Pressestelle, Mittwoch, 18. Juli 2007

Richtigstellung des Artikels: \"Wirbel um die elektronische Post\" ín der OP vom 18.07.07

Die Stadt Mühlheim stellt fest: Es gibt keinen „heftigen Streit mit DIKE" - die Stadt Mühlheim hat aus sachlichen Erwägungen heraus die Entscheidung treffen müssen künftig keine Weiterleitung der ‚@muehlheim.de' Adressen anzubieten.

„DIKE war nicht mehr in der Lage das Portal ‚www.muehlheim.de' in Zukunft zu betreuen und hat die Stadtverwaltung gebeten das Werk DIKEs, nämlich den Auftritt der „Digitalen Stadt" zu übernehmen, was die Stadt nicht getan hat. Nach langen Bitten und Betteln haben wir uns breit schlagen lassen, die Mails weiterzuleiten. Dies obwohl die Benutzer von DIKE seit rund einem ¾ Jahr darüber informiert waren, dass sie für ihre E-Mailadressen einen Umleitung zu einer anderen Mailadressen benötigen oder gleich eine neue Mailadresse einrichten sollen. Zur Erklärung: DIKE war ein Jugendprojekt, das Ende Dezember 2006 zu Ende ging. Die Stadt hat lediglich die ihr zustehende Domain ‚www.muehlheim.de' übernommen - nichts weiter! Unser jetziger Auftritt hat nichts mit DIKE zu tun, sondern bildet die Stadtverwaltung und die Tochtergesellschaften ab", so Erster Stadtrat Heinz Hölzel.

DIKE hatte es in der Vergangenheit versäumt, nicht nur die abgemeldeten Benutzer zu streichen, die Postfächer hätten ebenfalls geschlossen werden müssen. „Über ‚@muehlheim.de' kamen die meisten Spams auch auf andere private Adressen an, die jemals über muehlheim.de angeschrieben wurden. Da kann ich privat ein Liedchen davon singen", so Hölzel.

DIKE hat nicht umsonst und aus Nächstenliebe für die Stadt gearbeitet, über das Rathaus hat DIKE pro Jahr 6.000 Euro für den Dienst der Jugendorganisation erhalten.

Es gibt keinen Zweifel darüber, wer rechtlich für die E-Mail-Adressen ‚@muehlheim.de' verantwortlich ist, denn in dem Moment in dem die Stadt rechtmäßiger und eingetragener Inhaber der Domain ‚www.muehlheim.de' ist, zeichnet die Stadtverwaltung für alles verantwortlich, was über die Domain passiert. Dazu gehören die Inhalte auf der Website ebenso wie der E-Mail-Verkehr über ‚@muehlheim.de'. „Und wer die Verantwortung trägt, muss sein Handeln auf www.muehlheim.de auch rechtlich verantworten können".

In diesem Zusammenhang muss erwähnt sein, dass es keine rechtmäßige Möglichkeit gibt, E-Mails von Dritten sortiert zuzustellen!

„Der Unterschied zwischen dem hochgelobten DIKE System und der Weiterleitung der Stadt Mühlheim liegt ganz eindeutig darin, dass DIKE eigene Postfächer eingerichtet hatte über die die jeweiligen Nutzer ihre Mails abgerufen haben und diese Postfächer verfügten über einen Spam-Ordner, wo die als Spam gekennzeichneten Mails eingingen.

Im Rahmen nur einer Weiterleitung (DIKE wurde nicht von der Stadt übernommen) ist es jedoch so, dass alle Mails, die als Spam gekennzeichnet sind automatisch in den Posteingang der Weiterleitungsadresse wandern. Alternativ könnte man höchstens rechtswidrig alle als Spam gekennzeichneten Mails löschen- ohne diese zuzustellen", erklärt Heinz Hölzel den Sachverhalt.

„Wir wissen, dass wir die richtige Entscheidung getroffen haben - auch wenn es für einzelne Nutzer zu Unannehmlichkeiten kommt. Bei allen Nutzern, die nichts mit den unschönen Vorkommnissen zu tun haben, entschuldigt sich die Stadt hiermit nochmals ausdrücklich. Die in der OP angedrohten rechtlichen Schritte seitens DIKE sehen wir als reine Muskelspiele. Auf dieses Niveau lassen wir uns nicht herab. Trotzdem wünschen wir dabei selbstverständlich gute Verrichtung", so der Erste Stadtrat abschließend.

