IT-ADMINISTRATOR.DE

08/2009

iladministrator

Das Magazin für professionelle System- und Netzwerkadministration

4. Heinlein Mailserver-Konferenz, 1. bis 3. Juli 2009, Berlin

Rechtssicher und spamfrei

Sonderdruck für Heinlein Professional Linux Support

4. Heinlein Mailserver-Konferenz 2009, 1. bis 3. Juli, Berlin

Rechtssicher und spamfrei

Auf der 4. Mailserver-Konferenz drehten sich die Themen um rechtliche Aspekte und Spam

von Daniel Richey

Typischerweise kämpfen Mailserver-Administratoren an mehreren Fronten: Sie müssen Sorge dafür tragen, dass der E-Mailverkehr ohne Ausfälle funktioniert, die Nachrichten frei von Spam und Viren sind und all das rechtssicher vonstattengeht. In großen Unternehmen steht für diese Bereiche genügend Personal und Technik zur Verfügung, während kleinere Unternehmen oft schon froh sind, dass ihre Infrastruktur ohne größere Ausfälle funktioniert. Entsprechend aufgebaut waren die Themen auf der 4. Mailserver-Konferenz des Linux-Support-Dienstleisters Heinlein in Berlin.

Rechtlich gesehen bewegen sich Mailserver-Administratoren sowie Arbeitgeber oft am Rande der Legalität oder in Grauzonen. So verwunderte es nicht, dass der erste Konferenztag sich ausschließlich mit juristischen Themen befasste. Zahlreiche Rückfragen der Teilnehmer zeugten vom großen Interesse und Aufklärungsbedarf. So räumten denn auch vier Anwälte in ihren Vorträgen mit so manchen Rechtsmythen und Missverständnissen auf. Vilma Niclas, Rechtsanwältin aus Berlin, zeigte auf, was alles für einen rechtssicheren E-Mailverkehr nötig ist. So gelten etwa beim elektronischen Geschäftsverkehr die gleichen Aufbewahrungsfristen wie bei postalischen Nachrichten – sechs Jahre beziehungsweise zehn Jahre bei Buchungsbelegen. Anstatt auf Datenträgern gespeichert könnten E-Mails dabei auch ausgedruckt archiviert werden.

Viele Fallstricke bei E-Mails

Grundsätzlich gilt bei Werbemails das Opt-In-Verfahren, bei dem der Empfänger dem Versand ausdrücklich zustimmen muss. Gibt es bereits einen Geschäftskontakt, dürfen Unternehmen jedoch unter bestimmten Voraussetzungen auch ohne vorherige Zustimmung Werbenachrichten in eigener Sache versenden. Dies gilt für bis zu zwei Jahre, sofern der Kunde dem Erhalt nicht widersprochen hat. Auch bei Newslettern muss der Empfänger ausdrücklich zustimmen, da die allermeisten Newsletter letztendlich auch Werbung sind. Am besten eignet sich laut Vilma Niclas das Double-opt-in-Verfahren. Dabei melden sich die Nutzer an und erhalten eine Bestätigungsmail, die angeklickt werden muss. Nicht vergessen sollten die Verantwortlichen natürlich das Impressum – sowohl im Newsletter als auch in regulären E-Mails.

Eine Alternative, die jedoch höchstens bei Kleinstunternehmen sinnvoll angewendet werden kann. Ebenfalls wichtig zu wissen ist für die Verantwortlichen, unter welchen Umständen das eigene Unternehmen Werbung oder Newsletter versenden darf. Denn schnell drohen für Werbemails ohne Zustimmung der Empfänger Abmahnungen sowie bis zu 50.000 Euro Geldbuße.

Auf besonders große Hürden treffen Administratoren, wenn sie mit Postfächern arbeiten, in denen sich auch private E-Mails befinden. Daher warnte Rechtsanwalt Thomas Feil davor, die private Mailnutzung am Arbeitsplatz als Unternehmen zu dulden. Denn dadurch würde der Arbeitgeber selbst zum Telekommunikationsanbieter und müsse die strengen gesetzlichen Datenschutzregeln beachten. Befinden sich etwa in einem E-Mailaccount auch private Nachrichten, dürfe das Unternehmen nicht ohne weiteres Einsicht in das Postfach nehmen – auch wenn der Mitarbeiter längere Zeit krank und damit abwesend sein sollte. Insgesamt könne ein Unternehmen bei geduldeter Privatnutzung gar nicht alle Rechtsvorschriften einhalten. Der beste Weg führe daher über Betriebsvereinbarungen, die die Privatnutzung klar regeln oder am besten ganz verbieten.

Deutschland als Cybercrime-Versuchsfeld

Über die Entwicklungen in der Cyberkriminalität klärte André Dornbusch, Kriminalkommissar beim Bundeskriminalamt, auf. Insgesamt befassen sich rund 40 Beamte im Referat "SO 43" mit der Ermittlung und Auswertung von Online-Verbrechen. Nach den Erkenntnissen der Ermittler ist Deutschland dank seiner hohen Sicherheitsstandards ein Versuchsland für Cyberkriminelle geworden. So gebe es Malware und Angriffsformen, die speziell auf deutsche Rechner und deren Sicherheitsmechanismen abgestimmt würden. Seien diese hier erfolgreich, könnten sie quasi überall angewendet werden.

