Der Newsletter von Heinlein Support.

logfile-20903

- SPAM-Tagging und Mailverlust
- RAID-Mathematik für Admins
- RBL-Listen abgeschaltet

SPAM-Tagging sorgt für Mailverlust

Die Angst vor dem Verlust von E-Mails wird als Hauptgrund für die Einführung von Quarantäne-Verzeichnissen auf dem Spamfilter oder für ein Spam-Tagging im Betreff verdächtiger E-Mails angeführt. Doch es ist äußerst fraglich, ob diese Taktik tatsächlich für einen zuverlässigeren Mailversand sorgt. Bei genauerer Betrachtung wird man vielmehr zu dem Schluss kommen: Gerade Quarantäne und Spam-Tagging sorgt in vielen Fällen erst recht für Mailverlust.

In den Anfängen der Spamfilterung vor vielen Jahren haben Entscheider wie Anwender viele negative Erfahrungen mit unzuverlässigen Spamfiltern gemacht. Unausgereifte Software, aber auch falsche Konfiguration durch den Administrator haben oft zu mangelhaften Filterergebnissen geführt. Bei dem Versuch, Spam möglichst zu 100 % zu erkennen, sind viele aggressiv eingestellte Spamfilter über das Ziel hinausgeschossen. Die Folge: Ein oft über lange Zeit aufgebautes Misstrauen gegen Filter und die stete Angst vor verlorengegangenen E-Mails. Zu Unrecht – denn gute und richtig konfigurierte Filtersysteme produzieren so gut wie keine Fehler.

Doch in vielen Unternehmen wird weiterhin gefordert, dass Spam getaggt werden muss, um dann trotzdem in die Postfächer der Mitarbeiter zugestellt zu werden. Allenfalls automatische Spamverdachtsordner oder eine Mailquarantäne sorgen dafür, dass die Spamflut wenigstens etwas kanalisiert wird, um den Nutzern ein halbwegs freies Postfach zu ermöglichen. Auch die einschlägigen Hersteller der oft nicht günstigen Anti-Spam-Software haben das Dogma der Mailquarantäne oder des Betreff-Taggings stets hochgehalten. Kein Wunder, schließlich muss dem Kunden tagtäglich vor Augen geführt werden, welche Bedrohung weiterhin existiert und warum die gekaufte Software ihr Geld wert ist. Und so muss man zu dem Schluss kommen: Viele Systeme verwalten lieber Spam, statt ihn aus der Welt zu schaffen.

Doch gerade getaggter Spam sorgt dafür, dass Probleme und Schäden maximiert werden. Denn so schön die getaggte E-Mail theoretisch auch sein mag – der Empfänger lässt sie oft automatisch löschen oder in ein Unterverzeichnis verschieben, wo sie dann ungelesen verschwindet. Postmaster größerer Mailsysteme können schnell verifizieren: Fast alle Mails in Spamverdachtsordnern oder Mailquarantäne bleiben über Wochen ungelesen. Fälschlich klassifizierte E-Mails werden nicht gefunden. Die eigentlich erwünschte Kontrolle durch den Nutzer? Fehlanzeige.

Doch auch wenn der Nutzer morgens im Akkord sein Postfach aufräumt, bleibt es oft bei einem flüchtigen Blick auf Absender und Betreff. Und so ist es kein Wunder, wenn Anwender eklatante False Positives-Raten unter 1:1.000 erreichen, während ausgereifte Spamfiltersysteme mit 1:1.000.000 glänzen können. Der Mensch als relevanter Fehlerfaktor.

