Computer Club Weinheim

Themenabend 24.09.2012

SPAM ist ursprünglich ein Markenname für Dosenfleisch, bereits 1936 entstanden aus *SPiced hAM*, fälschlich auch *Spiced Pork And Meat/hAM* oder *Specially Prepared Assorted Meat* genannt.
Im Internetzeitalter ist der Markenname zum **Synonym für Massen-E-Mails** geworden.

Wie das Dosenfleisch zur Massen-E-Mail wurde, darüber gibt es viele Geschichten. Eine besagt, es beruhe auf einem Sketch der Comedy-Gruppe "Monty Python". Darin kam der Begriff über 120 mal innerhalb weniger Minuten vor und übertönte jede andere Konversation.

Was sagt der Gesetzgeber zu Spam ?

Nach deutschem Recht ist es verboten, Personen unaufgefordert Werbung per E-Mail zuzusenden. Spam ist aber weit mehr als nur ein lästiges Übel: Jedes Jahr entstehen **Kosten in Milliardenhöhe** durch die Übertragungskosten für den Versand, den Zeitverlust für das Lesen, Löschen oder Beantworten dieser Belästigungen. Zur Zeit wandern täglich 26 Milliarden E-Mails durchs Internet. 5,61 Milliarden davon sind SPAM-Mails (Quelle: Marktforschungsinstitut IDC) Ärgerlich wird es vor allem dann, wenn die Mailbox zugestopft ist und reguläre Post aufgrund der Größenbeschränkung der Mailbox abgewiesen wird.

Kommerzielle Spammer führen Datenbanken mit teilweise mehreren Millionen Adressen. Diese Datenbanken werden mit E-Mail-Saugern erzeugt. Das sind kleine Programme, die das Internet (Newsgroups, E-Mailverzeichnisse, Homepages) nach E-Mail Adressen durchsuchen und damit die Datenbank füttern.

Die Versender von Werbemails (Spammer) verschleiern ihre Identität weil ja das Versenden von Spams in Deutschland ungesetzlich ist. Daher bleiben die Urheber lieber anonym. Andererseits rechnen Spammer damit, dass Nachrichten von missbräuchlich verwendeten seriösen oder persönlich bekannten Absendern mit größerer Wahrscheinlichkeit geöffnet werden.

Manche Spammer sind so gewitzt, dass sie in den Emails gegen Ende erklären, dass man sich von diesem Verteiler auch austragen kann. Man solle einfach dem Link folgen und zum Austragen aus dem Spam Verteiler die E-Mail Adresse eintippen. Am besten auch gleich alle anderen privaten Adressen, damit auch dort nie Spam ankommt.

Natürlich ist das nur ein Trick und die Werbemails kommen weiterhin und meistens sogar noch häufiger. Die Spammer haben das eingeführt, um auszutesten welche E-Mail-Adressen wirklich gelesen werden. Denn wenn man als Privatperson versucht sich dort auszutragen, bestätigt man ja sozusagen mit dieser Aktion, dass man die Mail abgefragt und gelesen hat.

Gibt man nun gutgläubig auch seine anderen Adressen ein, um dort erst gar keinen Spam zu erhalten, freuen sich die Spammer besonders.
Das sind dann gleich eine Hand voll neue und sogar verifizierte Empfängeradressen für Werbemails.

Hinzu kommt das Risiko, Schadprogramme zu laden, indem unvorsichtigerweise via Klick auf Links in Spam-E-Mails von speziell präparierten Websites der eine oder andere Schadcode geladen wird und somit der Rechner in Gefahr ist.

Möglicherweise hat ein Mailboxbesitzer auch schon einmal Rückmeldungen auf Nachrichten erhalten, die er nie geschrieben hat. Dann wurde vielleicht die eigene Adresse missbraucht.

Dies ist eine weitere Form von SPAM, d.h. man erhält die Fehlermeldungen die durch eine SPAM-Attacke (von fremden Rechnern aber mit der eigenen E-Mail Adresse als Absender) ausgelöst wurden.
Diese Fehlermeldungen werden so gut wie nie von SPAM Filtern erfasst (es sind ja auch ganz "normale" Fehler-meldungen).