Nachfolgend Auszüge aus http://www.bsi.de/literat/studien/antispam/antispam.pdf**:**

Verletzung des Post- oder Fernmeldegeheimnisses, § 206 StGB

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekannt geworden sind, das geschäftsmäßig Post oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. **eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt** oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

Voraussetzung für die Anwendung der Vorschrift ist zunächst das Erbringen eines „geschäftsmäßigen Telekommunikationsdienstes". Darunter versteht das Telekommunikationsgesetz (TKG) ein „nachhaltiges Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht". Folglich ist weder eine Entgeltlichkeit noch ein gewerbliches Handeln erforderlich. Zum Kreis der Verpflichteten gehören daher neben Access- auch Internet-Service-Provider, die Maildienste anbieten. Diese Voraussetzung wird aber auch von Unternehmen und Behörden erfüllt, die ihren Mitarbeitern einen Online-Zugang bereitstellen und die private Nutzung des Internet gestatten oder dies zumindest tolerieren. „Dritter" im Sinne des § 206 StGB ist in diesen Fällen der Mitarbeiter. Nach der Entscheidung des OLG Karlsruhe fallen auch Hochschulen unter diese Vorschrift. Diese genehmigten nicht nur den Mitarbeitern und Studenten die zumindest auch private Nutzung der Mailaccounts, sondern handelten durch zunehmend engere Kontakte zwischen den Bildungseinrichtungen und Unternehmen zunehmend auch im wirtschaftlichen Bereich.

Keine Dienste für Dritte erbringen dagegen solche Unternehmen und Betriebe, die eine private Nutzung verboten haben. Diese unterfallen folglich auch nicht dem Anwendungsbereich des § 206 StGB. Möglich ist jedoch auch in diesen Fällen eine Strafbarkeit nach § 303a StGB, wie nachstehend dargelegt.

Weiterhin muss die E-Mail dem übermittelnden Server „zur Übermittlung anvertraut" sein. Nach Ansicht des OLG Karlsruhe ist dies zumindest dann eindeutig der Fall, wenn die Anfrage zur Übermittlung von Daten den Mailserver des Unternehmens erreicht hat und der versendende Rechner die Daten dem empfangenden Server übermittelt hat. In dem zu beurteilenden Sachverhalt wurden die E-Mails ordnungsgemäß vom Mailserver der Fakultät „angenommen und quittiert" und erst dann fakultätsintern ausgefiltert.

Die Sichtweise des OLG entspricht der technischen Betrachtung der Problematik. Danach liegt ein Wechsel der Verantwortung für den Mail-Transport vor, sobald der empfangende Server dem Absender-Client den Erhalt der E-Mail bestätigt, damit also im Rahmen des Simple Mail Transfer Protocol am Ende der so genannten DATA-Phase nach Übertragung der Kopfzeilen (header) und des eigentlichen Inhalts der E-Mail (body).

8.6 Behandlung nach der Bewertung

Prinzipiell gibt es mehrere Möglichkeiten mit einer als Spam oder Ham bewerteten E-Mail zu verfahren. Sie kann - möglicherweise mit einer **Markierung** versehen - **zugestellt** werden. Wenn der MTA sich noch im SMTP-Dialog befindet, kann er sie **abweisen.** Außerdem kann er die E-Mail kommentarlos **löschen.** Eine erkannte Spam-Mail zu löschen und dem Absender eine **Fehlermeldung** (bounce) zu senden, ist in keinem Fall zu empfehlen, da nahezu alle Spam-Mails eine gefälschte Absenderadresse tragen und die bounces somit nicht zustellbar sind oder den Falschen erreichen (siehe auch [RFC3834]). Eine Sonderform ist die Zustellung in eine **Quarantänemailbox.**

8.6.1 Zustellen

Als Ham bewertete E-Mails müssen auf jeden Fall normal zugestellt werden. Schwieriger ist es, mit E-Mails umzugehen, die mit mehr oder weniger großer Sicherheit als Spam erkannt wurden. In vielen Fällen wird man sie aber auch dann zustellen, schon um die E-Mail nicht möglicherweise rechtswidrig zu unterdrücken.

Soll die Bewertung überhaupt einen Sinn haben, muss spamverdächtige E-Mail entweder in einen anderen Ordner oder in irgendeiner Weise markiert zugestellt werden (siehe unten).

