KAPITEL 13

Regeln für Nutzer im Umgang mit Spam und Viren

Die bisherigen Kapitel haben allesamt technische Maßnahmen beschrieben, um das Aufkommen von Spam und Viren in der E-Mail zu vermindern. Aber dieses Problem hat auch einen menschlichen Faktor. Der unvorsichtige oder leichtgläubige Umgang mit E-Mails macht es erst möglich, dass sich Spam lohnt und dass sich Viren verbreiten können.

In diesem Kapitel sind einige Regeln und Richtlinien zusammengetragen, die dazu beitragen sollen, dass die Endanwender von E-Mail durch bewussteren Umgang mit dem Medium die Spam- und Virenproblematik eindämmen können.

Angesprochen sind hier aber vor allem auch Systemadministratoren als Referenzpersonen aller Anwender von E-Mail-Systemen. Die Administration eines E-Mail-Systems ist nicht nur eine technische Dienstleistung. In Zusammenarbeit mit der Geschäftsleitung und den Anwendern sollte auch eine sinnvolle Prophylaxe betrieben werden. Mitarbeiter sollten zum sorgsamen Umgang mit der Technologie geschult werden, und regelmäßig sollten Erfahrungen und Anregungen zur Verbesserung der Benutzerfreundlichkeit und Sicherheit ausgetauscht werden. Wenn allgemeine Sicherheitsvorschriften für einen Betrieb bestehen, ist auch die Aufnahme von Vorschriften zum Umgang mit E-Mail denkbar. Die folgenden Regeln sollen für diese Unternehmungen als Ausgangspunkte dienen und beiden Seiten, Administratoren und Nutzern, dabei helfen, die komplexen technischen Prozesse in einfach nachvollziehbare Handlungsoptionen einzuordnen.

Regel 1: Kontrollieren Sie die Veröffentlichung Ihrer E-Mail-Adresse

Die wichtigste Verhaltensregel, um unerwünschtes E-Mail-Aufkommen zu vermeiden, ist, die eigene E-Mail-Adresse nicht unkontrolliert zu veröffentlichen. Spammer sammeln E-Mail-Adressen automatisch von Webseiten, Mailinglisten, in Chat-Räumen, öffentlichen Mitgliederverzeichnissen, dem Usenet und befreundeten Dienstleistern ohne Datenschutzrichtlinien. Sobald eine E-Mail-Adresse durch

einen dieser Kanäle veröffentlicht wird, ist die Sache verloren. Sie steht dann in Adresslisten, die nicht kontrolliert werden können und rege gehandelt werden. Außerdem steht die E-Mail-Adresse dann im Cache von Suchmaschinen und Archiven, so dass es unmöglich ist, sie wieder aus der Öffentlichkeit zu entfernen.

Die Effizienz und Dreistigkeit dieser Adresssammler kann man am Selbstversuch testen: Zwischen der ersten Veröffentlichung einer E-Mail-Adresse auf einer populären Website oder in einer großen Mailingliste und dem Eintreffen des ersten Spams vergehen oft nur Stunden.

Gelegentlich wird versucht, E-Mail-Adressen bei ihrer Veröffentlichung zu verschleiern, um automatische Adresssammler zu täuschen. Dazu gehört zum Beispiel das Umschreiben des @-Zeichens (`user(at)domain.com`) oder die Angabe einer für menschliche Leser offensichtlich falschen E-Mail-Adresse (`user-nospamtome@domain.com`). Es kann davon ausgegangen werden, dass automatische Adresssammelprogramme diese Tricks problemlos durchschauen.

Etwas anspruchsvoller ist schon die Methode, E-Mail-Adressen auf Webseiten nur als Bilder darzustellen. Dies ist automatisiert schwer zu erkennen, und wenn, dann nur mit einem gewissen Aufwand an Rechenleistung. Ironischerweise wurde diese Technik gerade von Spammern populär gemacht, um ihrerseits den Inhalt von E-Mails vor Analysewerkzeugen zu verstecken. Die Technologie, E-Mail-Adressen automatisch in Bildern zu erkennen, ist jedoch verfügbar, und falls sich diese Verschleierungstechnik weiter verbreiten sollte, ist es nur noch eine Frage der Zeit, bis sie von Spammern eingesetzt wird.

