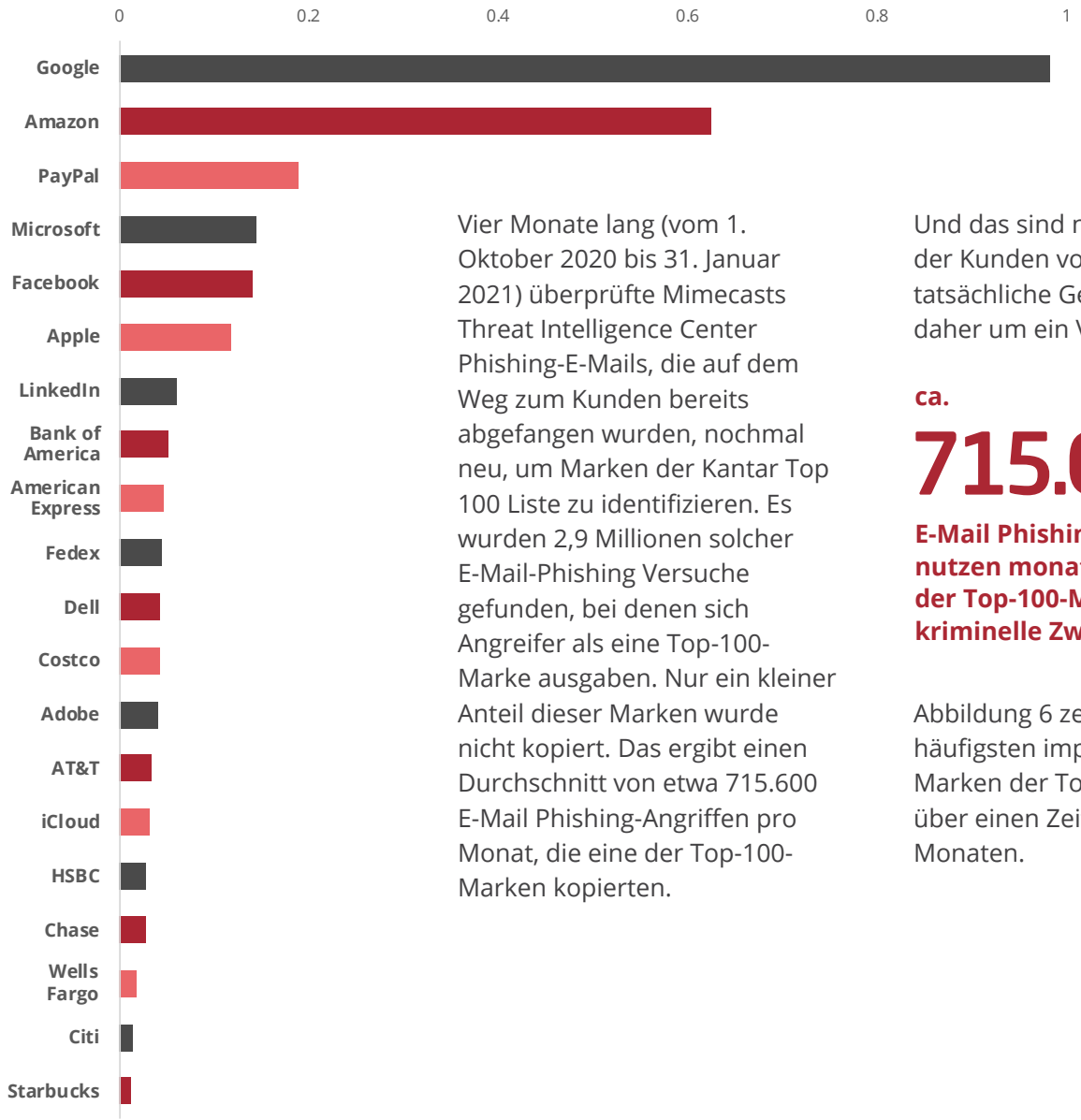


Abbildung 6: 20 der am häufigsten impersonierten der Top-100-Marken im Zeitraum von vier Monaten, 01.10.2020 – 31.01.2021

Vier Monate lang (vom 1. Oktober 2020 bis 31. Januar 2021) überprüfte Mimecasts Threat Intelligence Center Phishing-E-Mails, die auf dem Weg zum Kunden bereits abgefangen wurden, nochmal neu, um Marken der Kantar Top 100 Liste zu identifizieren. Es wurden 2,9 Millionen solcher E-Mail-Phishing Versuche gefunden, bei denen sich Angreifer als eine Top-100-Marke ausgaben. Nur ein kleiner Anteil dieser Marken wurde nicht kopiert. Das ergibt einen Durchschnitt von etwa 715.600 E-Mail Phishing-Angriffen pro Monat, die eine der Top-100-Marken kopierten.

Und das sind nur die E-Mails, der Kunden von Mimecast, die tatsächliche Gesamtzahl liegt daher um ein Vielfaches höher.

