# E-Mail: Vorsicht beim Anklicken

## Maßnahmen zum Schutz vor Phishing, Betrug und sonstigen Fallen

cisco

# Inhalt

# Einleitung

**Letztes Jahr ist Spam 40 geworden. Das ist kein Scherz – 1978 wurde von Gary Thuerk, Marketing Manager bei Digital Equipment Corporation, die erste Spam-Nachricht an 393 Personen im ursprünglichen ARPANET gesendet, um ein neues Produkt zu vermarkten. Es wird nicht überraschen, dass diese Nachricht in etwa genauso gut ankam wie viele der heutigen Spam-Mails. Thuerk wurde abgemahnt und aufgefordert, dies künftig zu unterlassen.**

Wäre es nur heute so einfach. 40 Jahre später ist das Spam-Aufkommen geradezu explodiert und überschwemmt unsere Posteingänge mit unerwünschten Angeboten zu Arzneimitteln, Diätprodukten und offenen Stellen. Nicht nur das, inzwischen sind auch noch seine weitaus gefährlicheren Verwandten im Spiel: Phishing und Malware. Phishing wurde erstmals vor mehr als 30 Jahren entwickelt, und Malware blickt ebenfalls auf eine jahrzehntelange Geschichte der E-Mail-Verbreitung.

Heutzutage ist es leider so, dass viele E-Mails unerwünschter Spam und schlimmere Betrugsmaschen sind. Das Volumen ist erschütternd – laut Talos Intelligence waren 85 Prozent aller E-Mails im April 2019 Spam-Mails. Auch der Umfang der unerwünschten E-Mails steigt. Spam hat im April einen 15-monatigen Höhepunkt erreicht.

## Absender vs. Empfänger

Man könnte argumentieren, dass sich die Struktur von E-Mails nahezu perfekt für Betrüger eignet. Die E-Mail-Adresse zwingt den Benutzer, die empfangenen Informationen zu lesen und zu bewerten und dann zu entscheiden, ob die Mail geöffnet oder angeklickt wird. Das perfekte Maß an Social Engineering, das die Gutmütigkeit des Einzelnen anspricht, kann den Benutzer zum Handeln verführen.

Dieses Social Engineering ist nicht nur ein hervorragendes Lockmittel, sondern macht auch die systematische Abwehr so schwierig. Selten, wenn überhaupt, wird ein per E-Mail-übertragener Angriff den Benutzer umgehen. Zwar sind Mittel wie URLs, die zu angegriffenen oder schädlichen Websites mit Exploit-Kits führen, äußerst beliebt, allerdings sind die Betrüger immer noch darauf angewiesen, dass der Benutzer zuerst auf einen Link in einer E-Mail klickt.

## Bedeutung für das Unternehmen

Es verwundert nicht, dass E-Mails zu den dringlichsten Problemen gehören, die CISOs nachts den Schlaf rauben. In unserer letzten CISO-Benchmark-Studie waren 56 Prozent der befragten CISOs der Ansicht, dass sie gegen das Benutzerverhalten, z. B. das Klicken auf einen schädlichen Link in einer E-Mail, nahezu machtlos sind. Damit wiegt dieses Problem schwerer als alle anderen in der Umfrage genannten Sicherheitsbedenken – sogar schwerer als Daten in der Public Cloud oder die Nutzung von Mobilgeräten.

Es ist auch die Häufigkeit solcher Angriffsversuche, die die CISOs beschäftigte. 42 Prozent der befragten CISOs mussten beispielsweise bereits einen Sicherheitsvorfall bewältigen, der daraus resultierte, dass eine schädliche Spam-E-Mail in ihrem Unternehmen geöffnet wurde. 36 Prozent beschäftigten sich mit einem ähnlichen Vorfall als Ergebnis von Daten, die bei einem Phishing-Angriff gestohlen wurden. Laut unseren CISO-Benchmark-Daten betrachten CISOs E-Mail-Bedrohungen als das größte Sicherheitsrisiko in ihren Unternehmen.

In einer separaten Studie, die von Cisco in Auftrag gegeben und von ESG im Jahr 2018 durchgeführt wurde, gaben 70 Prozent der Befragten an, dass der Schutz vor E-Mail-Bedrohungen immer schwieriger wird. Im Hinblick auf die Folgen von E-Mail-basierten Angriffen gaben 75 Prozent der Befragten an, dass sie erhebliche betriebliche Auswirkungen hatten, und 47 Prozent berichteten über beträchtliche finanzielle Auswirkungen.

## Reaktion erforderlich

Wie schützen Sie etwas, das gleichzeitig eine Notwendigkeit und ein Risiko ist? Für viele Unternehmen wurde der Umstieg auf die Cloud als Lösung angesehen. Allerdings ist auch die Cloud keine Wunderwaffe gegen die Gefahren von E-Mails. Meist wird das Problem einfach verlagert. Die Sicherheitsprobleme lösen sich nicht in Luft auf, sondern bleiben bestehen.

Es gibt mehrere Möglichkeiten, um die Gesamtauswirkungen von E-Mail-Bedrohungen einzudämmen. In diesem Artikel besprechen wir die aktuelle Bedrohungslandschaft und bieten einen Überblick über die derzeit gängigsten E-Mail-Angriffstypen. Wir werden aufschlüsseln, wie sie sich entwickeln, sowie ihre Ziele und die Infrastruktur dahinter beleuchten. Wir besprechen, was Sie tun können, um Ihr Unternehmen zu schützen, und wie sich E-Mail-Bedrohungen erkennen lassen, wenn Ihre Benutzer darauf stoßen.

**„An einem durchschnittlichen Tag erhalten wir rund 412.000 E-Mail-Nachrichten, von denen 266.000 Nachrichten nicht einmal bis zu unseren SMTP-Engines gelangen, da Talos sie basierend auf seiner globalen Threat-Intelligence blockiert.“**

**Milind Samant, leitender Sicherheitsbeauftragter, SUNY Old Westbury**

„Unternehmen müssen die **Sicherheit gegen das Geschäftsrisiko und die Benutzerfreundlichkeit abwägen.** Sobald Sie ein ausgewogenes Verhältnis haben, benötigen Sie ein Programm, das Ihr System mit einer aktiven Reaktion verteidigt, wenn etwas schief läuft. Menschliches Versagen ist nicht zu vermeiden, und es gibt heute eine mehrere Milliarden US-Dollar schwere Cyberkriminalitätsbranche, die darauf setzt. Sie müssen diesen Fehler einkalkulieren und in der Lage sein, im Ernstfall schnell zu reagieren. **Tagtäglich finden wir aufgrund menschlicher Fehler erfolgreiche Versuche, unsere Sicherheitsstrategie zu besiegen**, oder engagierte Übeltäter, die unsere Vermögenswerte oder Software-Sicherheitslücken im Visier haben; und tagtäglich stellen wir fest, ob unsere aktiven Erkennungs- und Reaktionsmechanismen diese Angriffe aufspüren und in Schach halten. So weiß ich, dass wir ein voll funktionsfähiges Sicherheitsprogramm haben.“

Steve Martino, Chief Information Security Officer (CISO), Cisco

# Die aktuelle E-Mail- und Phishing-Landschaft

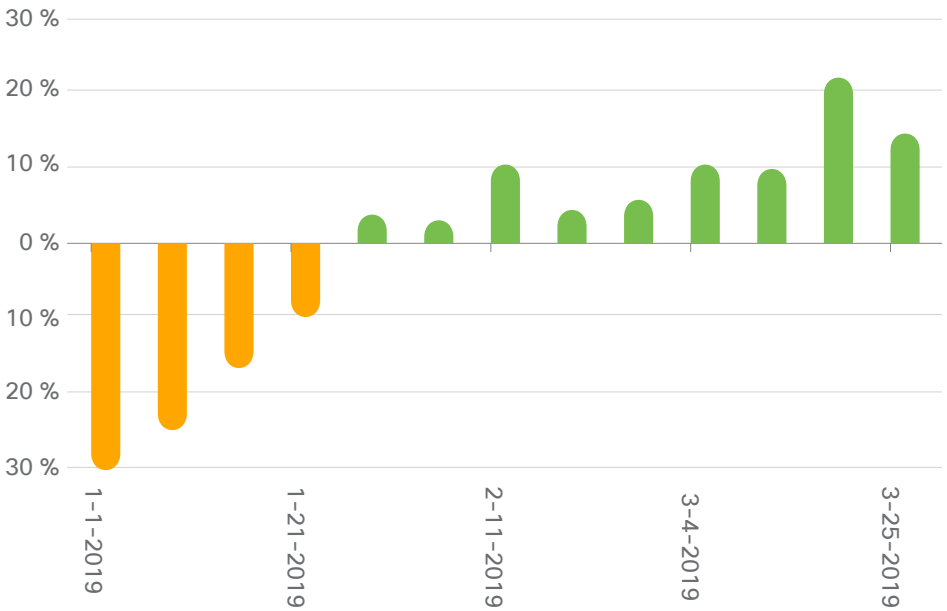
Von E-Mails gehen unzählige Gefahren aus. Laut dem 2018 Data Breach Investigations Report von Verizon, an dem auch Cisco beteiligt ist, ist E-Mail der wichtigste Vektor für die Verbreitung von Malware (92,4 Prozent) und Phishing (96 Prozent). Reagieren Sie einmal auf die falsche E-Mail, und schon können Sie Opfer von Cryptomining oder gestohlenen Anmeldeinformationen werden. Sollten Sie auf einen entsprechenden Social-Engineering-Betrug hereinfallen, können Sie hohe Geldbeträge verlieren. Geschehen derartige Angriffe auf Unternehmensebene, kann die falsche E-Mail verheerende Folgen haben.