Viele Viren, die über E-Mails verbreitet werden, nutzen Sicherheitslücken oder Bedienfehler in E-Mail-Programmen aus und verschicken sich beispielsweise an alle Einträge im jeweiligen Adressbuch. Steht die eigene E-Mail-Adresse in diesem Adressbuch, wird man ebenfalls eine Kopie erhalten. Viren-Autoren und Spammer stehen auch zunehmend in Allianz: Die von Viren aus Adressbüchern gesammelten Adressen landen mitunter direkt in der Adressliste eines Spammers. Es reicht also nicht, E-Mail-Adressen nicht zu veröffentlichen, sondern man darf sie im Prinzip gar nicht weitergeben.

In bestimmten Fällen ist es übrigens auch sinnlos, eine E-Mail-Adresse geheim zu halten. Bei bestimmten großen Domains, zum Beispiel hotmail.com, ist es möglich, dass man schon Minuten nach der Registrierung einer E-Mail-Adresse Spam bekommt, weil die Spammer einfach auf gut Glück alle möglichen Benutzernamen durchprobieren. E-Mail-Adressen wie info@ oder sales@ werden regelmäßig mit Spam bedacht, egal ob die Adresse jemals bekannt gegeben wurde.

Natürlich ist es relativ sinnlos, eine E-Mail-Adresse nicht zu veröffentlichen, wenn man wünscht, dass andere diese Adresse zur Kommunikation verwenden. Aber man kann bestimmen, wo und wie man welche Adresse veröffentlicht.

E-Mail-Adressen, die mit Kosten verbunden sind, zum Beispiel weil sie eine SMS auf ein Mobiltelefon senden, sollten auf gar keinen Fall irgendwo auf fremden Com-

putersystemen gespeichert werden. E-Mail-Adressen, die für betriebliche Zwecke gedacht sind, sollten auch nur für betriebliche Zwecke verwendet und nicht auf Privatcomputern gespeichert werden. Wenn auf Websites oder bei der Registrierung für einen Dienst eine E-Mail-Adresse angegeben werden muss, sollte man eventuell eine zweite »Wegwerf«-E-Mail-Adresse anlegen. Wenn E-Mail-Adressen beim Online-Handel angegeben werden müssen, sollte man sich die jeweilige Datenschutzrichtlinie ansehen und darauf achten, dass alle Ankreuzfelder, mit denen Werbematerialien bestellt werden, ausgeschaltet sind.

Natürlich ist diese Regel nicht absolut und auch nicht absolut einzuhalten. Aber es gilt: Je weniger Menschen die E-Mail-Adresse kennen, desto weniger können sie missbrauchen.

Regel 2: Haben Sie gesundes Misstrauen – bei jeder E-Mail

Da jeder jedem E-Mails senden kann, und das quasi kostenlos, unbegrenzt und anonym, ist die Menge des gesendeten Unsinns ebenso unbegrenzt. Wer das Medium E-Mail wenig verwendet, wer nur in der Firma oder von Bekannten gelegentlich eine E-Mail bekommt, der mag mit der Zeit zu der Annahme kommen, dass jede E-Mail wahrheitsgetreue Kommunikation darstellt. Sobald die E-Mail-Adresse aber weitere Verbreitung gefunden hat, wird früher oder später eine Spam-E-Mail oder eine E-Mail mit einem Virus eintreffen. Daher sollte man dem Inhalt von E-Mails von vornherein misstrauisch gegenüberstehen. Man glaubt ja auch nicht alles, was bei einem im Briefkasten landet – wie oft hatte man denn »schon gewonnen«? –, und auch am Telefon kauft man nicht alles, wenn überhaupt irgendetwas.

Man muss davon ausgehen, dass trotz aller Schutzmechanismen in den E-Mail-Protokollen und aller Vorkehrungen der Administratoren der E-Mail-Systeme in einer E-Mail im Prinzip *alles* gefälscht sein kann. Angefangen bei Absender und Empfänger sowie dem Text natürlich, kann auch das Datum, der Versandweg, die Kodierung und das verwendete E-Mail-Programm frei erfunden – oder eher noch: heimtückisch gefälscht – sein. Selbst plausible Kombinationen können fabriziert sein: Spam-Software kann durch Suche in Datenbanken herausfinden, wer mit wem oft über was kommuniziert hat, und kann versuchen, die eigenen E-Mail-Sendungen daran anzupassen. E-Mail-Viren suchen sich die Empfänger einfach im Adressbuch des befallenen Rechners und versuchen durch geschickt formulierte Texte Vertrauen zu erwecken.