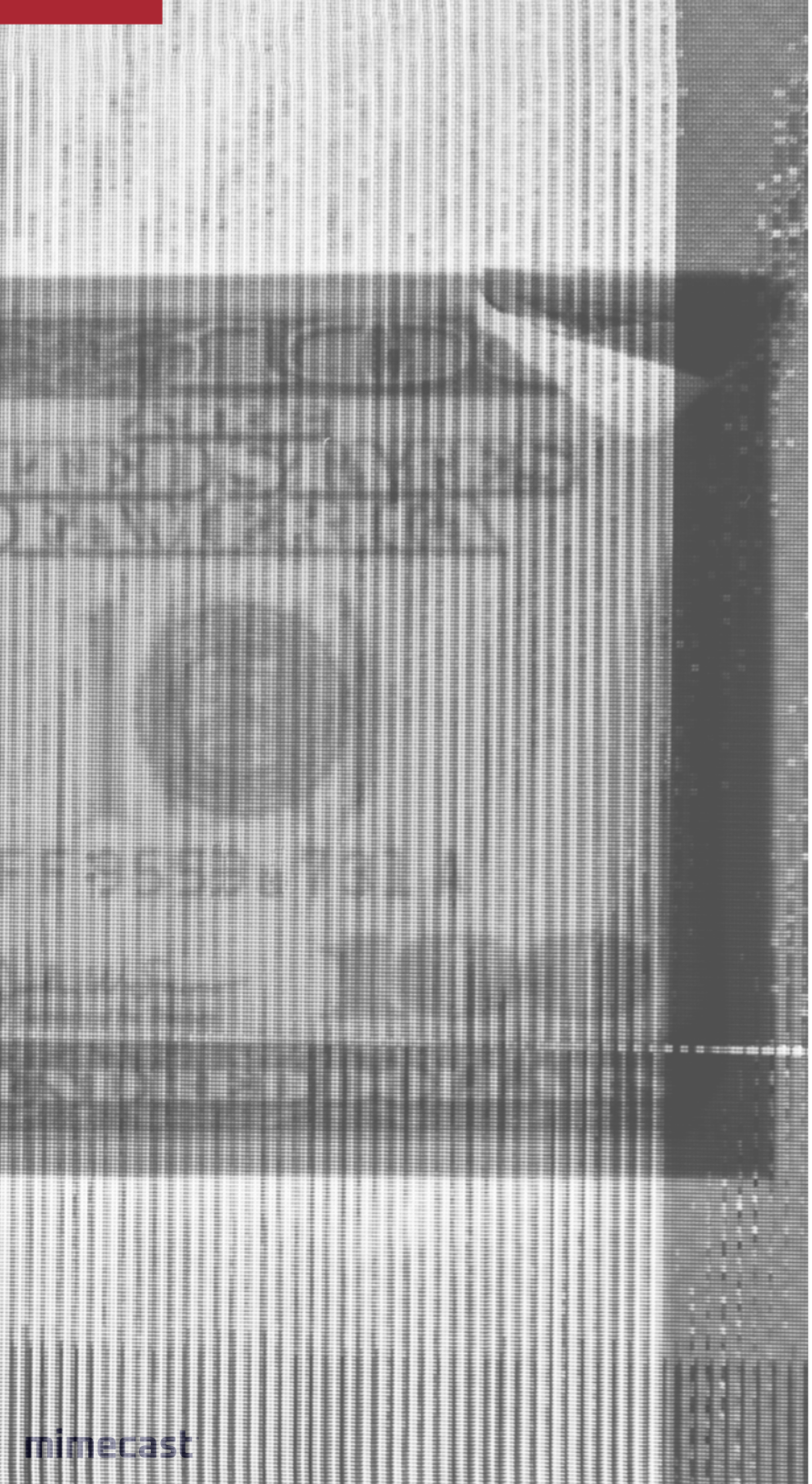
ca.

715.600

E-Mail Phishing-Angriffe nutzen monatlich eine der Top-100-Marken für kriminelle Zwecke aus

Abbildung 6 zeigt die 20 am häufigsten impersonierten Marken der Top-100 Liste über einen Zeitraum von vier Monaten.

Natürlich sind nicht nur die größten und bekanntesten Unternehmen anfällig für Markenimitationen. Kleinere Organisationen können auch mit finanziellen und rufschädigenden Auswirkungen einer Markenausbeutung konfrontiert werden. Schlimmer noch, sie sind oft weniger gut ausgestattet, um Abhilfe zu schaffen, als die größeren, bekannteren Unternehmen.



Verstehen der finanziellen und reputationsbezogenen Auswirkungen

Marken-Impersonation ist kostspielig. Laut dem IC3 2019 Internet Crime Report wurden allein in diesem Jahr über 1,7 Milliarden Dollar durch Impersonation über die Kompromittierung von Geschäfts-E-Mails und andere Phishing-Attacken verloren.[7] Und in der europäischen Studie zum Markenvertrauen gaben 50% der Verbraucher an, dass sie dieGeld für ihrer Lieblingsmarke auszugeben, die sie regelmäßig verwenden oder mit der sie vertraut sind, wenn sie Opfer eines Phishing-Angriffs wurden, der diese Marke betraf. Marken-Impersonation ist ein größerer Komplex und weitreichendes Thema mit vielfältigen Auswirkungen. Jedes Mal, wenn eine Marke für einen Cyberangriff ausgenutzt wird, sind sowohl die Marke als auch ihre Kunden gefährdet, und zwar auf vielfältige Weise.

Monetarisierung von Marken-Imitation. Cyberkriminelle könnten eine Marke ausnutzen, um Kunden-Anmeldedaten abzugreifen, die sie dann auf dem Schwarzmarkt verkaufen oder verwenden, um auf die persönlichen E-Mails, die Arbeits-E-Mails oder Finanzdaten des Opfers zuzugreifen.

Letztlich können Cyberkriminelle dann potenziell Konten übernehmen, Daten stehlen, Malware einsetzen oder Ransomware-Angriffe starten. Das bedeutet, dass nicht nur die Empfänger von Impersonation-Angriffen gefährdet sind, sondern die Organisation für die sie arbeiten ebenfalls. All die möglichen Folgen können von einem einzigen Opfer ausgehen, das durch eine E-Mail getäuscht wird, die sich als eine Marke ausgibt, die es kennt und der es vertraut.

