Ergänzungen des RZ Trier zur Benutzungsordnung

RECHENZENTRUM
HOCHSCHULE TRIER I STUDIENORT TRIER

1. Behandlung unerwünschter Werbemails (SPAM)

Das Rechenzentrum der Hochschule Trier bietet den Nutzern des E-Mail-Service an den Standorten Trier und Idar-Oberstein die Möglichkeit, ungewollte Werbe-Mails („SPAM-Mails“) auszufiltern. Eingehende E-Mails werden durch ein Bewertungsprogramm nach mehreren, ständig aktualisierten Kriterien auf das Vorliegen von Merkmalen unerwünschter E-Mail Werbung untersucht. Wir verwenden mehrere Praktiken um SPAM zu filtern in der folgenden Reihenfolge:

Blacklisting: Stammt die E-Mail von einem im Internet allgemein bekannten SPAM-Verteiler, wird die Annahme verweigert. Wenn der sendende Mailserver richtig konfiguriert ist, wird der Absender über die Nichtzustellbarkeit informiert. Um solche SPAM-Verteiler zu identifizieren, prüfen wir bei jeder eingehenden E-Mail, ob der Absender auf einer von mehreren öffentlich verfügbaren, regelmäßig aktualisierten Listen bekannter SPAM-Verteiler verzeichnet ist.

Greylisting: Wir haben Greylisting nach der RFC 6647 Richtlinie (https://tools.ietf.org/html/rfc6647) implementiert. Die meisten SPAM-Verteiler entsprechen diesen Anforderungen nicht, deren E-Mails werden demnach nicht angenommen. Auch hier hängt es von der Konfiguration des sendenden Servers ab, ob der Absender über die Unzustellbarkeit informiert wird.

Bewertungssystem: Nicht zurückgewiesene E-Mails werden nach einem ständig aktualisierten Verfahren bezüglich ihrer Spam-Wahrscheinlichkeit bewertet. Wird ein im System vorgegebene Bewertungsschwelle überschritten, markiert unser Mailserver die betreffende E-Mail durch das Voranstellen der Sequenz „{ SPAM }“ in der Betreff-Zeile. Die E-Mails werden nach der Bewertung zugestellt.

Der Empfänger kann über unseren Dienst **Spamblock** (http://www.hochschule-trier.de/go/spamblock) einstellen, ob diese E-Mails in seinem regulären Postfach oder in einem von Spamblock kontrollierten Postfach abgelegt werden. Im Spamblock Postfach werden E-Mails nach einer Verweildauer von 9 Tagen automatisch gelöscht. Weitere Informationen zur Funktionsweise von Spamblock können auf der Website des Dienstes eingesehen werden.

Haftung:

Die Bewertungsprogramme stellen nur den Versuch einer Bewertung dar. Ungeachtet ihrer bereits erreichten Zuverlässigkeit besteht immer die Möglichkeit eines Irrtums im Einzelfall. Es wird daher ausdrücklich darauf hingewiesen, dass der Nutzer für die weitere Behandlung markierter E-Mails selbst verantwortlich ist. Die Hochschule haftet nicht für die Folgen einer unterbliebenen Zustellung.

Datenschutz:

Die Behandlung der E-Mails geschieht völlig automatisiert, außer einer möglichen Hinzufügung der Textsequenz „{SPAM}“ in der Betreff-Zeile, wird der Inhalt der E-Mail weder verändert noch werden E-Mails oder Teile davon von uns gelöscht. Der Datenschutz ist daher nicht beeinträchtigt.

2. Behandlung potenziell virenbehafteter E-Mails

Grundsätzliches:

Mit Viren und Würmern behaftete E-Mails stellen eine große Gefahr für die Informationsinfrastruktur dar. Zum Schutz der Infrastruktur ist eine effektive und zugleich dem Nutzer entgegenkommende Abwehr erforderlich.

Um interne wie externe Verbreitung von Viren über E-Mails zu verhindern, prüfen alle vom RZ administrierte E-Mail Server alle **ein- und ausgehenden** E-Mails. Alle Virenscanner sind mit einer automatisierten Update-Funktion ausgestattet, so dass in der Regel nach dem Auftreten neuer Viren und Würmer die aktualisierte Schutzfunktion wirksam wird, sobald der Hersteller der Software ein entsprechendes Update bereitstellt.

Verfahrensweise:

Virenverseuchte E-Mails werden abgefangen und **nicht weitergeleitet!** Nur wenn eine Analyse des Virus/Wurms ergibt, dass dieser die Absenderadresse nicht fälscht, wird der Absender automatisch darüber informiert, dass seine E-Mail wegen Virenbefalls nicht zugestellt wurde.

Außerdem werden E-Mails mit Anhängen des Typs .exe, .vbs, .pif, .scr, .bat, .com wegen des hohen Gefährdungspotentials grundsätzlich nicht weitergeleitet. Der Absender wird darüber informiert. Solche Dateien müssen vor dem Versenden in ein .zip-Archiv verpackt werden.

Haftung:

Die Analyse von E-Mails bezüglich Viren und Würmern ist nur so gut, wie die Datenbasis mit Erkennungsmerkmalen, die dem Virenscanner zur Verfügung steht. Obwohl diese automatisch aktualisiert werden, ist nicht auszuschließen, dass durch den unvermeidlichen Zeitverzug zwischen Auftreten eines neuen Virus/Wurms und der Verfügbarkeit einer aktualisierten Datenbasis virenbehaftete E-Mails den Virenscanner passieren können. Der Virenscan des RZ entbindet den Nutzer daher nicht von seiner Sorgfaltspflicht im Umgang mit E-Mails. Er sollte daher jede E-Mail dahingehend prüfen, ob der Absender bekannt ist, ob eine entsprechende E-Mail (ggf. mit Anhang) erwartet wird und ob der Textteil der E-Mail in sinnvollem Zusammenhang mit dem Absender steht. Die Hochschule haftet nicht für die irrtümliche oder unbewusste Zustellung virenbehafteter E-Mails.

Datenschutz:

Die Überprüfung von E-Mails nach Viren oder Würmern geschieht völlig automatisiert und ist daher datenschutzrechtlich unbedenklich. Das hohe Gefahrenpotential erfordert hier jedoch einen Eingriff derart, dass unter Umständen Teile von E-Mails oder ganze E-Mails nicht zugestellt werden. Insofern ist nicht auszuschließen, dass dem Empfänger wichtige oder zeitkritische Informationen vorenthalten bleiben. Dies ist jedoch auch aufgrund allgemeiner technischer Probleme im E-Mail-Verkehr nicht ausgeschlossen. Es ist daher ohnehin ratsam, den Transfer wichtiger oder zeitkritischer Informationen durch Mehrfachkommunikation (Bestätigung erbitten, Rückfragen etc.) abzusichern.

Trier, den 05.01.2015