Um E-Mail als sicheres Medium einsetzen zu können, ist Umsicht, Sorgfalt und etwas gesunder Menschenverstand nötig. Um E-Mail als vertrauenswürdiges Medium einsetzen zu können, ist darüber hinaus die Verwendung von elektronischen Signaturen erforderlich.

Regel 3: Seien Sie besonders vorsichtig bei E-Mails von Banken und anderen Dienstleistern

Onlinebanking erfreut sich großer Beliebtheit. Fast ebenso großer Beliebtheit – in bestimmten Kreisen – erfreuen sich die Versuche, den Anwendern von Onlinebanking und anderen Online-Diensten durch gefälschte E-Mails mit abenteuerlichen Geschichten die Zugangsdaten zu entlocken. Dies wird auch Phishing genannt. Wahr ist: Seriöse Einrichtungen fragen *nie* nach den Zugangsdaten ihrer Kunden. Erstens weil dies eben unsicher ist und zweitens weil sie diese gar nicht benötigen. Falls es doch einmal vorkommen sollte, dass die Zugangsdaten der Kunden verloren gegangen sind, würden neue Zugangsdaten erstellt und den Kunden zugesendet werden, nicht umgekehrt.

Insbesondere Banken versenden oft aus Prinzip keine E-Mails im Zusammenhang mit ihren Onlinebanking-Angeboten, eben weil E-Mail zu oft für betrügerische Aktivitäten verwendet wird. Wenn eine Bank also zum Beispiel per E-Mail auf eine neue URL zu ihrem Onlinebanking-Angebot hinweist, ist dies garantiert eine Fälschung, mit der unvorsichtige Anwender verlockt werden sollen, ihre Zugangsdaten auf anderen Webseiten zum Mitprotokollieren einzugeben. Um das Onlinebanking einer Bank oder eines ähnlichen Diensts aufzurufen, sollten daher immer die in den eigenen Lesezeichen gespeicherte Webadresse verwendet werden, und man sollte in diesem Zusammenhang auch auf korrekte SSL-Zertifikate auf den Websites achten.

Regel 4: Üben Sie besondere Sorgfalt beim Öffnen von E-Mail-Anhängen

E-Mail-Viren im weitesten Sinn versenden getarnte E-Mails mit Anhängen, die, wenn sie auf dem Computer des Empfängers geöffnet werden, Schaden anrichten können. Der Variantenreichtum ist hier groß. Offensichtliche Kandidaten sind Programmdateien, *.exe* und *.com*, sowie direkt ausführbare Skriptdateien wie *.bat* und *.vbr*. Diese können auf dem Computer beliebige Aktionen ausführen, und das ohne besondere Tricks. Auch andere Dateiarten können aktiven Inhalt haben, die das gesamte Computersystem gefährden, insbesondere Microsoft-Office-Dateien (Word, Excel, PowerPoint, Access) mit eingebetteten Makros. Aber E-Mail-Anhänge können auch Programmierfehler oder Sicherheitslücken in den dazugehörigen Programmen ausnutzen, um diese zum Absturz zu bringen oder beliebigen Code auszuführen, was zum Beispiel beim Bildformat JPEG einst der Fall war.

Es wäre sinnlos zu versuchen, hier eine Liste von gefährlichen Dateitypen aufzustellen. Alle Dateitypen bis hin zur einfachen Textdatei können theoretisch gefährlich sein. Sorgfalt ist daher beim Öffnen von allen Anhängen Pflicht. Insbesondere sollte man folgende Punkte bedenken:

- Man sollte prüfen, ob man den Absender kennt und ob die E-Mail vertrauenswürdig ist, zum Beispiel durch elektronische Signaturen. Wenn nicht, kann sie eine Fälschung sein.
- Man sollte sich fragen, ob man die E-Mail erwartet und dafür im Rahmen der zu erledigenden Arbeiten Verwendung hat. Wenn nicht, ist der Anhang vielleicht eine Fälschung mit Schadensabsichten.
- Man sollte Anhänge nicht unbedingt mit dem dazugehörigen Programm öffnen, sondern eventuell mit einem Viewer-Programm, das weniger Funktionalität bei der Bearbeitung, aber dafür mehr Sicherheit bei der Betrachtung bietet. Dies gilt insbesondere für Microsoft-Office-Dateien.
- Man sollte informiert bleiben, bei welchen Dateiformaten und Programmen Sicherheitsprobleme aufgetreten sind, und diese Formate und Programme meiden, bis die Probleme gelöst sind.
- Man sollte eventuell besonders gefährliche Dateiformate im Mailserver blockieren und nicht über E-Mail senden lassen.

Das Entscheidende ist, dass jede Datei, die von einem fremden Computersystem gesendet wurde, ein gefährlicher Angriff auf das eigene System sein *könnte*. Sorgfalt und Umsicht mit allen solchen Dateien ist deshalb notwendig.

Regel 5: Konfigurieren Sie Ihren E-Mail-Client sinnvoll

E-Mail-Programme untergraben oft das Bestreben des Anwenders, im Umgang mit E-Mails und insbesondere Anhängen vorsichtig zu sein. Beim Versuch, hilfreich zu sein, werden Anhänge automatisch geöffnet, HTML-E-Mails werden automatisch dargestellt und Links aus dem Internet automatisch heruntergeladen. Derartiges Verhalten ist heutzutage nicht mehr angebracht. E-Mail-Clients sollten so konfiguriert werden, dass Anhänge nur auf unmittelbare Aufforderung des Anwenders hin geöffnet werden. Ausnahmen könnten eventuell für Textdateien oder statische Bilder gemacht werden. Die HTML-Darstellung sollte entweder komplett ausgeschaltet oder zumindest so konfiguriert werden, dass aktive Inhalte wie JavaScript deaktiviert sind. Das automatische Laden von Bildern und anderen Links aus dem Internet muss ebenfalls ausgeschaltet werden. Außerdem ist es nicht hilfreich, wenn E-Mail-Clients die Endungen von Dateinamen verstecken, da damit die wahre Natur einer Datei verschleiert werden kann.

Dies ist alles eine Konsequenz aus den anderen Regeln. E-Mail-Clients sollten so konfiguriert werden, dass der Anwender kontrollieren kann, was sie machen, und so, dass sie potenziell gefährliche Aktionen nur auf Nachfrage oder gar nicht ausführen.

Leider sind die Standardeinstellungen der meisten E-Mail-Clients auf die eine oder andere Weise unsicher. Systemadministratoren sollten daher dafür sorgen, dass den Anwendern die E-Mail-Clients in einer sicheren Konfiguration zur Verfügung gestellt werden. Die Anwender sollten angewiesen werden, die Konfiguration der E-Mail-Clients nicht ohne Rücksprache mit den Administratoren zu ändern. Bei manchen Produkten lässt es sich auch realisieren, dass es den Anwendern unmöglich gemacht wird, bestimmte Einstellungen im E-Mail-Client zu verändern.

Regel 6: Antworten Sie niemals auf Spam

Klar ist, man sollte niemals etwas bestellen oder kaufen, das in Spam-E-Mails angeboten wird. Wenn die Spammer keinen wirtschaftlichen Erfolg mit ihren Methoden haben, werden sie irgendwann verschwinden. Dazu kommt, dass die meisten der angebotenen Produkte und Dienstleistungen betrügerisch oder illegal sind.

Man sollte allerdings auch nie auf Spam antworten, um sich zu beschweren, sich aus einer Verteilerliste austragen zu lassen oder Ähnliches, selbst wenn eine solche Möglichkeit in der E-Mail erwähnt wird. Eine Antwort auf eine Spam-E-Mail ist nur eine Bestätigung dafür, dass die E-Mail-Adresse gültig ist (viele in den Adresslisten sind es nicht). Die eigene E-Mail-Adresse wird daher für Spammer noch wertvoller, und statt einer Abmeldung erhält man danach womöglich noch mehr Spam als vorher.

Gleichermaßen sollte man nie irgendwelche Links in Spam-E-Mails anklicken, selbst wenn diese angeblich zum Abbestellen der E-Mail-Sendungen führen sollen oder wenn man aus Neugier einfach nur mal gucken will. Diese Links sind in der Regel so angelegt, dass damit der Erhalt der E-Mail bestätigt wird und die E-Mail-Adresse verifiziert ist, womit sich das gleiche Problem wie oben ergibt.

