Schützen Sie Ihren Brand vor Phishing E-Mails indem Sie DMARC einsetzen[1]

Dringende Empfehlung der CSA von AOL, Microsoft und Google befürwortet

Im folgenden Artikel möchten wir erläutern, warum Marketeers DMARC implementieren sollten, um sich vor Phishing zu schützen. Aussagen und Interviews relevanter internationaler ISPs untermauern unseren Standpunkt. Für diejenigen, die einen technischen Gesamtüberblick bekommen möchten, haben wir DMARC auch im Rahmen der technischen Zustellung betrachtet.

Ist Phishing heutzutage relevant? Welche Firmen sind betroffen?

Mit der steigenden Anzahl von E-Mails und neuen Methoden der Spammer und Phisher, müssen sich ISPs immer mehr der Herausforderung stellen, zu bewerten, ob eine E-Mail angenommen oder abgelehnt werden sollte. Laut Kaspersky Labs, "wird Spam besonders problematisch, wenn es dazu verwendet wird, Malware zu verbreiten oder Phishing zu betreiben. Im ersten Quartal 2015 wurde auf den Computern der Kaspersky Lab Nutzer im Anti-Phishing System 50 077 057 Mal Alarm ausgelöst. Das ist eine Million Mal mehr als im vorangegangenen Quartal."[2] Andere Berichte betonen ein in der Tat zunehmendes Risiko für Geschäftsdaten durch E-Mail-basierte Malware.[3]

"42% der Befragten sind der Auffassung, dass ihr Brand einen großen Vertrauensverlust hinnehmen müsste, wenn sie eine Phishing E-Mail empfangen würden, die vorgibt, von diesem Unternehmen zu kommen."[4]

Die meisten Attacken konzentrieren sich auf Banken, Online-Shops und elektronische Zahlungssysteme. Doch dies ist noch nicht alles. In Q1 2015 hat Kaspersky eine neue Kategorie "Zustellfirmen" in seine Beurteilung aufgenommen, die kürzlich ein starkes

1 DMARC = Domain-based Message Authentication, Reporting and Conformance of messages (https://dmarc.org)
2 https://business.kaspersky.com/spam-and-phishing-in-q1-2015-banks-and-banking-trojans/4113/
3 http://pages.cyren.com/TrendReport_2015Q1.html?utm_campaign=ALL_ALL_2015_Q1_Trend_Report&utm_medium=press_release&utm_source=press_release
4 https://www.cloudmark.com/en/press/reputation-of-uk-brands-dramatically-affected-by-phishing-attacks-according-to-survey-commissioned-by-cloudmark

Wachstum verzeichnen konnte(+0.04). DHL, eine der Firmen dieser Kategorie, war unter den Top 100 Organisationen mit den meisten Phishing Attacken.[5]

"Neben den zuvor genannten attraktivsten Branchen ist jeder Brand ein potenzielles Ziel, der einen guten Ruf basierend auf Verbrauchervertrauen innehat. Firmen, die in Branding investiert haben, stehen vor der Herausforderung, dass ihre vertrauensvollen Kunden E-Mails erhalten, in denen persönliche Angaben oder sogar Zahlungsinformationen abgefragt werden" sagt Alexander Zeh, Engineering Manager und verantwortlich für die technische Zertifizierung bei der CSA.

Wie kann DMARC Brands vor Phishing Attacken schützen?

Mit Hilfe von DMARC und den verwandten Technologien Sender Policy Framework (SPF) und DomainKeys Identified Mail (DKIM) hat ein Brand die Möglichkeit, seine E-Mails für einen ISP klar erkennbar zu machen und zugleich festzulegen wie der ISP E-Mails handhaben sollte, die nur vorgeben von dem Brand zu stammen. Infolgedessen können Phishing E-Mails zuverlässig von den ISPs erkannt und gefiltert werden bevor sie den Empfänger erreichen. Im Gegensatz zu klassischen Ansätzen, die auf Content-Filtern basieren, kann schon eine einzelne Phishing E-Mail identifiziert und geblockt werden.

5 https://business.kaspersky.com/spam-and-phishing-in-q1-2015-banks-and-banking-trojans/4113/

Warum internationale ISPs von Marketeers die Implementierung von DMARC fordern

AOL:

"DMARC ermöglicht mehr Sicherheit, wobei Phishing ein schwerlösbares Problem darstellt. Ein hoher Anteil von Phishing Mails wird noch immer an Nutzer zugestellt. Durch die Anwendung von DMARC mit entsprechender Policy und Reporting kann die Anzahl gefälschter E-Mails auf nahezu Null reduziert werden.

DMARC funktioniert heute, also implementieren Sie es auch heute! Verbessern Sie Ihre Zustellbarkeit, und pflegen Sie eine gute Beziehung zur ISP Community. Tun Sie dies nicht, so konkurrieren Sie mit den bösen Jungs, die auch versuchen, nicht wie böse Jungs auszusehen."

