

Bewerbung

der

**Byte Action GmbH
Auf der Beune 83-85**

64839 Münster

für den

**KVD Service Management Preis 2006
des
Kundendienst-Verband
Deutschland e.V.**

SPAM – ein unterschätztes Unternehmensrisiko

Darstellung einer Service-Dienstleistung zum Schutz des elektronischen Geschäftsverkehrs für Unternehmen vor unerwünschtem und massenhaft zugestelltem elektronischen Werbemüll.

ByteAction GmbH
Auf der Beune 83-85
64839 Münster
www.byteaction.de

Tel: +49 (0)700 ByteAction
+49 (0)700 29832284
Fax: +49 (0)700 29832284
e-mail: info@byteaction.de

AG Darmstadt, HRB 33271
Steuernummer: 07229 50569
Ust-Id: DE206997247

Geschäftsführung:
Thomas Volkert

Sparkasse
Langen-Seligenstadt
Konto 38 111 761
BLZ 506 521 24

Vereinigte Volksbank
Maingau eG
Konto 74 213 38
BLZ 505 613 15



1.	Zusammenfassung	3
1.1	ByteAction	4
1.2	Argumente (Ausschnitt)	4
2.	Spam	5
2.1.	Entwicklung von Spam	5
2.2.	Herkunft von Spam	6
2.3.	Risiken	6
3.	Das Projekt	8
3.1.	Kein Spam in Aschaffenburg	8
3.2.	Eskalation	8
4.	Lösung	9
4.1.	Hardware	9
4.2.	Software-Architektur	10
4.2.1.	RBL	10
4.2.2.	Heuristische Filter	10
4.2.3.	Bayes'sche Filter	10
5.	Datenschutz	12
6.	Kosten	12
7.	Herausforderung Service	13
8.	Fazit	14
9.	Projekt Snapshot	15
10.	Anlagen: Ergänzende Informationen	

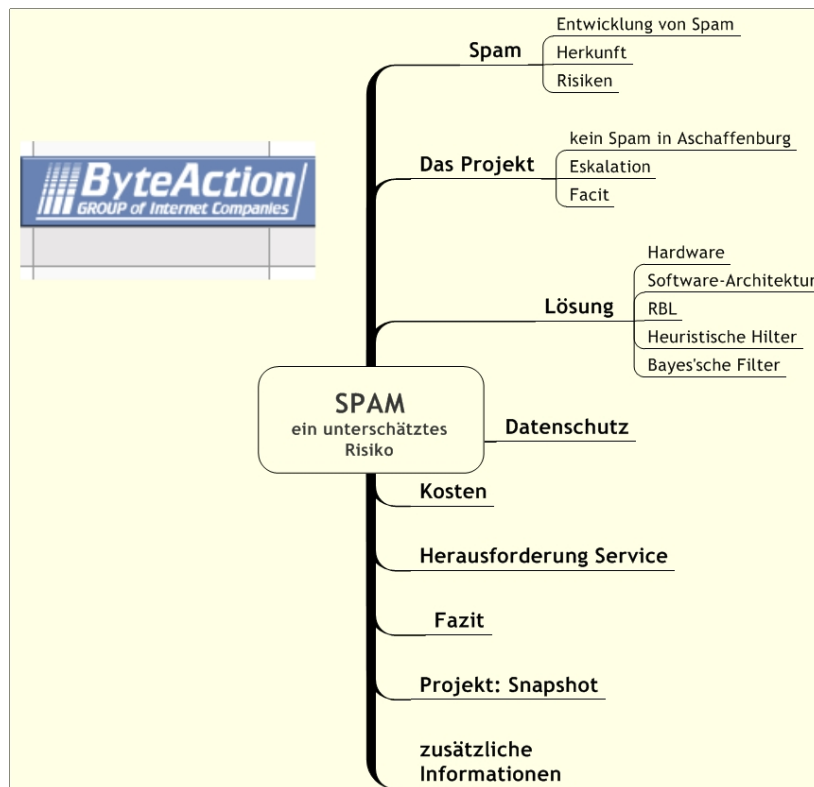
1. Zusammenfassung

Ziel der Ausarbeitung ist die Darstellung der Risiken von Spam-Mails bei der Unternehmenskommunikation. Am Beispiel einer realen „Best Practise“ Installation wird aufgezeigt, welche massiven Beeinträchtigungen und Störungen durch fehlende Spam-Filterung entstehen können.

