News Release - German

For Immediate Release

M³AAWG veröffentlicht neue Best Practices für DKIM infolge der Bekanntgabe einer Schwachstelle bei der Schlüssellänge

SAN FRANCISCO, CA--(Marketwire - November 8, 2012) [Aktualisiert: 11. Dezember 2013] - Das Spoofing, also die Fälschung von E-Mails von Unternehmen, die einen überholten, schwachen Verschlüsselungsschlüssel zur Authentifizierung ihrer E-Mails einsetzen, stellt nach jüngsten Berichten eine aktuelle Bedrohung dar. Die Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) fordert Unternehmen dringend auf, ihre DKIM-Verfahren umgehend anzupassen, um den Schutz der Endbenutzer zu verbessern, und hat dazu heute neue Best Practices bekanntgegeben, die speziell auf diese Schwachstelle abzielen. Neben anderen Empfehlungen zur Validierung der Authentizität von E-Mail-Absendern appelliert die M³AAWG an die Unternehmen, insbesondere ihre vormals sicheren 512- und 768-Bit-Verifizierungsschlüssel durch eine 1024-Bit- oder eine noch höhere Verschlüsselung zu ersetzen.

"Wir haben ein kurzes Dokument erstellt, das die relativ einfachen und unmittelbaren Schritte erläutert, die große E-Mail-Versender ergreifen können, um ihre Marken zu schützen und damit auf jüngste Bedenken hinsichtlich einiger Verschlüsselungs- und Nutzungslevel zu reagieren. Die Technologien entwickeln sich weiter, und um mit den Hackern Schritt halten zu können, muss die Branche ihre Praktiken angesichts ihrer zunehmenden Einsatzmöglichkeiten neu überdenken. Wir möchten die Unternehmen über die Änderungen informieren, die sie kurzfristig umsetzen können, um Konsumenten und ihre Marken gegen diese Bedrohung zu schützen", betonte Chris Roosenraad, stellvertretender Vorsitzender von M³AAWG.

Das Dokument "M³AAWG Best Practices for Implementing DKIM To Avoid Key Length Vulnerability" (www.maawg.org/sites/maawg/files/news/M3AAWG_Key_Implementation_BP-2012-11.pdf) beschreibt detailliert die technischen Schritte, die auf eine Behebung der derzeitigen Schwachstellen abzielen, und ist im Bereich "Published Documents" der Website der Organisation unter www.maawg.org/published-documents erhältlich. Zu den Empfehlungen zählen u.a.:

- Aktualisierung auf eine Mindest-Schlüssellänge von 1024 Bit. Kürzere Schlüssel können unter Verwendung billiger Cloud-Dienste binnen 72 Stunden geknackt werden.
- Wechseln der Schlüssel ~~alle drei Monate~~ mindestens zweimal pro Jahr. [1]
- Einstellung der Signaturen, so dass sie nach der aktuellen Frist für den Wechsel der Schlüssel ablaufen, und Annullierung alter Schlüssel im DNS.
- Verwendung des Testmodus des Schlüssels nur für einen kurzen Zeitraum und Annullierung des Testschlüssels nach der Anlaufzeit.
- Implementierung von DMARC im Monitoring-Modus und Verwendung von DNS, um zu kontrollieren, wie oft Schlüssel abgefragt werden. DMARC (Domain-based Message Authentication, Reporting and Conformance) ist ein weiterer Standard, der häufig in Verbindung mit DKIM verwendet wird.
- Verwendung von DKIM anstelle von DomainKeys, das ein überholtes Protokoll ist.
- Zusammenarbeit mit Dritten, die mit dem Versand der E-Mails eines Unternehmens beauftragt wurden, um sicherzustellen, dass diese die genannten Best Practices auch verwenden.

