Kurz erklärt: Brand Indicators for Message Identification

Gestempelt

Sven Krohlas

Phishing beschäftigt seit Jahren die IT-Branche und die Anwender. Ein Verfahren namens BIMI soll die Lage verbessern, indem authentifizierte Nachrichten ein verifiziertes Logo erhalten.

Zum Verifizieren von E-Mail-Absendern gibt es seit Jahren ein ganzes Rahmenwerk. Doch weder „Domain-based Message Authentication, Reporting and Conformance“ (DMARC, RFC 7489, siehe ix.de/ix1809117) noch die zugrunde liegenden Verfahren DomainKeys und Sender Policy Framework (SPF) verhindern Phishing-Versuche, wenn die Täter eigene Domains einrichten, die dem Original ähneln. Wer weiß schon, ob sommergewinnspiel-meinebank.de wirklich zu einer offiziellen Kampagne von meinebank.de gehört? Zudem ist DMARC auf E-Mail beschränkt und für viele Markeninhaber mit einem hohen Implementierungsaufwand verbunden, besonders, wenn einzelne Abteilungen eigene E-Mail-Systeme betreiben. Eine Weiterentwicklung sollte also auch den Markeninhabern größere Vorteile jenseits des Phishing-Schutzes bieten, um die Einführungskosten rechtfertigen zu können.

Eine Initiative formiert sich

Die BIMI-Initiative mit den Mitgliedern Microsoft, Google, Oath (AOL, Yahoo), Comcast, Agari, RP, Valimail und PayPal setzt hier an. Das Ziel lautet schlicht, dass die Oberfläche der E-Mail-Clients authentifizierte Nachrichten mit Markenlogo anzeigt. Dies wäre für Nutzer ein einfacher Weg, die Echtheit der Nachricht zu erkennen. Teilnehmende Unternehmen hätten im Erfolgsfall nicht nur mit weniger Beschwerden wegen gefälschter E-Mails zu tun, sondern hätten auch durch die Verbreitung ihrer Markenlogos einen Marketingvorteil.

Der Entwurf des BIMI-RFC findet sich auf GitHub (siehe ix.de/ix1809117). Für E-Mails basiert es auf DMARC. Falls sich der empfangende Mailboxprovider entscheidet, ein verifiziertes Logo anzuzeigen, kann er dessen URL über das DNS der DMARC-Domain erfahren. Hierzu gibt es einen speziellen BIMI Resource Record unter dem DNS-Label <selektor>._bimi (etwa default._bimi.example.com):

```
v=BIMI1; l=https://images.example.7
                        com/somedir/logo.svg;
```

Ein Domaininhaber kann also unterschiedliche Logos veröffentlichen; zudem ist BIMI nicht auf E-Mails beschränkt. Auch andere Dienste können Logos auf diesem Weg beziehen. Dazu müssen sie die Domain der Marke kennen und sicherstellen, dass diese berechtigt ist, das per BIMI verbreitete Logo zu nutzen. Als Basis könnte eine Zertifizierungsinfrastruktur dienen, die den aus der TLS-Welt bekannten Certification Authorities ähnelt.

Die Aufgabe dieser „Mark Verification Authorities“ bestünde darin, zu zertifizieren, dass ein bestimmtes Logo tatsächlich zu einer bestimmten Domain gehört. Hier sind jedoch bisher weder Teilnehmer noch technische Details bekannt. Von Listen verifizierter Domains bis hin zu Signaturverfahren ist vieles denkbar.

Derzeit läuft ein erster BIMI-Test bei Yahoo, für den sich Markeninhaber über eine Website von Agari oder per E-Mail an info@authindicators.org anmelden können (siehe ix.de/ix1809117). Mit dabei sind der US-Versicherer Aetna, Groupon und SparkPost. Die Prüfung auf Korrektheit des Logos übernimmt Yahoo in diesem Pilotversuch noch selbst. Yahoo nutzt die Gelegenheit dazu, strengere DMARC-Policies zu forcieren: Markenlogos bekommen die Anwender nur angezeigt, wenn die Domaininhaber p=quarantine oder p=reject als Policy in ihren DMARC-DNS-Einträgen gesetzt haben – wenn also bei Phishing-Versuchen entsprechende Filtermaßnahmen greifen können.

Markeninhaber können auf diesem Weg sanft dazu gezwungen werden, sich an Best Practices im Mailversand zu halten. Dies wiederum könnte für Nutzer spürbare Vorteile bedeuten – sprich: eine verbesserte Spamfilterung und weniger Phishing-Mails in der Inbox.
Sobald erste Logos angezeigt werden, dürfte die Konkurrenz teilnehmender Marken ebenso motiviert sein, ihre Sichtbarkeit in den Postfächern zu erhöhen und dabei auch ihre Kunden besser als bisher zu schützen. Im internationalen Maßstab haben Google, Microsoft und Oath – die drei größten Mailboxprovider weltweit – eine hinreichend große Kundenbasis, um BIMI damit entscheidend voranzubringen. Falls Microsoft auch Outlook auf dem Desktop anpasst und ein teilnehmendes Unternehmen Erweiterungen für andere populäre Mailclients wie Thunderbird bereitstellt, würde das der Initiative weiter Schub verleihen. Wenn zudem andere Protokolle jenseits der E-Mail-Welt schließlich BIMI integrierten, könnte sich der kommende Standard rasch durchsetzen.

In Deutschland sieht die Situation jedoch anders aus: Hier gibt es mit trusted-Dialog ein für Markeninhaber kostenpflichtiges Logoprogramm der United Internet Media. Die größten Mailboxprovider (WEB.DE, GMX, 1&1, freenet sowie die Deutsche Telekom) nehmen daran teil und werden wenig Interesse daran haben, ihr Geschäftsmodell ohne Grund zu ändern. Endkunden, die Logos für ihre Sicherheit fordern, und Markeninhaber, deren Marketing an kostenlosen Logoanzeigen Gefallen finden dürfte und die einen entsprechenden Druck ausüben, könnten über die Reaktion der hiesigen Provider und damit den Erfolg der BIMI-Initiative mitentscheiden. (un@ix.de)

Sven Krohlas

ist E-Mail-Spezialist und IT Security Consultant bei BFK edv-consulting GmbH in Karlsruhe.

Alle Links: ix.de/ix1809117