E-Mail-Sicherheit für Office 365

Nichts geht mehr. So wird es repariert.

Verletzungen von Daten nehmen zu.
Ihr Netzwerk und Assets des Unternehmens werden angegriffen.
Malware mutiert ständig und breitet sich aus.
Ransomware wird ein beunruhigender Faktor des Lebens.

Was ist der gemeinsame Faktor hinter all diesen Trends? E-Mail.

VadeSecure
Predictive Email Defense

Inhalt

EINLEITUNG

An 93 Prozent aller Netzwerkverletzungen ist ein Phishing- oder Spear Phishing-Angriff beteiligt.

In den meisten Fällen sind die Perimeter der wachsamsten Organisationen in angemessener Weise dicht. Firewalls sind vorhanden, Server sind gepatcht, und die physische Sicherheit steht. Dennoch ist E-Mail ein riesiges, klaffendes Loch in Ihren Netzwerk-Verteidigungsanlagen.

E-Mail ist der Vektor für praktisch alle Ängste, die Sie nachts wach halten.

Und noch schlimmer: Die bösen Jungs nützen E-Mail aus, um auf die größte Schwachstelle aller IT-Verantwortlichen zu zielen: ihre Mitarbeiter.

Wenn Sie meinen, dass Ihre Organisation gegen von E-Mail transportierte Attacken gerüstet ist, weil Sie Office 365 mit E-Mail-Sicherheitspaketen wie EOP, Proofpoint, McAfee oder Barracuda eingerichtet haben, müssen Sie das überdenken. Diese Sicherheitspakete können Spear Phishing-Attacken oder Angriffe ab Tag Null nicht zuverlässig abfangen.

Entsprechend einer Untersuchung von Vanson Bourne zu IT-Entscheidungsträgern aus dem Jahre 2016 haben 84 Prozent der Organisationen erklärt, dass eine Spear Phishing-Attacke 2015 bei ihnen erfolgreich eingedrungen ist. Freilich haben 71 Prozent auch angegeben, dass sie schon eine gewisse Technologie für E-Mail-Sicherheit einsetzen.

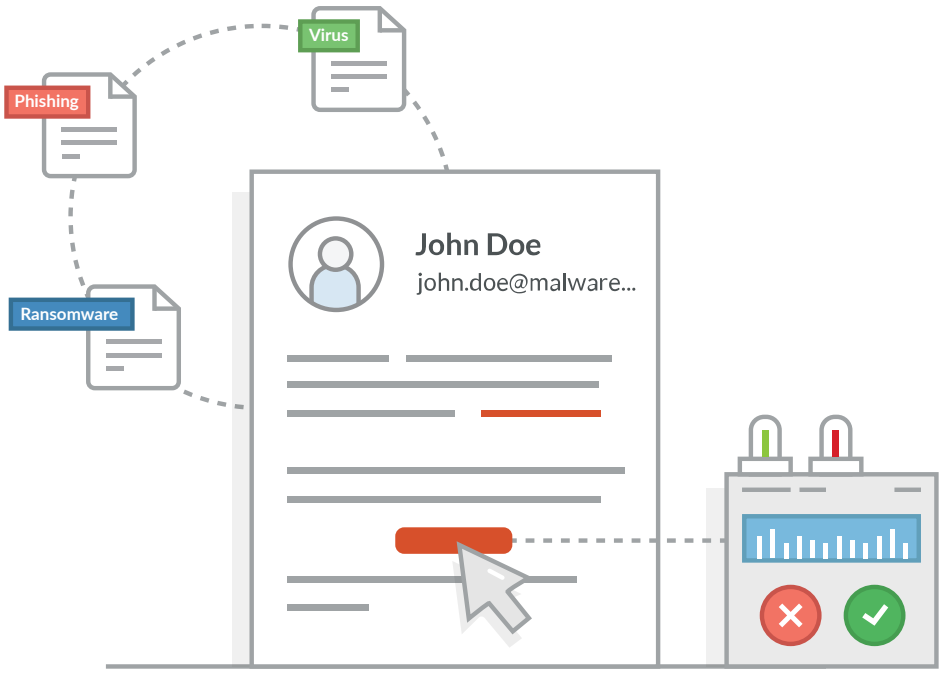
Die E-Mail-Sicherheit ist deutlich geknackt.

Das Problem hat zwei Aspekte:

1. **Technologie:** Die meisten „Sicherheits"-Systeme für E-Mail sind in Wirklichkeit nur überbewertete Spamfilter. Sie wurden konzipiert, um bekannte Angriffe mit Massen-E-Mails zu stoppen. Die diesen Lösungen zugrunde liegende Architektur eignet sich nicht, um Bedrohungen ab Tag Null oder einmalige Spear Phishing-E-Mails abzufangen.

2. **Personen:** Viele Mitarbeiter klicken auf eine geschickt formulierte Phishing- oder Spear Phishing-E-Mail, die in ihrer Inbox landet, oder beantworten sie. Trotz Aufklärungsarbeit öffnen 20 bis 30 Prozent der Empfänger Standard-Phishing-Nachrichten, die in ihrer Inbox ankommen, und 12 bis 20 Prozent davon klicken auf darin enthaltene Phishing-Links. Diese bereits hohen Raten steigen auf mehr als das Doppelte, wenn es um Spear Phishing-E-Mails geht.[1]

Wir führen Sie durch die Ausmaße des Problems und sprechen dann darüber, wie Sie die in Ihrer Office 365-Konfiguration klaffenden Sicherheitslücken schließen können.