Marcel Becker
Director Product, Mail
AOL

Microsoft:

"Mit der steigenden Anzahl von E-Mail Bedrohungen und Spearphishing sollte jedes Unternehmen eine E-Mail-Authentifizierung, insbesondere DMARC, mit hoher Priorität umsetzen um seine Kunden, Mitarbeiter und seinen Brand zu schützen.

E-Mail Authentifizierung und eine strenge DMARC Policy können Sie vor einer Rufschädigung durch Spoofing Ihrer Domain schützen. Da große E-Mail Empfänger zunehmend auf Domain-basierte Reputation vertrauen, ist dies entscheidend für die kontinuierliche Zustellbarkeit Ihrer E-Mail."

Terry Zink
Program Manager
Microsoft Corporation

Google:

CSA: *"Sollten E-Mail Versender Ihrer Meinung nach DMARC implementieren? Wenn ja, warum?"*

Sri Somanchi: *""Ja, es ist eine einfache Möglichkeit um sicher zu stellen, dass ihre Domain (und der Brand) nicht durch gefälschte E-Mails gefährdet wird und E-Mail Nutzer vor Phishing Angriffen geschützt werden."*

CSA: *"Können E-Mail Versender mit einer besseren Zustellbarkeit rechnen, nachdem sie DMARC implementiert haben? Welchen Vorteil sehen Sie hier für die Versender, und wie geht Google mit Versendern um, die DMARC nicht einsetzen?"*

Sri Somanchi: *"Während Zustellbarkeit und DMARC in keiner direkten Beziehung zueinander stehen, steigert der von DMARC gebotene Identitätsschutz das Vertrauen des Empfängers in den Absender und verhindert dabei, dass der Anwender die E-Mail irrtümlicherweise als Spam markiert. DMARC sorgt außerdem dafür, dass die Reputation des Versenders nicht durch gefälschte E-Mails zu leiden hat."*

Sri Somanchi
Google

Fazit:

Durch die Implementierung von DMARC können Marketeers sicherstellen, dass ihre Identität nicht missbraucht wird. Dieser Missbrauch könnte einen großen Schaden der ISP Infrastruktur und der Markenreputation verursachen und bei dem Brand in einem Vertrauensverlust seitens der Kunden resultieren.

Marketeers im Bereich E-Mail Marketing sollten das Thema der Implementierung von DMARC bei Ihrem E-Mail Service Provider ansprechen. Die Certified Senders Alliance bietet zu diesem Thema Informationen und Unterstützung auf dem CSA Summit vom 20-22 April 2016 in Köln, Deutschland, an.

Anhang

Wie DMARC in das antispam und anti-phishing Toolkit der ISPs passt

Sehen wir uns die Wertschöpfungskette an. Es gibt immer ein Unternehmen (Brand), das eine E-Mail an einen Empfänger zustellen möchte. Manchmal nimmt sich der Brand einen Email Service Provider (ESP) zu Hilfe, der die technische Auslieferung übernimmt. Der Internet Service Provider (ISP), dem die Mailbox des Empfängers gehört, muss entscheiden, ob er die E-Mail entgegen nimmt oder ablehnt.

Der Postausgangsserver des E-Mail Service Providers verbindet sich mit dem Posteingangsserver des ISPs. Der ISP sieht die IP-Adresse des Verbindungsservers.

Entlang der E-Mail Wertschöpfungskette gibt es Unterschiedliche Kommunikationslevel zwischen den Servern. Je höher das Level, desto ausgefeilter die Kommunikation und somit die Wahrscheinlichkeit der Zustellung bzw. des Schutzes vor Phishing.

1. Einfache Kommunikation: Die "Envelope" Prüfung:

   Der E-Mail Server des ISPs überprüft im Domain Name System, ob die IP-Adresse wirklich zum Host Domain Namen gehört, wie im HELO angegeben. Auch wenn diese Überprüfung erfolgreich abläuft, ergeben sich für den ISP Probleme in Bezug auf die eindeutige Identifizierung des Versenders: IP- Adressen können weitergegeben oder geteilt werden, so dass es viele Brands geben könnte, die von dieser IP senden oder gesendet haben. Außerdem könnte der Domain Name gefälscht sein.

   Fazit: ISPs verlassen sich nicht auf diese einfache Art der Kommunikation, wenn es

darum geht, eine E-Mail zuzustellen oder nicht, da die IP-Adresse gefälscht sein könnte oder mehrere Domains einer IP-Adresse zugeordnet sein können. Ersteres gilt auch für den Host Domain Namen. Des Weiteren haben sie zu dem Zeitpunkt noch keine Information über die Mailfrom Domain erhalten. **Somit wird die E-Mail eventuell nicht zugestellt.**

2. Erweiterte Kommunikation: Die "Header" Prüfung:

   ISPs überprüfen die Mailfrom Domain der E-Mail, um herauszufinden, wer diese tatsächlich verfasst hat. Ein Problem besteht jedoch nach wie vor: Die Mailfrom Domain könnte von jemandem missbraucht werden, der vorgibt der Besitzer der Domain zu sein.

