Weissbuch

Jeder erhält diese Mails…

Hintergrund und Folgen betrügerischer E-Mails – und was Sie dagegen tun können.

protect-it in Zusammenarbeit mit proofpoint.

Betrügerische E-Mails werden zunehmend zur globalen Bedrohung

Die blauen Teile der Info-Grafik zeigen die Auswirkungen betrügerischer E-Mails in aller Welt.

QUELLE: http://fsroundtable.org/business-email-compromise-costing-its-victims-millions-simple-tips-can-help-foil-fraudsters/

Bei den Bedrohungen der fortschrittlichen Art finden wieder einmal Veränderungen statt – auch Sie und Ihr Unternehmen dürften im Fadenkreuz einer neuartigen Bedrohung stehen. Betrügerische E-Mails, die unter eingehender Recherche sorgfältig geplant werden, zielen auf bestimmte Personen in Ihrer Firma ab. Auch wenn Sie nicht unbedingt ein direktes Ziel der Attacke sein müssen, könnten Sie ihr unwissentlich zum Opfer fallen. Betrügerische E-Mails brauchen keine Schadsoftware oder URLs, wie sie bei typischen Anmeldedaten-Phishing-Kampagnen vorkommen. Bei Angriffen dieser Art geht es meistens nicht darum, persönlichen oder finanziellen Daten von Mitarbeitern oder Kunden abzugreifen oder Kreditkartennummern zu erhaschen.

Betrügerische E-Mails, die das FBI als „Business Email Compromise" betitelt und die ferner die Bezeichnung CEO Fraud (Geschäftsführer-Schwindel), Man-in-the-E-Mail, Walfang-Attacke und andere unrühmliche Titel erhielten, werden gezielt darauf ausgerichtet, Führungskräfte zu imitieren und ahnungslose Mitarbeiter auszutricksen. Nach Aussage des Internet Crime Center (IC3) des FBI haben Betrugsattacken allein 2015 um mehr als 270 % zugenommen. Die betroffenen Unternehmen stammen aus knapp 80 Ländern und den ganzen USA, seit Ende 2013 belaufen sich die Verluste auf über 2 Mrd. USD.[1]

Vielleicht merken Sie es noch nicht einmal sofort, wenn Sie Oper einer betrügerischen E-Mail geworden sind. Sicherheitstools schlagen nicht Alarm. Es gibt keinen erpresserischen Hinweis. Ihre Systeme laufen weiter, nichts deutet auf eine Unregelmäßigkeit hin. Das ist genau der Punkt.

Betrügerische E-Mails haben mittlerweile globale Ausmaße angenommen und zielen nun auf große wie kleine Firmen überall auf der Welt ab. Von Neuseeland bis Belgien – in jeder Branche gibt es Unternehmen, die furchtbare Verluste erlitten haben.

- Ein in Hong Kong ansässiges Tochterunternehmen der Ubiquiti Networks Inc. fand heraus, dass es über einen längeren Zeitraum mehr als 45 Mio. USD an Hacker überwiesen hatte, die sich mit betrügerischen E-Mails als Lieferant ausgaben.[2]

- Die belgische Bank Crelan verlor neulich über 70 Mio. USD durch betrügerische E-Mails. Der Schwindel flog erst bei einer internen Betriebsprüfung auf.[3]

- In Neuseeland verlor TWoA, Anbieter von Hochschulstudien, mehr als 100.000 USD, weil der CFO einer betrügerischen E-Mail zum Opfer fiel und glaubte, die Zahlungsanordnung käme vom Präsidenten der Organisation.[4]

- Luminant Corp, ein Stromlieferant aus Dallas (Texas) überwies etwas mehr als 98.000 USD aufgrund einer E-Mail-Anordnung, die nach Ansicht der Mitarbeiter von einem leitenden Angestellten der Firma stammte. Später erfuhren sie, dass Hacker Ihnen eine betrügerische E-Mail gesendet hatten, bei der lediglich zwei Buchstaben des Domain-Namens vertauscht worden waren.[5]

Betrüger Ante Portas

Damit eine betrügerische E-Mail Erfolg hat, wenden die Hacker verschiedenste Strategien an, um Nachforschungen über Ihre Firma anzustellen. Dazu gehört u. A. das Durchkämmen von Social-Media-Websites und Ankündigungen irgendwelcher Neuheiten, um im Informationswust der Unternehmen zu stöbern und mehr über deren Geschäftsfeld, Führungskräfte und direkte Untergebene zu erfahren. Möglicherweise gehen bei Ihnen geschickt eingefädelte Anrufe zu unterschiedlichsten Themen ein, die darauf abzielen, Ihnen Informationen über Ihre Mitarbeiter, Kunden und Lieferanten zu entlocken. Nur wenn er Ihre Geschäftsprozesse und Partner kennt,wird ein Hacker erfolgreich sein.

