6. Infektionswege

Wenn Sie ein Antivirenprogramm haben, kann die meiste Malware nur noch mit Ihrer unbewußten Mithilfe auf den PC gelangen. Eins der „Haupteinfallstore“ für Malware sind Spam-E-Mails.

6.1. SPAM

Als Spam bzw. Junk-Mail werden unerwünschte E-Mails bezeichnet, die meist der Werbung dienen oder einen Angriff auf Ihren PC darstellen. In manchen Postfächern erreicht der Spam-Anteil 90 %, mit steigender Tendenz. Spam stiehlt Ihnen nicht nur die Zeit, sondern wird auch zum Einschleusen von Malware auf Ihren PC benutzt. Was kann man gegen Spam tun?

- Versuchen Sie, nicht zum Ziel zu werden.

Wenn Ihre Vorsichtsmaßnahmen nicht ausgereicht haben und Spam bei Ihnen eintrifft:

- Verringern Sie den Spam mit Mailfiltern.
- Vermeiden Sie Fehler im Umgang mit Spam.

6.1.1. Wie kann ich vermeiden, Spam zu bekommen?

Es gibt durchaus Leute, die viele Jahre lang oder noch nie eine unerwünschte Mail bekommen haben. Warum aber werden Sie mit Spam überschüttet? Woher haben die Spammer Ihre Adresse erhalten?

Zunächst ein wenig Theorie. Als local-part (lokaler Bestandteil) wird der Teil einer E-Mail-Adresse bezeichnet, der die Adresse innerhalb einer Domain eindeutig bezeichnet. Einfacher ausgedrückt: Der Teil vor dem @. Hinter dem @ folgt der Domain-Name des Anbieters, z. B. gmx.net, web.de oder auch der Name der Firma, z. B. ikea.com. Die Adresse darf Buchstaben, Ziffern und einige Sonderzeichen enthalten. Erlaubt sind 82 Zeichen:

```
A-Z  a-z  0-9  .!#$%&'*+-/=?^_`{|}~
```

Die meisten Provider unterscheiden nicht zwischen Groß- und Kleinschreibung. Sie können also Klaus@ oder kLauS@ oder KlAuS@ oder klaus@ schreiben. Wenn Groß- und Kleinbuchstaben gleich behandelt werden, gibt es insgesamt 56 verschiedene Zeichen: 26 Buchstaben, 10 Ziffern und die oben genannten 20 Sonderzeichen. Für einen Namen, der aus zwei Zeichen besteht, gibt es 56 x 56 = 3136 Kombinationsmöglichkeiten. Für Namen aus drei Zeichen gibt es 56 x 56 x 56 = 175 616 Kombinationen. Verwendet man zehn Zeichen, gibt es bereits 303 305 489 096 114 176 mögliche Adressen. Nehmen wir an, ein Spammer würde alle möglichen Kombinationen aus zehn Zeichen durchprobieren, um Ihre Adresse zufällig zu „erraten“. Wenn er es schaffen würde, jede Sekunde eine Spam-Mail abzuschicken, also etwa 30 Milliarden pro Jahr, bräuchte er 10 000 Jahre, um alle aus zehn Zeichen bestehenden Adressen durchzuprobieren. Allerdings würde kein Spammer eine große Zahl identischer Mails abschicken können, ohne auf die schwarzen Listen der Provider zu geraten. Es ist also für einen Spammer unmöglich, eine ausreichend lange E-Mail-Adresse zu erraten.

Daraus folgt glasklar: Es ist kein Zufall, wenn die Spammer Ihre Adresse haben: Entweder aus dem Adress-Schwarzmarkt, jemand war unachtsam oder Sie selbst haben sie veröffentlicht.

Vielleicht haben Sie oder einer Ihrer Bekannten die E-Mail-Adresse gedankenlos weitergegeben? Häufig geschieht das beim Versand von gleichlautender E-Mails an mehrere Empfänger. Wenn der Absender alle Empfängeradressen im Feld „An:“ aufzählt, sieht jeder der Empfänger die Adressen aller anderen Empfänger. Und wenn auf nur einem der Empfänger-PCs ein Trojaner lauert, freut sich die Adressen-Mafia.

Es gibt ein einfaches Gegenmittel: die „Blindkopie“, engl. „**b**lind **c**arbon **c**opy“, abgekürzt „BCC“. Bei Windows Live Mail müssen Sie rechts vom Adressfeld auf „Cc und Bcc anzeigen“ klicken, damit das BCC-Feld sichtbar wird. Das Feld „An:“ lassen Sie leer oder Sie setzen Ihre eigene Adresse ein, damit auch Sie eine Kopie bekommen. Die Empfängerliste tragen Sie in das Feld BCC ein. Auf diese Weise bekommt kein Empfänger die Adressen der anderen Empfänger zu sehen.