Dagegen kann man praktisch nichts unternehmen. Die Versender verwischen Ihre Spuren nämlich im Regelfall so gründlich, dass eine Nachverfolgung nicht möglich ist. Hier eine Stellungnahme des BSI (Bundesamt für Sicherheit in der Informationstechnik) die von deren Homepage in diese Präsentation kopiert wurde.

Keine Panik, wenn Ihre Adresse missbraucht wird

Falls Sie feststellen, dass Ihre eigene E-Mail-Adresse missbraucht wurde, so können Sie dagegen kaum etwas unternehmen. Ignorieren und löschen Sie die Nachrichten, in denen Ihnen unbekannte Personen auf von Ihnen nicht verfasste Mails reagieren. Es ist derzeit praktisch nicht möglich, die Fälscher Ihrer Adresse zu ermitteln.

Wie schütze ich mich gegen Spam?

Wer im Internet unterwegs ist z.B. an Diskussionen in Foren und Newsgroups teilnimmt, muss in der Regel eine Adresse angeben. Hier sollte man auf keinen Fall die Haupt-E-Mail Adresse verwenden. Hierfür sollte man sich eine weitere Adresse einrichten z.B. bei „web.de“, „yahoo.de“ oder „gmx.de“.

Es existiert auch die Möglichkeit sogenannte Wegwerf Adressen zu benutzen. Ob und wie diese Adressen zu benutzen sind ist auf der jeweiligen Anbieterseite zu erfahren.

Eine weitere gute Quelle für Spam sind Freunde und Bekannte die "wichtige, lustige" Mails an alle Bekannte weiterleiten. Hierbei wird oft über "CC:" an eine ganze Liste von Empfängern gemailt.

Besser sollte man mit "BCC:" (Blind Carbon Copy) arbeiten (siehe nächste Folie). Die Mails werden damit auch an alle Empfänger versandt, die Empfängerliste bleibt aber unsichtbar! Allerdings hat diese Methode auch einen Nachteil. Einige Spamfilter bewerten Mails, die den Empfänger per BCC erreichen, negativ, das heißt, sie sehen den Versand via Blind Carbon Copy als ein mögliches Kriterium für Spam.

Goldene Regel: Bei Mehrfachempfängern immer die BCC-Adressierung benutzen! Schicken sie die Mail an sich selbst (AN) und listen alle anderen Empfänger unter BCC.