$1.7 Milliarden

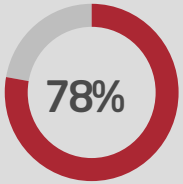
gingen 2019 durch die Kompromittierung von Geschäfts-E-Mails und andere Phishing-Angriffen verloren

Rechtskosten und behördliche Bußgelder. Geht man noch einen Schritt weiter, muss eine imitierte Marke wahrscheinlich mit Bereinigungskosten und Rechtskosten rechnen. Im berüchtigten Fall von British Airways gelang es Cyberkriminellen, etwa 500.000 Kunden auf eine realistische, aber betrügerische Website umzuleiten, die persönliche Daten wie Namen, Adressen, Zahlungsdaten und Anmeldeinformationen sammelte. Obwohl die Fluggesellschaft wohl selbst ein Opfer war, musste sie zunächst eine Geldstrafe in Höhe von 230 Millionen US-Dollar zahlen, weil sie den Betrug nicht schneller erkannt und gestoppt hatte (die Strafe wurde später auf 26 Millionen US-Dollar gesenkt).[8]

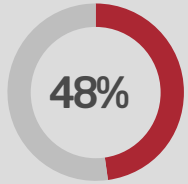
Reputationsschäden. Zu den kostspieligen Folgen von Markenimitationen gehören auch Reputationsschäden und belastete Geschäftsbeziehungen. Der Aufbau von Markenwerten kann schon schwer genug sein, und das Vertrauen der Verbraucher sinkt aufgrund der alarmierenden Zunahme von Datenschutzverletzungen bereits, so die Studie Global State of Online Digital Trust von Frost & Sullivan. Der Bericht ergab, dass der digitale Vertrauensindex der Verbraucher bei 61 von 100 Punkten liegt, was einer schlechten Note entspricht.[9] Darüber hinaus gaben 78% der Verbraucher an, dass es sehr wichtig oder entscheidend ist, dass ihre persönlichen Daten online geschützt werden, und 48% haben die Nutzung eines Online-Dienstes eingestellt, wenn dieser von einem Datenschutzverstoß betroffen war. Wenn Kunden Opfer von Marken-Imitationsangriffen werden, ist es wahrscheinlich, dass sie diese beunruhigende Erfahrung mit der Marke in Verbindung bringen- obwohl die Marke selbst auch ein Opfer war. Das bedeutet, dass sie möglicherweise zögern, auf Links zu klicken, die mit der Marke in Verbindung stehen, und künftige legitime E-Mail-Interaktionen vermeiden, wodurch der ROI des digitalen Marketings der Marke sinkt. Sie könnten sogar einen ansonsten loyalen Kunden auf Lebenszeit verlieren.

Ein Brand Exploit Protect-Kunde teilte uns Folgendes mit: “Selbst wenn wir keinen Geldverlust durch diese Angriffe auf die Markenausnutzung feststellen, ist das Bild, das wir nach außen tragen, eines der wichtigsten Dinge, die wir schützen möchten. Wir übernehmen den Service, weil wir unser Image schützen möchten. Wenn das auch dem Kunden hilft, dann ist es für uns beide gut.”

Eine Untersuchung von Frost & Sullivan fand heraus, dass der digitale Vertrauensindex 61 von 100 für Verbraucher das Äquivalent einer schlechten Note ist.[9]



der Verbraucher gaben an, dass es sehr wichtig oder entscheidend **ist, dass ihre persönlichen Daten online geschützt sind.**



haben **die Nutzung eines Online-Dienstes** eingestellt, wenn dieser von einer Datenschutzverletzung betroffen war.

Sinkender E-Mail-ROI: Erinnern Sie sich an den unglaublichen 42-zu-1-ROI für E-Mail-Marketing? Das ist nicht garantiert, und die von Frost & Sullivan beschriebene Kundenreaktion kann direkt zu einem Rückgang der Marketing-Leads, zu steigenden Kosten pro Lead oder zu beidem führen. Darüber hinaus kann E-Mail-Spoofing zu Problemen bei der Zustellbarkeit von E-Mails führen, da Internet Service Provider versuchen, Marken-Imitatoren zu blockieren, selbst wenn darunter auch legitime Marketingorganisationen sind, die E-Mails im Namen einer Marke versenden. Web-Domain-Spoofing leitet potenzielle Kunden von legitimen Webseiten weg. Ein Beispiel: Cyberkriminelle können gefälschte Websites erstellen, die vorgeben, eine legitime Seite zu sein, die Werbung enthält.

Medienkäufer kaufen dann unwissentlich Anzeigen auf der gefälschten Seite, weil sie denken, dass diese legitim ist, und ermöglichen Hackern damit von den Domains seriöser Verlage zu profitieren. Ein von News UK durchgeführter Test ergab, dass 2,9 Milliarden Anzeigengebote pro Stunde auf gefälschten Websites abgegeben wurden, die sich als die Zeitungsmarken The Sun und The Times of London ausgaben, und schätzte, dass Marketer bis zu 1.000.000$ pro Monat für Domain-Spoofing-Inventar verschwenden könnten.[10]

Es wird geschätzt, dass Marketers bis zu 1.000.000 $ pro Monat für gefälschtes Domain-Inventar verschwenden.[10]

2.9 Milliarden

Anzeigengebote pro Stunde wurden, laut einem von News UK durchegführten Test, auf gefälschten Seiten, die sich als The Sun oder The Times of London ausgaben, abgegeben.

Stand der Verteidigung: Eine Lücke in der Markensicherheit

Trotz der rasant zunehmenden Virulenz von Cyberangriffen auf Markenidentitäten und der wachsenden Liste möglicher Konsequenzen sind sich viele - wenn nicht sogar die meisten - kleinen und mittelständischen Unternehmen nicht bewusst, welche Gefahren ihren Marken drohen. Ironischerweise arbeiten Brand-Marketers eng mit Rechtsteams zusammen, um ihre Marken "im wirklichen Leben" zu schützen, und achten genau auf Markensicherheit im Zusammenhang mit der Platzierung von Werbung im Internet, sind sich aber meist nicht bewusst, wie sehr Marken-Imitations-E-Mails die Markensicherheit bedrohen. Gleichzeitig sind sich einige Verbraucher der allgemeinen Bedrohung nicht bewusst und wissen nicht, welche Prüfungen sie durchführen sollten, um die Legitimität von E-Mails und Websites festzustellen.

Um Marken-Impersonation zu bekämpfen, müssen Brand-Marketers eine Bestandsaufnahme machen, wie Cyberkriminelle die zahlreichen digitalen Touchpoints nutzen, um ihre Kunden anzusprechen.

Wie es einer unserer Interviewpartner treffend formulierte:

"Wenn Sie einen Markenschutz für eine Marke angemeldet oder ein eingetragenes Urheberrecht haben, müssen Sie auch einen Online-Markenschutz als Teil der Strategie in Betracht ziehen."