Was für eine E-Mail-Adresse sollten Sie wählen, damit sie nicht leicht zu erraten ist?

- Am besten wäre natürlich eine wilde Kombination von Zeichen, aber Ihre Kommunikationspartner werden davon nicht begeistert sein, milde ausgedrückt.
- Am schlechtesten wäre es, einfach Vorname und Name aneinanderzufügen. Alle werden erfreut sein, dass Sie eine leicht zu erkennende und leicht zu merkende Adresse haben, vor allem die Spammer. Alle Kombinationen der 20 häufigsten Familiennamen mit den 20 häufigen Vornamen bzw. deren Abkürzungen durchzuprobieren geht ruck-zuck, eine reiche Adressen-Ernte ist gewiss. Optimal wäre es, eine Kombination aus Vorname, Nachname, Beruf, Hobby oder Wohnort ein wenig zu verstümmeln, indem man Buchstaben austauscht, verdoppelt oder Sonderzeichen einstreut. Beispiel: man-fred!hof'mannn enthält gleich vier „harte Nüsse". Bereits zwei davon würden den Namen „unerratbar" für den Computer machen, aber Ihre Bekannten werden den Namen trotzdem problemlos erkennen.

Ihre Adresse sollte grundsätzlich nicht auf Ihrer eigenen oder einer anderen Internetseite sichtbar sein. Der Grund: Die Adressen-Mafia durchsucht systematisch alle Seiten des Internets mit sogenannten „Harvester-Programmen" (das ist das englische Wort für Erntemaschine) nach E-Mail-Adressen. Das Problem: Wenn Sie eine eigene Webseite ins WWW stellen, sind Sie verpflichtet, ein Impressum einschließlich gültiger Email-Adresse einzubinden. Allerdings verlangt der Wortlaut des Gesetzes nicht, dass die Adresse computerlesbar ist. Wenn Sie Ihre E-Mail-Adresse in Druckbuchstaben aufschreiben, einscannen und als Grafikdatei im Impressum einbinden, erfüllen Sie die gesetzlichen Anforderungen, und die Adress-Mafia erkennt die Adresse nicht. Wenn Sie keinen Scanner haben, schreiben Sie die Adresse mit der Schrift-Funktion von Paint. Selbst wenn Sie Ihre Webseite schon länger haben, lohnt sich das Ersetzen von Text durch eine Grafik auch jetzt noch. Weil das „Ernten" von Adressen so einfach für die Spammer ist, greifen diese nur selten auf Ergebnisse früherer Suchläufe zurück, sondern starten eher einen neuen Suchlauf.

Für einen Test hatte ich ein E-Mail-Konto eingerichtet und dessen Adresse im Impressum meiner Website im Klartext angegeben. Nach wenigen Tagen begann der Spam das Postfach zu fluten. Nach nunmehr drei Monaten treffen täglich durchschnittlich 30 Spam-Mails ein. Jetzt habe ich den Klartext durch eine Grafik ersetzt und warte gespannt darauf, wie bald und wie weit der Spam zurückgeht.

Wofür dürfen Sie Ihre Adresse auch nicht verwenden?

- Geben Sie nie Ihre korrekte E-Mail-Adresse in Gästebüchern an, wo sie jeder verwerten kann. Der Betreiber eines Gästebuches hat normalerweise kein Interesse daran, Ihnen eine Mail zu schicken, und Sie wohl auch kaum.
- Veröffentlichen Sie Ihre echte Email-Adresse nicht in Foren und Communities im Klartext. Oft gibt es die Möglichkeit, die Adresse versteckt zu hinterlegen. In der Wikipedia beispielsweise hat jeder Autor eine Benutzerseite, wo er so leichtsinnig sein darf, private Daten über sich zu veröffentlichen, einschließlich seiner E-Mail-Adresse im Klartext. Besser ist es, seine Adresse in den Einstellungen zu hinterlegen. Dann kann jeder Nutzer E-Mails an Sie verschicken, ohne Ihre Adresse zu erfahren. Sinngemäß gilt das Gleiche auch für YouTube, Clipfish, MyVideo, MySpace und andere Social Networking Sites. Amazon beispielsweise, ganz vorbildlich, löscht aus der Kommunikation zwischen Käufern und Verkäufern jegliche E-Mail-Adressen heraus.