1. Die niedrigen Zahlen stammen aus dem 2016 Data Breaches Report von Verizon, die höheren Zahlen aus einer Untersuchung vom August 2016 der Friedrich-Alexander-Universität Erlangen, werden aber durch ähnliche Ergebnisse vieler anderer Untersuchungen unterstützt.

PHISHING

Phishing ist eine Hackertechnik, die durch Senden von irreführenden E-Mails nach Opfern „fischt“. (Das „ph“ anstelle des „f“ ist eine Hommage für die ersten Hacker, die „Phone Phreaks“ aus den 1960er und 1970er Jahren.) Praktisch jeder im Internet hat schon eine Phishing-Attacke gesehen. Phishing-Attacken sind Massen-E-Mails, die unter einem Vorwand vertrauliche Informationen oder Anmeldedaten anfordern, einen Link zu schädlichen Websites herstellen oder in der Anlage Malware enthalten.

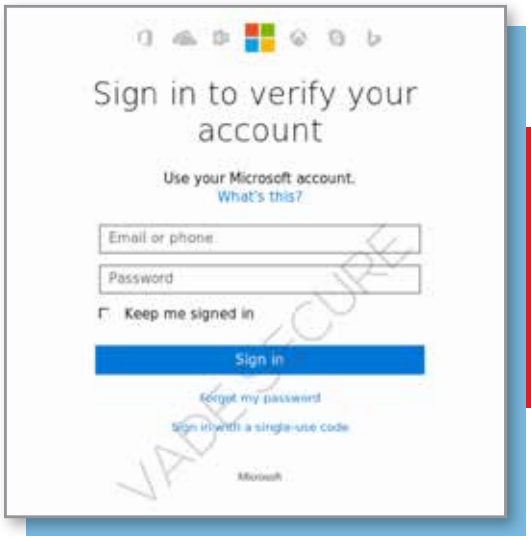


Abbildung 1 - Viel beschäftigte Leute fallen auf realistische Login-Displays herein. Wenn sie erst mal ihre Anmeldedaten eingegeben haben, ist Ihr Netzwerk verbrannt.

Viele Phishing-Sites sehen wie die legitime Site aus, die sie personifizieren möchten. Oft ist der einzige Unterschied zu den nachgeahmten Websites eine kleine, leicht übersehene Differenz der URLs. Besucher können leicht getäuscht werden, damit sie dem Hacker Anmeldedaten oder vertrauliche Informationen übermitteln, wenn sie verleitet werden können, auf den Link zu klicken. Selbst Phishing-Sites, die auf eine schwarze Liste gesetzt wurden, können Standardfilter häufig anhand URL-Zeitbombentechnik überlistet werden. Der URL führt anfänglich zu einem harmlosen URL, um an den Filtern vorbeizukommen und dann zu einer schädlichen Site umzuleiten.

Obwohl es schwieriger ist, Malware an Filtern vorbeizuschmuggeln, hat erst kürzlich entdeckte oder Tag-Null-Malware hervorragende Chancen, Standardfilter zu übergehen und angeklickt zu werden, insbesondere, wenn die Malware in einer nicht ausführbaren Datei versteckt ist, zum Beispiel in einem PDF- oder Office-Dokument. So wurden viele der jüngsten Ransomware-Angriffe verbreitet.

Trotz der mangelnden Personalisierung klicken erstaunliche 20 Prozent der Empfänger auf praktisch alles, was es in ihre Inbox schafft.[2]

Wir werden sehen, dass alle diese Angriffe noch verheerender werden, wenn sie sorgfältig angepasst und individuell mit einer Spear Phishing-E-Mail gesendet werden.

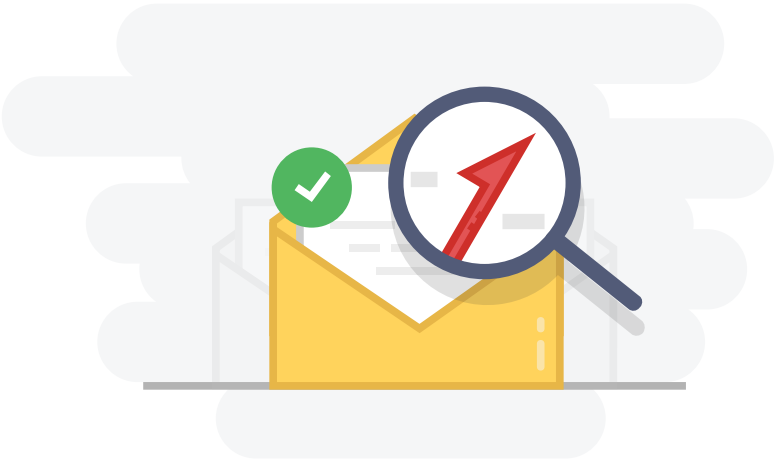
2. Ibid.

SPEAR PHISHING

Spear Phishing ist eine ausgefeiltere Version von Phishing, die bestimmte Mitarbeiter einer Organisation im Fadenkreuz ins Visier nimmt. Ziel ist in der Regel, unbefugten Zugriff auf Netzwerke, Daten und Anwendungen zu erreichen. Im Gegensatz zum Ansatz von Phishing mit Massen-E-Mails, bei denen binnen weniger Stunden Hunderttausende von Angriffsnachrichten an zufällig ausgewählte Empfänger gesendet werden, richtet sich Spear Phishing an einen einzelnen, methodisch eingekreisten Empfänger. Oft enthält die einleitende E-Mail keinen URL und keine Anlage. Vielmehr wird damit einfach versucht, eine Antwort zu provozieren und eine „Unterhaltung“ zu provozieren, um den Empfänger einzulullen und ihm das Gefühl zu geben, dass der Absender unabhängig von der Rolle, die er vorgibt, legitim ist. Erst später werden die Hacker vertrauliche Anmeldedaten oder Informationen verlangen oder ein URL oder eine Anlage als versteckte Bombe senden.