Es wird dargestellt, mit welchen technischen Mitteln und mit welcher Software, schnell und kostengünstig ein angemessenes Schutzniveau erreicht werden kann.

Als Referenzlösung wurde ein neutrales Projekt (kein Wettbewerber zu KVD-Mitglieder) ausgewählt.

Das Projekt wurde zum Jahreswechsel 2004/2005 bei der Stadtverwaltung Aschaffenburg geplant, installiert und abgeschlossen. Die dort vorhandenen Kriterien sind auf jede andere Firma übertragbar, welche das „Medium –eMail“ als wichtige Kommunikationslösung einsetzt.



1.1 ByteAction GmbH

Die Byte Action GmbH, mit derzeit 25 Mitarbeitern, ist ein mittelständisches IT- und ISP-Unternehmen. Unser Anspruch ist seit Jahren die qualifizierte, kompetente Erbringung von Full-Service-Dienstleistungen. Als erfahrenes Systemhaus und Hersteller eigener richtungweisender Lösungen im IT-Umfeld (Kernkompetent eMail / IP-Kommunikation) agieren wir in einem wachstumsstarken Markt.

Wir verstehen uns als „Internet Solution Company“ mit innovativen Produkten in den Bereichen Organisation von E-Mail, Netzwerken und Internet. Das Leistungsspektrum reicht von der Spamfilterung über Virenschutz, Web-Design, Content-Management, Ticketing- und Troubleshooting-systeme sowie rechtskonforme E-Mail Archivierung gemäß der GDPdU.

1.2 Argumente (kleiner Ausschnitt) für die Lösung (Spamfilter):

Thema Erreichbarkeit / Effizienz usw...

dies optimiert das eMailaufkommen für die Mitarbeiter	nur die relevanten eMail zugestellt werden
und spart Zeit	weil die Mitarbeiter dann nicht mehr sortieren / suchen müssen
diese spart zusätzliche Kosten für weiteres Gerät	der vorhandene Mailserver entlastet wird
dies reduziert Unterhaltungskosten	Service und Updates aus einer Hand
steigert Ihre Produktivität	Mitarbeiter mehr Zeit haben
steigert Ihre Effizienz	Mitarbeiter können sich um Kernaufgaben kümmern
schützt Sie vor Rechtsstreitigkeiten	da automatische Sortierung erfolgt (Datenschutz)

Weitere Module, z.B. für die Einhaltung der Gesetzesvorgaben zur eMail-Archivierung sind verfügbar.

2. SPAM – ein unterschätztes Unternehmensrisiko

Spam?

Als **Spam** [*'spɛm*] werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt und unerwünscht zugestellt werden und massenhaft versandt wurden oder werbenden Inhalt haben. >Quelle Wikipedia<

2.1. Entwicklung von Spam / „Massenrundschriften“

Seit 1988 wurden weltweit zunächst Briefe und später Faxe verschickt, in denen z.B. den Empfängern große Summen versprochen werden, wenn sie afrikanischen Geschäftsleuten behilflich seien, riesige Dollarbeträge außer Landes zu schaffen. Dabei handelt es sich regelmäßig um Beträge in Millionen Dollar und auch der Anteil, der dem Empfänger zufallen soll, liegt in entsprechender Höhe. Natürlich hat niemand jemals dieses Geld gesehen und seinen Einsatz erst recht nicht. Diese als „Nigeria-Connection“ bekannt gewordene Masche gibt es bis heute. Aber auch dieser Personenkreis hat aufgerüstet und nützt E-Mails, um neue Opfer zu finden.

Auch Kettenbriefe „geistern“ seit geraumer Zeit durch das Internet und sind genauso ein Ärgernis wie die, die mit der Post kamen.

Konventionelle Kettenbriefe nach Pyramiden-Schemata verführen zum scheinbar schnellen Gelderwerb oder sind als Hilfsaktionen getarnt. Ein beliebter Streich besteht darin, eine unbeliebte Person als Absender anzugeben, damit sie anschließend ihre helle Freude an Beschwerdebriefen hat. Solche Opfer können dann über Monate hinweg mit täglich mehreren Dutzend Reaktionen rechnen. Da hilft dann oft nur noch sich eine neue Mailadresse zuzulegen (wenn dies überhaupt geschäftlich möglich ist). Jeder Versuch zu antworten und Aufklärung zu betreiben verschlimmert die Situation nur.