Wie regelmäßig fallen Benutzer auf E-Mail-Betrügereien herein? Fragen Sie einfach die Leute bei Duo Security. Das Team hat vor ein paar Jahren das kostenlose Duo Insight-Tool erstellt, mit dem Benutzer ihre eigenen gefälschten Phishing-Kampagnen erstellen und in ihren eigenen Unternehmen testen können, um zu sehen, wer darauf hereinfällt und wer nicht.

Leider fallen viele Menschen den Tricks zum Opfer. Laut dem 2018 Duo Trusted Access Report konnten 62 Prozent der simulierten Phishing-Kampagnen, die durchgeführt wurden, mindestens einen Satz an Anmeldeinformationen abgreifen. Von allen Empfängern hat fast ein Viertel den Phishing-Link in der E-Mail angeklickt. Und die Hälfte davon hat ihre Anmeldeinformationen auf der gefälschten Website eingegeben.

Angesichts dieser Erfolgsquote verwundert es nicht, dass E-Mails eine so beliebte Wahl für den Start von Phishing-Kampagnen sind. Tatsächlich scheint es, dass die Phishing-Aktivitäten zunehmen könnten, wenn wir die Anzahl der neuen Phishing-Domänen betrachten, die von Cisco Umbrella identifiziert wurden. Wir haben einen wöchentlichen Durchschnitt im ersten Quartal 2019 errechnet und anschließend jede Woche mit diesem Durchschnitt verglichen. Die Ergebnisse in Abbildung 1 zeigen, dass die Werte zu Jahresbeginn noch gemäßigt waren, aber die Anzahl der neu eingerichteten Domänen schnell anstieg. Von der ersten Woche des Quartals bis zur letzten wurde eine Zunahme von 64 Prozent verzeichnet.

**Abbildung 1** Wöchentliche neue Phishing-Domänen im Vergleich zum wöchentlichen Durchschnitt im ersten Quartal.




*Quelle: Cisco Umbrella*

# Häufige E-Mail-Angriffstypen

Nachfolgend finden Sie die derzeit gängigsten E-Mail-basierten Betrügereien. Schnappen Sie sich Ihren Laptop, öffnen Sie Ihren Posteingang, und stellen Sie sich vor, dass die folgenden ungelesenen Nachrichten auf Sie warten.

## Office 365-Phishing

*Ähnliche Phishing-Angriffe wurden auch bei anderen Cloud-basierten E-Mail-Diensten wie Gmail und G Suite beobachtet.*

Die E-Mail scheint von Microsoft zu stammen. Darin steht, dass Ihre Office 365-E-Mail-Adresse aufgrund von Fehlern oder Richtlinienverstößen gesperrt wird. Die einzige Möglichkeit, dies zu verhindern, besteht darin, die Adresse unter dem bereitgestellten Link zu verifizieren.

Dies ist ein Phishing-Versuch, um an Ihre Office 365-Anmeldeinformationen zu gelangen. Die verwendeten E-Mails und URLs können sogar wie Informationen aussehen, die Sie im Bereich von Office 365 erwarten würden, beispielsweise micros0ftsupport@hotmail.com. Wenn Sie auf den Link klicken, gelangen Sie zu einer offiziell aussehenden Anmeldeseite, auf der Sie aufgefordert werden, Ihre E-Mail-Adresse und Ihr Kennwort einzugeben.

Allerdings ist die Website gefälscht. Sobald die Betrüger Ihre Anmeldeinformationen haben, können sie versuchen, sich bei anderen mit Microsoft zusammenhängenden Diensten anzumelden und auch an Ihre Kontakte zu gelangen. Eine gängige Technik besteht darin, sich bei Ihrem E-Mail-Konto anzumelden und Ihren Kontakten eine informelle E-Mail (z. B. Betreff: FYI) zu senden, die eine weitere Phishing-URL enthält.

Diese Art von Angriffen ist auf dem Vormarsch. Laut den Daten, die von unseren Partnern bei Agari in ihrem Bericht Q2 2019 Email Fraud and Identity Deception Trends veröffentlicht wurden, erfolgen 27 Prozent der modernen E-Mail-Attacken über angegriffene E-Mail-Konten. Dies bedeutet einen Anstieg um sieben Prozentpunkte gegenüber dem letzten Quartal 2018, als 20 Prozent der Phishing-Angriffe von kompromittierten E-Mails ausgingen.

Und Office 365 ist nicht das einzige Ziel. Ähnliche Phishing-Angriffe wurden auch bei anderen Cloud-basierten E-Mail-Diensten wie Gmail und G Suite, dem Cloud-E-Mail-Angebot von Google, beobachtet. Angesichts der weiten Verbreitung von Google-Konten und der Art und Weise, wie sie über das Internet genutzt werden, um sich bei verschiedenen Websites anzumelden, ist es kein Wunder, dass Angreifer auch in diesem Bereich Phishing-Sites erstellt haben.

**Abbildung 2** Phishing-Site, die absichtlich so aufgebaut ist, dass sie wie die Anmeldeseite von Microsoft aussieht.

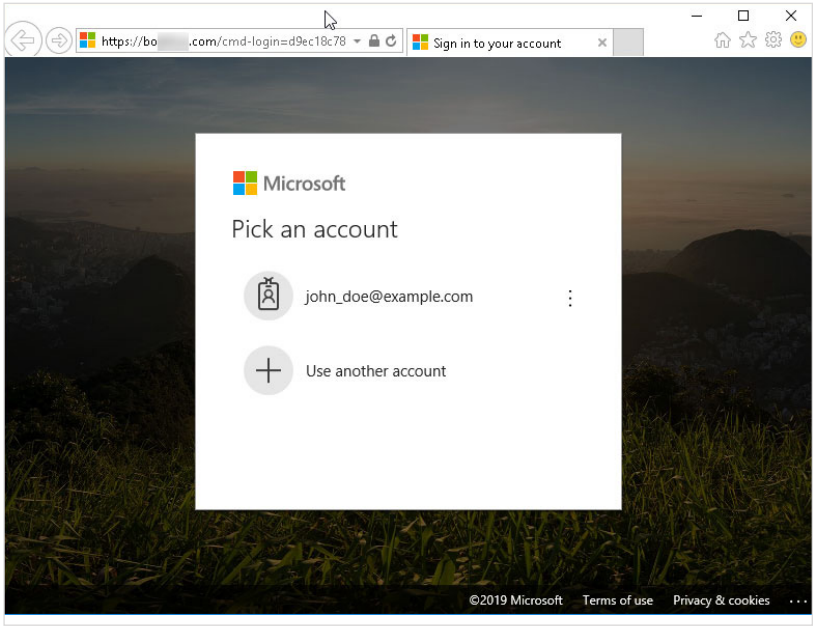
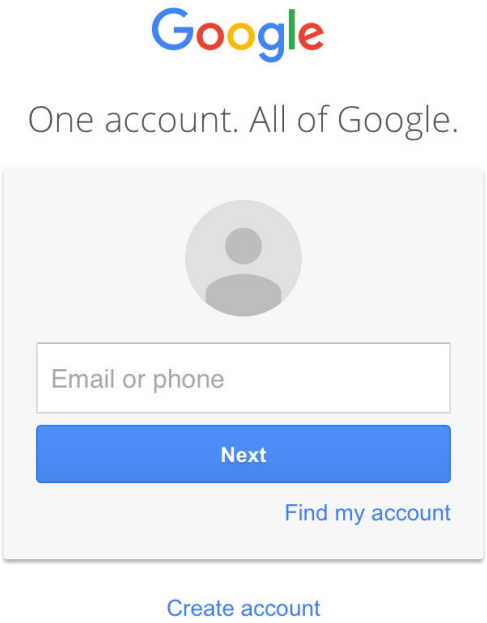


**Abbildung 3** Beispiel für eine Anmeldung beim Google-Konto. Erkennen Sie den Unterschied zwischen dem Original und der Fälschung?