1 Manipulierte Geschäfts-E-Mails, eine zunehmende globale Bedrohung, August 28, 2016, https://www.fbi.gov/news/stories/2015/august/business-e-mail-compromise/business-e-mail-compromise

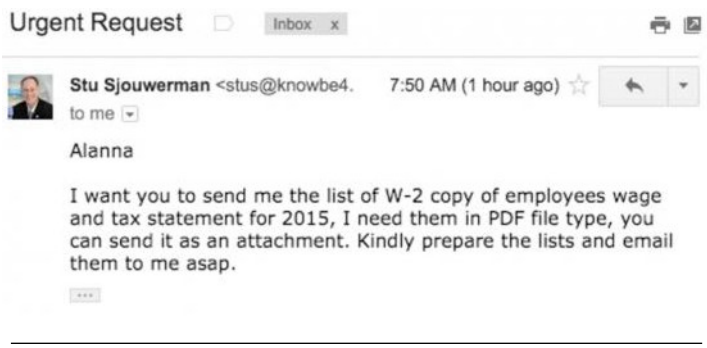
2 Tech-Firma Ubiquiti erleidet 46 Mio. USD Schaden – Cyberheist, 15. August 2015, http://krebsonsecurity.com/2015/08/tech-firm-ubiquiti-suffers-46m-cyberheist/

3 Belgische Bank verliert 70 Mio. € durch klassischen Social-Engineering-Trick (CEO Fraud), 25. Januar 2016, http://news.softpedia.com/news/belgian-bank-loses-70-million-to-classic-ceo-fraud-social-engineering-trick-499388.shtml)

4 Neuseeländer verlieren 12 Mio. USD an Gauner, 1. Januar 2016, http://www.stuff.co.nz/business/money/75536670/New-Zealanders-lose-12m-to-scams

5 Nigerianer wegen raffinierten E-Mail-Schwindels in Dallas inhaftiert, 1. January 2016, http://www.dallasnews.com/news/crime/headlines/20160101-nigerian-charged-in-sophisticated-email-scam-is-in-custody-in-dallas.ece

Angreifer mit einer soliden Aufklärungsstrategie investieren Zeit und Geld in die Informationsgewinnung. Der erste Schritt besteht darin, ein lohnenswertes Ziel auszumachen. Wenn Ihr Unternehmen eine große Zahl an Lieferanten/Partnern und Führungskräften hat, die häufig ins Ausland reisen, ist es das ideale Ziel für eine betrügerische E-Mail. Der Schlüssel zu einer erfolgreichen Attacke liegt darin, den Zeitunterschied sowie die vielen Stunden, die ein leitender Angestellter unterwegs und nicht zu erreichen ist, auszunutzen.



Führungskräfte werden auf zweierlei Art und Weise ins Visier genommen. Da ist zum einen der ständig verreiste Manager – die Person, die der Hacker studiert, um sie nachzuahmen. Dazu wird jede erdenkliche Ressource herangezogen, um sich über Zeitplan, Sprachgewohnheiten, Kollegen und direkte Untergebene zu informieren. Mit großer Wahrscheinlichkeit geht bei der Firma ein Anruf ein, um weitere Informationen zu erhalten, die mehr über Lieferanten und Kunden verraten. Für einen Hacker kann beispielsweise die Information, bei welcher Agentur Ihre Firma Reisen bucht, wertvoll sein.

> Betrügerische E-Mails wirken oft dadurch glaubhaft, dass streng gehütete Details zu aktuellen Projekten oder auch Firmenkürzel angegeben werden.

Oft ist der Geschäftsführer die ständig verreiste Führungskraft, daher die Bezeichnung „Geschäftsführer-Schwindel“. Als Empfänger könnte ein leitender Angestellter mit Befugnissen finanzieller Art im Visier stehen, der in letzter Minute „vor dem Besteigen des Fliegers“ eine vermeintliche Zahlungsanordnung vom CEO erhält. Die Anweisungen beinhalten vielleicht eine Überweisung an einen Lieferanten, der zufällig im selben Gebiet ansässig ist, zu dem der Manager reisen wollte.