Inzwischen sind die Techniken der Spammer erheblich verfeinert. Viele, besonders private Computer, sind als so genannte „Zombies“ unbemerkt durch Trojaner übernommen worden und dienen Versendern als Relaystationen um massenhaft Spam zu versenden. Diese in Millionenaufgabe ge-mailte Werbung erreicht offensichtlich ihren wirtschaftlichen Zweck. Wenn nur ein Bruchteil der Empfänger die beworbenen Produkte bestellt, dann ist das Ziel erreicht. Die wachsende Flut der Spam-Mails lässt also vermuten, dass auf diese Art ein erhebliches Gewinnpotential für Spammer und Ihre Auftraggeber vorhanden ist.

Sie werden also weitermachen und Ihre Aktivitäten ausweiten. Inzwischen ist Spam längst kein Scherz mehr, sondern es besteht ein massives wirtschaftliches Interesse als Antriebsfeder.

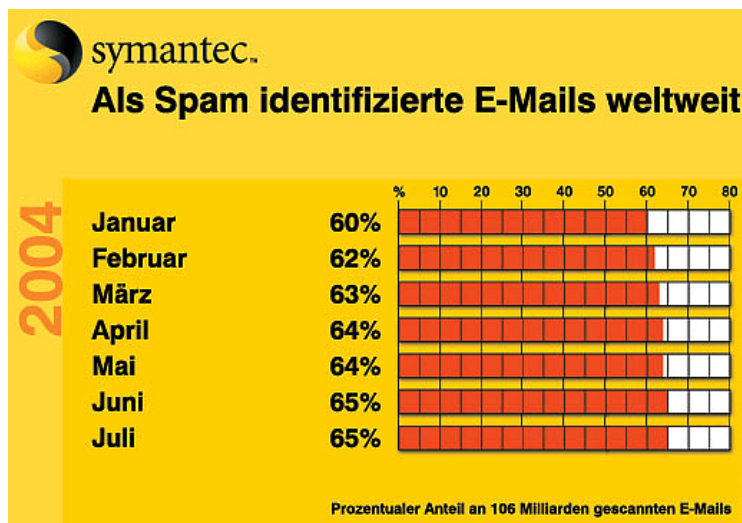
2.2. Herkunft von der Bezeichnung „Spam“

Die Bezeichnung SPAM leitet sich aus einem „Sketch“ von Monty Python ab. Darin werden einem Gast im Restaurant immer wieder Gerichte mit Spam angeboten. Diese haben zum Teil mehrfach die Bezeichnung Spam im Namen. Als der Gast nach einem Gericht ohne Spam verlangt wird ihm eines mit wenig Spam angeboten. Im Sketch wird das Wort Spam über 100 Mal verwendet. Erstmals wurde der Begriff dann im Usenet (dem Vorläufer des Internet) für das unsinnige wiederholen von Beiträgen mit gleichem Inhalt verwendet.



2.3 Risiken

Nicht zu unterschätzen sind die erheblichen Gefahren, die von den neuesten Spam-eMails ausgehen. Wenn in der Vergangenheit im Wesentlichen für „Viagra & Co“ geworben wurde beinhalten die neusten Spambotschaften immer häufiger Viren, Würmer und Trojaner. Damit sind diese Mails nicht mehr nur ein zeitraubendes Ärgernis für die Systemadministratoren und Anwender, sondern bergen höchstes Risiko für die betroffenen Unternehmen. Inzwischen verbergen sich „Schadsoftware“ auch in Bildern oder aktivieren sich zu Teil unbemerkt und selbsttätig wenn z.B. die HTML-Vorschauansicht in Outlook eingeschaltet ist.