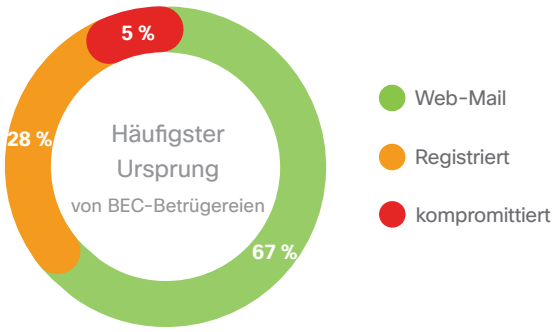

## Business E-Mail Compromise

Es ist die Woche des großen Unternehmensgipfels, und bis auf wenige Menschen, die wichtige Funktionen aufrecht erhalten, ist praktisch jeder dort zu finden. Sie arbeiten in der Finanzabteilung und ein Teil der Stammbesetzung ist noch in der Firma. Plötzlich kommt eine E-Mail mit dem Betreff „Zahlung versäumt“ in Ihrem Posteingang an, die vom Finanzchef zu stammen scheint. In der E-Mail wird erläutert, dass eine Zahlung, die letzte Woche fällig war, versäumt wurde, was zu Störungen in der Lieferkette des Unternehmens führen könnte. Die Überweisungsanleitungen sind beigefügt. Der Absender endet mit den Worten, dass er Sie innerhalb der nächsten Stunde zu diesem Thema anrufen werde.

Dies ist im Wesentlichen ein Angriff vom Typ Business E-Mail Compromise (BEC). BEC-Betrügereien sind eine Form von E-Mail-Betrug, bei dem sich der Angreifer als Mitglied der Geschäftsleitung oder leitender Angestellter ausgibt und versucht, den Empfänger dazu zu bringen, seine geschäftliche Position für einen unrechtmäßigen Zweck zu missbrauchen, beispielsweise für Geldüberweisungen an den Absender. Manchmal geht der Betrüger sogar so weit, dass er das Opfer anruft und im Gespräch den leitenden Mitarbeiter imitiert. Und es scheint zu funktionieren. Laut dem Internet Crime Complaint Center (IC3) verursachten BEC-Betrügereien im Jahr 2018 Verluste in Höhe von 1,3 Mrd. US-Dollar.

Eigentlich würde man vermuten, dass die Angreifer in BEC-Betrügereien gehackte Konten nutzen, genau wie beim Office 365-Phishing-Betrug. Überraschenderweise ist dies laut dem Bericht Agari Q2 2019 Email Fraud and Identity Deception Trends lediglich bei etwa fünf Prozent dieser Betrügereien der Fall. Zwei Drittel dieser Angriffe nutzen nach wie vor kostenlose Webmail-Konten, um die Angriffe zu starten, während die restlichen 28 Prozent mit registrierten Domains maßgeschneiderte Angriffe durchführen. Bei diesen maßgeschneiderten Angriffen erstreckt sich das Ausmaß der Personalisierung bis auf den Hauptteil der E-Mail, wobei laut Agari eine von fünf BEC-E-Mails den Namen des Zielempfängers enthält.

**Abbildung 4** Ausgangspunkt von BEC-E-Mails.




*Quelle: Agari Data, Inc.*

**Abbildung 5** Ein aktuelles Beispiel für eine digitale Erpressung.

**SIE SOLLTEN DAS SEHR ERNST NEHMEN**

MR [redacted]
Montag, den 4.8.2019 08:30
Sie

fragen sich jetzt wahrscheinlich, weshalb Sie diese E-Mail erhalten?

Ich habe eine Malware auf einer nicht jugendfreien Website platziert (...P...0...r...n-Website), und als Sie diese Seite besucht und sich das Video angesehen haben, wurde Ihr Gerät angegriffen und das System wurde mit einer Spyware infiziert. Diese hat Sie sowohl mit einer Webcam aufgenommen als auch den Bildschirm aufgezeichnet, während Sie Ihren Spaß hatten. So konnte ich genau sehen, was Sie gesehen haben.

Über einen Exploit wurde auch Ihr Smartphone infiziert. Denken Sie also nicht auch nur einen Moment lang, dass Sie diesem Angriff entgehen können, indem Sie Ihr Betriebssystem neu installieren. Sie wurden bereits aufgezeichnet.

Danach sammelte meine Malware alle Ihre Messenger-, E-Mail- und Social-Networking-Kontakte.

Ich schätze, das ist keine gute Nachricht für Sie, stimmt's?

Aber machen Sie sich keine allzu großen Sorgen, denn es gibt eine Möglichkeit, wie wir dieses Problem lösen können, um Ihre Privatsphäre zu wahren. Alles, was ich benötige, ist eine Bitcoin-Zahlung von £ 850, was meines Erachtens unter Berücksichtigung der Umstände ein fairer Preis ist.

Die Zahlung erfolgt in Form von Bitcoins.

Meine Bitcoin-Wallet-Adresse lautet wie folgt: 36QEsMKieqmfCBuAdcWg9beAj3ANAp6cAN (da die Groß-/Kleinschreibung beachtet werden muss, kopieren Sie die Adresse am besten und fügen sie ein).

Nach dem Lesen dieser E-Mail haben Sie nur 48 Stunden Zeit, um die Zahlung zu senden (seien Sie gewarnt, ich weiß, wann Sie diese E-Mail geöffnet und gelesen haben, da ich ein Pixel-Bild darin platziert habe. Dadurch erfahre ich auf den Tag und die Uhrzeit genau, wann Sie diese Nachricht geöffnet haben.)

Wenn Sie sich entscheiden, diese E-Mail zu ignorieren, habe ich keine andere Wahl, als das Video an alle gesammelten Kontakte weiterzuleiten, die Sie in Ihrem E-Mail-Konto haben, sowie auf Ihren Social-Media-Konten zu posten und als persönliche Nachricht an alle Facebook-Kontakte zu senden. Außerdem werde ich natürlich das Video im Internet, über YouTube und auf entsprechenden Websites für Erwachsene öffentlich zugänglich machen. Angesichts Ihres Rufs bezweifle ich sehr, dass Sie derzeit auf diese Weise vor Ihrer Familie und Ihren Freunden oder Kollegen bloßgestellt werden möchten.

Wenn ich die Zahlung erhalte, wird das gesamte Material vernichtet und Sie werden nie wieder von mir hören. Wenn ich das Geld aus irgendeinem Grund nicht erhalte, z. B. weil Sie kein Bargeld an eine Wallet auf einer Blacklist senden können, ist Ihr Ruf ruiniert. Verschwenden Sie also keine Zeit.

Versuchen Sie nicht, Kontakt mit mir aufzunehmen, da ich die E-Mail-Adresse eines Opfers verwende, die gehackt und ausgespäht wurde.

Wenn Sie mir nicht glauben und einen Beweis möchten, müssen Sie diese E-Mail einfach nur mit „PROOF“ beantworten, und ich werde Ihr Video an 5 Ihrer Kontakte per E-Mail senden und auf Ihrer Facebook-Pinnwand posten. Dort können Sie es einmal entfernen, aber nicht für immer.

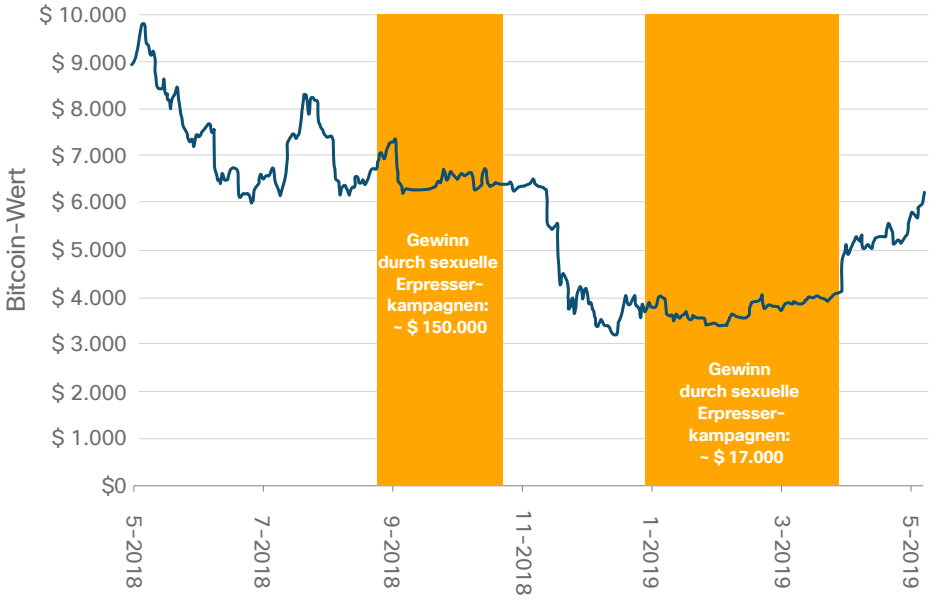
## Digitale Erpressung

Sie finden in Ihrem Posteingang eine E-Mail mit dem Betreff **„SIE SOLLTEN DAS SEHR ERNST NEHMEN.“** Der Absender der E-Mail-Nachricht behauptet, eine Website mit Erotikfilmen gehackt zu haben. Weiterhin behauptet er, Sie hätten diese Website besucht. Er oder sie gibt außerdem vor, Sie über Ihre Webcam aufgenommen zu haben, zusammen mit den Videos, die Sie sich angeblich angesehen haben. Darüber hinaus behauptet der Absender, den Zugriff auf Ihre Kontakte erlangt zu haben und ihnen alle Aufnahmen zu senden, es sei denn, Sie zahlen ihm Hunderte, wenn nicht gar Tausende von Dollar in Bitcoins.