DKIM ist ein allgemein anerkannter Standard, der von Unternehmen, Behörden, großen E-Mail-Providern und anderen Organisationen genutzt wird. Der Standard ermöglicht es dem Absender, E-Mails auf eine Weise zu

versenden, die es dem Empfänger gestatten, die Identität des Absenders zu verifizieren. So implementieren z.B. E-Mail-Dienste wie etwa AOL, Gmail und Yahoo und kommerzielle Marken diesen Standard als Bestandteil ihres Messaging-Protokolls. Es versieht die Message-Header mit einem Verschlüsselungsschlüssel, der von ISP und anderen Empfängern verwendet wird, um zu verifizieren, ob die Mitteilung tatsächlich von dem angegebenen Unternehmen verschickt wurde.

Mit der Implementierung von DKIM wird es für Kriminelle schwieriger, rechtswidrige E-Mails zu erstellen, die den Anschein erwecken sollen, als kämen sie von einem angesehenen Unternehmen - ein Trick, der oft verwendet wird, um personenbezogene Daten von arglosen Benutzern zu stehlen. Ende Oktober berichtete die Wired-Journalistin Kim Zetter, dass viele Unternehmen im Rahmen der DKIM-Implementierung eine nur schwache Verschlüsselung und andere fragwürdige Praktiken verwenden, wodurch ihre E-Mails einem möglichen Spoofing durch Cyber-Kriminelle ausgesetzt sind.

Über die Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Die Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) stellt einen Zusammenschluss mehrerer Unternehmen dar, um gemeinsam gegen Bots, Malware, Spam, Viren, Denial-Of-Service-Attacken und ähnliche Online-Angriffe vorzugehen. M³AAWG (www.M3AAWG.org) repräsentiert über eine Milliarde Postfächer einiger der größten Netzwerkbetreiber weltweit. Dabei setzt M³AAWG auf die gesamte Erfahrung seines globalen Mitgliedernetzwerks, um mit Hilfe von Technologien, Zusammenarbeit und politischen Maßnahmen gegen Angriffe auf bereits bestehende Netzwerke und neue Dienste aktiv vorgehen zu können. Sie informiert außerdem Entscheidungsträger weltweit über technische und operative Probleme im Zusammenhang mit Online-Missbrauch und Messaging. Die M³AAWG hat ihren Sitz in San Francisco im US-Bundesstaat Kalifornien und ist ein offenes Forum, das sich mit den Anforderungen des Marktes beschäftigt und von größeren Netzwerkbetreibern und Messaging-Anbietern unterstützt wird.

[1] HINWEIS: Als das Best-Practice-Dokument im Jahr 2012 veröffentlicht wurde, lautete die Empfehlung, DKIM-Schlüssel quartalsweise zu rotieren. Aufgrund neuerer Forschungsergebnisse, die auch in ein noch detaillierteres M³AAWG Best-Practice-Dokument zum Thema Schlüsselrotation eingeflossen sind, wurde diese Empfehlung angepasst auf eine mindestens zweimal jährliche Rotation. Weitere Informationen über Best Practices zur DKIM-Schlüsselrotation finden Sie unter: [Einfügen: http://www.m3aawg.org/sites/maawg/files/news/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf]

M³AAWG-Vorstand: AT&T (NYSE: T); Cloudmark, Inc.; Comcast (NASDAQ: CMCSA); Constant Contact (NASDAQ: CTCT); Cox Communications; Damballa, Inc.; Eloqua; Facebook; France Telecom (NYSE und Euronext: FTE); La Caixa; Message Bus; PayPal; Return Path; Time Warner Cable; Verizon Communications und Yahoo! Inc.

M³AAWG-Vollmitglieder: 1&1 Internet AG; Adaptive Mobile Security LTD; Adobe Systems Inc.; AOL; BAE Systems Detica; Cisco Systems, Inc.; Dynamic Network Services Inc.; Email Sender and Provider Coalition; Genius; iContact; Internet Initiative Japan (IIJ NASDAQ: IIJI); McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scality; Spamhaus; Sprint; Symantec; Trend Micro, Inc. und Twitter.

Die gesamte Mitgliederliste steht unter http://www.m3aawg.org/about/roster zur Verfügung.

Medienkontakt:
Linda Marcus, APR, +1-714-974-6356, LMarcus@astra.cc
Astra Communications