

News Release - German

For Immediate Release

M³AAWG veröffentlicht umfassende DMARC-Schulungsvideos zur Bekämpfung von E-Mail-Spoofing

SAN FRANCISCO, CA--(Marketwire - February 6, 2013) - Infolge der zunehmenden Akzeptanz des DMARC-Authentifizierungsstandards veröffentlichte die M³AAWG nun eine kostenlose Reihe von Schulungsvideos, um die Branche dabei zu unterstützen, die Bedeutung von Anti-Phishing-Technologien zu erkennen und diese zu implementieren. Die DMARC-Schulungsmodule von M³AAWG bieten fast zweieinhalb Stunden Anleitungen von technischen Fachkräften von DMARC.org, einschließlich Information für Domain-Inhaber, die ihre Marken gegen Spoofing schützen wollen, sowie für Internetanbieter (ISP) oder Mailbox-Anbieter, die ihre Endbenutzer gegen betrügerische E-Mails schützen möchten.

Die DMARC-Schulungsreihe von M³AAWG enthält sechs Segmente mit einer Länge von 15 bis 40 Minuten, die ursprünglich von dem stellvertretenden Vorsitzenden der M³AAWG und Mitglied von DMARC.org, Michael Adkins, sowie dem stellvertretenden Vorsitzenden von DMARC.org, Paul Midgen, im Oktober 2012 im Rahmen eines M³AAWG-Meetings als Schulungssitzungen vorgestellt wurden. Die Video-Reihe bietet allgemeine Hintergrundinformation zur DMARC-Spezifikation (Domain-based Message Authentication, Reporting and Conformance) und ihre Zielsetzung sowie Anleitungen zum Einsatz der Technologie und Details zu ihren Meldeverfahren.

Die Video-Reihe enthält auch eine Breakout-Sitzung, in der Themen speziell für Domain-Inhaber und Fremdanbieter angesprochen werden, die E-Mails für Unternehmen versenden, sowie eine weitere Breakout-Sitzung, die Themen für ISP und Mailbox-Provider behandelt. Die Videos betonen praktische Aspekte, die von Adkins und Midgen anhand zahlreicher Beispiele erläutert werden. Die vollständige DMARC-Schulungsreihe von M³AAWG ist auf der M³AAWG-Website unter dem Menüpunkt "Activities" auf der Seite "Training Videos" verfügbar (<https://www.maawg.org/activities/maawg-training-series-videos>).

"Die M³AAWG spielte in seinen Meetings eine zentrale Rolle in der Entwicklung von DMARC und unterstützt diese Technologie nun in der Implementierungsphase mit der Veröffentlichung einer umfassenden Reihe von Schulungsvideos. DMARC wurde entwickelt, um Marken und Mailbox-Anbieter dabei zu helfen, betrügerische E-Mails zu erkennen. Diese Videos sind einzigartig, da in ihnen die technischen Fachkräfte zu Wort kommen, die an der Entwicklung von DMARC mitgewirkt haben, und nun in den Videos erklären, wie man die Implementierung der Technologie durchführen muss, um optimale Ergebnisse zu erreichen", sagte Trent Adams, Vorsitzender von DMARC.org.

AOL, Gmail, Hotmail, Yahoo! und andere E-Mail-Empfänger nutzen bereits DMARC, um Endbenutzer und Marken zu schützen. Laut Adams integriert diese Technologie die häufig verwendeten SPF- und DKIM-Spezifikationen und bietet zudem Verfahren für Feedback, Monitoring und Fehlerbehebung.

Der stellvertretende Vorsitzende der M³AAWG, Chris Roosenraad, erklärte: "Die Benutzer sind oft nicht in der Lage, mit einem Blick auf den Inhalt einer Mail zu erkennen, dass es sich bei einer E-Mail, die vermeintlich von ihrer Bank oder einem bekannten Geschäft stammt, in Wirklichkeit um einen Betrugsversuch von Kriminellen handelt. Das Spoofing oder das Nachahmen einer bekannten Marke in einer E-Mail wird zunehmend zu einem Problem: Die Benutzer werden in betrügerischer Absicht getäuscht, um z.B. personenbezogene Daten preiszugeben. Wir haben

diese Video-Reihe produziert, weil gemeinsame Anstrengungen in der Branche wie zum Beispiel DMARC von zentraler Bedeutung sind für den Schutz der Benutzer und die Bekämpfung dieser Art von Missbrauch."

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, die gemeinsam gegen Bots, Malware, Spam, Viren, Denial-Of-Service-Attacken und ähnliche Online-Angriffe vorgehen. M³AAWG (www.M3AAWG.org) repräsentiert über eine Milliarde Postfächer einiger der größten Netzbetreiber 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 beschäftigt sich mit den Anforderungen des Marktes. Sie wird von größeren Netzbetreibern und Messaging-Anbietern unterstützt.

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); Google; PayPal; Return Path; Symantec; 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: IIJ); Mailchimp; McAfee Inc.; Message Systems; Mimecast; Nominum, Inc.; Proofpoint; Scalify; Spamhaus; Sprint und Twitter.
Die gesamte Mitgliederliste steht unter <http://www.m3aawg.org/about/roster> zur Verfügung.

Pressekontakt:

Linda Marcus, APR
1+714-974-6356 (US-Pazifik), L.Marcus@astra.cc
Astra Communications