Dies ist digitale Erpressung. Die einzige Sache, die diese Erpressung von herkömmlicheren Erpressungsszenarien trennt, ist, dass die Behauptungen völlig aus der Luft gegriffen sind. Die Betrüger haben keine Website gehackt, sie haben Sie nicht aufgezeichnet, und sie haben auch Ihre Kontaktliste nicht. Sie hoffen einfach , Sie dazu zu bringen, ihren Behauptungen zu glauben.

**In unserem Blogbeitrag über die Bedrohung des Monats beschäftigen wir uns mit den vielen verschiedenen Arten von E-Mail-Betrügereien: Your money or your life: Digital extortion scams.**

**Abbildung 6** Vergleich der Gewinne von sexuellen Erpressungskampagnen als Bitcoin-Wert (USD).




*Quelle: Cisco Talos*

Dies ist ein interessanter und für die Angreifer lukrativer Trick, der Ende 2018 in einer digitalen Erpressungskampagne Gewinne im sechsstelligen Bereich einbrachte. Laut der neuesten Analyse von Cisco Talos, die von Januar bis März 2019 reicht, sind die Gewinne jedoch zurückgegangen. Allerdings folgen der Anstieg und Rückgang dieser Gewinne weitgehend dem Bitcoin-Wert, wenn auch mit größeren Rückgängen. Da der Bitcoin-Wert derzeit anzuziehen scheint, wird es interessant sein zu sehen, ob auch die Zahlungen aufgrund von digitalen Erpressungen ansteigen.

## Spam mit Paket- und Rechnungsinformationen

„Ich erinnere mich nicht, dass ich ein Abonnement für diese mobile App gekauft habe", sagen Sie sich selbst. Das ist zumindest das, was die E-Mail impliziert: ein lebenslanges Abonnement für, sagen wir, einen Filmklub. Oh, Moment, der in der Rechnung genannte Ort besagt, dass es in Sri Lanka erworben wurde. Und Sie leben nicht einmal in Sri Lanka. „Das muss ein Irrtum sein", sagen Sie zu sich selbst, als Sie die angehängte PDF-Datei schnell öffnen, um das Ganze zu überprüfen.

Leider enthielt diese PDF-Datei einen Exploit, der schließlich Emotet auf Ihr Gerät heruntergeladen hat. Der Betrug variiert, konzentriert sich aber in der Regel auf ein Paket, das Sie nicht bestellt haben, eine Rechnung für etwas, das Sie nicht gekauft haben, oder eine monatliche Zahlung für ein Abonnement oder einen Service, bei dem Sie sich nicht registriert haben. Dies kann viele negative Folgen haben, von gestohlenen Bankdaten bis hin zu Cryptomining.

**Abbildung 7** E-Mail eines Emotet-Betrugs, die angeblich von UPS stammt.

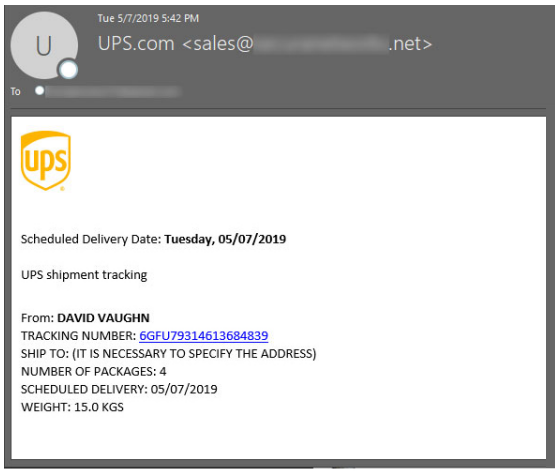


**Abbildung 8** Aktuelles Beispiel für einen Vorkassenbetrug.

**Herr Christoper A. Wray**

CW

Direktor des Federal Bureau of Investigation (FBI)
An: [redacted]
Antwort an: [redacted]

Betreff: Begünstigter.

Es entspricht den Standardgrundsätzen eines Amtes, dass die Vorstellung bei einer ersten Kontaktaufnahme stets sehr wichtig ist. Ich bin Herr Christopher A. Wray, Direktor des Federal Bureau of Investigation (FBI). In diesem offiziellen Memorandum möchten wir Ihnen mitteilen, dass wir folgenden Sachverhalt festgestellt haben: Einige Beamte, die für die Regierung der Vereinigten Staaten arbeiten, haben versucht, Ihre Gelder durch einen Back-Door-Kanal umzuleiten. Wir haben dies heute durch unsere Geheimagenten im Disziplinaramt des Federal Bureau of Investigation (FBI) entdeckt, nachdem wir einen Verdächtigen festgenommen haben.

Der besagte Verdächtige wurde am frühen Morgen am Dulles International Airport verhaftet, als er versuchte, die enormen Bargeldsummen außer Landes zu schaffen. Laut Geldwäsche-Erlass der Vereinigten Staaten kann ein solcher Geldbetrag nicht in bar an ein Land außerhalb der Vereinigten Staaten transferiert werden, weil ein solcher Versuch eine Straftat ist und nach dem Geldwäschegesetz von 1982 der Vereinigten Staaten von Amerika strafbar ist. Bei dieser Verordnung handelt es sich um ein globalisiertes Gesetz, das in den meisten Industrieländern anwendbar ist, um Terrorismus und Geldwäsche zu bekämpfen.

Aus unseren gesammelten Informationen hier in diesem Amt geht hervor, dass die fraglichen finanziellen Mittel tatsächlich Ihnen gehören, aber die Auszahlung wurde absichtlich verzögert, weil die für Ihre Zahlung verantwortlichen Beamten in gewisse Unregelmäßigkeiten verwickelt sind, was völlig gegen die Ethik eines jeden Zahlungsinstituts verstößt. Diese Mittel stehen derzeit unter der Obhut der zahlenden Bank. Ich kann Ihnen versichern, dass ihre Gelder ohne Probleme an Sie fließen werden, vorausgesetzt, dass Sie in dieser Angelegenheit uns gegenüber aufrichtig sind. Darüber hinaus benötigen wir Ihre positive Zusammenarbeit auf allen Ebenen, da wir genau diese Transaktion engmaschig überwachen, um die moderne Gesellschaft vor derartigen Straftaten zu schützen.

Heute am 9. Mai 2019 haben wir die Geschäftsleitung der Zahlbank angewiesen, die genannten Gelder an Sie als den betreffenden zertifizierten Begünstigten herauszugeben, da wir über wichtige Informationen/Akten zur Echtheit verfügen und nachgewiesen ist, dass die genannten Gelder wirklich Ihnen gehören. Dennoch müssen Sie uns die unten aufgeführten Informationen (zur amtlichen Überprüfung) zur Verfügung stellen.

1. Vorname, zweiter Vorname und Nachname.
2. Alter.
3. Beruf.
4. Familienstand.
5. Ihre Telefon-/Faxnummer.
6. Wohnanschrift.

Wir erwarten Ihre sofortige Erfüllung dieser behördlichen Verpflichtung, damit Sie von einer autorisierten Zahlbank bezahlt werden können.

Amtlich besiegelt.

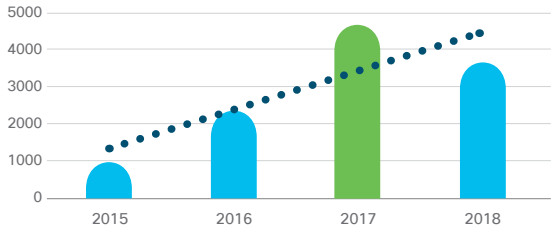
Herr Christopher A. Wray
Direktor des Federal Bureau of Investigation (FBI)

## Vorkassenbetrug

Nicht jeden Tag erhalten Sie eine E-Mail vom FBI. Und noch seltener erhalten Sie eine E-Mail, in der Sie über eine ausstehende Überweisung in Höhe von 10,5 US-Dollar Millionen informiert werden! Alles, was Sie tun müssen, ist die E-Mail zu beantworten, und schon werden Sie angewiesen, was Sie tun müssen, um die Zahlung zu erhalten.

Dies ist ein klassischer Vorkassenbetrug. Wie der Name schon sagt, werden die Betrüger Sie um eine Gebühr bitten, bevor sie Ihnen das versprochene Geld senden – Geld, das niemals ankommt. Hierbei handelt es sich um eine ältere E-Mail-Betrugsmasche, die über die Jahre immer wieder in unterschiedlicher Form aufgetreten ist: Das eine Mal wollte ein ausländischer Prinz seinen Reichtum teilen, ein anderes Mal wurden Kredite an Menschen mit schlechter Kreditwürdigkeit bewilligt usw. Und diese Art des Betrugs reißt nicht ab. Jedes Jahr werden Tausende solcher E-Mail-Betrügereien an das U.S. Better Business Bureau (BBB) gemeldet.