ByteAction GmbH
Auf der Beune 83-85
64839 Münster
www.byteaction.de

Tel: +49 (0)700 ByteAction
+49 (0)700 29832284
Fax: +49 (0)700 29832284
e-mail: info@byteaction.de

AG Darmstadt, HRB 33271
Steuernummer: 07229 50569
Ust-Id: DE206997247

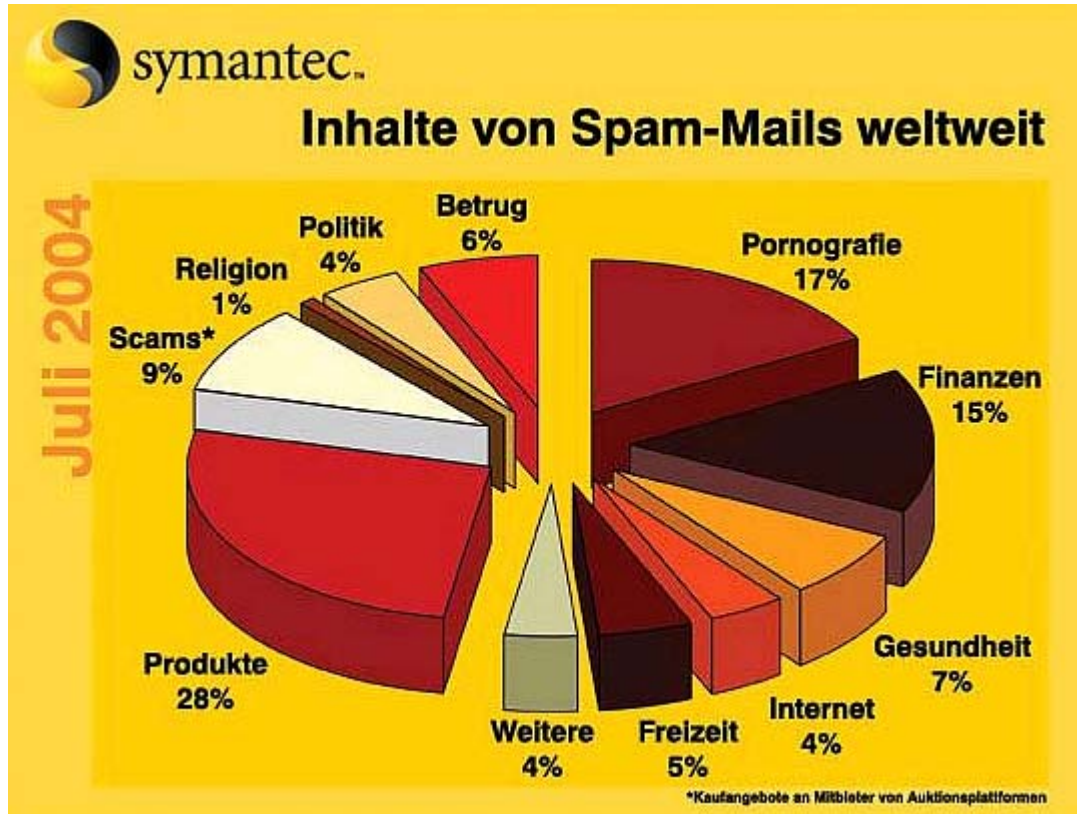
Geschäftsführung:
Thomas Volkert

Sparkasse
Langen-Seligenstadt
Konto 38 111 761
BLZ 506 521 24

Vereingte Volksbank
Maingau eG
Konto 74 213 38
BLZ 505 613 15

ByteAction
GROUP of Internet Companies

Von daher ist es unabdingbar sich nachhaltig vor Spam zu schützen. Dies bedeutet eine Erweiterung der vorhandenen Schutzmechanismen wie z.B. Firewall und Anti-Virensoftware und ein erhöhtes Maß an Sensibilisierung der Administratoren und Anwender.



Das Spamaufkommen ist bis heute kontinuierlich gestiegen und es ist keine Trendwende in Sicht. Selbst eine Gesetzesänderung würden die meisten Spammer nicht betreffen, da sie sich im Ausland befinden und nicht unter der deutschen Gerichtsbarkeit fallen.

Die Inhalte können jedoch für die Geschäftsleitung (in einem deutschen Unternehmen) zu einem sehr großen Risiko werden. Wenn z.B. Kinderpornografische Bilder von einem Spammer angeboten und dann von einem Mitarbeiter geladen werden (kein Bussgeld sondern ein Straftatbestand!).