Dies ist besonders wichtig, wenn man bedenkt, dass 75% der europäischen Verbraucher dieser Marken, erwarten, dass deren Website, E-Mail und Kommunikationsdienste sicher sind, und dass mehr als die Hälfte es als Aufgabe der Marke ansieht, sie vor gefälschten Websites oder E-Mails zu schützen.

Die gute Nachricht ist, dass sich Unternehmen zunehmend mehr Gedanken über den Schutz vor Angriffen durch Marken-Impersonation machen. Laut der Mimecast-Studie SOES 2021 wären 91% der Befragten besorgt, wenn ihr Unternehmen eine betrügerische Web-Domain oder eine bösartige Website hätte, die ihre Domain fälscht, und 93% wären besorgt über einen E-Mail-basierten Angriff, der direkt ihre E-Mail-Domains fälscht.

Obwohl die befragten Unternehmen sich bereits mehr Gedanken zu dem Thema machen, nimmt das Volumen der Angriffe weiter zu - Im gesamten Jahr 2020 sahen 73% der SOES. Befragten ein gleichbleibendes oder steigendes Volumen an E-Mail-Spoofing, das ihre Marken missbrauchte, und 69% sahen ein gleichbleibendes oder steigendes Volumen an Web-Domains, die ihre Marken fälschten.

Aus unseren Kundeninterviews ergab sich ein ganzheitliches, fünfteiliges Rahmenwerk zum Schutz vor Markenimitation, das Marketers und Cybersicherheitsexperten gemeinsam umsetzen sollten. Wir nennen es ganzheitlich, weil zwar auch jeder Teil einzeln nützlich ist, sie aber trotzdem zusammenhängen und gemeinsam angewendet werden sollten, um als OnlineMarkenschutz hoch effektiv zu sein

Die fünf Bestandteile des effektiven Markenschutzes:

01.

Überbrücken der Silos von Marketing und IT-Sicherheit

02.

Verwendung von Proof of Concepts (PoCs), um das Bewusstsein für den Markenschutz auf alle Beteiligten auszuweiten

03.

Markenschutzdienste von Drittanbietern verwenden

04.

DMARC durchführen

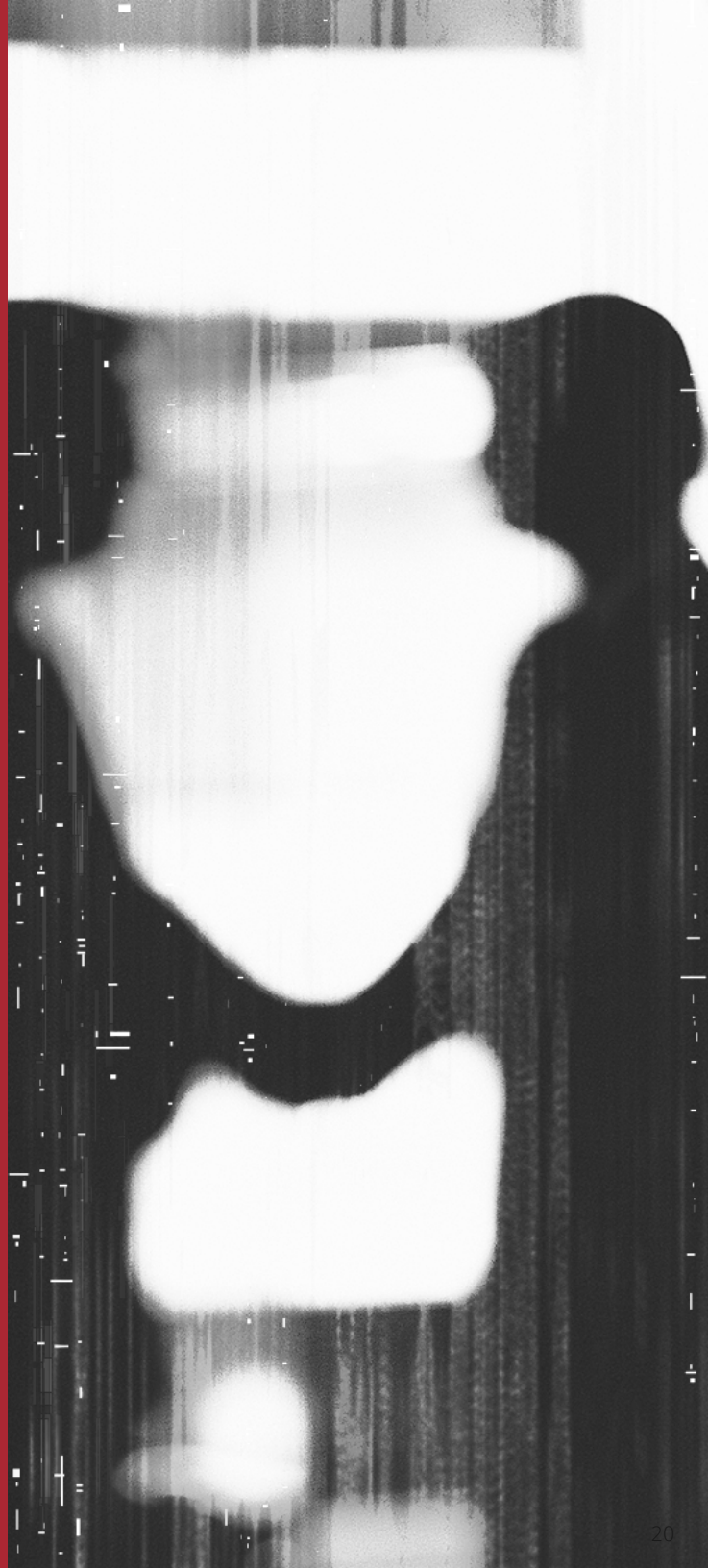
05.

Dem Kunden gegenüber transparent sein

eins.