**Abbildung 9** Nach Jahren gestaffelte Betrugsdelikte im Bereich Vorkassenbetrug, die dem BBB gemeldet wurden.
(Summe des Vorkassendarlehens, Betrugstypkategorien nigerianischer/ausländischer Geldwechsel, Partnerschaft, Bonitätsverbesserung/Schuldenerlass, Investitionen und Reisen/Urlaub.)




*Quelle: Better Business Bureau*

# Malware in E-Mail

Ein Großteil der Malware verbreitet sich nach wie vor per E-Mail. Früher war sie leichter zu erkennen, da EXE-Dateien direkt an E-Mails angehängt wurden. Aber seit die Benutzer begriffen haben, dass sie besser keine ausführbare Datei öffnen sollten, haben die Übeltäter ihre Taktik geändert.

Heutzutage wird Malware viel häufiger indirekt verbreitet, entweder durch weniger verdächtige Anhänge wie gängige Geschäftsdokumente oder durch URLs, die im Nachrichtentext enthalten sind – allesamt Elemente, die regelmäßig in jeder üblichen und nicht betrügerischen E-Mail-Kommunikation gesendet werden. Dahinter steckt die Absicht, traditionelle E-Mail-Scans zu umgehen, die eine Binärdatei oder andere selten verteilte Anhänge abfangen und unter Quarantäne stellen würden.

Dies wird am deutlichsten, wenn wir die bisher in diesem Jahr gekennzeichneten E-Mail-Anhänge (Januar bis April 2019) betrachten. Binärdateien machen weniger als zwei Prozent aller schädlichen Anhänge aus – und das bezieht sich nicht nur auf EXE-Dateien, sondern auf alle Binärdateien. Dies ist eine deutliche Veränderung gegenüber den vergangenen Jahren, als ausführbare Dateien sowie Java- und Flash-Dateien regelmäßig zu finden waren. Tatsächlich sind Java und Flash so sehr in Ungnade gefallen, dass die Binärdateien selbst unter Einbeziehung dieser Dateitypen immer noch nur 1,99 Prozent der Anhänge ausmachen.

*Archivdateien, z. B. ZIP-Dateien, bilden fast ein Drittel der schädlichen Anhänge und stellen vier der zehn bei den Angreifern beliebtesten Dateitypen.*

**Tabelle 1** Schädliche Anhangstypen.

| Typ | Prozentsatz |
|---|---|
| Büro | 42,8 % |
| Archiv | 31,2 % |
| Skript | 14,1 % |
| PDF | 9,9 % |
| Binär | 1,77 % |
| Java | 0,22 % |
| Flash | 0,0003 % |

*Quelle: Talos Intelligence*

**Die gebräuchlichsten Anhangstypen sind einfach die Typen, die an einem normalen Tag im Büro gesendet werden – zwei von fünf schädlichen Dateien sind Microsoft Office-Dokumente.**

Welche Art von Anhängen haben bei den Angreifern hingegen an Beliebtheit gewonnen? Archivdateien, z. B. ZIP-Dateien, bilden fast ein Drittel der Anhänge und stellen vier der zehn verbreitetsten Dateitypen. Skripte wie JS-Dateien machen 14,1 Prozent aus. Bei diesen Skripten wurde ein drastischer Anstieg verzeichnet, seit wir die Anhangstypen im Annual Cybersecurity Report (ACR) 2018 unter die Lupe genommen hatten. Damals machten JS-Dateien in Verbindung mit XML und HTML gerade einmal ein Prozent der schädlichen Dateierweiterungen aus.

Ihre Häufigkeit als schädliche Anhänge hat weiter zugenommen und ist seit dem ACR im Jahr 2018 um fast fünf Prozentpunkte gestiegen. Wenn wir dann noch PDF-Dokumente einbeziehen, sind mehr als die Hälfte aller schädlichen Anhänge regelmäßig verwendete Dokumenttypen, die am modernen Arbeitsplatz allgegenwärtig sind.

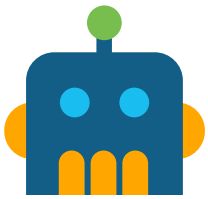
**Tabelle 2** Die zehn wichtigsten schädlichen Erweiterungen in E-Mails.

| Erweiterung | Prozentsatz |
|---|---|
| .doc | 41,8 % |
| .zip | 26,3 % |
| . js | 14,0 % |
| .pdf | 9,9 % |
| .rar | 3,9 % |
| .exe | 1,7 % |
| .docx | 0,8 % |
| .ace | 0,5% |
| .gz | 0,5% |
| .xlsx | 0,2% |

*Quelle: Talos Intelligence*

# Infrastruktur der E-Mail-Zustellung

Treten wir hinter die Kulissen, weg von den E-Mail-Arten oder Payloads, und befassen wir uns mit der Frage, wie schädliche E-Mails verbreitet werden. Es gibt zwei primäre Methoden, die Betrüger verwenden, um Spam-Kampagnen zu starten: Botnets und Toolkits für Massen-E-Mails.



## Botnets

Spam-Botnets gelten mit Abstand als Hauptverursacher für die meisten Spam-Mails, die heutzutage gesendet werden. Im Folgenden finden Sie einige der wichtigsten Akteure in der Spam-Botnet-Landschaft.

### Necurs

Das Necurs-Botnet tauchte erstmals 2012 auf und hat eine Vielzahl von Bedrohungen verbreitet, von Zeus bis Ransomware. Während seine Aktivitäten in der Vergangenheit deutlich mehr Beachtung fanden, scheint Necurs zumindest in Bezug auf die Berichterstattung in der Presse in den Hintergrund gerückt zu sein. Allerdings ist dieses Botnet immer noch sehr aktiv. Tatsächlich ist das Necurs-Botnet das wichtigste Verbreitungsinstrument für eine Vielzahl von Betrügereien, einschließlich digitaler Erpressung.

**Weitere Informationen zu Necurs finden Sie in der Analyse The Many Tentacles of the Necurs Botnet, die von Cisco Talos durchgeführt wurde.**

### Emotet

Ein Großteil der von Emotet gesendeten Spam-Mails fällt in die Kategorie „Paket“ und „Rechnung“. Emotet ist eine modulare Malware, die ein Spambot-Plug-in beinhaltet. Aufgrund der Art und Weise, wie die Akteure hinter Emotet Geld verdienen, indem sie es als Verbreitungskanal für andere Bedrohungen nutzen, ist das Ziel der meisten vom Spambot-Modul versendeten Spam-Mails, weitere Systeme mit Emotet zu infizieren und die Reichweite des schädlichen Verbreitungskanals weiter zu erhöhen.

Da Emotet Inhalte aus den Postfächern von Opfern stiehlt, ist es oft in der Lage, schädliche, aber echt aussehende Thread-Nachrichten zu erstellen, die den Empfängern als Teil der bestehenden Konversationen erscheinen. Außerdem stiehlt Emotet bekanntermaßen SMTP-Anmeldeinformationen und missbraucht damit die eigenen Server für ausgehende E-Mails der Opfer als Instrument für ausgehende Spam-Mails.

**Weitere Informationen zu Emotet finden Sie in unserem früheren Bericht Defending against today’s critical threats** aus unserer Berichtsreihe zur Cybersicherheit.

> **„Cisco E-Mail Security verringerte die Zeit für die Erkennung und reduzierte das Spam-Aufkommen um etwa 80 %.“**
>
> **Jacquelyn Hemmerich, Security Officer, City of Sarasota, FL**

### Gamut

Beim Gamut-Botnet dreht sich alles darum, Spam-Mails rund um Dating und Partnerschaft zu versenden, die in erster Linie Begegnungen mit Menschen aus Ihrer Region versprechen. In anderen Kampagnen verschicken die Akteure hinter dem Botnet Nachrichten, die sich mit Pharmazeutika oder Stellenangeboten befassen (siehe Abbildung 10).

Sie haben eine Vielzahl von Domänen registriert, obwohl die Infrastruktur selbst ziemlich einfach erscheint, mit mehreren Subdomänen unter einer Domäne, wobei häufig auf eine IP-Adresse verwiesen wird. Zwar hat Cisco nicht geprüft, ob die angebotenen Services legitim sind, allerdings scheint der Registrierungsprozess zu versuchen, persönliche Informationen abzugreifen.