Die zusätzliche Personalisierung und gezielte Ausrichtung einer Spear Phishing-E-Mail in Verbindung mit der Abwesenheit leicht erkennbarer, auf schwarzen Listen stehender URLs oder Malware ermöglicht im Allgemeinen die Umgehung von Standardfiltern für E-Mail. Noch schlimmer ist, dass diese Personalisierung zu Klickraten von mehr als 50 Prozent führt![3]

Für eine Demonstration der Arbeitsweise eines Spear Phishing-Prozesses wollen wir einen Angriff auf ein fiktives Unternehmen namens Namenlos AG untersuchen, das 10.000 Mitarbeiter an fünf Standorten in verschiedenen Städten hat. Dieses Unternehmen beschäftigt mehr als 500 Mitarbeiter in der Verwaltung. Hacker möchten Zugriff zu der Datenbank der Namenlos AG erhalten, die Hundertausende von Mitarbeiter-Datensätzen enthält. Sie können dann die vertraulichen Informationen der Mitarbeiter abernten, zum Beispiel die Sozialversicherungsnummern und für Überweisungen genutzte Bankkonten, und diese dann auf dem Schwarzmarkt an Identitätsdiebe verkaufen.



2. Ibid.

Abbildung 2 - Der Fortschritt eines Spear Phishing-Angriffs: Es geht los mit der Suche nach einer Zielorganisation und der Identifizierung einer bestimmten Person innerhalb der Organisation. Dann folgt eine Reihe von E-Mails mit der Absicht, Vertrauen bei der Zielperson aufzubauen

Abbildung 2 zeigt den typischen Ablauf eines Spear Phishing-Angriffs. Der erste Schritt des Angreifers besteht in Ermittlungen über Namenlos AG, um ein Gefühl dafür zu bekommen, wie ein Spear-Phishing-Angriff am besten vorzubereiten ist. Nach der Katalogisierung der Führungskräfte im Abschnitt „Unser Team“ auf der Website von Namenlos AG erstellen die Angreifer Querverweise mit persönlichen Diagrammen unter Verwendung von Facebook- und LinkedIn-Konten, um Listen zu erstellen, aus denen hervorgeht, welche Personen sich bei Namenlos AG kennen. Dann werden die persönlichen Informationen zusammengesetzt, und die Angreifer können zum Spear Phishing übergehen.

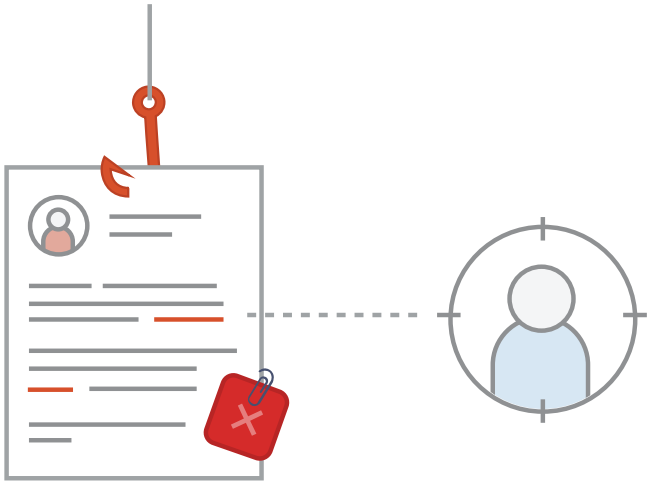
Die Angreifer finden einen Mitarbeiter in der Personalabteilung von Namenlos AG namens Hans Niemand. Die Hacker geben sich als Hans Niemand aus und nehmen Niemands Facebook-Freund und Kollegen Fritz Flieger, einen Personalmanager bei Namenlos AG, ins Visier, um Vertrauen in die gefälschte E-Mail-Adresse aufzubauen, und senden an dessen „Freund“, Hans Niemand, eine Nachricht mit der Frage zu dem Ferienort, an dem er sich derzeit mit seiner Familie befindet (wie aus Bildern hervorgeht, die auf Facebook veröffentlicht wurden). Falls Fritz Flieger antwortet, ist das ein guter Anfang für den Hacker. Er hat sich erfolgreich als anderer Mitarbeiter von Namenlos AG ausgegeben und beginnt, bei seiner Zielperson Vertrauen in die gefälschte E-Mail aufzubauen. Fritz Flieger antwortet und sagt, dass ihm seine Zeit mit der Familie im Urlaub gut tut. Die beiden witzeln weiter über den Familienurlaub von Fritz Flieger und über Vorgänge im Büro unter der Nennung der Namen von Leuten, über die nachgeforscht wurde und die mit dem sozialen Umfeld assoziiert sind.

Wie kann der Angreifer damit durchkommen? Hat Hans Niemand nicht eine eindeutige, domain-spezifische E-Mail-Adresse bei Namenlos AG? Schon. Aber wegen der „Bring Your Own Device“ („BYOD“) genannten Politik von Namenlos AG können Mitarbeiter ihre eigenen mobilen Endgeräte verwenden, um sich gegenseitig Nachrichten zu senden. In diesem Fall weiß der Angreifer aus LinkedIn, dass Hans Niemand eine persönliche E-Mail-Adresse hat, hansniemand1@gmail.com. Der Angreifer legt ein Gmail-Konto für hansniemand.1@gmail.com an. Fritz Flieger bemerkt den Unterschied nicht, und damit ist die Bühne frei für den wirklichen Angriff.