Diesem Szenario fallen leicht direkte Untergebene des Geschäftsführers zum Opfer, die routinemäßig Zahlungen verarbeiten. Eine andere Masche setzt darauf, Ihre Lieferanten sowie deren Art der Rechnungsstellung, Sprachgewohnheiten, Formulare und Verfahren (z. B. Änderung der Bankkontoangaben für eine bevorstehende Zahlung) zu studieren. Wenn der Trick des Angreifers funktioniert, überweisen Sie ihm vielleicht monatelang Geld, ohne es überhaupt zu merken.

So ahmen Schwindler Ihre Absenderadresse nach

LinkedIn und andere Social-Media-Websites sind die „angesagte“ Ressource zum Ausloten der Ziele und potenziellen Opfer. Hacker erstellen einen Steckbrief des leitenden Angestellten, indem sie Social-Media-Websites, PR-Veröffentlichungen und Artikel mit Neuigkeiten über das Unternehmen auf deren Inhalte überprüfen. Davon ausgehend, finden sie in detektivischer Kleinarbeit Ihre direkten Untergebenen heraus. Neue Mitarbeiter in der Buchhaltung oder Rechnungsstelle sind bei Hackern, die mit betrügerischen E-Mails arbeiten, heiß begehrt. Sie stellen das perfekte Opfer einer Betrugsattacke dar. Als Neuling in der Organisation haben sie meist noch kein rechtes Gespür dafür, wenn etwas an einer Zahlungsanordnung nicht stimmt. Sie wissen nicht genug über Ihre Lieferanten oder wollen ja keine Verzögerung in Kauf nehmen, um einen guten Eindruck zu machen. Und sie wissen nicht, wann es besser ist, eine Transaktion aufzuschieben und zu hinterfragen.

> Oft erstellen Hacker die Domain und E-Mail-Adressen nur wenige Stunden vor dem Absenden der betrügerischen E-Mail.

Sind die Nachforschungen über Ihre Firma und deren Führungskräfte erst abgeschlossen, verfügen die Angreifer über ein umfassendes

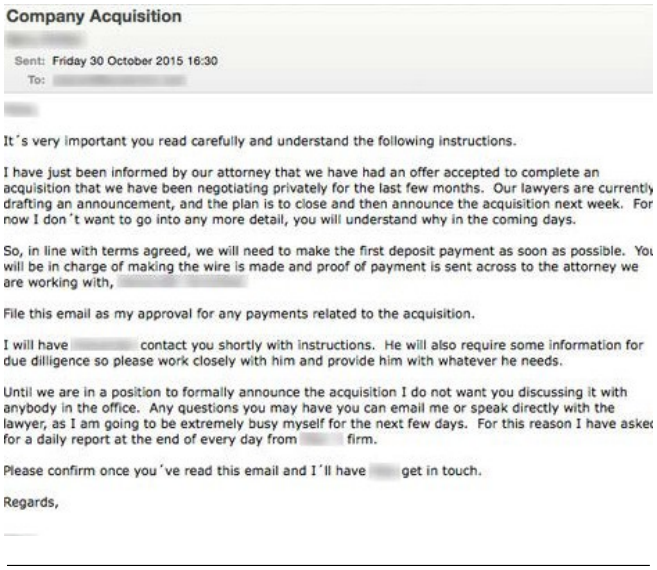
Profil des Unternehmens. Außerdem haben sie einen guten Teil Ihrer Geschäftsbeziehungen ausgelotet und kennen vielleicht ein paar spezielle Projekte oder Codebezeichnungen des Unternehmens. Sie haben Dossiers zu den meisten oberen Führungskräften angelegt, besonders über jene in Finanzpositionen; sie wissen, wer ihre direkten Untergebenen sind und welche Funktion sie ausüben. In der nächsten Phase holen sie ihren technischen Zauberkasten hervor, mit dem sie Ihre Firma (oder jeden Manager, der ein lohnenswertes Ziel abgibt) imitieren. Alternativ dazu ahmen sie vielleicht einen Ihrer regulären Lieferanten nach – oder eine Buchführungsfirma, die mit Ihrem Unternehmen zusammenarbeitet.