Und der Absender? Er geht von einer erfolgreichen Zustellung aus und ahnt nichts davon, dass der Empfänger seine E-Mail nie zur Kenntnis genommen hat. Er erhält keine Bounce-Meldung, die ihn über Probleme beim Mailversand informiert. Ganz im Gegenteil: Der Mailserver des Absenders besitzt in seinen Logfiles das Protokoll über eine erfolgreiche Zustellung – vom Empfangssystem mittels „250 OK“ quittiert, was dem digitalen Abbild eines Einschreiben mit Rückschein entspricht. Kommt es zum Schaden, weil relevante E-Mails untergegangen sind, könnte ein gewiefter Absender hier den Aufhängepunkt einer Schadenersatzklage sehen, schließlich ist offensichtlich, dass

(h|b)log

Eine Winterpause wäre schön gewesen, doch uns in Berlin war sie nicht vergönnt. Von der allgemein beklagten Rezession ist nichts zu spüren, unser mittlerweile 12köpfiges Team ist trotz Jahresanfang gut ausgelastet gewesen. Das Akademie-Programm 2009 steht und mit einer CeBIT-Bühne und zwei Fachkonferenzen haben wir uns für dieses Jahr viel vorgenommen. Sascha Genennig verstärkt darum seit 1. Januar unser Team, um alles zu koordinieren – und als eines seiner ersten Ergebnisse halten Sie dieses „Logfile“ in den Händen, mit dem wir Sie ab sofort vierteljährlich auf dem neuesten Stand halten wollen.

Schöne Grüße aus Berlin,
Peer Heinlein

die Mail im Macht- und Haftungsbereich des Empfängers gelandet ist, dieser die Nachricht jedoch schlichtweg nicht ordnungsgemäß bearbeitet hat.

Erst wenn der Absender sich über das Ausbleiben einer Antwort wundert und er beim Empfänger nachhakt, fliegt der Verlust auf. Die Folge: Zeitverlust, unnötiger Kommunikationsaufwand für alle Beteiligten – oder am Ende gar gerade der befürchtete Verlust eines Auftrages, vor dem Spam-Tagging ja schützen sollte. Denn was ist, wenn der Absender beim Ausbleiben eines angefragten Angebots nie nachfragt, sondern stattdessen lieber verwundert zur Konkurrenz geht?

Archivierung elektronischer Handelsbriefe

Seit 1. Januar 2008 fordert der Gesetzgeber die revisionssichere Archivierung elektronischer Handelsbriefe. Und das bedeutet in aller Konsequenz: Auch getaggte Spam-Mails müssten archiviert werden, andernfalls kann nicht sichergestellt werden, dass lückenlos alle Handelsbriefe erfasst wurden. Immense Spam-Mengen müssen für sechs oder gar zehn Jahre gespeichert und verwaltet werden. Angesichts eines heutigen Spam-Anteils von über 95% hat Spam-Tagging finanzielle Auswirkungen, die jeden verantwortbaren Rahmen sprengen. Wird jedoch Spam in Echtzeit gefiltert und abgelehnt, so wurden diese Mails auch nie vom Unternehmen empfangen – und können bzw. müssen auch nicht archiviert werden.

Außerdem: Autoresponder und Backscatter

Und noch aus einem anderen Grund ist ein sofortiges Ablehnen verdächtiger E-Mails wichtig: Autoresponder. Die gerade in Unternehmen sehr weit verbreitete Sitte, seine Urlaubsabwesenheit per automatischer Antwort jedem Absender mitzuteilen, sorgt für zahlreiche Auto-Replys auf Spam-Mails. Neben der unnötigen Belastung der Mailserver (Archivierung!) werden so schnell unschuldige Dritte, deren Absender für den Spamversand missbraucht wurden, mit Tausenden von Antwort-Mails bombardiert. Ein Distributed Denial of Service ist es, was sich die Postmaster hier gegenseitig antun. In der Fachsprache heißt dieses Problem: „Backscatter" – Server, die Spam „zurückstreuen".

