

News Release

For Immediate Release (German)

Von weltweiten MAAWG-Mitgliedern entwickelte „Best Practices“ zu gemeinsam genutzten dynamischen IP-Adressen und Mail-Umleitung erschienen; Thema: Botnetze und verbesserte Benutzerfreundlichkeit

SAN FRANCISCO, 26. Juni/PRNewswire/ -- Netzbetreiber und Internetdiensteanbieter (Internet Service Providers, ISPs) aus aller Welt haben zwei Veröffentlichungen über bewährte Verfahren („Best Practice“) erarbeitet, die auf technischem Weg dabei helfen können, durch Botnetze verursachte Spam-E-Mails zu blockieren und die Zustellbarkeit von persönlichen E-Mails von Anwendern zu verbessern. Auf dem Arbeitstreffen der Messaging Anti-Abuse Working Group (MAAWG) vergangene Woche in Heidelberg (Deutschland) wurden Empfehlungen für die gemeinsame Nutzung von IP-Adressräumen und für das Weiterleiten von E-Mails verabschiedet. Diese Empfehlungen stehen ab heute zur Verfügung.

Die „Methoden der MAAWG zur gemeinsamen Nutzung dynamischer IP-Adressrauminformationen“ („MAAWG Methods for Sharing Dynamic IP Address Space Information with Others“) lösen ein Problem, das durch die schnelle Verbreitung von Botnetzen, die oft dynamische IP-Adressen zum Versand von Spam nutzen, weiter verschärft wird. Die Veröffentlichung beschreibt vier Lösungsansätze, wie Mailbox-Anbieter sich diese Adressen einfacher beschaffen können; gleichzeitig werden in dem Artikel auch die Vor- und Nachteile der jeweiligen Lösung erörtert.

Die in den „Empfehlungen der MAAWG: Bewährte Verfahren zur E-Mail-Weiterleitung“ („MAAWG Recommendations: Email Forwarding Best Practices“) beschriebenen Methoden helfen ISPs bei der Unterscheidung zwischen Spammern und legitimen Anwendern, die einen Weiterleitungsdienst nutzen. In dem Artikel werden darüber hinaus Verfahren zur Verbesserung der Zusammenarbeit zwischen Massen-E-Mail-Versendern und Netzbetreibern aufgezeigt. So soll verhindert werden, dass gültige E-Mail-Konten aufgrund missbräuchlicher E-Mail-Eingänge blockiert werden.

Hilfe bei der Unterscheidung zwischen legitimen und potenziell kriminellen Nutzern

Die Empfehlungen zur gemeinsamen Adressennutzung wurden entwickelt, um Mailbox-Anbietern zu helfen, die E-Mails, die von dynamischen IP-Adressen aus versendet werden, nicht akzeptieren. Obwohl die meisten Anwender sich über ein Modem ins Internet einwählen und ihnen dabei eine dynamische IP-Adresse zugewiesen wird, werden ihre E-Mails normalerweise durch den Mailserver des ISP, der eine statische (unveränderliche) IP-Adresse besitzt, geschleust. Wenn aber ein Bot in den Computer von Anwendern eindringt, umgeht dieses häufig den Mailserver des ISP, sodass die vom Bot aus gesendeten Spam-E-Mails direkt von der dynamisch zugewiesenen Adresse des Anwenders kommen. Die Netzwerkadressbereiche auszumachen, die jeder ISP als dynamische Adressen zuweist, sodass Mailbox-Anbieter von Botnetzen verursachte Spams identifizieren und ausfiltern können, war ein komplexer und schwieriger Prozess.

„Innerhalb der Branche wird seit Jahren über die gemeinsame Nutzung von dynamischen IP-Adressen diskutiert und es gab dazu sogar einige Vorschläge. Mit dieser Veröffentlichung jedoch hat sich erstmalig eine größere Gruppe von ISPs zusammengetan und sich darüber verständigt, wie man dabei vorgehen soll. Die Empfehlungen sind ein weiterer notwendiger Schritt vorwärts, der Mailbox-Anbietern bei der Eliminierung von Spam-E-Mails aus Botnetzen hilft, bevor sie in die Posteingänge der Anwender gelangen“, erklärte J.D. Falk, Mitglied im Vorstand der Arbeitsgruppe MAAWG und Leiter für Produktmanagement bei Return Path.

Die bewährten Verfahren zur Mail-Umleitung bieten ebenfalls technische Empfehlungen zur Verbesserung der Kommunikation zwischen sendenden und empfangenden Einheiten. Viele Mailbox-Anbieter und Einrichtungen bieten Anwendern entweder dauerhafte oder kurzlebige, temporäre E-Mail-Adressen, die eingerichtet wurden, um Nachrichten an das eigentliche Konto des Anwenders beim ISP weiterzuleiten. Mit der Zeit kann es vorkommen, dass diese Adressen sehr viele Junk-Mails erhalten und weiterleiten, was den ISP des Anwenders zu der Annahme veranlasst, dass der Mail-Umleitungsdienst eine Quelle für Spam darstellt, und der ISP schließlich alle eingehenden E-Mails von diesem Dienst blockiert. Der MAAWG-Artikel zeigt auf, welche Schritte Weiterleitungsdienste implementieren können, um die Zustellbarkeit zu verbessern sowie Lösungen für die Geschwindigkeitsprobleme, wie etwa die Trennung der Sende- und Umleitungsfunktionen des Servers, umzusetzen. Die Verfahren für Empfänger beinhalten Richtlinien im Web und Erkennen des für Weiterleitungen reservierten IP-Adressraums.