Die E-Mail als klassisches Transportmittel für Phishing-Versuche und Schädlinge spielt nach Aussagen des Kriminalkommissars dabei schon länger kaum mehr eine Rolle.Vielmehr dienen heute geschickt platzierte aktive Inhalte auf Webseiten der Verbreitung von Trojaner und Co. In der Untergrundwirtschaft finde dabei eine starke Malware-Fokussierung durch Spezialisten statt. Hinzu komme, dass 53 Prozent der 2008 gefundenen Schwachstellen nicht gepatcht wurden. Antiviren-Software sei dabei auch nicht mehr das Maß aller Dinge als Schutz. Nur durchschnittlich vier Prozent der im Umlauf befindlichen Schadsoftware würde laut IBM-X-Force-Report von aktuellen Antiviren-Programmen entdeckt.

Spammer im Visier

Spamhaus ist einer der bekanntesten Antispam-Dienstleister. Carel van Straten erläuterte in seinem Vortrag, auf welche Techniken die Spambekämpfer zurückgreifen und wie sich diese von Unternehmen nutzen lassen. Besonders bemerkenswert war für van Straten die Tatsache, dass Spammer heutzutage meist besser international aufgestellt sind als viele große Firmen. So verteilen sich die Botnetze schnell über mehrere Länder und beziehen zahlreiche Provider mit ein. Doch auch die Nutzerbasis von Spamhaus kann sich sehen lassen: 1,5 Millionen Nutzer greifen auf die Filterungsdaten der Briten zurück. Diese Verantwortung mache es für Spamhaus schwierig, restriktive Filterungsmethoden einzusetzen. Ganze Länder lassen sich etwa nicht so einfach blockieren. Aus diesem Grund spiele die Qualität der Daten eine entscheidende Rolle.

Insgesamt stellt der Dienstleister vier verschiedene Blocklisten zur Verfügung: SBL (Nameserver-Einträge von Spam-URLs), XBL (einzelne IP-Adressen), PBL (Filter-Policies) sowie die Drop-Liste mit IP-Adressen, zu denen am besten gar keine Verbindung hergestellt wird. Die in Spam-Hinsicht auffälligsten Länder sind nach Spamhaus-Zahlen derzeit Brasilien (16,3 Prozent), Indien (11 Prozent), Russland (7,6 Prozent), Türkei (6,7 Prozent) und Polen (5,5 Prozent). Diese Länder hätten gemein, dass in ihnen erst kürzlich großflächig Breitband für Privatnutzer zur Verfügung stünde. Die Nutzer dort haben laut van Straten noch keine große Erfahrung mit Sicherheitsmaßnahmen. Nächstes Jahr könnte Polen aus den Top-5 fallen, da sich die Online-User dort zunehmend schützten. Dafür mache sich Algerien auf den Weg.

An Technologien machen Peer-to-Peer-Botnetze zunehmend die Kontrollserver überflüssig. Bislang konnten Provider oder Ermittlungsbehörden gezielt diese "Command and Control"-Server abschalten und damit ganze Botnetze lahmlegen. Doch nun verteilen sich diese Kontrollfunktionen ebenfalls über viele Rechner in unterschiedlichen Ländern. Ein weiterer Trend ist das Fast-flux-Hosting: Dabei werden beispielsweise Phishing- oder Schadcode-Webseiten auf zahlreichen kompromittierten Rechnern gehostet, damit zumindest ein paar davon funktionieren. Die Liste ändert sich dabei alle paar Minuten. Damit machen laut van Straten auch Abuse-Beschwerden bei Providern keinen Sinn, da sich die IP-Adressen Provider-übergreifend laufend ändern.

Best Practices

Eine umfassende Übersicht, wie Administratoren mit ihren Mailservern in Bezug auf Spam umgehen sollten, gab Peer Heinlein als Geschäftsführer von Heinlein Support. So seien Backscatter-Mails heute eines der größten Probleme im Spamumfeld. Mit diesen Nachrichten antworten Mailserver auf den Erhalt von E-Mails, wenn etwa der Empfänger unbekannt oder abwesend ist. Doch nehmen Mailserver Nachrichten dabei oft erst an und versuchen anschließend, die Mail intern zuzustellen. Klappt dies nicht, erzeugen Sie eine Antwortmail an die Absenderadresse. Wurde diese jedoch durch Spammer gefälscht, landet dieser Backscatter bei völlig Unbeteiligten. Daher sollten laut Heinlein die Mailserver noch während der Zustellphase – also während des SMTP-Dialogs – bereits prüfen, ob ein Empfänger valide ist. So erhält der einliefernde Mailserver direkt die Rückmeldung und bricht die Übertragung gegebenenfalls ab.

Auch erhalten Absender eine direkte Rückmeldung, dass ihre Nachricht herausgefiltert wurde. Ansonsten besteht die Gefahr, dass Spam-Nachrichten in spezielle Ordner aussortiert werden und die Nutzer False Positives darin nicht wiederfinden. Absender und Empfänger wissen dann nichts von der verlorengegangenen Nachricht und das Unternehmen hat im Zweifelsfall diese E-Mail rechtlich gesehen angenommen. Um sicherzustellen, dass die eigenen E-Mails nicht versehentlich von den Empfängern als Spam identifiziert werden, sollten Unternehmen zudem auf korrekte Reverse-Lookups achten. Das bedeutet, die IP-Adresse des sendenden Mailservers löst korrekt auf die Domain in der HELO-Nachricht auf und beweist damit ihre Zugehörigkeit zum Netzwerk des Absenders. Zum Abschluss wies Peer Heinlein noch auf ein besonderes Anliegen hin, was IT-Sicherheit anbelangt. So fokussierten sich Unternehmen viel zu sehr auf die Redundanz von IT-Geräten. Doch wenn es um den Administrator gehe, sei oft Not am Mann. Hier auf gut ausgebildetes Personal zu setzen mit vernünftigen Vertretungsregeln im Krankheits- oder Urlaubsfall sei wesentlich zielführender, als massiv in immer neue Hardware zu investieren.