Wenn ein Hacker versucht, einen festen Mitarbeiter Ihrer Firma zu imitieren, kann er einen Domain-Namen registrieren lassen, der sich nur um einen oder zwei Buchstaben von Ihrem unterscheidet. In einer betrügerischen E-Mail, verbunden mit gefälschten E-Mail-Adressen von zuvor ausgeloteten Managern, sieht die Domain dem Original schon sehr ähnlich. Oft erstellen Hacker die Domain und E-Mail-Adressen nur wenige Stunden vor dem Absenden der betrügerischen E-Mail. In anderen Fällen tun sie vielleicht das Gleiche, ahmen jedoch einen Lieferanten oder eine andere Firma nach, z. B. eine Buchführungsfirma oder Anwaltskanzlei, die Ihnen routinemäßig Zahlungsanordnungen schickt.

„Fake“-E-Mails – Übung macht den Betrüger

Der erste Kontakt eines Hackers mit Ihrer Firma kann auf vielerlei Art und Weise eingeleitet werden. Aber normalerweise

läuft alles auf eine einmalige, gezielte E-Mail oder einen eher dialogorientierten Ansatz hinaus, der mehrere E-Mails und Telefonate umfasst.



Company Acquisition

Sent: Friday 30 October 2015 16:30
To:

It´s very important you read carefully and understand the following instructions.

I have just been informed by our attorney that we have had an offer accepted to complete an acquisition that we have been negotiating privately for the last few months. Our lawyers are currently drafting an announcement, and the plan is to close and then announce the acquisition next week. For now I don´t want to go into any more detail, you will understand why in the coming days.

So, in line with terms agreed, we will need to make the first deposit payment as soon as possible. You will be in charge of making the wire is made and proof of payment is sent across to the attorney we are working with,

File this email as my approval for any payments related to the acquisition.

I will have contact you shortly with instructions. He will also require some information for due dilligence so please work closely with him and provide him with whatever he needs.

Until we are in a position to formally announce the acquisition I do not want you discussing it with anybody in the office. Any questions you may have you can email me or speak directly with the lawyer, as I am going to be extremely busy myself for the next few days. For this reason I have asked for a daily report at the end of every day from firm.

Please confirm once you´ve read this email and I´ll have get in touch.

Regards,

Neue Mitarbeiter in der Buchhaltung oder Rechnungsstelle sind bei Hackern, die mit betrügerischen E-Mails arbeiten, heiß begehrt. Sie stellen das perfekte Opfer einer Betrugsattacke dar. Als Neuling in der Organisation haben sie meist noch kein rechtes Gespür dafür, wenn etwas an einer Zahlungsanordnung nicht stimmt.

Wenn der eine Schuss sitzen muss

Betrügerische E-Mails nach dem One-Shot-Prinzip bauen in erster Linie darauf, dass die E-Mail genau zum richtigen Zeitpunkt gesendet wird. Im Idealfall stimmt der Hacker des Sendezeitpunkt einer betrügerischen E-Mail auf die Reisezeiten der Zielperson ab. Diese Informationen erhalten sie vielleicht dadurch, dass sie sich den Zugriff auf den Posteingang eines oder mehrerer Mitarbeiter verschafft haben. Nun muss der Hacker noch den günstigsten Zeitpunkt abpassen, um sich dem Opfer mit einer betrügerischen E-Mail anzunähern. Die Nachricht kann eine dringende Botschaft beinhalten: „Die Überweisung muss erledigt sein, bevor ich in Hongkong lande.” Oder sie kommt auf die lässige Tour daher: „Ich sitze gleich im Flieger und wir müssen heute noch an ... überweisen.”

Es kommt oft vor, dass eine betrügerische E-Mail nicht erkannt wird. Schließlich enthalten solche E-Mails keine Schadsoftware, URLs oder gefährliche Anhänge. Es handelt sich um eine einfache Textnachricht von einer Domain, zu der es keine Reputationsbewertung gibt. Manchmal steht sogar „Gesendet von meinem iPad“ oder Ähnliches in der Signaturzeile, um über die schlechte Grammatik hinweg zu täuschen, die oft bei betrügerischen E-Mails aus einem anderen Land auffällt.

Auch Vermögensverwaltungs- oder Investmentfirmen gehören zur Zielgruppe des One-Shot-Ansatzes. In diesem Fall werden eigenkapitalstarke Investoren mit ansehnlichen Anteilswerten anvisiert. Ihr Finanzberater ist dann das potenzielle Opfer. Die Angreifer konzentrieren sich auf vermögende Investoren, genauso, wie sie höhere Führungskräfte aufs Korn nehmen. Sie legen ein Profil der Investoren an und verschaffen sich Informationen über ihre finanziellen Verbindungen, um einer gefälschten Aufforderung zur Überweisung den amtlichen Charakter zu verleihen.