Doch nicht nur aus Gründen des eigenen Verantwortungsbewußtseins müssen Backscatter-Systeme tunlichst vermieden werden – auch aus ganz egoistischen Motiven heraus darf ein Postmaster nie solche Setups betreiben: Denn ein Backscatter-Server wird von der Postmaster-Gemeinschaft zu Recht wie ein Spammer-System behandelt. Auch Backscatter-Spam ist Spam! Und so ist es ist nur eine Frage der Zeit, bis diese Antwort-Mails auch die Detektoren der Anti-Spam-Organisationen treffen.

Die Folge: Backscatter-Mailserver landen über kurz oder lang immer wieder auf den internationalen RBL-Sperrlisten, so dass der Mailversand an quasi alle relevanten Provider zum Erliegen kommt. Backscatter-Postmaster spielen Russisch Roulette und riskieren einen hausgemachten Denial of Service gegen sich selbst.

Und dabei ist es doch heute so einfach

Gute Spamfiltersysteme – und dazu zählen gerade auch die Open Source-Vertreter wie amavisd-new und Postfix – können problemlos alle eingehenden E-Mails noch während des Annahmevorgangs filtern und bewerten. Nicht erwünschte E-Mails werden gar nicht erst angenommen. Es ist damit nicht mehr Problem des empfangenden Servers, die Mail als Bounce an den Absender zurückzusenden. Diese Aufgabe wird vom einliefernden System übernommen. Sollte es sich ausnahmsweise um eine falsch klassifizierte echte E-Mail handeln, wird der Absender umgehend und zuverlässig über das Versandproblem informiert. Eine klare Ablehnung von spamverdächtigen Nachrichten schafft Rechtssicherheit (was die Unternehmensleitung interessiert), entlastet die Systeme und ein etwaiges Mailarchiv (was den Admin freut) und vor allem auch die Postfächer der Nutzer (die damit in aller Regel gar nicht mehr belästigt werden wollen).

Peer Heinlein

Unsere Veranstaltungstermine: Januar bis Juli 2009

KW	Datum	Kurs	Dozent
12	16.03.–18.03.	Systematische Fehler- u. Netzwerkdiagnose	Stefan Semmelroggen
12	16.03.–20.03.	Sichere Mailserver mit Postfix	Peer Heinlein
13	23.03.–27.03.	Linux Admin Grundlagen	Peer Hartleben
13	23.03.–27.03.	LDAP-Server	Stefan Kania
14	30.03.–01.04.	PHP-/Webserversicherheit	Peter Prochaska
14	30.03.–03.04.	Hochverfügbarkeit mit Heartbeat2 u. LVS	Dr. Michael Schwartzkopff
17	20.04.–24.04.	PostgreSQL für Profis	Hans-Jürgen Schönig
17	20.04.–24.04.	Apache2 Webserver	Sven Velt
18	27.04.–29.04.	Automatische Installation mit FAI	Christian Meissner
18	27.04.–29.04.	NEU High-End-Mailserver: Postfix am Limit	Peer Heinlein
19	04.05.–08.05.	LPI-Zertifizierung (LPIC-1)	Andreas Niederländer
19	04.05.–08.05.	Xen – Virtualisierte Server	Timo Benk

KW	Datum	Kurs	Dozent
20	11.05.–15.05.	Linux Admin Fortgeschrittene	Peer Hartleben
20	11.05.–15.05.	Nagios Networkmonitoring	Sven Velt
22	25.05.–29.05.	Samba und LDAP	Stefan Kania
22	25.05.–29.05.	LPI-Zertifizierung (LPIC-2)	Andreas Niederländer
24	08.06.–09.06.	NEU Scalix - der Groupwareserver	Dirk Ahrnke
24	08.06.–09.06.	Hochverfügbarkeit mit Heartbeat2 und LVS	Dr. Michael Schwartzkopff
24	10.06.–12.06.	NEU Windows-Software-Verteilung mit opsi	Detlef Oertel
25	15.06.–19.06.	Linux Admin Grundlagen	Peer Hartleben
25	15.06.–19.06.	Sichere Mailserver mit Postfix	Peer Heinlein
27	29.06.–01.07.	SpamAssassin und AMaViS	Peer Heinlein
27	29.06.–01.07.	Cyrus IMAP-Server	Peer Hartleben
27	02.07.–03.07.	4. Mailserver-Konferenz in Berlin	Konferenz

