Spam- und Virenschutz

Die Nutzung elektronischer Post („E-Mail“) ist mittlerweile auch in Privathaushalten schon genau so verbreitet, wie die unangenehmen Begleiterscheinungen dieses Kommunikationsmediums – vor allem „Spam“, d.h. massenweises Versenden unerwünschter Werbemails durch zwielichtige Unternehmen, die damit Ihr Geld verdienen. Der Name „Spam“ rührt von einem alten Sketch der „Monty Python“-Truppe her, in dem in einem Restaurant unzählige Male das Wort „SPAM“ vorkommt und damit jegliche Kommunikation überlagert. Der Name selbst war die Handelsmarke einer bekannten Fleischkonserve (es gibt dafür sogar ein Museum – siehe unter http:/www.spam.com/).

Wie schützen Sie sich gegen „Spam“?

Spam ist eine echte Landplage und auch von Profis nicht immer so richtig in den Griff zu bekommen. Wie bei Landplagen so üblich, muss dass Problem zuerst einmal an der Wurzel gepackt werden. Dazu müssen wir einmal wissen, woher die „Spammer“ eigentlich unsere E-Mailadresse bekommen haben, wir haben denen ja nie davon erzählt.
Die einfachste Methode, um an fremde E-Mailadressen zu kommen, ist das sogenannte „Harvesting“. Dieses „Ernten“ funktioniert mit Software, die Unmengen von Webseiten auf E-Mailadressen absucht und diese in einer Adressliste speichert. Leider haben viele Homepagebetreiber immer noch nicht verstanden, dass es eine absolute Unart ist, solche Adressen im Klartext auf Webseiten zu veröffentlichen (die Adressen können nur für Harvester unkenntlich gemacht werden).
Wie können Sie sich nun präventiv schützen?

- verwenden Sie mehrere E-Mailadressen, 1 „Hauptadresse“ und mehrere „Nebenadressen“ (z.B. Alias oder Freemailadressen)

- geben Sie **niemals** die Hauptadresse bei Gästebüchern, Foren, Newsgroups, etc. an, die Hauptadresse sollte nur im eigenen vertrauten Bekanntenkreis bekannt sein

- wenn Sie über eine Nebenadresse „zugespammt“ werden, können Sie diese einfach löschen – Ihre Bekannten werden sie trotzdem weiter erreichen können

- Veröffentlichen Sie auf Ihrer eigenen Homepage Ihre E-Mailadresse nicht im Klartext, fragen Sie einen Experten nach Verschlüsselungsmethoden

Zu spät – ich werde „zugemüllt“

Falls Sie schon massenweise E-Mails à la „VIAGRRAAA“ in der Betreffzeile erhalten, so sollten Sie Gegenmaßnahmen ergreifen, um nicht stundenlang mit dem Löschen sinnloser Wer-

bebotschaften zu verbringen. Am besten Sie fragen zuerst bei Ihrem Provider nach, ob es Spamfilter gibt und was das zusätzlich kostet. Es ist mittlerweile bei vielen Providern standardmäßig ein kostenloser Spamfilter verfügbar, sodass Sie diese E-Mails gar nicht mehr bekommen oder sie speziell gekennzeichnet werden.
Bei den Freemail-Providern sind Sie auf die Maßnahmen des Providers angewiesen, wenn Sie z.B. mit Outlook arbeiten, können Sie jedoch zusätzlich Software einsetzen, die Spam erkennt und auf Wunsch löscht. Diese Funktion gibt es z.B. in Microsoft Outlook 2003 – hier sorgt der „Junkmail Filter“ für die Erkennung unerwünschter Post, es sind aber auch unzählige andere Produkte zur Filterung von Spam verfügbar (kostenlos sind z.B. „Spamihilator“, „SpamPal“ – lassen Sie das aber von Experten installieren).
Wenn Sie Software einsetzen, beachten Sie bitte auch immer, dass diese auch gewüschte Post löschen könnte (auch Software macht Fehler). Dieses Problem können Sie aber leicht mit einer sogenannten „Positivliste“ umgehen, d.h. Sie definieren E-Mails von einer bestimmten Absendergruppe als „erwünscht“ – für diese Absender wird damit der Spamfilter nicht angewendet.

Viren – wenn der Computer krank wird

Wohl noch etwas gefährlicher als Spam sind die Computerviren, die über E-Mails eingeschleust werden können. Diese Viren verbreiten sich nach dem Schneeballsystem in rasender Geschwindigkeit weiter (dabei fungiert Ihr Computer ohne Ihr Zutun als Verteiler). Öffnen Sie bitte niemals Anhänge von unbekannten Absendern in Ihren E-Mails, denn mit dem Öffnen (Doppelklick) wird ein Virus erst aktiv. Sorgen Sie jedenfalls dafür, dass Sie ein aktuelles Virenschutzprogramm installiert haben, das auch regelmäßig aktualisiert wird. Sie müssen als Privatperson nicht unbedingt dafür bezahlen (z.B. „AVG“-Antivirus bei www.grisoft.com ist privat – leider nur englisch kostenlos verfügbar). Virenschutzprogramme prüfen alle Ihre eingehenden E-Mails auf verdächtige Inhalte und hindern Sie daran, Viren durch Doppelklick zu aktivieren.

Alias … anderslautende E-Mailadresse, die als Aliasname verwendet wird und an Ihrer Hauptadresse sichtbar ist.
Freemail … kostenlose Mailbox bei z.B. GMX, Lycos, etc.
Spam … unerwünschte E-Mails, die massenweise und automatisiert an Computerbenutzer versendet werden.
Harvesting … automatisierte Beschaffung von E-Mailadressen durch Scannen von Webseiten, Mailinglisten, etc.
Mailen … umgangssprachlich für Versenden und Lesen von elektronischer Post (e-Mail)
Download … „Herunterladen“ von Dateien aus dem Internet auf den eigenen Computer
Mailbox … elektronischer Postkasten zum Speichern und Versenden von E-Mails
Provider … Unternehmen, das Dienstleistungen um den Internetzugang bereitstellt

Wir wünschen Ihnen jedenfalls ein spam- und virenfreies Leben mit der elektronischen Post und wollen in der nächsten Folge andere Sicherheitsfragen behandeln, wobei es insbesondere um Telebanking gehen wird.

Für Detailfragen senden Sie bitte Ihre E-Mail an:
Müller & Kanduth OEG
support@mko.at