3. Projekt:

3.1. „Kein Spam in Aschaffenburg“

Seit Mitte 2004 wurde auch die Stadtverwaltung Aschaffenburg immer wieder Opfer von Spam-Mail. Aber das Aufkommen hielt sich in Grenzen und Anwender und Administrator erledigten die Löschung einfach nebenher. Nur nach längerer Abwesenheit, z.B. nach dem Urlaub fiel störend auf, dass dann immer ein erheblich



größerer Zeitaufwand erforderlich war, die Spam-Mails zu bearbeiten und zu löschen. Nach den Urlaubstagen waren üblicherweise 200 Spam Mails zu identifizieren. Dies machte dann über 50% der erhaltenen elektronischen Post des Betroffenen aus.

Es nervte zwar und störte den Arbeitsablauf aber man war doch immer noch der Auffassung eine zusätzliche Investition für eine automatisierte Spam-Abwehr sparen zu können. Noch glaubte man, dass das Sicherheitskonzept aus Firewall und Virens Scanner auf dem Mailserver und allen Workstations ausreichen würde.

3.2. Eskalation

Dann, im Dezember 2004 eskalierte die Situation. Auf einmal trafen zwischen 10.000 und 14.000 Spam-Mails täglich ein. Der Spitzenwert lag bei knapp 30.000 Mails innerhalb von 24 Stunden. Eine geregelt Bearbeitung der elektronischen Post war nicht mehr möglich. Der Mailserver und die vorhandene Virenschutzsoftware kam den Anforderungen nicht mehr nach. Anwender und Systemadministrator waren völlig überfordert, zumal der größte Teil der Spam-Mails mit Viren verseucht war. Damit kam es dann zwangsläufig zum zeitweiligen Stillstand des Mailservers.

Wenn auch bisher die IT-Organisation der Meinung war die Situation beherrschen zu können war dies der Zeitpunkt dringend nach einer Lösung zu suchen. In dieser Situation war es natürlich nicht möglich, lange Vorbereitungszeiten und Recherchen durchzuführen. Eine schnelle, effiziente aber auch kostengünstige Lösung musste her. – Jetzt aber sofort!

Für die Stadtverwaltung hatte Byte Action bereits 2003 die Internet und Web-Anbindung der Nebenstellen und der externen Betriebsstätten erfolgreich realisiert. Da die ByteAction den Kontakt mit der IT-Abteilung der Stadtverwaltung gepflegt hatte wurde ByteAction mit der Lösung des Problems beauftragt.

4. Lösung

Bereits nach zwei Tagen installiert ByteAction noch am 23. Dezember ein Testsystem. Dabei handelte es sich um die von ByteAction selbst entwickelte Linux-Software „Excubator“ die auf einem „Sun Fire V20z“ Server ausgeliefert wurde. Aufgrund der vorherigen intensiven Abstimmung mit der IT-Abteilung konnte der bereits vorinstallierte Server in weniger als einer Stunde in der Stadtverwaltung aufgebaut, die Firewall eingerichtet und der Mailserver wieder in Betrieb genommen werden. Eine kurze Einführung für die Systemadministratoren folgte und dann fiel der Startschuss für das Projekt.

„Wie ein Weihnachtsgeschenk“ war dies, nach Aussage des IT-Verantwortlichen, da auch erreicht werden sollte, dass nach den Weihnachtsferien zum Arbeitsbeginn im neuen Jahr nicht erst zehntausende Spam-Mails bearbeitet werden müssen.

Das System arbeite von Anfang an überzeugend und ging bereits Anfang Februar in den Regelbetrieb. Ab sofort war die Spam-Flut wieder beherrschbar. Der zusätzlich zu den bestehenden Viren-Scannern und der bestehenden Firewall eingezogene Schutzwall reduzierte die Spam-Belastung gegen Null.

4.1. Hardware

Als Hardwareplattform wurde ein handelsüblicher Sun-Fire-V20z-Server eingesetzt. Dieser wurde in Unternehmen vollständig vorkonfiguriert und getestet.