Aus LinkedIn wissen die Hacker, dass Johanna Wichtig eine neue Mitarbeiterin von Fritz Flieger ist. Der Hacker gibt sich als Hans Niemand aus und sendet an Fritz Flieger eine pdf-Datei mit Papieren für die neue Mitarbeiterin, in der ein Tasten-Protokollierer („Key Logging Malware“) versteckt ist. Wenn Fritz Flieger die Datei öffnet, wird sein Gerät direkt infiziert, seine Anmeldedaten werden abgegriffen, und der Einbruch ins Netzwerk ist perfekt.

Eine Alternative wäre, dass Hans Niemand folgende Nachricht sendet: „Hallo, Fritz, ich bin am Golfplatz, aber ich muss die Bank anrufen und sicherstellen, dass der Pensionsplan von Johanna Wichtig eingerichtet wurde. Mir fällt das Login für die Mitarbeiterdatenbank nicht ein — kannst Du mir aushelfen?“ Wenn Fritz Flieger sein Login für die Datenbank mitteilt, hat es der Hacker geschafft. So oder so kann der Phisher Hans Niemands Login-Daten abgreifen und hat freien Eintritt, um in die privaten Netzwerke von Namenlos AG einzudringen. Es besteht die Gefahr, dass unbefugter Zugriff auf alle vertraulichen Mitarbeiterdaten erfolgt.

In diesem Fall haben wir ein Beispiel aus der Personalabteilung verwendet, aber es hätte ebenso leicht die Finanzabteilung, Marketing und Vertrieb oder jede andere Abteilung treffen können. Die meisten Mitarbeiter haben so viele persönliche Informationen über sich im öffentlich zugänglichen Bereich, dass ihre Identität verwendet werden kann, um andere Mitarbeiter zu täuschen und Ihr Netzwerk zu kompromittieren.



GESCHÄFTLICHE AUSWIRKUNGEN VON SPEAR PHISHING

Welche geschäftlichen Auswirkungen hat ein solcher Störfall? Die Auswirkungen können unterschiedlich sein, aber vergrößern sich im Allgemeinen abhängig von der Raffinesse des Angreifers und der Größe des Ziels. Denken Sie an die finanziellen Auswirkungen eines Hackers, der Zugriff auf Ihre kritischen Daten erlangt. Was kann er/sie damit anstellen?

Beispiel: Sony Pictures

Als Beispiel möge der Fall von Sony Pictures 2014 dienen. Das Unternehmen erlitt einen hochgradigen Schaden seiner Reputation, als private E-Mail-Korrespondenz zwischen Führungskräften peinliche Bemerkungen über berühmte Persönlichkeiten offenbart wurde. Das Studio verlor die Kontrolle über fertig gestellte, noch nicht freigegebene Filme, die digitalen Piraten in die Hände fielen und übereilt vermarktet werden mussten. Potenzielle Einkünfte in Millionenhöhe gingen verloren. Die Marke Sony war beschädigt, was Einfluss auf ihre Bewertung und auf die Fähigkeiten für Geschäftsabschlüsse in Hollywood hatte. Mitbewerber gewannen Insiderwissen über die Vorgänge im Studio. Schließlich entstanden dem Unternehmen direkte Kosten, zum Beispiel 8 Millionen Dollar zur Beilegung von Prozessen mit Mitarbeitern, die gezwungen waren, nach dem Vorfall ihre Identitäten gegen Diebstahl zu schützen.[4]

Spear Phishing-Angriffe sind häufig nur der erste Teil einer weitaus breiter angelegten Hacker-Kampagne. Sind Hacker erst einmal ins Netzwerk eingedrungen, können sie verheerende Schäden anrichten, indem sie in vertraulichen Kundenlisten, geistigem Eigentum und E-Mails wühlen oder sogar kritische Daten löschen oder mit Ransomware verschlüsseln.

Firmen, die wegen Spear Phishing Hacking zum Opfer fallen, sind den Gefahren von Rufschädigung, Verlust von Marktwert, Wettbewerbsnachteilen, Schadenersatzforderungen und Compliance-Problemen ausgesetzt. Und natürlich können die Karrieren von Führungskräften im Gefolge solcher Vorfälle auf dem Spiel stehen.

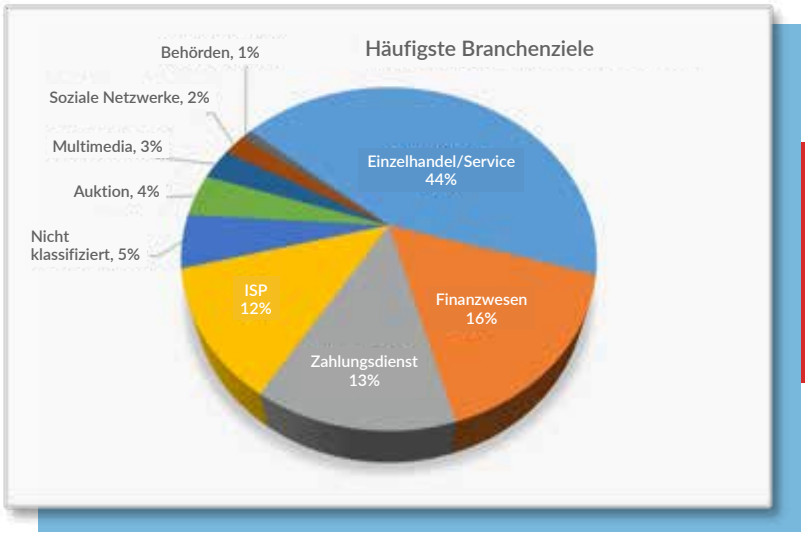


Abbildung 3 – Angriffe nach Branchen, 2. Quartal 2016

(Quelle: APWG Global Phishing Report 2Q 2016)

