News Release

For Immediate Release (German)

Neue Best Practices für Online- und mobile Anwendungen unterstützen Sicherheitsverfahren in Privatwirtschaft und Regierungseinrichtungen

BALTIMORE, MD – (Marketwire - October 25, 2012) - Ein seit heute verfügbarer Bericht, der in einer internationalen Gemeinschaftsanstrengung erstellt wurde, skizziert Best Practices für die Nutzung von Internet und mobilen Anwendungen, zielt auf die Einschränkung von Malware, Phishing, Spyware, Bots und andere Internet-Bedrohungen ab und bietet eine genaue Besprechung aktueller und künftiger Bedrohungen. Der Bericht "Best Practices to Address Online and Mobile Threats" ist eine umfassende Bewertung der aktuellen Internet-Sicherheit und erläutert in einer nicht-technischen Sprache die proaktiven Maßnahmen, die zu einer Reduzierung der Risiken beitragen können, folgt man den Ausführungen der beiden wichtigsten Mitautoren des Berichts, der M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group) und des LAP (London Action Plan).

Der Bericht stellt ferner eine der ersten internationalen Anstrengungen dar, staatliche Instanzen dazu anzuregen, Best Practices anzuwenden, die meist nur mit Wirtschaftsunternehmen in Verbindung gebracht werden. Der Bericht konzentriert sich auf vier Schwerpunkte: Schadprogramme und Botnetze, Social Engineering und Phishing, IP- und DNS-Exploits und mobile Bedrohungen. Um die Teilnahme von Regierungseinrichtungen zu fördern, wurde der Bericht auch der OECD (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung) mit ihren 34 Mitgliedstaaten zur Durchsicht vorgestellt.

Der Bericht "Best Practices to Address Online and Mobile Threats" greift auf Methoden zurück, die sich im vergangenen Jahrzehnt in der Reduzierung der Online-Risiken als wirkungsvoll erwiesen haben, und ergänzt diese dann mit zukunftsorientierten Empfehlungen hinsichtlich neuer Schwachstellen wie z.B. mobiler Text-Spam und Web-Missbrauch. Der umfassende Bericht ist auf den Websites verschiedener Organisationen abrufbar, darunter http://www.maawg.org/sites/maawg/files/news/M3AAWG_LAP_Best_Practices_to_Address_Online_and_Mobile_Threats.pdf, http://www.londonactionplan.com/files/reports/Best_Practices_to_Address_Online_and_Mobile_Threats_(Oct_2012).pdf und http://www.cauce.org/2012/10/best-practices-report.html.

"Als weltweite gemeinsame Anstrengung führte der Bericht ein einzigartiges Expertenteam zusammen, das in einer leicht verständlichen Sprache sichere EDV-Verfahren für Endbenutzer, große und kleine Unternehmen und staatliche Behörden skizziert. Zugleich handelt es sich hierbei um eine der ersten Anstrengungen, die Branchenempfehlungen zu aktualisieren und dabei anzuerkennen, dass staatliche Einrichtungen wichtige Online-Unternehmen sind und dass öffentliche Institutionen ebenso wie andere Unternehmen Best Practices implementieren müssen", betonte Alex Bobotek, stellvertretender Vorsitzender der M³AAWG.

Die internationale Gemeinde engagierte sich gemeinsam für die Ausarbeitung des Berichts im Rahmen einer Partnerschaft öffentlicher und privater Einrichtungen, die von Andre Leduc angeführt wurde. Leduc ist als Leiter der nationalen Anti-Spam-Koordinierungsinstanz im kanadischen Wirtschaftsministerium tätig. Daneben leisteten Branchenexperten der M³AAWG, des LAP und weiterer Organisationen wie z.B. die CAUCE (Coalition Against Unsolicited Commercial Email) einen Beitrag zur Studie.

Online-Bedrohungen entstehen infolge der zunehmenden Bedeutung des Internet und mobiler Technologien in vielen Geschäftsmodellen. Dadurch werden Cyberkriminelle auf den Plan gerufen, die Benutzer weitverbreiteter Plattformen wie z.B. Laptops, Tablets, Smartphones und anderer Handheld-Geräte anzugreifen. Die Implementierung der in

diesem Bericht beschriebenen Best Practices wird dazu beitragen, trotz des weiteren Wachstums der Internet-Wirtschaft gesetzwidrige Aktivitäten wie z.B. Spam, Phishing, Malware- und Spyware-Verbreitung, Botnet-Einsatz, Umleitung von Internet-Verkehr auf schädliche Websites und Denial-of-Service-Attacken zu unterbinden.

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 MAAWG hat ihren Sitz in San Francisco im US-Bundesstaat Kalifornien und ist ein offenes Forum, das sich mit den Anforderungen des Marktes beschäftigt und durch größere Netzwerkbetreiber und Messaging-Anbieter unterstützt wird.

Über den London Action Plan (LAP)

Beim LAP handelt es sich um eine Organisation mit 45 Strafverfolgungsbehörden und Branchenorganisationen, die sich der Bekämpfung von Spam und anderen Bedrohungen im Internet verschrieben haben. Der LAP führt regelmäßige Telekonferenzen und eine Jahresversammlung durch. Am letzten Treffen, das im Oktober 2012 in London abgehalten wurde, nahmen Vertreter aus Europa, Asien und Nordamerika teil.

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; Experian CheetahMail; 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 vollständige Liste aller Mitglieder finden Sie unter http://www.m3aawg.org/about/roster.

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