**Abbildung 10** Vom Gamut-Botnet gesendete Spam-E-Mails.

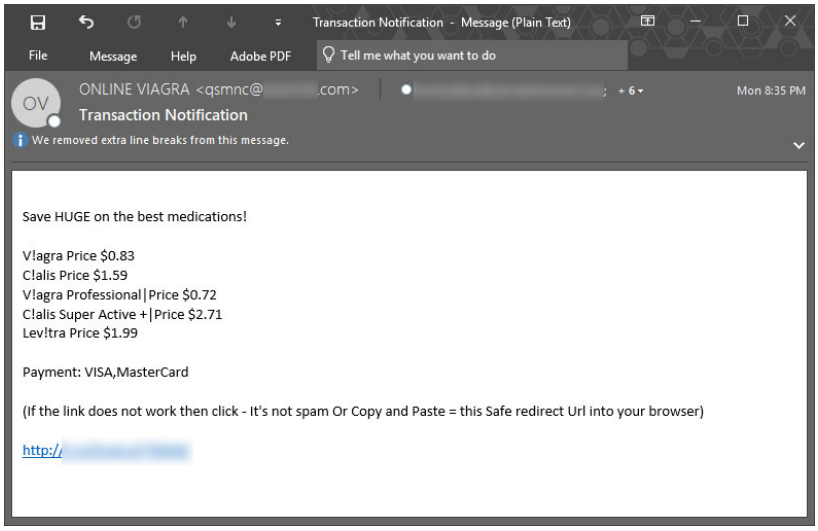
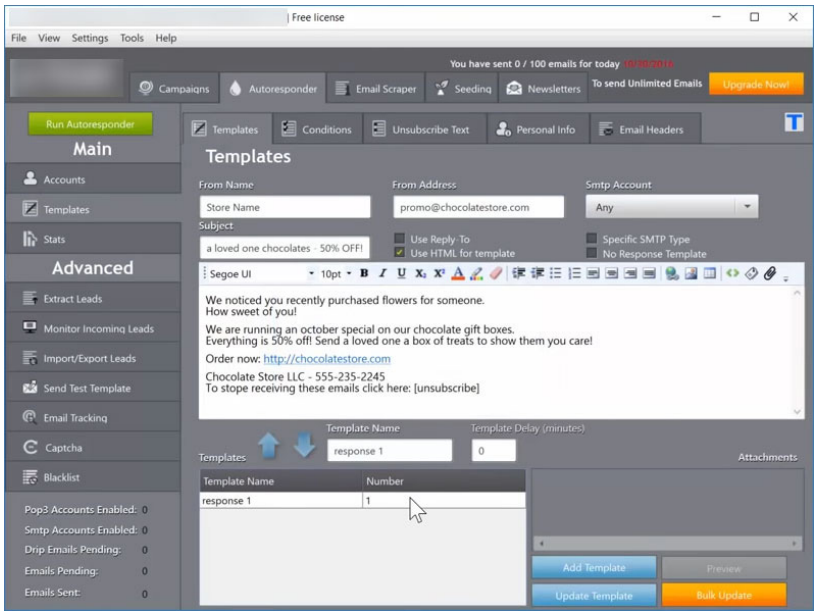



**Abbildung 11** Beispiel für ein Spam-Toolkit.




## Toolkits für Massen-E-Mails

Eine alternative Strategie vieler Spammer ist der Erwerb von Tookits, die eine hohe Anzahl von E-Mails versenden. Viele dieser Tools sind halblegitim, was bedeutet, dass Sie, wenn Sie Ihre eigenen handgefertigten, maßgeschneiderten Duschvorhänge verkaufen würden, eines dieser Toolkits technisch nutzen könnten, um die Markenbekanntheit per Massen-E-Mail an Ihre eigene Opt-in-Mailingliste zu erhöhen. Einige der in solchen Toolkits enthaltenen Funktionen, wie z. B. die Rotation der sendenden IP-Adresse und die benutzerdefinierte Neuerstellung von Anhängen, um eindeutige Hash-Werte zu erzeugen, werden in solchen Szenarien jedoch weitaus seltener verwendet.

Vor Kurzem deckten Ingenieure von Cisco Talos Facebook-Gruppen auf, in denen böswillige Akteure Massen-E-Mail-Tools zusammen mit umfangreichen E-Mail-Adresslisten verkauften, die wahrscheinlich aus Datensicherheitsverletzungen stammen. In diesen Fällen nutzten die Käufer solcher Tools diese eindeutig für üble Zwecke.

# Betrugsbekämpfung als Methode

*Wenn E-Mail der häufigste Vektor ist, ist Betrug die häufigste Methode – insbesondere im Hinblick auf die organisierte Kriminalität.*

Wenn E-Mail der häufigste Vektor ist, ist Betrug die häufigste Methode – insbesondere im Hinblick auf die organisierte Kriminalität. Böswillige Akteure hinter BEC-Scams versuchen, Unternehmen um Tausende von Dollar zu betrügen. Digitale Erpresser betrügen die Nutzer arglistig, damit diese in Bitcoins an sie zahlen. Und beim Vorkassenbetrug sagt der Name schon alles.

Nichts davon ist neu. E-Mail ist nur eines der moderneren Tools, mit denen Kriminelle Betrugsdelikte begehen. Historisch gesehen versuchen Kriminelle stets, die Möglichkeiten jeder Generation von Technologien für die Maximierung von illegalen Einnahmen zu nutzen.

Betrachtet man die Verluste, die vom Bundeskriminalamt (BKA) und dem FBI erfasst wurden, können mehr als 80 Prozent aller erfassten Cyberkriminalitätsverluste auf Betrugsdelikte zurückgeführt werden. Die Betonung liegt dabei auf „erfasst", da es möglicherweise nicht greifbare Verluste gibt, die schwer zu quantifizieren und präzise zu erfassen sind. Dies bedeutet dennoch, dass die erfassten Statistiken ziemlich zuverlässig sind.

Daher ist die Aussage, dass Betrug die treibende Kraft hinter den Verlusten aufgrund von Cyberkriminalität ist, richtig. Tatsächlich stellen wir bei der Untersuchung von zwei Betrugsmaschen, die in der FBI-Statistik genannt werden (Business E-Mail Compromise (BEC) und E-Mail Account Compromise (EAC)), fest, dass die Verluste im Jahr 2018 1,3 Milliarden US-Dollar betrugen. Zum Vergleich: Die für Ransomware, eine oft erwähnte und analysierte Form von Cyberkriminalität, verzeichneten äquivalenten Verluste betrugen 3,6 Millionen US-Dollar. Und die Tatsache bleibt: Alle Anzeichen deuten darauf hin, dass Verluste im Zusammenhang mit unerkanntem Betrug weiter zunehmen werden, da die Verluste im Zusammenhang mit BEC/EAC allein zwischen 2016 und 2017 um 78 Prozent anstiegen.

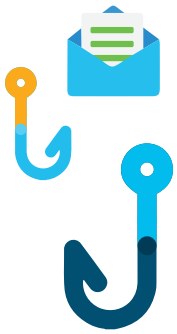
**„Cisco E-Mail Security hat uns beim Management buchstäblich vom Problem der E-Mail-Sicherheit befreit und uns erlaubt, uns auf andere Bereiche zu konzentrieren. Es fängt alles ab! Wir können uns ganz beruhigt zurücklehnen, da wir wissen, dass wir die perfekte Entscheidung für die E-Mail-Sicherheit getroffen haben! "**

**Steven Wujek, Senior IT Architect, Technology Concepts & Design, Inc.**

**Weitere Informationen zu Verlusten aufgrund von Betrug und Cyberkriminalität finden Sie in unserer Blog-Reihe zu Cyberkriminalität und Betrug.**

„Ein ganzheitlicher Sicherheitsansatz ist nicht nur eine Frage des Sicherheitsprodukts, sondern auch ein geschäftliches Muss. Es geht darum, Menschen, Prozesse und die Technologie in allen Bereichen des Unternehmens zu betrachten. Bei Cisco beginnen wir mit einem mitarbeiterorientierten Ansatz, der sich auf den Einzelnen und die Arbeit, die er leistet, konzentriert und ihm hilft, seine Arbeit sicher zu erledigen. Eine unserer Methoden ist es, Mitarbeitern praktische Tipps zu geben, damit sie verdächtige E-Mails erkennen und melden können, bevor sie darauf klicken.“

Steve Martino, Chief Informationssicherheit Officer (CISO), Cisco



# Schutz vor E-Mail-Angriffen

## Verräterische Anzeichen einer Phishing-E-Mail

Der Silberstreif am Horizont, wenn es um Bedrohungen per E-Mail geht, ist, dass es in der Regel Abweichungen gibt, die diese Mails als Bedrohungen verraten, wenn man nur weiß, worauf man achten muss. Nachfolgend finden Sie einige Beispiele. Ausführliche Informationen zu den einzelnen Beispielen finden Sie auf der folgenden Seite.