Überbrücken der Silos von Marketing und IT-Sicherheit

Marketing und Cybersicherheit waren in der Vergangenheit getrennt, oft aufgrund gegensätzlicher Motivationen: Marketingfachleute wollen Kunden anlocken, Cybersicherheitsexperten wollen Unbefugte fernhalten. Aber um sich am besten vor Marken-Imitation schützen zu könnnen, müssen Marketers und Cybersecurity-Teams eine produktive, konstruktive Partnerschaft eingehen. Wie einer unserer Interviewpartner es ausdrückte, “es ist die Aufgabe der Cybersicherheit und des Marketing im gleichen Boot zu rudern.” Er erklärte, dass Sicherheitsteams während des Markenaufbaus mitfahren und betrügerische Websites abschalten sollten, sobald sie auftauchen, damit sie den Leads der Marketers nicht in die Quere kommen. DMARC muss beispielsweise mit den Marketers gemeinsam gestartet werden, denn wenn Marketing-Teams massive E-Mail-Kampagnen oder regelmäßige E-Mails raus senden, müssen diese E-Mails immer als legitim angesehen werden. Und wenn die DMARC-Richtlinien eines Unternehmens nicht ordnungsgemäß festgelegt wurden, können wichtige E-Mails in Spam-Ordnern landen oder abgelehnt werden.

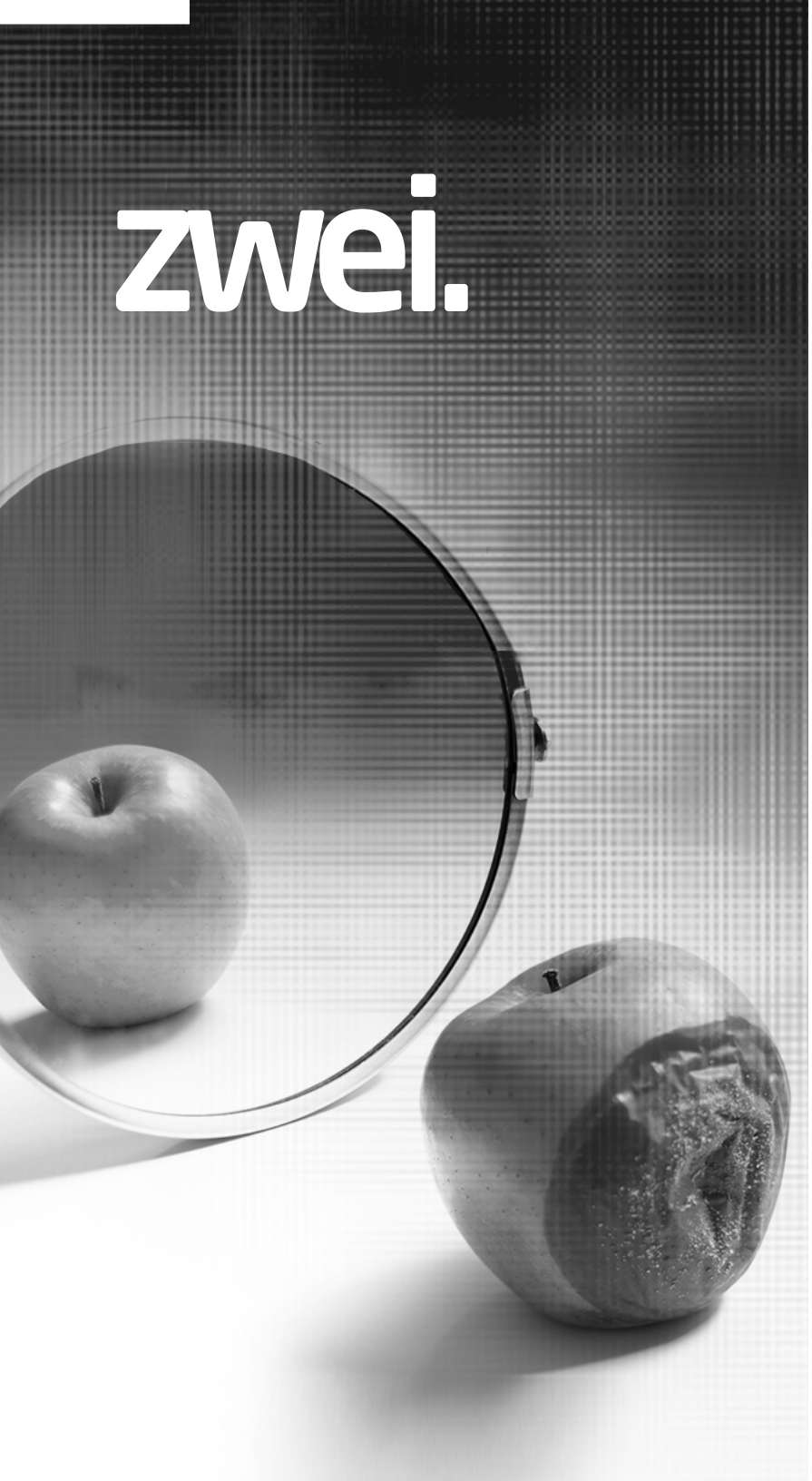


Wenn die Richtlinien eines Unternehmens zur DMARC Nutzung nicht richtig eingestellt sind, könnten wichtige E-Mails in Spam-Ordnern landen oder abgewiesen werden.

Der zuvor in diesem Bericht erwähnte Interviewpartner, der die Überwachung von Marken-Identitäten nutzte, um eine kollaborative Brücke zwischen seinem Team und die Marketing-Abteilung taten dies ausschließlich im Rahmen des IT-Sicherheitsbudgets des Unternehmens, da die Marketing-Mitarbeiter nicht wussten, dass es ein Problem mit der Marken-Identität geben könnte. Zuerst handelte es sich nur um einen Verdacht, aber es stellte sich heraus, dass die tatsächliche Zahl viel höher ist, als wir es jemals erwartet hätten – wir nehmen jeden Monat im Durchschnitt etwa 10 oder 11 betrügerische Websites vom Netz, normalerweise innerhalb von 48 Stunden nach der Benachrichtigung. Seine Marketing-Kollegen wurden zu aktiven Partnern, als sie das Ausmaß der Marken-Imitationsangriffe auf ihre Kunden sahen. Sie halfen dem Sicherheitsteam zu erkennen, welche E-Mails legitim waren und welche von Imitatoren stammten.