Die technischen Daten der verwendeten Hardware:

Sun Fire V20z GenPurpose 1U Rack Mnt
Linux/Solarisx86 Server: 1xAMD Opteron 242CPU,1GB
DDR1/333 Registered ECCDIMMs (2x512MB),
1x36GB 10K RPMUltra320 SCSI disk,
2x10/100/1000Ethernet ports, RAID 1,

Excubator® ist eine eingetragene Marke der ByteAction GmbH

ByteAction GmbH
Auf der Beune 83-85
64839 Münster
www.byteaction.de

Tel: +49 (0)700 ByteAction
+49 (0)700 29832284
Fax: +49 (0)700 29832284
e-mail: info@byteaction.de

AG Darmstadt, HRB 33271
Steuernummer: 07229 50569
Ust-Id: DE206997247

Geschäftsführung:
Thomas Volkert

Sparkasse
Langen-Seligenstadt
Konto 38 111 761
BLZ 506 521 24

Vereinigte Volksbank
Maingau eG
Konto 74 213 38
BLZ 505 613 15



4.2. Software-Architektur

Das auf Linux-basierte Filtersystem wird üblicherweise zwischen einer bestehenden Firewall und dem Exchange-Server installiert. Nachdem eine Nachricht die Firewall passiert hat, durchläuft sie das mehrstufige Prüfsystem des *ExcubaTor* (*Produktname*).

4.2.1. RBL (Real-Time Black Hole List)

Zuerst checkt das System entsprechend den Absendeinformationen im Mail-Header (technische Absendeadresse) alle bekannten Spam-Quellen durch. Die dabei verwendete RBL-Liste mit den bekannten Spam-Versendern wird natürlich fortlaufend aktualisiert. Sie wird per Update auf dem neusten Stand gehalten. Die Administratoren können zusätzlich als Spammer identifizierte Absenderadressen selbst ergänzen. Alle Mails mit diesen Absendern werden vom System nicht mehr durchgelassen, bzw. direkt abgelehnt.

4.2.2. Heuristischen Filter

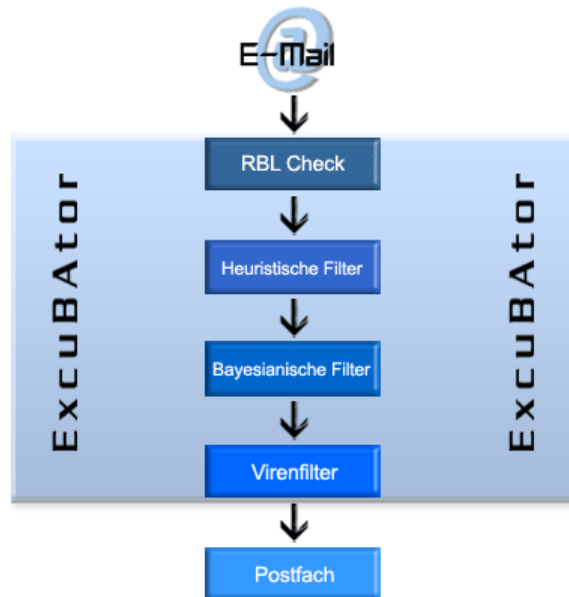
Die übrigen Nachrichten laufen dann in den Heuristischen Filter. Dieses auf bestimmte Regeln basierende System analysiert die eingehenden E-Mails aufgrund ihres Designs (HTML-Anteil, eingebettete Bilder, Farbverteilung, etc.). Werden dabei die vom Administrator festgelegten Schwellwerte überschritten kommen die Mails erst einmal in Quarantäne. In Abstimmung mit den Empfängern ist dann über die weitere Verwendung der Mails zu entscheiden.

4.2.3. Bayes' -scher Filter

Zuletzt durchlaufen die Mails den „Bayesianischen Filter“. Dieser ermittelt die Spam-Wahrscheinlichkeit aufgrund ihres Inhaltes. Die Bayes'sche Filtertechnologie basiert auf dem mathematischen Prinzip, dass Ereignisse voneinander abhängig sind und dass die Wahrscheinlichkeit eines künftigen Ereignisses aus vorhergehenden Eintrittsereignissen abgeleitet werden können.

Erfahrungsgemäß kommen bestimmte Begriffe und Inhalte überwiegend in Spam-Nachrichten vor. Werden diese in neuen E-Mails gefunden schließt das System mit großer Wahrscheinlichkeit auf Spam und stellt die Mail ebenfalls in Quarantäne.