Nur wenn man sich der Seriosität des Absenders sicher ist und sich erinnert, die E-Mail-Sendungen irgendwann einmal bestellt zu haben, sollte man versuchen, die Sendungen auf den angebotenen Wegen abzubestellen.

Wenn man einmal richtigen Spam erhält, hilft nur noch die Einrichtung eines Spam-Filters oder ein Wechsel der E-Mail-Adresse. Abmelden kann man sich nicht mehr.

Regel 7: Verwenden Sie elektronische Signaturen

Wie oben erwähnt, kann in einer E-Mail im Prinzip alles gefälscht sein. Um vertrauenswürdige Kommunikation zu gewährleisten, sollte daher der Einsatz von elektronischen Signatursystemen in Erwägung gezogen werden. Damit kann der Absender der E-Mail mit ziemlicher Sicherheit identifiziert werden, und die Unverfälschtheit des geschriebenen Texts ist gewährleistet, was ja in der Regel die beiden entscheidenden Aspekte von Kommunikation sind.

Für elektronische Signaturen bieten sich zwei verbreitete Systeme an: OpenPGP und S/MIME. Beide haben verschiedene Vor- und Nachteile, die hier nicht weiter erläutert werden sollen. Eine Variante von beiden sollte aber für die allermeisten Situationen geeignet sein.

Spammer und Viren schicken generell keine E-Mails mit elektronischer Signatur, zumindest ist dies bisher noch nicht aufgefallen. Sollten Sie dies trotzdem tun, dann könnte man die Signatur entweder zum tatsächlichen Absender zurückverfolgen und diesen zur Rechenschaft ziehen, oder die Signatur kann ungültig oder gefälscht sein, was sich automatisiert feststellen lässt. Es bietet sich daher an, E-Mails mit elektronischer Signatur in Spam-Filtersystemen bevorzugt zu bewerten. Dies ist leider noch nicht häufig der Fall, müsste also selbst eingestellt werden.

Die Verwendung von elektronischen Signaturen verhindert Spam oder Viren nicht, aber sie sorgt dafür, dass legitime E-Mails verlässlich erkannt werden können. Wenn mehr Anwender elektronische Signaturen verwenden würden, könnten unsignierte E-Mails besser auffallen und negativ bewertet werden. Diese Entwicklung ist jedoch zugegebenermaßen noch nicht absehbar.

In Zusammenhang mit elektronischen Signaturen ist auch oft die Rede von elektronischer Verschlüsselung. Es ist allerdings möglich, gültige verschlüsselte E-Mails anonym zu versenden. Daher bietet es zumindest im Kampf gegen Spam und Viren keine Vorteile, wenn man auf die Verschlüsselung von E-Mails besteht. In der Tat können durch Verschlüsselung vielmehr die Filtersysteme umgangen werden. Die Versendung von verschlüsselten Spam- oder Viren-E-Mails ist jedoch noch nicht aufgefallen, wohl wegen der erhöhten Rechenzeit, die für solche E-Mails benötigt würde, oder wegen der geringen Verbreitung von E-Mail-Verschlüsselungssystemen auf der Seite der potenziellen Empfänger.

Der Einsatz von elektronischen Signaturen und elektronischer Verschlüsselung sollte gerade im professionellen Einsatz sowieso selbstverständlich sein, um die Authentizität und Vertraulichkeit des E-Mail-Verkehrs zu gewährleisten. Die möglichen positiven Wechselwirkungen bei der Abwehr von Spam und Viren sind dabei nur ein Nebeneffekt.

Regel 8: Verwenden Sie Spam- und Virenfilter

Trotz aller Vorsichtsmaßnahmen wird fast jeder E-Mail-Benutzer einmal unerwünschte E-Mail erhalten. Man muss sich von der Vorstellung verabschieden, dass die Spam-Problematik in naher Zukunft durch technische Mittel oder politische Entwicklungen gelöst werden wird (eingedämmt möglicherweise, aber gelöst nicht). Es muss heute einfach zu einem E-Mail-System dazugehören, dass Abwehrmaßnahmen gegen Spam und Viren ergriffen werden. Der Umfang dieser Maßnahmen wird sicher stark von den jeweiligen Gegebenheiten abhängen.