An	mich@web.de
Kopie (CC)	
BCC	anna@web.de, jupp@we.de, hein@web.de, susi@web.de

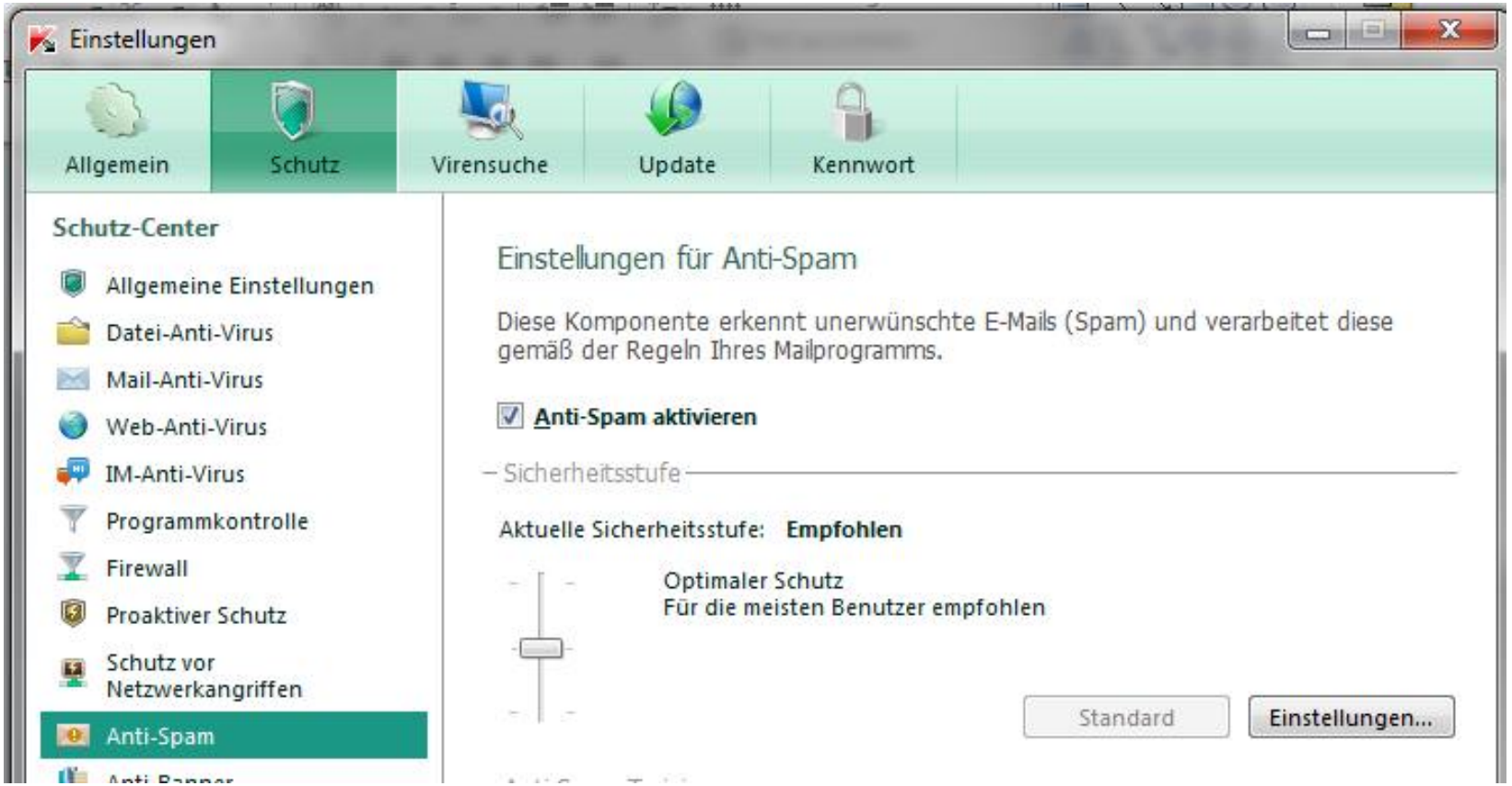
Generell ist es vorteilhaft mehrere E-Mail Adressen zu besitzen, sowie die Haupt-Adresse mit Bedacht einzusetzen

Einige E-Mail Provider bieten eigene Spamfilter an. Diesen Filter sollte man einschalten. Damit bleiben die Spam-Mails auf dem Server des Providers. Hierbei bleiben nicht selten in den Filtern des Providers E-Mails hängen die kein Spam sind. Deswegen sollte der SPAM-Ordner beim Provider überprüft werden.

Inzwischen gibt es eine Vielzahl verschiedener Spamfilter-Techniken zur automatischen Erkennung und Entfernung von Spam im Postfach. Einige E-Mail-Programme wie z. B. der Mozilla Thunderbird oder Microsoft Outlook haben integrierte, auf dem Bayesschen Filter basierende, selbstlernende Spamfilter, die Werbemails von vornherein aussortieren.

Diese werden dann im E-Mail Programm, hier im Beispiel Outlook 2010 im Ordner „Junk-E-Mail“, abgelegt und können dann gelöscht bzw. bearbeitet werden.

Einige Virenscanner/ Internet Security bieten auch einen Spam-Schutz an.
Hier z.B. Kaspersky PURE2, welcher sich in div. Mailprogramme einklinkt



Natürlich kann auch eine Anti-Spam Software installiert werden.

Auf der nächsten Folie sind einige Beispiele aufgeführt.

Es wird jedoch darauf hingewiesen das die Aufzählung dieser Software keinerlei positive oder negative Wertung der Software darstellt.

Vor allem wurde keines der Programme auf ihre Funktionsfähigkeit getestet.

http://www.spamihilator.com/

http://www.spamfighter.com/Lang_DE/Product_Info.asp

http://www.freeware.de/download/superspamkiller_7500.html

http://ashampoo-ip-spam-blocker.de.malavida.com/d2511-kostenloser-download-windows


Computer Club Weinheim