Bevor Nachrichten mit dieser Methode gefiltert werden können, muss eine Datenbank mit den „Spam-Beispielwörtern“ angelegt werden. Diesen Worten wird ein rechnerischer Wahrscheinlichkeitswert zugewiesen. Als Datenmaterial dienen die eigene ausgehende Benutzerpost und Analyseergebnisse bekannter Spam-Mitteilungen. Die Filterwörter werden in eine „Spam- und eine Ham-Liste“ eingeteilt. Damit ergeben sich eine positive und negative Auswahlliste. Im Laufe der Zeit kann eine optimale Filterquote von bis zu 99,9% erreicht werden. Dazu ist allerdings die Pflege und Aktualisierung der Wortlisten durch die Admins (oder auch Anwender) erforderlich. Schließlich dürften sich die Inhalte der Auswahllisten je nach Geschäftszweck stark unterscheiden. Während bei der Stadtverwaltung das Wort Viagra sicher auf der Negativliste zu finden wäre, kann es in einem Pharmakonzern schon geschäftsrelevant sein.



Zum Schluss durchlaufen die Mails das Virensystem (hier Trend Micro). Es kann aber auch jedes andere Virenabwehrsystem eingesetzt werden (kundenwunschabhängig, z.B. Symantec, H+B EDV, F-Secure usw.). Diese Entscheidung liegt letztendlich in den jeweiligen Präferenzen des Kunden. Die offene Architektur unter Linux ist ein entscheidender Produktvorteil von *Excubator* und war ein positives Auswahlkriterium der Stadtverwaltung. Bei Bedarf kann diese Komponente der Spam-Abwehr jederzeit angepasst oder ausgetauscht werden. Ebenso gibt es Zusatzmodule die auch die revisionssichere Archivierung ermöglichen (z.B. geschäftsrelevanter eMails nach GDPdU / Basel 2).

5. Datenschutz

Im Zusammenhang mit der Quarantänefunktion muss sichergestellt sein, dass der Administrator die E-Mails nicht einfach sehen kann. Das ByteAction System ist so konzipiert, dass der Administrator nur den Header und die Kopfzeile sieht. Im Einzelfall muss anschließend mit dem jeweiligen Mitarbeiter Kontakt aufgenommen werden, um über die weitere Vorgehensweise zu entscheiden.

Viele der vorwiegend amerikanischen System berücksichtigen dabei die gesetzlichen Bestimmungen des Bundesdatenschutzgesetzes an dieser Stelle nicht, sondern legen den Admins sämtliche Daten offen. Dies hätte bei diesem Projekt der Betriebsrat definitiv nicht zugelassen und auch der Datenschutzbeauftragte würde sein Veto eingelegt haben. Von der persönlichen Haftung des Geschäftsführung im Streitfall einmal ganz abgesehen.

6. Kosten

Die Investitionskosten hielten sich für die Stadtverwaltung in Grenzen. Die Gesamtsumme des Projektes belief sich auf ca. 3.500 EUR.

Bei einer Behörde mit 20 Servern und ca. 400 Arbeitsplätzen beträgt die Investition damit nur etwa 8 EUR pro Arbeitsplatz.

In einem mittelständischen Unternehmen mit 25 Mitarbeitern können die durch Spam verursachten Kosten (für die Identifizierung, Bearbeitung und Entfernung von Spam) leicht 10.000 EUR und mehr pro Jahr verursachen.

Beispielsrechnung:

Wenn jeder Mitarbeiter nur 5 Minuten pro Tag für Spam aufwenden muss und Probleme mit virenbehafteten Mails dabei noch nicht berücksichtigt sind, entstehen bei angenommenen 25 EUR Stundenkosten bereits Kosten von 12.500 EUR.

25 Mitarbeiter x 5 Minuten	= 125 Min./Tag
125 Min. x 20 Tage/Monat	= 2.500 Min/Monat
2.500 Min. x 12 Monate	= 30.000 Min. = 500 Stunden/Jahr
500 Std. x 25 EUR	= 12.500 EUR

Selbst bei kleinern Unternehmen dürften sich die Investitionskosten in kürzester Zeit amortisieren. Sollte es allerdings durch verseuchte E-Mails zu einer Störung oder sogar zum Verlust von Unternehmensdaten kommen, stehen Kostenaufwand für die Absicherung schnell in krassem Missverhältnis zum angerichteten Schaden.