An: Sie@IhreE-Mail-Adresse.com

1 Von: Amazon-Versand <amz@123fnord.com>

Betreff: Ihr letzte Bestellung

Sehr geehrte/r Herr/Frau ...,

2 Viele Dank für Ihre Bestellung. Die Details lauten wie folgt:

Kauf: monatliches Bereitstellungsabonnement für Puppy Food™

Marke Puppy Food

Monatliche Kosten: 121 USD

Datum und Uhrzeit: 3. Mai 2019 10:21

IP-Adresse: 254.189.234.159.01

Land des Kaufs: Guatemala

3 Wenn Sie das Abonnement nicht mehr wünschen, stornieren Sie es bitte sofort, indem Sie die Anweisungen im Anhang befolgen, oder geben Sie

4 Ihre Kreditkartendaten hier ein:

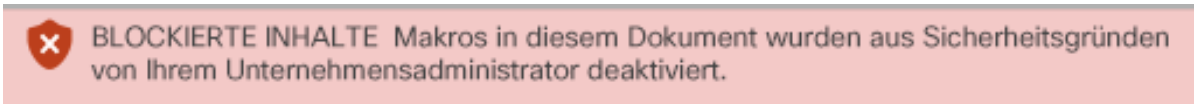
5 http://illegalePhishing-Site.com/nichtaufrufen.html

Freundliche Grüße

Amazon-Versand

6 nichtöffnen.illegal

**Abbildung 12** Microsoft Office-Warnung zu Makros im geöffneten Dokument.




1. **Die Absenderadresse.** Weicht der Name in der Absenderadresse von der E-Mail-Adresse ab?
2. **Zahlreiche Rechtschreib- und Grammatikfehler oder verschwommene Logos.** Wenn die E-Mail scheinbar nachlässig erstellt wurde, ist sie möglicherweise nicht legitim.
3. **Handlungsdruck.** Wenn Sie in einer E-Mail zu sofortigen Maßnahmen aufgefordert werden, die E-Mail Handlungsdruck ausübt oder Ihre Neugier weckt, sollten Sie sehr misstrauisch sein.
4. **Anforderung von persönlichen oder vertraulichen Informationen.** Antworten Sie niemals auf eine unerbetene E-Mail, in der Sie um persönliche, finanzielle oder vertrauliche Informationen gebeten werden.
5. **Unrechtmäßig aussehende URL.** Viele URLs von Phishing-E-Mails sehen bei genauerer Betrachtung ungewöhnlich aus und sollten nicht angeklickt werden. Wenn die URL in einem Text-Link verborgen ist, bewegen Sie den Mauszeiger darüber und sehen Sie sich den unteren Rand Ihres Browsers an, um die URL zu untersuchen. Wenn Sie Zweifel haben, klicken Sie nicht darauf.
6. **Nicht erkannter Dateityp.** In den meisten beruflichen Funktionen sollten nur wenige Dateitypen jemals per E-Mail versendet werden.Wenn der Dateityp merkwürdig aussieht, öffnen Sie die Datei nicht.

## Außerdem:

- **Nehmen Sie sich Zeit.** Die durchschnittliche Person verbringt 8 bis 10 Sekunden mit dem Überfliegen einer E-Mail, bevor sie handelt. Halten Sie einen Moment inne und suchen Sie nach den Hinweisen, die auf einen Phishing-Versuch hindeuten könnten.
- **Wenn es zu gut klingt, um wahr zu sein, ist es wahrscheinlich ein solcher Versuch.** Bietet Ihnen die E-Mail Millionen von Dollar? Droht sie Ihnen, Sie bloßzustellen oder zu verletzen? Dann ist die Wahrscheinlichkeit sehr hoch, dass alles frei erfunden ist.
- **Achten Sie genau auf Warnungen.** Wenn Sie den Absender erkennen und einen Anhang öffnen, achten Sie besonders auf Bannerwarnungen zu Erweiterungen oder Makros, die aktiviert werden müssen (Abbildung 12). Selten, wenn überhaupt, sind diese notwendig.

## Strategien zur Abwehr von Angriffen

Es gibt mehrere Ansätze, mit denen Sie das Risiko von E-Mail-Bedrohungen reduzieren können.

**Führen Sie regelmäßige Phishing-Übungen durch.** Ihre Mitarbeiter sind Ihre größte Verteidigung gegen Phishing, besonders bei maßgeschneiderten Phishing-Versuchen. Mitarbeiter, die in der Lage sind, die sofortige Erkennung eines Phishing-Versuchs zu erlernen, können der wichtigsten Quelle der Kompromittierung von Endgeräten ein Ende bereiten.

Um das Bewusstsein zu schärfen, sollten Sie regelmäßige Phishing-Übungen im Unternehmen durchführen, um Benutzer zu testen und zu schulen. Emulieren Sie die neuesten Techniken aus der Praxis, um die Mitarbeiter auf dem Laufenden zu halten, was sie möglicherweise antreffen. Cisco empfiehlt die monatliche Durchführung dieser Übungen, beginnend mit einfach zu erkennenden Test-Phishing-Kampagnen und einer schrittweise Erhöhung des Schwierigkeitsgrads. Für Benutzer, die auf emulierte Phishing-Angriffe hereinfallen, sollten Sie eine sofortige Schulung anbieten (indem Sie beispielsweise eine „schädliche" Test-URL senden, die zu weiteren Informationen über Phishing führt). Für Benutzer mit hohem Risiko in Ihrem Unternehmen, in deren Bereich erhebliche Schäden drohen, wenn sie auf eine List hereinfallen, müssen Sie maßgeschneiderte Übungen zu Phishing-Kampagnen durchführen.

**Verwenden Sie eine mehrstufige Authentifizierung.** Für den Fall, dass die Anmeldeinformationen eines geschäftlichen E-Mail-Kontos erfolgreich gestohlen werden, kann die mehrstufige Authentifizierung verhindern, dass Angreifer Zugriff auf das Konto erhalten und verheerenden Schaden anrichten.

Der Vorteil der mehrstufigen Authentifizierung liegt in ihrer Einfachheit. Nehmen wir an, dass es jemandem gelingt, Ihre Anmeldeinformationen oder die von jemandem in Ihrem Netzwerk zu erhalten und sich anzumelden. Bei der mehrstufigen Authentifizierung wird automatisch eine Nachricht an die Person gesendet, die die Anmeldeinformationen besitzt, um zu überprüfen, ob sie gerade versucht hat, sich anzumelden. Der Benutzer in diesem Szenario weiß, dass er nicht gerade versucht hat, sich anzumelden, und lehnt die Anfrage sofort ab. Dadurch wird der Angriff erfolgreich vereitelt.

**Halten Sie Ihre Software auf dem neuesten Stand.** In einigen Fällen können E-Mails, die schädliche URLs enthalten, Benutzer zu Seiten mit Exploits führen. Durch die regelmäßige Aktualisierung von Browsern und Software sowie von Plug-ins können die von solchen Angriffen ausgehenden Risiken verringert werden.

**Überweisen Sie niemals Geld an Unbekannte.** Dies ist besonders beim Vorkassenbetrug und bei BEC-Betrügereien wichtig. Wenn Sie bei einer Anfrage misstrauisch sind, reagieren Sie nicht. Insbesondere für BEC sollten strenge Richtlinien aufgestellt werden, die die Autorisierung einer hochrangigen Person innerhalb des Unternehmens für Banküberweisungen erfordern. Außerdem sollte ein Zweitunterzeichner bestimmt werden.

**Seien Sie vorsichtig, wenn Sie um eine Anmeldung gebeten werden.** Schädliche Akteure, die darauf bedacht sind, Anmeldeinformationen zu stehlen, setzen alles daran, um ihre Seiten wie die Anmeldeseiten aussehen zu lassen, mit denen Sie vertraut sind. Wenn Sie auf eine solche Anmeldeaufforderung stoßen, überprüfen Sie unbedingt die URL, um sicherzustellen, dass sie von der rechtmäßigen Website des Besitzers stammt. Wenn ein Popup-Fenster oder Ähnliches eingeblendet wird, erweitern Sie das Fenster, um sicherzustellen, dass die vollständige URL oder zumindest die vollständige Domäne sichtbar ist.

**Achten Sie darauf, ob die E-Mail plausibel klingt.** Im Falle von Betrügereien wie der digitalen Erpressung und dem Vorkassenbetrug werden die Absender oft sehr erfinderisch, um Sie davon zu überzeugen, dass die E-Mail rechtmäßig ist. Ergibt das dargelegte Szenario wirklich Sinn? Gibt es Lücken in den Geschichten, beispielsweise aus Sicht der Technik, im Hinblick auf einen finanziellen Prozess oder ähnliche Ungereimtheiten? Wenn ja, sollten Sie skeptisch sein.

# Rüsten Sie sich

Es gibt viele verschiedene Möglichkeiten, wie E-Mail-Bedrohungen versuchen, Sie dazu zu bringen, zu antworten, auf URLs zu klicken oder Anhänge zu öffnen. Dies rechtfertigt den Einsatz von E-Mail-Sicherheitssoftware, die schädliche E-Mails abfangen und isolieren sowie Spam-Mails filtern kann.

Leider haben wir einen beunruhigenden Trend festgestellt: Der Anteil der Unternehmen, die Vorkehrungen für die E-Mail-Sicherheit treffen, sinkt. Laut unserer neuesten CISO-Benchmark-Studie nutzen derzeit nur 41 Prozent der Befragten E-Mail-Sicherheit als Teil ihrer Bedrohungsabwehr, obwohl sie E-Mails als die Nummer eins unter den Bedrohungsvektoren angeben, die ihre Unternehmen gefährden. Dies bedeutet einen Rückgang gegenüber 2014, als 56 Prozent der Unternehmen E-Mail-Sicherheit nutzten.