Er fügte hinzu: “Ich vermute, wenn ich jetzt sagen würde: ‘Ich beende den Markenschutz Service für Ihr Unternehmen’, dann wäre die Antwort: ‘Bitte nicht, wir brauchen diesen Service.’”

“Ich habe den Fall meinem Chef und dem das Marketing-Team vorgestellt. Ich habe gesagt, dass Sie zwei Millionen Dollar für Ihre Marke ausgeben, aber suchen Sie auch nach den betrügerischen Websites, mobilen Apps und Social-Media-Konten, die Ihre Marke “verunglimpfen”? Ihre Antwort war ‘Nein’. Sie hatten keine Ahnung, dass eine Menge bösartiger Akteure versuchen, sich als Ihre Marke auszugeben””



Nutzen Sie PoCs, um das Bewusstsein für den Markenschutz auf alle Stakeholder auszuweiten

Die gleiche Unsichtbarkeit, die dazu führt, dass sich Marketers der Online-Markenimitation nicht bewusst sind, bis sie proaktiv danach suchen, betrifft auch andere Interessengruppen. Die beste Methode, um sicherzustellen, dass Ihr gesamtes Unternehmen die Notwendigkeit von Investitionen in den Markenschutz versteht, die unsere Interviews ergeben haben, ist, ihnen das Problem durch einen Proof of Concept (PoC) zu zeigen. Anstatt zu versuchen, DMARC in all seiner technischen Komplexität zu erklären, richtete ein Interviewpartner einen PoC eines DMARC-Tools ein, der zeigte, dass Betrüger Hunderttausende von E-Mails unter Missbrauch der Marke versenden. Das, so sagte er, veranschaulichte die Ausbeutung der Marke auf eine Weise, die allgemein verstanden wurde, und die Führung begann, das Thema sehr ernst zu nehmen. Der Befragte, der das Budget des IT-Sicherheitsteams für die Einführung einer Lösung zum Schutz vor Marken-Impersonation verwaltet, sagte, dass nach der Bereitstellung von C-Suite Führungskräfte mit Metriken wie monatlichen Takedowns über einen Zeitraum von sechs Monaten einverstanden waren und sich schnell über den Wert einer Lösung zum Schutz von Markenexploits einig waren.

Wenn Sie einen Schritt weiter gehen, ist es entscheidend, Ihre Mitarbeiter, Lieferanten und Kunden zu schulen. Menschen sind das schwächste Glied, wenn es darum geht, sich und ihr Unternehmen zu schützen, aber mit den richtigen Fähigkeiten können sie selbst die subtilsten Angriffe zur Ausnutzung von Marken erkennen. So wurden beispielsweise im Durchschnitt nur 6,85% der Klicks auf gefährliche URLs von Mitarbeitern von Mimecast-Kunden im Jahr 2020 (Abbildung 7) getätigt, die eine Cybersecurity-Awareness-Schulung absolviert hatten; 93,15% der Klicks wurden von Personen getätigt, die keine Schulung hatten.

Unsichere URL-Klickvolumen, Jan 2020-Jan 2021

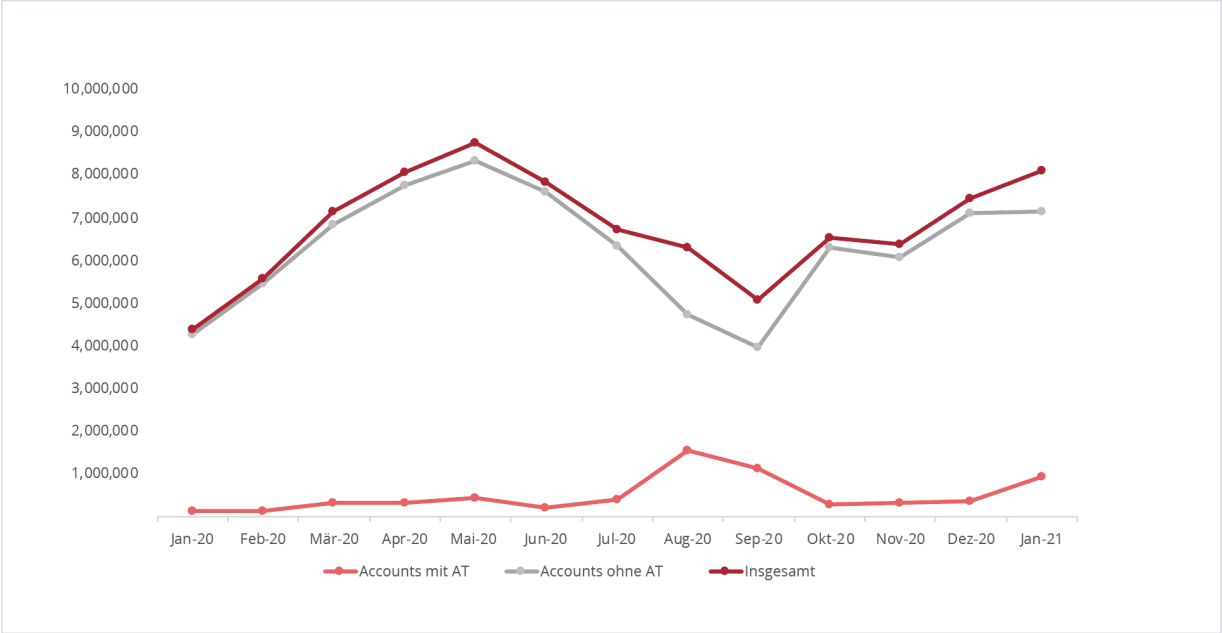


Abbildung 7: Unsichere URL-Klickvolumen, Jan 2020 - Jan 2021

13.6x

Mitarbeiter ohne Awareness-Schulungen klickten im Durchschnitt 13,6-mal häufiger auf bösartige Links!

drei.