8.6.2 Abweisen

Der MTA geht am sparsamsten mit den eigenen Ressourcen um, wenn er E-Mails möglichst frühzeitig ablehnt, denn er muss die E-Mail dann nicht auf Festplatte speichern und nicht weiterleiten. In vielen Fällen ist das die beste Lösung. Sie setzt allerdings voraus, dass der verwendete MTA eine E-Mail schon während des SMTP-Dialogs als Spam erkennen kann. Ältere Software ist dazu häufig nicht in der Lage. Inzwischen unterstützen aber fast alle Produkte ein entsprechendes Vorgehen oder bieten zumindest die Möglichkeit, eine solche Funktion einzubauen.

Vorteil dieser Lösung ist, dass der Absender im Falle eines false positive, also der irrtümlichen Abweisung einer Ham-Mail, erfährt, dass seine Nachricht nicht zugestellt wurde.

Nachteil dieser Methode ist, dass sie in der Regel keine benutzerspezifischen Kriterien für die Filterung verwenden kann. Das liegt einerseits an der Architektur der MTAs, die zum Zeitpunkt der Annahme der E-Mail häufig noch nicht wissen, in welche Mailbox eine E-Mail am Ende zuzustellen ist. Andererseits gibt es auch ein Problem mit dem SMTP. Der Absender einer E-Mail kann mehrere Empfänger für eine E-Mail angeben, die im SMTPDialog als mehrere RCPT-TO-Kommandos erscheinen. Zwar kann der Empfänger-MTA die E-Mail für einzelne Empfänger annehmen und für andere ablehnen, aber zu diesem Zeitpunkt im SMTP-Dialog hat er den Inhalt der E-Mail noch nicht gesehen, alle Verfahren, die eine Inhaltsanalyse erfordern, können also nicht greifen.

Vorsicht bei dieser Methode ist auch angebracht, wenn Mailinglisten im Spiel sind. Die Mailinglisten-Software löscht einen Benutzer häufig automatisch aus der Abonnentenliste, wenn sie eine E-Mail nicht zustellen kann. Sie nimmt fälschlicherweise an, dass die Mailadresse nicht mehr existiert.

Statt einer endgültigen Fehlermeldung (permanent negative completion reply) kann der MTA auch eine temporäre Fehlermeldung (transient negative completion reply) zurückgeben.[18] Der Provider des Absenders hat so eventuell die Chance, eine fehlerhafte Filterung zu erkennen und korrigierend einzugreifen, ohne dass der Endanwender etwas davon merkt. Sollte etwa ein legitimer Mailserver auf eine Blacklist geraten sein, kann der Betreiber des Mailservers eine Löschung veranlassen und dann eine erneute Zustellung versuchen. Spammer unternehmen hingegen meist keinen weiteren Zustellversuch (siehe auch das Greylisting-Verfahren in Kapitel 9.13).

8.6.3 Löschen

E-Mails kommentarlos zu löschen kommt kaum in Betracht. Niemand bekommt etwas davon mit, fehlerhafte Klassifizierungen sind nicht erkennbar und es gibt keine Möglichkeit, eine E-Mail nachträglich wiederzubeschaffen. Zudem verbietet der Mailstandard RFC 2821 (RFC2821 „In sending a positive completion

reply to the end of data indication, the receiver takes full responsibility for the message (see section 6.1). Errors that are diagnosed subsequently MUST be reported in a mail message, as discussed in section 4.4.") das Löschen der E-Mail.

Ganz anders ist die Situation bei erkannten Viren und Würmern. Hier ist es durchaus sinnvoll, die E-Mail nicht zuzustellen, da die Wahrscheinlichkeit, dass eine E-Mail fälschlicherweise als Virus klassifiziert wurde, viel niedriger ist als die Wahrscheinlichkeit einer Fehlklassifizierung als Spam. Darüber hinaus ist der Schaden, den ein Virus oder Wurm anrichten kann, viel größer als der potentielle Schaden durch Spam.

8.6.4 Markieren

Als Spam oder Ham bewertete E-Mails sollten vor der Zustellung entsprechend markiert werden. Typischerweise bringt Antispam-Software sowohl bei Spam als auch bei Ham eine Markierung an, die häufig die Wahrscheinlichkeit der Einschätzung als Spam enthält und weitere Details über die Kriterien der Bewertung. Dem MUA oder dem Anwender stehen damit genug Informationen für eine eigene Entscheidung zur Verfügung. Der MDA oder der MUA kann die „spamverdächtige" E-Mail in eine spezielle Spam-Mailbox einstellen, die der Benutzer von Zeit zu Zeit durchsieht.