Zur Bewertung der durch Spam vernichteten Unternehmensproduktivität findet sich auf dem Byte Action Webseite ein „Spam-Rechner. Dieser gibt eine exakte Vorstellung der Kosten die in Unternehmen durch Produktivitätsverlust anfallen.

<http://www.byteaction.de/typo/index.php?id=326>

7. Herausforderung Service

Einziges Wermutstropfen war der Ausfall eines Controllers des verwendeten Rechners in den ersten Tagen. Aber so ärgerlich die Störung auch war, bot Sie die Chance zu zeigen, dass auch der Kundendienst bei ByteAction reibungslos funktioniert.

Vier Stunden nach Eingang der Störungsmeldung war der Controller ausgetauscht und der Schaden behoben. Das System lief wieder zur vollen Zufriedenheit.

Der ByteAction Support und Service ist für seine Kunden 24 Stunden, 7 Tage die Woche erreichbar. Außerhalb der regulären Geschäftszeiten sind die Spezialisten über eine 0700-Vanity Nummer zu erreichen. In den meisten Störfällen kann die telefonische Unterstützung sofort weiterhelfen. Wenn erforderlich kommt der Mitarbeiter aber natürlich auch vor Ort.

8. Fazit

„Wie ein Weihnachtsgeschenk“ war die schnelle Umsetzung und Installation, nach Aussage des IT-Verantwortlichen. Schließlich wurde auch erreicht, dass nach den Weihnachtsferien zum Arbeitsbeginn im neuern Jahr nicht erst zehntausende Spam-Mails bearbeitet werden mussten.

Darüber hinaus stehen die E-Mails inzwischen wieder unmittelbar zur Verfügung. Mann muss nicht mehr bis zu zehn Minuten warten bis der Exchange-Server die Mails zustellen konnte. Vor der Installation des Byte Action Systems hatten sich Wartezeiten von bis zu zehn Minuten, durch die erhebliche Auslastung des Servers mit Virenprüfvorgängen ergeben.

Das beschriebene Projekt beweist. Das Risiko, das sich aus der Abwicklung des elektronischen Geschäftsverkehrs ergibt ist erheblich. Da aber dessen Bedeutung noch rasant zunehmen wird, sind angemessene Sicherungsmaßnahmen unbedingt erforderlich. Hohe und gesicherte Verfügbarkeit sind für die Unternehmenskommunikation unabdingbar geworden.

Spam ist neben Viren, Würmer und Co. ein nicht zu unterschätzender Risikofaktor für die Unternehmen und gefährdet die Datensicherheit und Integrität.

E-Mail und Internet bedürfen der besonderen Aufmerksamkeit der Geschäftsleitung, der Administratoren und letztendlich aller Anwender.

Investitionen in eine funktionierende Spamabwehr, in Verbindung mit Firewall und Virenschutz, dürften sich in den meisten Fällen bereits in kürzester Zeit amortisieren.

9. Projekt Snapshot:

Problembeschreibung	Erhöhtes Spam-Aufkommen reduzieren; das zu installierendes Filtersystem muss: <ul style="list-style-type: none"> - einfach bedienbar, - schnell zu realisieren, - in das bestehende System integrierbar, - kostengünstig, - datenschutzrechtlich unbedenklich sein
Kunde	Stadtverwaltung Aschaffenburg
Dienstleister	ByteAction GmbH, Münster www.byteaction.de
Lösung	Software "Excubator" von ByteAction GmbH Hardware: Sun Server Sun-Fire-V20z
Technologie-Lieferant HW	Sun Micro Systems
Software Lieferant	ByteAction GmbH, - Linux-basiertes E-Mail Filter-System
Verhandlungsdauer	2 Tage
Dauer von Auftragserteilung bis Installation	8 Tage
Dauer der Inbetriebnahme	1 Manntag Vorinstallation 1 Stunde Installation und Systemintegration vor Ort
Größte Herausforderung	Ausfall eines HW-Contollers kurz nach der Installation
Kostenumfang	Ca. 3.5000 Euro
Projektverteilung	60% Hardware 40 % Software und Dienstleistung
Schulung	8 Stunden Training für Systemadministrator
Benefit für den Kunden	Schnelle Reaktion und Projektrealisierung, unmittelbar nach der Installation sank das Spam-Aufkommen fast gegen Null, volle Wiederherstellung der Performance des Mailsystems