Markenschutzdienste von Drittanbietern verwenden

Marken-Impersonation findet größtenteils außerhalb der Sicherheitsgrenzen einer Marke statt, draußen im World Wide Web. Das macht es extrem schwer, sie zu erkennen, zumal Angriffe schwer zu fassen sind; Marken-Phishing-Seiten tauchen schnell auf und verschwinden wieder, um die Entdeckung zu umgehen. Während viele SOES 2021 Befragten angaben, dass sie über Teams zur Erkennung und zum Schutz vor bösartigen Websites verfügen, die ihre Marke fälschen, übernimmt fast ein Drittel (30%) die Verantwortung im eigenen Haus. Laut Frost & Sullivan ist das ein kostspieliger und zeitraubender Fehler. In Abbildung 8 zeigt das Marktforschungsunternehmen, wieviel Zeit ein mittleres bis großes Unternehmen und mehr als 1,14 Millionen Dollar pro Jahr sparen könnte, wenn es den BEP-Service von Mimecast nutzt, anstatt dasselbe im eigenen Haus zu versuchen, einschließlich der Rechtskosten. In diesem Fall ist der Selbstversuch teurer, zeitaufwändiger und weniger effektiv als der Schutz der Marken durch Dritte, da der Markenschutz das Kerngeschäft der Drittanbieter ist. Diese Drittanbieter verfügen über Fachwissen und enge Beziehungen zu Internet Service Providern (ISPs), wodurch sie in der Lage sind bösartige geklonte Websites in Sekundenschnelle zu entfernen, ohne dass es zu rechtlichen Auseinandersetzungen und Gebühren kommt.

	Handbuch Online Marrkenschutz	**Automatisiert Online Markenschutz**
Attribut	In-House Sicherheitsanalysten und rechtliche Ressourcen	Mimecast Brand Exploit Protect
Zeit bis zur Erkennung (MTTD)	Mehrere Wochen oder Monate	Zwischen Sekunden und 3 Stunden
Anzahl der beteiligten Analysten auf der Kundenseite	336 Stunden oder mehr (2+ Wochen)	Zwischen Sekunden und 3 Stunden
Für den Online-Markenschutz aufgewendete Stunden	5 bis 20	1 Analyst / 10 Minuten (Telefonat)
Häufigkeit der Überwachung	160 Stunden pro Monat	1 Stunde pro Monat
Ausgewertete Websites / Jahr	Sporadisch / wenn es die Zeit erlaubt	24/7/365
Kosten pro Angriff	Tausende / Jahr	Milliarden / Jahr
Kosten für die Überwachung & Protect 1 Domain / Jahr	Bis zu 13.920 USD	UBis zu 1.000 USD
Jährliche Anwaltskosten / Jahr	Bis zu 1.002.240 USD	Zwischen 12.000 - 60.000 USD
Annual Legal Fees / year	Bis zu 144.000 USD	0 USD

Quelle: Frost & Sullivan

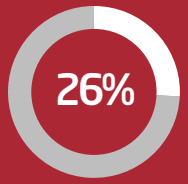
Abbildung 8: Der jährliche Budgetvorteil von Mimecast Brand Exploit Protect[11]

Mehrere Befragte sagten uns, dass sie in der Lage sind, bösartige Webseiten innerhalb von Stunden mit Hilfe von BEP zu entfernen. Das automatisierte 24/7/365-Modell des Dienstes trägt dazu bei, die Zeit bis zur Entdeckung (MTTD) von mehreren Wochen auf nur wenige Sekunden zu reduzieren und die Zeit bis zur Reaktion (MTTR) ebenso schnell ist. Mehr als ein Befragter äußerte sich dahingehend, dass die Kriminellen eher aufhören oder weiterziehen, je schneller die Websites entfernt werden - wenn die Bemühungen eines Kriminellen vergeblich sind, gibt es keinen Anreiz, sich erneut als dieselbe Marke auszugeben, sodass sie zu einem leichteren Ziel weiterziehen.

vier.

DMARC einführen

Weniger als ein Drittel der SOES 2021 Befragten (26%) nutzen das E-Mail-Authentifizierungsprotokoll DMARC, um bösartige Akteure daran zu hindern, schädliche E-Mails zuzustellen, die scheinbar von der Domain ihrer Marke stammen. Zwar ist es vielversprechend, dass 59% entweder planen, eine Strategie einzuführen oder dabei sind, eine solche einzuführen, doch es ist wichtig, nicht zu vergessen, dass DMARC nicht etwas ist, das einfach eingeschaltet werden kann - es erfordert Überwachung, trategische Analyse und Planung. Wenn eine Marke es nicht nutzt, um legitime E-Mails richtig zu authentifizieren, könnten diese legitimen E-Mails von Mailbox-Anbietern als Spam angesehen werden, was die Zustellbarkeit beeinträchtigt - und den E-Mail-Marketing-ROI.



Weniger als ein Drittel der Befragten von SOES 2021 nutzen das E-Mail-Authentifizierungsprotokoll DMARC, um böswillige Akteure daran zu hindern, schädliche E-Mails zu versenden, die scheinbar von der Domain ihrer Marke stammen.

Der Einsatz von DMARC erfolgt in drei Phasen:

1. Überwachung:
In der ersten Phase der Durchsetzung von DMARC werden alle E-Mails buntersucht, die von den Domains Ihrer Marke kommen oder zu kommen scheinen. Einige können von legitimen Dritten stammen, die vom Marketing oder anderen Gruppen innerhalb des Unternehmens beauftragt wurden; andere können illegitim sein. Eine Organisation, mit der wir sprachen, fand dabei 300.000 missbräuchliche E-Mails, die im Namen der Marke verschickt wurden, die sie gar nicht kannten.