4. Brandom, Russell, „Sony Pictures will pay up to $8 million to settle hack lawsuit with employees“ [Sony Pictures hat bis zu 8 Millionen Dollar zu zahlen, um den Hacker-Prozess mit Mitarbeitern beizulegen], The Verge, 20. Oktober 2015

Risiken nach Branchen

Finanzdienstleistungen: Finanzfirmen müssen Spear Phishing-Risiken managen, die zum Diebstahl von Informationen über Insiderhandel, persönlich zuordenbare Informationen, Kreditkartennummern, Bankverbindungen und mehr führen könnten. Zu den Auswirkungen zählen finanzielle Verluste, Schadenersatz und Bußgelder der Aufsichtsbehörden.

Einzelhandel: Wie mehrere Hacker-Angriffe in großem Maßstab kürzlich gezeigt haben, sind Einzelhändler bei Angriffen verwundbar, bei denen Kundendaten einschließlich Informationen zu Kreditkarteninhabern abgegriffen werden. Damit bekommen die Händler Schwierigkeiten mit den PCI-Vorschriften, die Bußgelder und kostspielige Geldstrafen für die Wiederherstellung der Compliance nach sich ziehen. Sie riskieren auch den Verlust von Kundenvertrauen und Markenwert, die über viele Jahre mit hohen finanziellen Kosten aufgebaut wurden. Außerdem tragen Händler auch ein indirektes Spear Phishing-Risiko, nämlich die Haftung für Betrug aus Käufen, die mit gestohlenen Kreditkartennummern getätigt wurden. Das mag trivial klingen, ist es aber nicht. Ermittlungen zeigen jetzt das Vorhandensein von ziemlich groß angelegten Raubzügen, bei denen Waren aus E-Commerce-Sites gestohlen und massenhaft ins Ausland versandt werden.[5]

Unternehmen im Bereich des geistigen Eigentums: Für Unternehmen, zum Beispiel in der Pharmaindustrie oder Technologie, bei denen digitale Informationen für massive Investitionen stehen können, kann Spear Phishing besonders kostspielige Auswirkungen haben. Mitbewerber können Zugriff auf vertrauliches geistiges Eigentum erhalten, für dessen Entwicklung viele Jahre und Kosten von Milliarden von Dollars erforderlich waren.

Industrielle Produktion und Landesverteidigung: Strategische industrielle Produktionsunternehmen und Auftragnehmer in der Rüstungsindustrie sind durch privat oder staatlich betriebene Industriespionage verwundbar. Unternehmen in der Rüstungsindustrie sind häufig Ziele von Angriffen ausländischer Staaten, zum Beispiel durch die Cyberkrieg-Einheiten fremder Mächte. Diese Unternehmen sind an einem tatsächlichen, nicht erklärten Cyberkrieg beteiligt, der trotz seines ruhigen, weitgehend unsichtbaren Profils erhebliche Schäden anrichtet. Insbesondere solche Unternehmen haben die Tendenz, derartige Verletzungen möglichst geheim zu halten, so dass es in dieser Branche wahrscheinlich wesentlich mehr erfolgreiche Angriffe gibt, als der Öffentlichkeit bekannt ist. Die Auswirkungen von Cyberspionage durch ausländische Staaten sind nicht leicht zu quantifizieren, doch könnte ein schwerwiegender Vorfall die nationale Sicherheit gefährden und die Fähigkeit eines Unternehmens beeinträchtigen, weitere Verträge im Bereich der Landesverteidigung zu erhalten.

Gesundheitswesen: Organisationen, die den Vorschriften des US-amerikanischen HIPAA („Health Insurance Portability and Accountability Act“) unterliegen, müssen umfangreiche und strikte Compliance-Richtlinien beachten. Bei Verletzungen des Datenschutzes sind sie mit strengen finanziellen und juristischen Bußen konfrontiert. Angesichts der Sensibilität von Patientendatenlecks bestehen Risiken für die Reputation. Wie mehrere große Krankenversicherungen kürzlich entdeckt haben, kann der Schutz gegen Identitätsdiebstahl erhebliche Kosten verursachen, wenn Namen, Adressen und Sozialversicherungsnummern von vielen Millionen Versicherten kompromittiert sind.

5. APWG Global Phishing Report 2Q 2016

WARUM SIND SO VIELE ORGANISATIONEN ANFÄLLIG FÜR VON E-MAIL VERBREITETE BEDROHUNGEN?

Das Problem besteht darin, dass für Office 365 entwickelte E-Mail-Filtersysteme wie EOP, Proofpoint, McAfee und Barracuda die typische Spear Phishing-E-Mail NICHT abfangen. Die Architekturen all dieser E-Mail-Sicherheitssysteme (genau wie die überwiegende Anzahl anderer Standard-E-Mail-Sicherheitssysteme) wurden ursprünglich zur Bekämpfung von Spam entwickelt. Daher konzentrieren sie sich auf Massen-E-Mail und verwenden dafür eine Signaturtechnik, um verdächtige E-Mails und bekannte Malware-Anhänge und Phishing-URLs zu blockieren.

Diese Prozesse sind bei der Bekämpfung von Spam zwar überaus erfolgreich, doch nicht sehr nützlich beim Kampf gegen Spear Phishing. Eine einmalige, gut redigierte E-Mail umgeht im Allgemeinen die meisten Spamfilter von Unternehmen, da sie keine Ähnlichkeit mit als „bösartig“ bekannten Signaturen aufweisen.