EGGENET: Migration von 120.000 Mailkonten auf eine neue Plattform

EGGENET, eine Marke der EWE TEL GmbH (Oldenburg) mit Sitz in Paderborn, ist ein bedeutender IT-Partner für Mittelstand, Kommunen und öffentliche Einrichtungen. Mit einem zertifizierten Kundenrechenzentrum und modernen IT-Lösungen im Bereich Sicherheitstechnik, Storage und Servervirtualisierung ist EGGENET für zukünftige Marktanforderungen bestens gerüstet.
Anfang 2008 stand EGGENET vor der herausfordernden Aufgabe, im laufenden Betrieb ca. 120.000 Mailkonten auf eine neue Mailplattform ins eigene zertifizierte Rechenzentrum zu migrieren. Durch das von Peer Heinlein und seinem Team mit viel persönlichem Engagement eingebrachte Know How und die tatkräftige Unterstützung auch ausserhalb der normalen Geschäftszeiten konnte das Projekt in kürzester Zeit und mit einem jederzeit guten Gefühl erfolgreich abgeschlossen werden.

Oliver Rolfes, Stellv. Leiter Systemtechnik EGGENET

Desktop-SATA: Restrisiko trotz RAID

Bei Betrachtung aktueller Festplattenverbundsysteme, die eine immer größere Anzahl Festplatten mit stetig wachsender Speicherkapazität in RAID-Sets zusammfassen, sollte heute überprüft werden, ob der Einsatz des Parity-RAID-5 bezüglich der Verfügbarkeit, Ausfallsicherheit und Speichereffizienz noch sicher genug ist. Denn: Je größer die Festplatten, desto größer das Ausfallrisiko im RAID.

Die zu betrachtenden Faktoren sind dabei die vom Hersteller definierte Lebenszeit der Festplatten (MTTF: Mean Time To Failure), die durchschnittliche Zeitspanne zur Reparatur (MTTR: Mean Time To Repair), die Festplattenanzahl im RAID-Verbund (N) sowie die Anzahl der Festplatten der ParityGroup (G).
Bei einem Parity-RAID wie RAID-5 oder RAID-6 entsteht ein Datenverlust durch den Ausfall einer Platte während eines bereits erreichten inkonsistenten Zustands. Die durchschnittliche Zeit bis zum Datenverlust (MTTDL: Mean Time To Data-Loss) ergibt sich also aus der Wahrscheinlichkeit eines mehrfachen Ausfalls von Festplatten vor dem vollständigen Abschluss eines Rebuilds.
Für RAID-5 definiert sich der Datenverlust beim Ausfall von zwei Festplatten (DDF: Double Disk Failure) anhand der Formel:

$$DDF = \frac{MTTF^2}{N \times (G-1) \times MTTR}$$

Da RAID-6 den Ausfall von zwei Festplatten verkraftet, ist die Wahrscheinlichkeit eines Triple Disk Failure (TDF) zu berechnen:

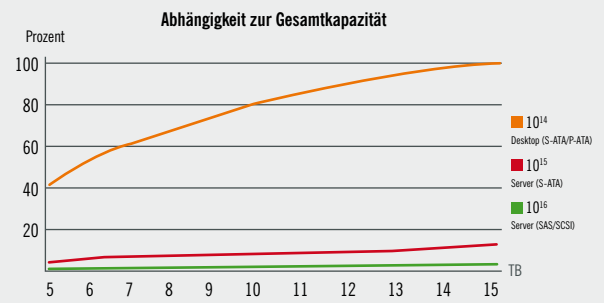
$$TDF = \frac{MTTF^3}{N \times (G-1) \times (G-2) \times MTTR^2}$$