Es gibt mehrere mögliche Gründe für diesen Rückgang. Eine Ursache könnte die Umstellung auf die Cloud sein. In einer kürzlich durchgeführten Studie von ESG im Namen von Cisco gaben mehr als 80 Prozent der Befragten an, dass ihr Unternehmen Cloud-basierte E-Mail-Services verwendet. Da sich immer mehr Unternehmen dafür entscheiden, ihre E-Mail-Services in der Cloud zu hosten, erscheinen dedizierte E-Mail-Appliances vor Ort weniger notwendig, und einige IT-Teams gehen davon aus, dass sie darauf verzichten können.

Zwar stellen viele Cloud-E-Mail-Services grundlegende Sicherheitsfunktionen bereit, allerdings kann nicht genug betont werden, wie wichtig ein mehrstufiger Schutz ist. Tatsächlich stellten in der gleichen Umfrage der ESG 43 Prozent der Befragten fest, dass sie nach dem Umstieg zusätzliche Sicherheit zur Verteidigung ihrer E-Mails benötigten. Letztendlich besteht für IT-Teams durchaus immer noch die Notwendigkeit, Richtlinien festzulegen, Transparenz und Kontrolle zu erlangen, Sandboxes zu nutzen und externe Blockierfunktionen einzusetzen.

Ein weiteres Problem, dem Sicherheitsteams derzeit gegenüberstehen, ist eine erhöhte Angriffsfläche, die folglich zu mehr Bereichen führt, in denen Schutz erforderlich ist. Wenn die Sicherheitsbudgets nicht an diese Zunahme angepasst wurden, müssen die Teams möglicherweise mit knappen Ressourcen die größere Angriffsfläche abdecken.

Angesichts der Tatsache, dass E-Mail der häufigste Bedrohungsvektor ist, kann die Bedeutung des E-Mail-Schutzes nicht genug betont werden. Bei der Durchführung einer Analyse des Cyberrisikos ist es wichtig, Ihre kritischsten Einstiegspunkte mit gründlichen Abwehr- und Risikomanagementsystemen zu priorisieren und bei der Reihenfolge die Angriffswahrscheinlichkeit und das Risiko für das Unternehmen im Fall eines Verstoßes zu berücksichtigen. Anschließend müssen Sie Ressourcen zuweisen, die der Schwere möglicher Verluste angemessen sind.

**Darüber hinaus schlägt Gartner vor, dass Sicherheits- und Risikomanager (SRMs) einen dreigliedrigen Ansatz verfolgen, um ihre Abwehr gegen Phishing-Angriffe zu verbessern:**

1. Aktualisieren Sie Ihr Secure-E-Mail-Gateway und andere Kontrollen, um den Schutz vor Phishing zu verbessern.
2. Binden Sie Mitarbeiter in die Lösung ein und erstellen Sie entsprechende Funktionen, um verdächtige Angriffe erkennen und darauf reagieren zu können.
3. Entwickeln Sie gemeinsam mit der Geschäftsleitung standardmäßige Betriebsverfahren für den Umgang mit vertraulichen Daten und Finanztransaktionen.

# So schützen Sie Ihre E-Mails

Wir haben uns vorhin die verräterischen Anzeichen einer Phishing-E-Mail und Strategien zur Abwehr von Angriffen angesehen. Betrachten wir nun die Erwartungen an die Technologie der E-Mail-Sicherheit für das Jahr 2019.

Wie in der Vergangenheit ist ein mehrstufiger Sicherheitsansatz entscheidend, um Ihr Unternehmen vor E-Mail-basierten Angriffen zu schützen. Es gibt mehrere erprobte und getestete Funktionen der E-Mail-Sicherheit, die auch heute noch enorm wichtig sind.

**Hier einige Beispiele:**

- Es muss immer noch ein Spam-Abwehrmechanismus implementiert sein, um unerwünschte E-Mails und schädliche Spam-Mails von den Posteingängen fernzuhalten.
- E-Mail-Bedrohungsabwehrfunktionen wie die Blockierung von Malware und URLs sind unerlässlich, um Malware, Spear-Phishing, Ransomware und Cryptoming in Anhängen zu blockieren, sowie eine URL-Intelligence, um schädliche Links in E-Mails zu bekämpfen.
- Integriertes Sandboxing sollte automatisch im Hintergrund für neue Dateien erfolgen, die in E-Mails ankommen, um schnell zu erkennen, ob sie schädlich sind.

Allerdings kann nicht genug betont werden, dass sich die Bedrohungslandschaft ständig weiterentwickelt und schädliche Akteure immer auf der Suche nach neuen Angriffsmöglichkeiten sind.

**Zusätzlich zu den bewährten und getesteten Sicherheitstechnologien sind die folgenden Technologien bei der Bekämpfung dieser sich ständig verändernden Landschaft hilfreich:**

- Es sind fortschrittlichere Phishing-Schutzmaßnahmen entstanden, bei denen maschinelles Lernen zum Verständnis und zur Authentifizierung von E-Mail-Identitäten und Verhaltensbeziehungen eingesetzt wird, damit ausgeklügelte Phishing-Angriffe blockiert werden können.
- Der DMARC-Domänenschutz kann nun aktiviert werden, um die Marke eines Unternehmens zu schützen, indem Angreifer daran gehindert werden, eine legitime Firmendomäne in Phishing-Kampagnen zu verwenden.
- Die Funktion der Nachrichtenquarantäne ist nützlich, um eine Nachricht aufzubewahren, während ein Dateianhang analysiert wird, bevor entweder eine Nachricht an den Empfänger freigegeben, der schädliche Anhang entfernt oder die Nachricht vollständig entfernt wird.
- Die E-Mail-Korrektur hilft, wenn eine Datei nach der Zustellung an den Empfänger als schädlich erkannt wird, so dass Sie die Nachricht mit einem schädlichen Anhang aus einem Postfach heraus isolieren können.
- Externe E-Mail-Bedrohungs-Feeds in STIX werden heute häufig von E-Mail-Sicherheitsprodukten verwendet, was hilfreich ist, wenn ein Unternehmen einen vertikal ausgerichteten Bedrohungs-Feed über die native Threat-Intelligence im Produkt hinaus nutzen möchte.
- Die Integration von E-Mail-Sicherheit in allgemeinere Sicherheitsportfolios wird ebenfalls immer häufiger genutzt, um zu erkennen, ob möglicherweise ausgeklügelte Malware oder Nachrichten in einer Umgebung an bestimmte Benutzer oder Posteingänge zugestellt wurden.

**„Cisco ist führend in der 2019 Forrester Wave for Enterprise Email Security und erhält die höchsten Bewertungen für Bereitstellungsoptionen, Angriffsschutz und E-Mail-Authentifizierung, Leistung und Betrieb (einschließlich Skalierbarkeit und Zuverlässigkeit) sowie Spitzentechnologie.“**

**The Forrester Wave™: Enterprise Email Security, Q2 2019**

# Die Cisco Reihe zur Cybersicherheit

Im vergangenen Jahrzehnt hat Cisco eine Fülle an maßgeblichen Sicherheits- und Bedrohungsinformationen für Sicherheitsexperten veröffentlicht, die sich für den aktuellen Stand der globalen Cybersicherheit interessieren. Diese umfassenden Berichte enthielten detaillierte Beschreibungen von Bedrohungslandschaften und ihren organisatorischen Auswirkungen sowie Best Practices zum Schutz vor den negativen Folgen von Datensicherheitsverletzungen.

In unserem neuen Ansatz für unsere Vordenkerposition veröffentlicht Cisco Security eine Reihe von forschungsbasierten, datengesteuerten Publikationen unter folgender Überschrift: Cisco Reihe zur Cybersicherheit. Wir haben die Anzahl der Titel erweitert, sodass sie jetzt auch verschiedene Berichte für Sicherheitsexperten mit anderen Interessen enthalten. Die vorherige Berichtssammlung für 2019 greift auf die tiefgreifenden und umfangreichen Kenntnisse von Bedrohungsforschern und Innovatoren in der Sicherheitsbranche zurück und enthält die Benchmark-Studie zum Datenschutz, den Bedrohungsbericht und die CISO-Benchmark-Studie. Weitere Berichte sollen im Jahresverlauf folgen.

Weitere Informationen und Zugriff auf alle Berichte und archivierte Kopien finden Sie auf www.cisco.com/go/securityreports.


**Hauptgeschäftsstelle Nord- und Südamerika**
Cisco Systems, Inc.
San Jose, CA

**Hauptgeschäftsstelle Asien/Pazifik**
Cisco Systems (USA) Pte.
Singapur

**Hauptgeschäftsstelle Europa**
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter www.cisco.com/go/offices.

Veröffentlicht im Juni THRT_02_0519_r1

© 2019 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Cisco und das Logo von Cisco sind Handelsmarken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Handelsmarken von Drittanbietern sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)