Standard-E-Mail-Sicherheit ist OK, wenn es um Angriffe mit Massenspam geht ...

Die von der Spam-E-Mail-Sicherheit abgeleiteten Systems arbeiten zur Abwehr der meisten Versuche massenhafter Phishing E-Mail befriedigend, da sie neue Varianten von Phishing-Angriffen blockieren können, nachdem die ersten paar Zehntausend solcher E-Mails gesendet wurden und die ersten Berichte dazu zurückgemeldet werden. (Das ist natürlich nur ein schwacher Trost, falls einer Ihrer Mitarbeiter das Glück hatte, eine dieser ersten Exploits zu empfangen ...)

... aber zum Blockieren raffinierter Spear Phishing-E-Mails absolut untauglich.

Signaturbasierte E-Mail-Sicherheit ist jedoch absolut unwirksam bei der Abwehr von raffinierten, einmaligen, gezielten Spear Phishing-Attacken und Tag-Null-Malware, den primären Bedrohungen der Sicherheit Ihres Netzwerks.

Das moderne Unternehme benötigt ein zweckorientiertes E-Mail-*Sicherheits*-System, das alle per E-Mail transportierten Bedrohungen stoppt ... nicht nur einen überbewerteten Spamfilter.

WAS IST LOS MIT MICROSOFT EXCHANGE ONLINE PROTECTION (EOP)?

Wie schon gesagt, kann EOP gegen *bekannte* Bedrohungen einen gewissen Schutz bieten. Das Problem besteht darin, dass es bei der Bekämpfung unbekannter Bedrohungen fast völlig hilflos ist, mögen diese aus einem in einer Excel-Datei verborgenen Tag-Null-Code oder aus eine Spear Phishing-Attacke mit kompromittierten Geschäfts-E-Mails (Business Email Compromise - „BEC“) stammen.

Was EOP aus einer Sicherheitsperspektive gesehen verpasst:[6]

- die Fähigkeit, neue und sich entwickelnde Bedrohungen zu identifizieren, für die keine bekannte Signatur vorliegt;
- die Fähigkeit, *alle* Anlagen, zum Beispiel zip-Dateien, in einer Sandbox zu isolieren;
- Sandbox-Isolierung von URLs in Echtzeit, um sicherzustellen, dass Links sicher und gegen URL-Zeitbomben geschützt sind;
- robustes Anti-Spoofing;
- Benachrichtigungen für Verwaltung und Benutzer im Fall eines Verdachts versuchten Phishings.

In mehr oder weniger großem Umfang bauen praktisch alle anderen E-Mail-„Sicherheits“-Systeme wie McAfee, Barracuda und Proofpoint auf Spamfiltertechnologie auf und haben dieselben Sicherheitsschwächen, insoweit sie unbekannte Bedrohungen nicht zuverlässig identifizieren können, darunter Spear Phishing-Angriffe oder unbekannte Malware, die sich als nicht ausführbare Datei darstellt. Obwohl manche dieser Anbieter behaupten, über bestimmte Analysetechniken zu verfügen, mit denen BEC entdeckt werden kann, sind sie doch nur in der Lage, schwerfällige Fälschungen zu entdecken, zum Beispiel bei einem Unterschied zwischen den Domains *„From“* und *„Reply-to“* oder einer internen Domain. Diese Arten der Analyse sind sehr schlicht und können von einigermaßen raffinierten Hackern leicht umgangen werden.

6. EOP lässt auch manche nette Optionen aus, zum Beispiel effektive Einordnung von Graymail (E-Mail mit niedriger Priorität), Abmeldungen mit nur einem Klick oder Archivierungsfunktionen.

Vergleich von Anbietern

	Proofpoint Essential	McAfee	Vade Secure	Barracuda	EOP
Bekannte Bedrohungen					
Einfacher, signaturbasierter Schutz für bekannte Bedrohungen	√	√	√	√	√
Spam auf Schwarzer Liste	√	√	√	√	√
Malware auf Schwarzer Liste	√	√	√	√	√
Phishing auf Schwarzer Liste	√	√	√	√	√
Unbekannte Bedrohungen					
Entdeckung von Tag-Null-Malware/-Phishing/-Spam					
Einfaches Maschinenlernen und Heuristik	√		√		
Komplexe Reputationsanalyse	√		√		
Fortgeschrittene KI-basierte Analyse			√		
Anti-Phishing Entdeckung und Schutz					
Echtzeit URL-Erkundung			√		
Schutz gegen URL-Zeitbomben	√		√	√	
Anforderung sensibler Daten			√		
Exaktes Anti-Spoofing	√		√		
Anti-Spoofing ähnliche Absender			√		
DKIM-Absenderauthentifizierung	√	√	√	√	√
SPF-Absenderauthentifizierung	√	√	√	√	√
Komfort					
Einordnung von E-Mail mit geringer Priorität	√		√		
Abmelden in einem Schritt	√		√		
Abmelden mit erweiterten Funktionen			√		
Archivieren	√	√		√	
SMTP-Speicherung	√	√	√	√	√
Einführung					
Cloud/SaaS	√	√	√	√	√
Vor Ort	√	√	√	√	
Installation in 30 Minuten			√		
Kompatibel Exchange	√	√	√	√	√
Kompatibel Office 365	√	√	√	√	√
Kompatibel Google Apps	√	√	√	√	
Zimbra (Zimlet)			√		
cPanel-Plugin			√		

MEHR ALS SIGNATURBASIERTER SCHUTZ

Vade Secure hat schon vor einigen Jahren erkannt, dass ein signaturbasiertes Filtersystem eine sich stetig beschleunigende, immer in der Sackgasse endende Sysiphus-Arbeit ist. Was wirklich nötig ist, ist eine flinke Verteidigung, die ausgehend von vorhergehenden Mustern brandneue Bedrohungen erkennen kann. Kurz gesagt, benötigt wurde künstliche Intelligenz („KI"), die speziell trainiert worden ist, um diese Tag-Null-Bedrohungen ausfindig zu machen.