Bei einem weiteren Beispiel einer einmaligen betrügerischen E-Mail wird nicht unbedingt um eine Überweisung gebeten; stattdessen werden in einzeiligen E-Mails vertrauliche Informationen rasch angefordert. Beispielsweise werden Angestellte in einer betrügerischen E-Mail, die derzeit in Umlauf ist, unter dem Vorwand einer „Steuerprüfung" nach ihrer Steuernummer gefragt. Mit E-Mails dieser Art kann ein höherer Angestellter der Personalabteilung anvisiert werden, indem eine betrügerische E-Mail mit der Bitte um Angabe der Steuernummer an einen oder mehrere seiner direkten Untergebenen geschickt wird.

Gewandte Gesprächspartner

Manchmal läuft eine betrügerische E-Mail-Kampagne über einen längeren Zeitraum. Bei diesem Ansatz könnte die Zielperson ein Manager sein, der mit M&A-Aktivitäten, neuen Produkten oder strategischen Partnerschaften zu tun hat. Hierbei erstellen Hacker eine betrügerische E-Mail, die das Opfer auf eine angeblich bevorstehende Übernahme, Partnerschaft oder ein anderes „super-eiliges" Projekt hinweisen, bei dem eine Überweisung ansteht. Solche betrügerischen E-Mails gehen üblicherweise mit der Bitte um Verschwiegenheit bezüglich der Überweisung einher, da es sich ja um eine streng geheime Aktivität des Unternehmens handelt. Betrügerische E-Mails wirken oft dadurch glaubhaft, dass streng gehütete Details zu aktuellen Projekten oder auch Firmenkürzel angegeben werden. In diesem Fall verleitet der Betrüger sein Opfer dazu, die Transaktion unter dem Deckmantel der Verschwiegenheit auszuführen.

Ein gewandter Gesprächspartner kann auch einen Lieferanten imitieren und ein scheinbar harmloses Gespräch über den aktuellen Rechnungsstatus einleiten. Wird die Anfrage erwidert, können nach und nach auch Bankkontodaten in das Gespräch mit einfließen. Manchmal enthält eine betrügerische E-Mail fiktive E-Mail-Dialoge zwischen höheren Angestellten, die den Eindruck der Notwendigkeit einer Überweisung verstärken. Wenn das Opfer die List nicht durchschaut und die gefälschten E-Mail-Adressen und Anfragen echt genug aussehen, können die betrügerischen E-Mails dazu führen, dass Gelder lange Zeit unerkannt von Ihrem Firmenkonto in dunkle Kanäle gelangen.

So richtig dreist wird die Bedrohung durch den gewandten Gesprächspartner oftmals dadurch, dass er per Telefon sogar auf unternehmenseigene Richtlinien eingeht, die eine mündliche Bestätigung von Zahlungsanordnungen vorschreiben. Es kann vorkommen, dass die betrügerische E-Mail Kontaktdaten eines Drittanbieters enthält, beispielsweise von einer Person, die angeblich bei der Buchführungsfirma oder Anwaltskanzlei Ihres Unternehmens arbeitet und als Ansprechpartner für weitere Anweisungen fungiert. Da möglicherweise anschließend ein Telefonat zu erwarten ist, werden entsprechende Kontakt-Telefonnummern eingerichtet. Der Angreifer kann vorbeugend im Voraus anrufen, um das Opfer darauf hinzuweisen, dass demnächst eine Zahlungsanordnung bei ihm eintrifft. Das passiert in der Regel außerhalb der Geschäftszeiten – vielleicht weiß der Angreifer, dass der anvisierte Manager unterwegs, im Ausland oder aus anderen Gründen nicht abkömmlich ist.

Der Betrüger, der aus dem Nichts kam

Es gibt verschiedene Ansätze, die zum Schutz Ihrer Firma vor betrügerischen E-Mails beitragen. Zwar sind diese Maßnahmen hilfreich, aber gegen einen entschlossenen Betrüger bieten sie keinen absoluten Schutz.