Jordan Rosenwald, Mitherausgeber der Empfehlungen zu E-Mail-Weiterleitungen und Leiter Anti-abuse Technologies bei Comcast, erklärte: „Jede Adresse zieht einiges an Spam an. Eingehender Datenverkehr von einem weitergeleiteten Konto, das schon jahrelang in Benutzung ist, sieht häufig aus wie von Spam geradezu überschwemmt, was einen ISP natürlich veranlasst, diesen zu blockieren. Zudem entwickeln die Spammer neue Wege, um umgeleitete E-Mails zu ihren Gunsten zu nutzen. Deshalb können die in diesen Empfehlungen skizzierten Schritte zu Kosteneinsparungen bei Weiterleitungsdiensten und auch bei Empfängern führen und, was noch viel wichtiger ist, sie helfen außerdem dabei, ein nicht erforderliches bzw. nicht beabsichtigtes Blockieren von Anwendern zu verhindern.“

Beide Veröffentlichungen stehen kostenlos auf der MAAWG-Website unter www.MAAWG.org zur Verfügung. Die Endfassung der Artikel wurde im Rahmen der 13. Hauptversammlung der MAAWG ausgearbeitet, an dem über 230 Fachleute für Datenmissbrauch und Datenschutz von ISPs, E-Mail-Providern und Anbietern aus 18 Ländern teilnahmen. Das letzte Treffen des Branchenverbandes im Jahr 2008 wird vom 22. bis 24. September in Fort Lauderdale in Florida stattfinden. Für die Veranstaltung sind Arbeitssitzungen und Fachvorträge zu einer Vielzahl von Themen geplant, u.a. zu Botnetzen und zur zunehmenden weltweiten Zusammenarbeit gegen Missbrauch auf diesen Gebieten.

Informationen zur Messaging Anti-Abuse Working Group (MAAWG)

Die Messaging Anti-Abuse Working Group (MAAWG) ist die Arbeitsgruppe der E-Mail-Branche, die in diesem Rahmen gemeinsam gegen Spam, Viren, Denial-of-Service-Angriffe und sonstigen Online-Missbrauch kämpft. Die MAAWG (www.MAAWG.org) vertritt nahezu eine Milliarde E-Mail-Postfächer von etlichen der weltweit größten Netzbetreiber. Die MAAWG ist die einzige Organisation, die einen ganzheitlichen Ansatz bei der Bekämpfung von Missbrauch beim E-Mail-Versand verfolgt, indem sie systematisch alle Aspekte des Problems, einschließlich technologischer Aspekte, die branchenweite Zusammenarbeit sowie gesetzliche Rahmenbedingungen angeht. Die MAAWG nutzt die umfassende Kompetenz und Erfahrung seiner weltweiten Mitglieder, um den Missbrauch bestehender Netzwerke und neu aufkommender Dienste zu bekämpfen. Die MAAWG mit Hauptsitz in San Francisco (Kalifornien) ist ein offenes Forum, das sich an den Marktanforderungen orientiert und von den wichtigsten Netzbetreibern und Messaging-Anbietern unterstützt wird.

Ansprechpartner Medien: Linda Marcus, APR, Tel.: +1-714-974-6356, E-Mail: lmarcus@astra.cc, Astra Communications

Vorstand der MAAWG: AOL; AT&T (NYSE: T); Bell Canada; Charter Communications (Nasdaq: CHTR); Cloudmark; Comcast (Nasdaq: CMCSA); Cox Communications; France Telecom (NYSE and Euronext: FTE); Goodmail Systems; Openwave Systems (Nasdaq: OPWV); Return Path, Inc. (Vollmitgliedsvertreter im Vorstand); Time Warner Cable; Verizon Communications sowie Yahoo! Inc.

MAAWG-Vollmitglieder: 1&1 Internet AG; AG Interactive; Bizanga LTD; BlueTie, Inc.; Eloqua Corporation; Google, Inc.; Internet Initiative Japan, (IIJ NASDAQ: IIJI); IronPort Systems; McAfee Inc.; MX Logic; Outblaze LTD; Return Path, Inc.; SPAMHAUS (The Spamhaus Project); Sprint; Sun Microsystems, Inc.; Symantec sowie Telefonica SA.

Eine vollständige Liste der Mitglieder finden Sie unter <http://www.maawg.org/about/roster>.