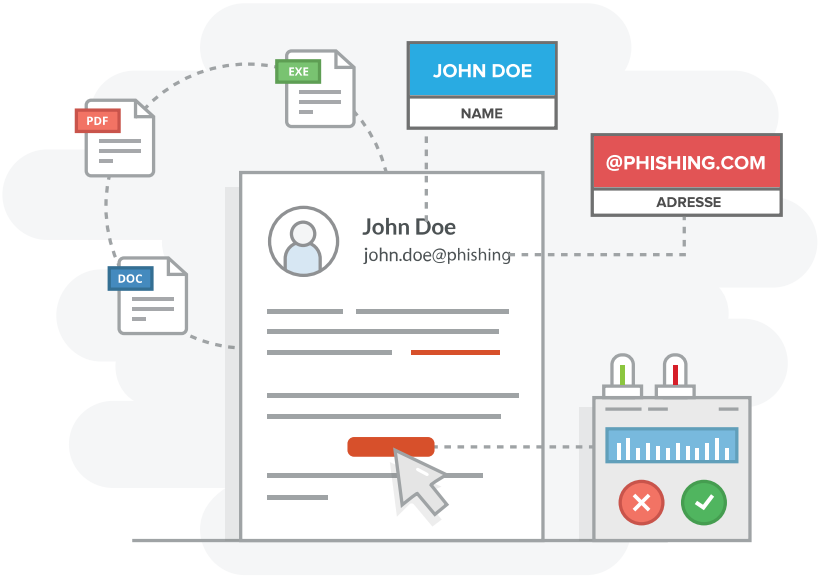
Vade Secure verarbeitet täglich viele Milliarden E-Mails. In Europa nehmen wir eine beherrschende Stellung ein (zum Beispiel strömen mehr als 90 Prozent des gesamten französischen E-Mail-Verkehrs durch unsere Filter); in Nordamerika und weltweit sind wir stark vertreten.

Dadurch verfügten wir über sehr große Datenmengen, um mit dem Training unseres KI-Systems zu beginnen, damit es lernt, wie bösartige E-Mails, Phishing-Sites und Malware aussehen und an welchen Stellen sie sich verändern. Gegenwärtig ist unser System in der Lage, einmalige Spear Phishing-E-Mails, Anforderungen sensibler Daten und in ausführbaren Dateien, PDF-Dateien, Office- und anderen Dokumenten versteckte Malware zuverlässig zu identifizieren.

Vade Secures maschinelles Lernen verbessert sich konstant und gewinnt an Komplexität. Neue, diese Bedrohungen betreffende Regeln und Informationen werden in unseren Gateways für E-Mail-Sicherheit laufend aktualisiert und weltweit 24/7 in unseren Zentren für globale Bedrohungsbewertung eingesetzt.

Künstliche Intelligenz und herkömmliche Filter

Vade Secures KI-System wird durch eine weitreichende Kette zusätzlicher Absicherungen ergänzt, darunter herkömmliche, signaturbasierte Spamfilter, eine umfangreiche schwarze Liste, die ein sehr großer OEM-Kunde das „Beste, was wir kennen" genannt hat, und zwei Virenscanner zur Verstärkung.



Vade Secures Lösung

Die komplette E-Mail-Lösung von Vade Secure deckt Spam, Graymail-Einstufung und die robusteste E-Mail-Sicherheitslösung des Markts ab.

Anfängliches Filtern: E-Mails werden auf bekannte Phishing- und Malware-Signaturen einschließlich ausführbarer Dateien analysiert. Damit werden alle Spam- und Massenangriffe schnell ausgemerzt.

Anti-Malware:

- Wir lesen den eingebetteten Code nicht nur in ausführbaren Dateien, sondern auch in Office-Dokumenten, PDF-Dateien und mehr.
- Dieses tiefgestaffelte, proprietäre Verteidigungssystem wird durch zwei ergänzende Antivirus-Lösungen verstärkt.

URL-Sandboxing: Alle URLs werden untersucht, um sicherzustellen, dass sie keinen Link zu Malware, Phishing-Sites oder anderen bösartigen Sites herstellen. Anders als andere Software zur URL-Behandlung untersucht Vade Secure den URL sowohl bei seinem ersten Empfang im System als auch, sobald ein Benutzer versucht, auf einen Link zu klicken; damit werden URL-Zeitbomben entschärft.

Künstliche Intelligenz: Alle verbleibenden Nachrichten werden auf *unbekannte* Malware- und Phishing-Taktiken analysiert, um Spear Phishing- und Tag-Null-Angriffe zu verhindern, die andernfalls durch die Filter rutschen könnten. Unsere regelbasierte Software beruht auf mehreren Milliarden E-Mails pro Tag und lernt und verbessert sich dadurch laufend.

- **Überprüfung der Identität:** Unser Identity Match™-System zieht Hunderte subtiler technischer und verhaltensbezogener Faktoren in Betracht, um festzustellen, ob die Absender diejenigen sind, die sie zu sein behaupten, um Schutz gegen E-Mail-Betrüger zu bieten.
- **Domain-Überprüfung:** Die Domain des Absenders wird doppelt auf Authentizität geprüft.
- **Inhaltsanalyse:** Vade Secure führt eine tiefgreifende Analyse jeder E-Mail aus, um Versuche von Hackers zu finden, persönliche Informationen zu stehlen. Die KI-Software gibt eine Warnung aus, wenn in der E-Mail Anforderungen von sensiblen Daten enthalten sind, zum Beispiel die Bitte um persönliche Informationen oder Anmeldedaten.