Aufmerksamkeitstrainings

An der Spitze der Strategien zur Bekämpfung von Attacken dieser Art steht eine gute Schulung. Diese kann von einem freundlichen Hinweis per E-Mail, sich jede Zahlungsanordnung zwei Mal anzuschauen, bis zum Online-Unterricht reichen, der den Mitarbeitern helfen soll, betrügerische E-Mails zu durchschauen. Der Schulungsteilnehmer sollte lernen, E-Mail-Adressen auf ihre Echtheit zu prüfen und bei E-Mails, die zur Geheimhaltung oder zum raschen Handeln auffordern, misstrauisch zu werden.

Zwar gehört das Training zu jedem guten Sicherheitsprogramm dazu – allerdings sollte man seine Mitarbeiter nicht damit überfordern, der langen Liste wichtiger Dinge, die es zu beachten gilt, zu viele Facetten hinzuzufügen. Das gilt umso mehr, wenn man bedenkt, dass mit diesen betrügerischen E-Mails sehr gezielt die Reisepläne von Managern und detaillierte Kenntnisse über das

Unternehmen und seine Belegschaft ausgenutzt werden.

Dank granularer Kontrollen können E-Mail-Lösungen der nächsten Generation betrügerische E-Mails erkennen und in Quarantäne stellen, bevor sie überhaupt den Posteingang eines Angestellten erreichen.

Authentifizierungsstandards

DMARC und DKIM filtern einige betrügerische E-Mails heraus – aber nicht alle. DMARC ist ein relativ neuer Standard, und viele regionale ISPs befinden sich noch in der Planungsphase der Umsetzung, was eine inkonsistente Verwendung bei den verschiedenen Standorten zur Folge hat. Außerdem bietet es keinen Schutz vor Angreifern, die mit manipulierten Anzeigenamen, ähnlich lautenden Domains oder DNS-Servern arbeiten, die erfundene Routing-Informationen verwenden.

SPF (Sender Policy Framework) beschränkt sich auf einige Varianten gefälschter E-Mails, kann jedoch keine betrügerischen E-Mails erkennen, die von einer absichtlich falsch buchstabierten Domain stammen.

Verbesserung der Zahlungsprüfverfahren

Eine weitere Methode, mit der Unternehmen versuchen, sich vor betrügerischen E-Mails zu schützen, ist die Einrichtung strengerer Richtlinien in Bezug auf Zahlungen. Das FBI empfiehlt, einen zweistufigen Prüfprozess einzuführen, zu dem telefonische Kontrollen gehören. Verschlüsselten E-Mails tragen dazu bei, dass Mitarbeiter jeweils mit der richtigen Person kommunizieren.

Eine Verbesserung der Zahlungsrichtlinien kann definitiv helfen, bietet jedoch keinen Schutz vor einem entschlossenen Betrüger, der eigene Telefonnummern zur Gegenprüfung einrichtet oder sich mit echt wirkenden Folgeanrufen an die Mitarbeiter wendet. Sie können auch dann versagen, wenn ein neuer Mitarbeiter unter Zeitdruck steht oder mit einer Situation konfrontiert wird, die nicht mit den Unternehmensrichtlinien im Einklang steht.

Abwehr gegen Betrügereien

Der Hintergrund moderner betrügerischer E-Mails ist der, dass Hacker neue Taktiken austüfteln, um Sicherheitslösungen zu umgehen, die auf die Erkennung von Schadsoftware-Anhängen und gefährlichen URLs ausgelegt sind. Man sollte sich stets darüber im Klaren sein, dass betrügerische E-Mails eine einmalige Sache sind und keine Angriffskampagne wie z. B. Dridex. Daher treten

betrügerische E-Mails, wenngleich in fast jedem Land, in sehr kleiner Zahl auf. Ein geringerer Umfang macht es dem Betrüger leichter, seine E-Mails an Ihre Mitarbeiter zu bringen, da traditionelle Abwehrmechanismen im Allgemeinen ein Muster benötigen, damit sie diese E-Mails identifizieren können.

Die beste Möglichkeit, ein Unternehmen vor betrügerischen E-Mails zu schützen, bietet eine Kombination aus strengeren Unternehmensrichtlinien und einer E-Mail-Sicherheitslösung der nächsten Generation. Unternehmen müssen Lösungen einführen, die nicht ausschließlich auf Reputation und simpler E-Mail-Filterung basieren. Dank granularer Kontrollen können E-Mail-Lösungen der nächsten Generation betrügerische E-Mails erkennen und in Quarantäne stellen, bevor sie überhaupt den Posteingang eines Angestellten erreichen. Nur so können Sie den Schaden, den diese Art von Bedrohungen Ihrer Organisation zufügen können, entscheidend verringern.