Sehr viele Internet Service Provider und auch Betreiber von Firmennetzwerken und ähnlichen Einrichtungen bieten heutzutage derartige Dienste, die dem Endanwender das Leben erheblich erleichtern. Endanwender sollten sich aber darüber informieren, welche Dienste der Netzbetreiber anbietet und wie diese eingeschaltet und konfiguriert werden können. Netzbetreiber sollten wiederum dafür sorgen, dass adäquate Spam- und Virenfiltermaßnahmen installiert sind und die Endanwender über diese informiert werden. Gleichzeitig müssen sich alle Beteiligten darüber im Klaren sein, dass Spam- und Virenfilter nicht hundertprozentig genau arbeiten, dass also trotzdem Spam und Viren ankommen können und dass eventuell E-Mail verloren gehen kann.

Regel 9: Halten Sie Ihre Software stets aktuell

Der Kampf gegen Spam und Viren ist ein dauerhaftes Wettrüsten. Virenautoren finden neue Schwachstellen in E-Mail-Software, und die Vertreiber dieser Software berichtigen diese Schwachstellen (hoffentlich). Spammer erfinden neue Tricks, um Filtersysteme zu umgehen, und Autoren von E-Mail-Software erfinden neue Features, um diese Tricks zu entdecken. Daher ist es wichtig, dass die Software in allen Teilen des E-Mail-Systems, also MTA, Filtersysteme, E-Mail-Clients und andere Hilfsprogramme, immer aktuell gehalten wird.

Viele Betriebssystemhersteller legen Wert darauf, ihre Software nach der Veröffentlichung einer Betriebssystemversion nur noch wenn unbedingt nötig, etwa bei Sicherheitsproblemen, zu ändern. Dieses Vorgehen ist in vielen Fällen sinnvoll und wünschenswert, aber die Effektivität eines Spam- und Virenerkennungssystems wird nach einer Weile nachlassen. Dies gilt auch, obwohl Virenscanner ihre internen Datenbanken unabhängig von der Software-Installation sehr viel häufiger aktualisieren, denn in vielen Fällen kann man bestimmte neue Viren nicht durch einfache Datenbank-Updates erfassen. Je nachdem, wie akut die Spam- und Virenproblematik auf dem jeweiligen System ist, wird man daher den Upgrade-Zyklus des Herstellers ignorieren und selbst Software-Updates einpflegen müssen oder aber einen anderen Betriebssystemhersteller oder eine andere Betriebssystemvariante mit anderen Release- oder Update-Zyklen wählen müssen.

In Firmennetzwerken mit vielen Computern stellt die regelmäßige Aktualisierung der Software eine besondere logistische Herausforderung dar. Nicht nur der Mailserver muss aktualisiert werden, sondern alle Arbeitsplatzrechner und andere Systeme wie Firewall, Fileserver und Printserver müssen regelmäßige Sicherheits-Updates erhalten. Dies erfordert einen hohen Aufwand, ist aber nötig, um gegen Angriffe über das E-Mail-System einigermaßen abgesichert zu sein.

Regel 10: Denken Sie auch an die Alternativen zur E-Mail

Für einige Anwendungen ist es sinnvoller, auf E-Mail als Technologie zu verzichten. Statt E-Mail-Adressen für Kontaktaufnahme, Kunden-Feedback oder Issue-Tracking zu veröffentlichen, noch dazu mit offensichtlichen Namen wie info@ oder feedback@, kann man dafür auch Web-Formulare einrichten. Dies ist mittlerweile auf vielen Firmen-Websites der Normalfall. Statt Nachrichten per E-Mail zu verschicken oder sich schicken zu lassen, kann man zum Beispiel auch RSS-Feeds verwenden. Zum Versenden von Dateien gibt es verteilte Dateisysteme oder bekannte Techniken wie FTP oder WebDAV, um nur einige zu nennen. Und zwischenmenschliche Kommunikation kann zum Beispiel auch über Instant-Messaging-Systeme wie Jabber oder althergebrachte Systeme wie IRC geschehen. Oder man geht mal ein paar Schritte ins Nachbarbüro ...