Als durchschnittliche Lebenszeit von RAID-5 und RAID-6 ergibt sich:

Disks	6	10	20	40
RAID-5 $_{MTTDL}$	9.937	3.312	784	191
RAID-6 $_{MTTDL}$	25.876.945	4.312.732	453.972	52.381

Berechnungsgrundlage: MTTF 250.000 h, MTTR 24 h, MTTDL in Jahren

Bei der einfachen Berechnung hätte RAID-5 selbst mit 40 Festplatten noch eine durchschnittliche Lebenszeit von ca. 190 Jahren.
Doch leider gilt dies nur bei oberflächlicher Betrachtung ohne Berücksichtigung der Bitfehlerwahrscheinlichkeit (BER). Dahinter verbirgt sich das Ausfallrisiko einzelner Sektoren einer Festplatte. Während eines Rebuilds muss gewährleistet sein, dass auf den verbliebenen Festplatten absolut alle Sektoren fehlerfrei ansprechbar sind, andernfalls ist ein Datenverlust nicht mehr abzuwenden. Das Risiko eines defekten Plattensektors ist abhängig von Bitfehlerwahrscheinlichkeit und Größe der verwendeten Festplatten. Dabei gilt: Je größer die Platte, desto kleiner die Wahrscheinlichkeit P, nach der alle Sektoren noch erfolgreich und fehlerfrei gelesen werden können.



Je höher die Kapazität desto höher steigt das Ausfallrisiko.

Die vollständigen Formeln lauten also:

$$RAID\text{-}5:\ DF + BER = \frac{MTTF}{N \times (1-p_{disk}^{(G-1)})}$$

$$RAID\text{-}6:\ DDF + BER = \frac{MTTF^2}{N \times (G-1) \times (1-p_{disk}^{(G-2)}) \times MTTR}$$

Große Festplatten erhöhen also das Ausfallrisiko. Je nach eingesetzten Platten und ihrer Qualität können plötzlich Zeiträume erreicht werden, die gerade bei minderwertigen Desktop-P/SATA-Platten einen Datenverlust in sehr riskante Nähe rücken können.

Disks	6	10	20	40
RAID-5 $_{MTTDL}$	26	9	3	1
RAID-6 $_{MTTDL}$	65.956	11.888	1.507	242

Berechnungsgrundlage: MTTF 250.000 h, Desktop-SATA mit P = 96%, MTTR 24 h, TTDL in Jahren

Zugegeben: Die hier gezeigten Zahlen basieren jeweils auf worst-case-Annahmen in MTTF, MTTR, Plattengröße und Bitfehlerwahrscheinlichkeit. Gute Serverhardware lässt die Rechenergebnisse schnell anders aussehen.
Aber es ist deutlich zu sehen: Auch im RAID können nicht beliebig billige große Platten risikolos eingesetzt werden.

Holger Uhlig

HEINLEIN

LINUX: AKADEMIE · SUPPORT · HOSTING

Impressum:

Heinlein Professional Linux Support GmbH

Schwedter Straße 8/9 B, 10119 Berlin

Telefon: 030/40 50 51-0, Telefax: 030/40 50 51-19

http://www.heinlein-support.de, mail@heinlein-support.de

V.i.S.d.P.: Peer Heinlein, Schwedter Str. 8/9 B, 10119 Berlin

Tool der Ausgabe: „screen“

Wer kennt das nicht: Man startet einen langwierigen Prozess auf einem entfernten Rechner aber die Internetverbindung ist nicht besonders stabil und reißt gerne mal ab. Um dennoch dafür zu sorgen, dass der Prozess fertig wird, erinnert man sich gerne an die Zeit der langsamen Modemverbindungen zurück. „screen“ ist hier genau das Mittel der Wahl.