2. Analyse:
The next step is to sDer nächste Schritt ist das Aufspüren illegitimer Absender, und es erfordert eine Zusammenarbeit von Sicherheitsteam und Marketing und möglicherweise anderer Abteilungen. Je nachdem, wie viele Dienstanbieter E-Mails im Namen der Organisation versenden, kann dies ein langwieriger Prozess sein - insbesondere dann, wenn Marketing-Teams üblicherweise mit Dutzenden von Drittanbietern von E-Mails zusammenarbeiten, um näher an Kunden und Interessenten heranzukommen. Mit eine Sperr- und Erlaubnisliste können Sie Ihre DMARC-Richtlinie so einstellen, dass verdächtige E-Mails unter “Quarantäne” zgestellt werden, indem sie in das Postfach des Empfängers gesendet werden und dort im Spam-Ordner landen.

3. *Ablehnung!:*
Das ultimative Ziel von DMARC ist es, eine “Zurückweisungs”-Richtlinie zu erreichen, bei der jedes Mal, wenn ein unautorisierter Absender die Domain einer Marke verwendet, diese E-Mail vom empfangenden E-Mail-Server zurückgewiesen wird - sie erreicht also niemals den vorgesehenen Empfänger.

Lösungen von Drittanbietern stehen zur Verfügung, um den DMARC-Prozess zu optimieren, und sind laut Gartner Inc. “oft der effektivste Weg, um an den Punkt zu gelangen, an dem E-Mails zurückgewiesen werden können, wenn sie DMARC nicht bestehen”.[12] Wie uns ein Interviewpartner sagte: “Ich bin begeistert von DMARC. Ich denke, es wird ein weiteres Schlupfloch schließen, das von Cyberkriminellen ausgenutzt wird, und so das Internet zu einem sichereren Ort für unsere Kunden und Mitarbeiter machen.”

Seien Sie transparent im Umgang mit Ihren Kunden

Obwohl Markenschutzlösungen und DMARC-E-Mail-Authentifizierung die Versuche von Angreifern, sich als Ihre Marke auszugeben, stark reduzieren können, wird die Bedrohung in absehbarer Zeit nicht verschwinden.

Eine robuste Strategie zum Schutz Ihrer Marke muss also auch die Aufklärung der Kunden beinhalten. Einem Interviewpartner zufolge ist dies der Schlüssel: “Wir sind stolz darauf, sehr eng mit unseren Kunden zusammenzuarbeiten. Wir kommunizieren viel mit ihnen und warnen sie, sobald wir von den Tricks eines Hackers erfahren. Uns ist wichtig, dass wir ein vertrauenswürdiger Name und ein vertrauenswürdiger Partner sind.” Wenn Sie in Bezug auf Markenimitationen transparent sind und gleichzeitig Richtlinien bereitstellen, die Ihre Kunden in die Lage versetzen, sich sicher zu verhalten - wie z. B. grundlegende Awareness-Schulungen und Cyber-Hygiene-Praktiken, können Sie Ihre Kunden beruhigen und zeigen, dass eine Marke aktiv in ihrem besten Interesse arbeitet und somit Markenwert schafft. Betrachten Sie den Ansatz von dem U.S. Internal Revenue Service (IRS): Angesichts vieler gängiger IRS-Scams erinnert die Behörde die Bürger regelmäßig daran, dass die IRS niemals Telefonanrufe tätigt, in denen bestimmte persönliche Informationen verlangt werden.

Was lässt sich daraus schließen?

Zweifellos verlieren Marketers Leads, Markenaffinität und Kundentreue an Cyberkriminelle, die sich als ihre Marken ausgeben, um ihre Kunden und Interessenten zu betrügen. Und unsere Analyse der 100 wertvollsten Marken der Welt zeigt: Je größer und angesehener eine Marke ist, desto eher ist sie der Gefahr der Markenimitation ausgesetzt. Aktuell sind sich viele Marketers, vor allem bei kleineren Marken, dieser Risiken nicht bewusst, da Markenimitation für sie praktisch unsichtbar ist - es sei denn, sie überwachen sie proaktiv.

Selbst wenn sie einmal identifiziert sind, kann es zeitaufwändig und kostspielig sein, Marken-Imitationen aus dem Internet zu entfernen, was oft rechtliche Schritte erfordert.

Relativ neue Technologien zum Markenschutz und zur E-Mail-Authentifizierung können Marketers jedoch dabei helfen, wieder Herr über ihre eigenen Markendomains zu werden. Dies erfordert eine siloübergreifende Zusammenarbeit zwischen den Marketing- und Sicherheitsteams des Unternehmens und kann durch den Einsatz von fachkundigen Markenschutzdiensten von Drittanbietern erheblich beschleunigt werden.

mimecast®

Relentless protection. Resilient world.™

1. *2020 Global Marketing Trends*, Deloitte | 2. *The Global State of Online Digital Trust*, Frost & Sullivan
3. *CMO's Guide to Email Marketing ROI*, Litmus | 4. *Phishing Activity Trends Report*, 4th Quarter 2020, Anti-Phishing Working Group
5. Ibid. | 6. Ibid. | 7. *2019 Internet Crime Report*, FBI Internet Crime Complaint Center | 8. "*The biggest GDPR penalties for noncompliance*," Spirion
9. *The Global State of Online Digital Trust*, Frost & Sullivan | 10. "*News UK finds high levels of domain spoofing to the tune of $1 million a month in lost revenue*," Digiday
11. *Managing Digital Risk: The Security Challenge Beyond Your Perimeter*, Frost & Sullivan | 12. *Protecting Against Business Email Compromise Phishing*, Gartner Inc.

Mimecast ist ein Anbieter für Cybersicherheit, der Tausenden von Unternehmen weltweit hilft, E-Mails sicherer zu machen, das Vertrauen wiederherzustellen und ihre Cyber Resilience zu stärken. Die erweiterte Cloud-Suite von Mimecast ermöglicht es Unternehmen, eine umfassende Cyber-Resilience-Strategie zu implementieren. Von E-Mail- und Web-Sicherheit über Archiv- und Datenschutz bis hin zu Awareness-Schulungen, Mimecast hilft Unternehmen, Cyberangriffen, menschlichem Versagen und technischem Versagen zu trotzen.