Menschliche Intelligenz: Vade Secure unterhält 24/7 ein globales Bedrohungsinformationszentrum mit E-Mail-Sicherheitsspezialisten. Diese überwachen die eingehenden Informationen permanent, damit wir neue, interessante Bedrohungen identifizieren können.

Spamkontrolle: Vade Secure erreicht eine Fangrate von 99,99 Prozent mit einer **False-Positive-Fehlerrate von praktisch 0 Prozent** (<0,00001 Prozent).

Management von kommerziellen E-Mails/Graymail: Ihre Kunden werden sich über die Einordnung kommerzieller E-Mails und automatische Abmeldungen mit einem Klick freuen.

Optionen bei der Einführung:

Die Einführung von Vade Secure ist einfach. Es kann auf Ihrem Office 365-System in weniger als zehn Minuten entweder als *zusätzlicher* Sicherheitsprozess neben vorhandenen Lösungen wie EOP oder Barracuda oder als *Ersatz* solcher Lösungen installiert werden.

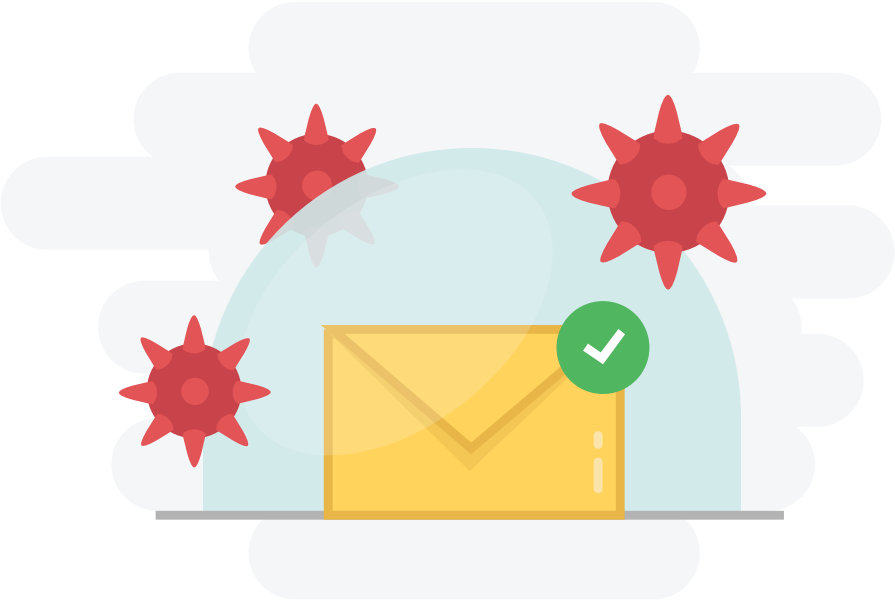
Anti-Spam, anfängliches Filtern und Malware-Ermittlung sind bei der Einführung alle sofort zu 100 Prozent effektiv. Eine Lernphase ist nicht erforderlich. Die Ermittlung von Spear Phishing startet mit einer Effektivität von rund 90 Prozent. Die maximale Effektivität wird nach etwa zwei Wochen erreicht, in denen sich das System selbständig auf die spezifischen Gewohnheiten und Stile Ihrer Organisation einstellt.

Zusätzliche Plug-in-Module sind für Unternehmens-Gmail und Zimbra lieferbar. Vade Secure ist als Cloud-Service oder als Gateway auf Ihrem eigenen Server lieferbar.

FAZIT

Die Abwehr von Phishing, insbesondere in der Variante Spear Phishing, ist ein nicht enden wollender Prozess. Tagtäglich kommen in jeder Organisation frische Versionen der Bedrohung in den Inboxen der Mitarbeiter an. Gegenmaßnahmen müssen stark, aber auch anpassungsfähig sein. Künstliche Intelligenz und spezialisierte E-Mail-Sicherheit sind für die Aufrechterhaltung der Sicherheit Ihrer Organisation entscheidend.

Wenn die bösen Jungs es schaffen, auch nur eine E-Mail einzuschmuggeln, kann das verheerende Ergebnisse haben.



Über Vade Secure

Vade Secure ist der globale Marktführer bei Anti-Phishing-Software und bietet einen kompletten Satz von Sicherheitsfunktionen gegen Phishing, Malware und Spam an. Dem Unternehmen wird der Schutz von mehreren hundert Millionen Mailboxes weltweit anvertraut. Dieses breite Einsatzspektrum hat Vade Secure einzigartige Einsichten in die Art von bösartigen E-Mails verschafft. Das sich daraus ergebende proprietäre Wissen ermöglicht Vade Secure, umfassende Lösungen im Kampf gegen E-Mail-Bedrohungen aller Art zu liefern, mit denen selbst kleine E-Mail-Schwemmen ab Tag Null geschützt werden. Vade Secure ist auch führend bei generellerem Filtern von E-Mail und stellt dafür einen umfassenden Satz produktivitätserhöhender Tools zur Verfügung, um die als Graymail bekannten kommerziellen E-Mails zu managen. Die Lösungen von Vade Secure sind maßgeschneidert für ISPs, OEMs, Hosting-Firmen und Unternehmen im Allgemeinen.

Weitere Informationen zu
Vade Secures AI-basierter E-Mail-Sicherheit
finden Sie bei uns unter www.vadesecure.com
oder wenn Sie uns anrufen: +1 (415) 745 3630.