Startet man „screen“ ohne weitere Parameter, erhält man eine leere Shell zur freien Verwendung. Mit [ctrl]+[a] [c] lassen sich Shell-Fenster öffnen, durch die man mit [ctrl]+[a] [n] bzw. mit [ctrl]+[a] [p] navigieren kann. Mit [ctrl]+[a] [S] kann die Ansicht gesplittet werden. Mit [ctrl]+[a] [TAB] kann man zwischen den einzelnen Fenstern hin und her switchen. Möchte man einen Screen verlassen, ohne die darin laufenden Programme zu beenden, lässt sich dies mit [ctrl]+[a] [d] erledigen. Um später wieder auf eine derart ‚detachete‘ Session aufspringen zu können, startet man „screen -rd“.

Übrigens: Screen ermöglicht auch die gemeinsame Nutzung einer Session. Perfekt für eine gemeinsame remote-Administration oder zu Schulungszwecken. Dazu öffnet User A ganz normal einen screen, auf den sich User B mittels „screen -x“ dazuschalten kann.

Vortragsbühne auf der CeBIT 2009

Wir freuen uns auf viele spannende Projekte 2009 und auf interessante Gespräche auf der CeBIT. Denn hier werden wir dieses Jahr zusammen mit Univention etwas Neues probieren: Auf 50 Quadratmetern werden wir nicht nur unseren Stand, sondern auch eine eigene Bühne unterbringen. Dort bieten wir Vorträge zu vielen wichtigen Themen rund um die Linux-Serveradministration, die Sie jeden Werktag hören können. Wir präsentieren dabei Know-how zu Fachthemen, keine Produkt- oder Sales-Präsentationen. Das Vortragsprogramm haben wir als Appetizer auf **http://www.heinlein-support.de/cebit** hinterlegt. Besuchen Sie uns doch einfach – wir freuen uns auf ein Wiedersehen! Eintrittskarten erhalten Sie auf Anfrage gerne von uns.

Neue LPI-Prüfungen

Zum 1. April veröffentlicht das Linux Professional Institute (LPI) neue Inhaltsangaben und neue Fragen für die LPI Level-1 und Level-2. Wer sich auf die Prüfungen vorbereitet, sollte nach den neuen Vorgaben lernen, um unliebsame Überraschungen zu vermeiden. Server-Themen wie Apache, Samba und NFS wurden in die Level-2-Prüfung verschoben. Gleichzeitig kamen Themen wie USB, SQL, aptitude/yum, Lokalisierung und PGP/GnuPG in die Level-1-Prüfung hinein. Das LPIC-1-Buch von Peer Heinlein ist ab März in einer entsprechend überarbeiteten 4. Auflage verfügbar: **http://www.lpi-buch.de**

RBL-Listen abgeschaltet

In den letzten Monaten haben diverse RBL-Listen (Blacklists gegen Spamversand) ihren Dienst eingestellt. Postmaster müssen penibel darauf achten, keine abgeschalteten RBL-Listen in ihrer Konfiguration zu haben. Andernfalls kann es dazu kommen, dass Mailserver plötzlich sämtliche Mails ablehnen.

Folgende Listen haben ihren Dienst eingestellt:

- list.dsbl.org
- blackholes.easynet.nl
- opm.blitzed.org
- relays.ordb.org

Heinlein Support empfiehlt, sich ausschließlich auf die drei besten RBL-Listen zu verlassen. Der Einsatz weiterer kleinerer Listen verbessert kaum noch die Qualität, bringt oft sogar schlechtere Ergebnisse und erhöht das Ausfallrisiko.

Nutzen Sie bevorzugt:

- zen.spamhaus.org
- bl.spamcop.net
- ix.dnsbl.manitu.net

Diese bringen gute 60-70 % Trefferquote bei 0 % false positives (http://stats.dnsbl.com). Oder greifen Sie auf einen Dienst wie policyd-weight zurück, der verschiedene RBLs gewichtet.