   Fazit: ISPs verlassen sich bei der Entscheidung, eine E-Mail zuzustellen oder nicht auf diese Form der erweiterten Kommunikation. **Folglich wird die E-Mail eventuell nicht zugestellt.**

3. Erweiterte Kommunikation mit dem **S**ender **P**olicy **F**ramework:

   Die "Envelope" Prüfung ermöglicht den Brands, IP-Adressen im DNS zu listen. Diese sind dann autorisiert für den Versand von E-Mails mit ihrer Mailfrom Domain. Die Auflistung der IP-Adressen kann auch von dem ESP durchgeführt werden wie oben beschrieben. Brands stehen dabei möglicherweise vor der organisatorischen Herausforderung, die gesamte Liste der IP-Adressen zu identifizieren und zugleich jeglichen Missbrauch einer Mailfrom Domain frühzeitig verhindern zu können. Der SPF Failure Report ist ein erforderliches Aufnahmekriterium der CSA.

   Fazit: ISPs verlassen sich nicht allein auf SPF Checks, da ein Brand (Mailfrom Domain Besitzer), der von der gleichen (geteilten) IP versendet wie ein anderer Brand, dessen Markenidentität missbrauchen könnte. Dieses potenzielle Risiko steigt mit der Anzahl des Mailfrom Domain Versandes über die gleichen IPs. **Infolgedessen wird die E-Mail eventuell nicht zugestellt.**

4. Erweiterte Kommunikation mit **D**omain **K**eys **I**dentified **M**ail

   Die "Header mit digitaler Unterschrift" Prüfung: Die digitale Unterschrift eines Brands oder ESPs (mittels der Technik DKIM) ermöglicht es den ISPs zu beweisen, dass die versendende Domain wirklich die ist, die sie vorgibt zu sein. Es gibt zwei Schlüssel, die generiert werden müssen, um DKIM signierte E-Mails versenden zu

können: Ein privater Schlüssel, der dazu verwendet wird, die Unterschrift herzustellen, und ein öffentlicher Schlüssel, mit dem die ISPs die Unterschrift überprüfen können. Der ESP generiert beide Schlüssel und behält den privaten Schlüssel. Der öffentliche Schlüssel muss von dem Brand im DNS bereitgestellt werden. Alternativ kann der Brand dem ESP eine Domain- oder Subdomain Delegation erteilen, der dann die Herausgabe des öffentlichen Schlüssels übernimmt.

Fazit: ISPs vertrauen auf DKIM, da es die eindeutige Identifikation eines Brands ermöglicht. Jedoch kann es weiterhin zu Missbrauch von Schlüsseln kommen. Das DKIM Verfahren ist zwingende Anforderung der CSA Aufnahmekriterien. Nur DKIM und SPF zusammen ermöglichen es den ISPs, eine Entscheidung bezüglich der Zustellung oder Nicht-Zustellung zu treffen basierend auf der realen Mailfrom Domain und der dazugehörigen IP-Adresse. Sind DKIM und SPF nicht eingerichtet, oder die Überprüfung schlägt fehl, kann der ISP nur eine Entscheidung fällen im Hinblick auf die IP-Reputation samt ihrer Problematik in Punkt 1. **Folglich landen die E-Mails mit großer Wahrscheinlichkeit im Spam Ordner.**

5. 5. Moderne Kommunikation mit **DMARC**:

   Die "wie gehe ich mit E-Mails um, bei denen DKIM und SPF fehlschlagen?" DMARC ist eine Policy, die von Brands im DNS der Mailfrom Domain veröffentlicht werden kann. Sie schlägt dem ISP vor, wie er mit E-Mails umgehen sollte, bei denen die DKIM oder SPF Prüfungen fehlschlagen. Mögliche Optionen: „none" (=normale Zustellung), „quarantine" oder „reject". Bei jeder fehlgeschlagenen DKIM oder SPF Prüfung erhalten die Brands einen Bericht, wobei der „Daily Aggregated Report" am häufigsten vorkommt. Gründe für ein Fehlschlagen können auftreten, wenn der Besitzer der Mailfrom Domain teilweise selbst versendet (ohne SPF & DKIM) und zum Teil über einen ESP. Dies kann zu Verwirrung seitens des ISPs führen, dass der Mailstream gefälscht sei und daher geblockt wird. Kurz gesagt, der Bericht ermöglicht den Brands Folgendes:

   - Seine Kunden zu schützen, indem potenziell Phishing und deren Quellen erkannt werden
   - Ihre Infrastruktur zu analysieren und IP-Adressen ohne SPF und DKIM abzuschalten

- DKIM und SPF für IP-Adressen einzurichten, die zu dem Brand gehören und nach erfolgreicher Einrichtung aus zukünftigen Berichten verschwinden werden

In seinem detaillierten Rechtsgutachten über DMARC empfiehlt die eco Kompetenz Gruppe E-Mail deutschen ISPs, „Aggregated Reports“ zu versenden.

Autoren: Julia Janßen-Holldiek, Manager ISP Relations & Business Development