Bedenken Sie: Es genügt **ein einziger Fehler**, und Ihre Adresse wird von einem Spammer an den nächsten weiterverkauft. Innerhalb von Monaten kann der Spam wie eine Lawine anschwellen.

Was kann man tun, um nicht in die Listen von Spam-Versendern zu geraten?

6.1.2. Legen Sie sich mehrere Adressen zu

Sie brauchen mindestens eine vertrauliche und eine oder mehrere öffentliche Adressen sowie Wegwerfadressen nach Bedarf. Verwenden Sie vorzugsweise die Wegwerfadresse. Wenn das nicht sinnvoll ist, nehmen Sie die öffentliche bzw. eine der öffentlichen Adressen.

Vertrauliche Adresse

Halten Sie Ihre vertrauliche Adresse geheim und geben Sie diese nur an vertrauenswürdige Freunde und Bekannte heraus. Vertrauenswürdig in diesem Sinne ist jemand, dem Sie unbesorgt 100 Euro leihen würden oder dem Sie während des Urlaubs Ihren Briefkasten- oder Wohnungsschlüssel anvertrauen würden.

- Geben Sie Ihre E-Mail-Adresse nicht an Leute weiter, die absichtlich oder leichtsinnig Ihre Adresse weiterverteilen. Wenn Sie eine Mail an mehrere Adressaten verschicken wollen, benutzen Sie die Funktion „**B**lind **C**arbon **C**opy“ (BCC) Ihres Mail-Clients.
- Machen Sie Leuten die Hölle heiß, die Ihre E-Mail-Adresse veröffentlichen oder weitergeben.
- Verwenden Sie die vertrauliche Adresse im Verkehr mit Firmen, mit denen Sie regelmäßig zusammenarbeiten.

Öffentliche Adresse

- Hinterlassen Sie ihre öffentliche Email-Adresse nur bei Firmen, die Sie für seriös halten.
- Ebay ist nicht völlig vertrauenswürdig, weil Sie nach einem erfolgreichen Kauf mit gänzlich unbekannten Menschen ihre Adressen austauschen müssen.
- Wenn Sie eine eigene Website haben, legen Sie sich eine Adresse speziell für das Impressum Ihrer Webseite zu.

Wegwerfadresse

Bei Anbietern wie `www.10minutemail.com`, `www.spamsalad.in`, `Squizzy.de` oder `topranklist.de` kann man eine kurzzeitig gültige E-Mail-Adresse einrichten, die – je nach Anbieter – nach 10 bis 60 Minuten automatisch gelöscht wird. Wann sollten Sie diese verwenden?

- Bei Teilnahme an Wettbewerben und Gewinnspielen. Gewinnspiele, ob im Internet oder als Postwurfsendung, dienen ohnehin nur der Adressgewinnung.
- Wenn die Adresse einmalig für eine Verifizierung gebraucht wird.
- Wenn der Hersteller einer gekauften Hard- oder Software auf einer Registrierung besteht und Sie nicht erkennen können, dass Ihnen aus der Registrierung ein Vorteil entsteht.

Es gibt Nutzer, die sich für jeden einzelnen Webshop ein eigenes Postfach zulegen. Sie können dadurch genau erkennen, welcher Webshop die Adressen seiner Kunden für Werbung oder schlimmeres weiterverkauft. Dann löscht man nur das betroffene Postfach, die anderen Fächer sind nicht betroffen.

Ist das nicht sehr aufwändig, mehrere Adressen auf Posteingang zu überprüfen? Wenn Sie die Benutzeroberfläche von GMX, WEB, YAHOO und Co. benutzen und sich für jede Adresse einzeln anmelden und durchklicken müssten, wäre das tatsächlich schrecklich aufwändig. Die Mails lassen sich aber auch mit jedem gängigen Mailclient beim Provider abholen, es lassen sich sogar mehrere Konten mit einem Klick abfragen. Das geht sowohl mit POP3-Konten als auch mit dem IMAP-Protokoll.

Sie wollen keinen Client installieren? Bei vielen Providern gibt es die Möglichkeit, E-Mails automatisch auf eine andere Adresse weiterzuleiten. Leiten Sie die Mails von allen Konten auf die vertrauliche oder auf eine geheime Adresse weiter und Sie brauchen nur noch diese eine Adresse abzufragen. Wenn auf einem Konto der Spam überhand nimmt, geben Sie diese Adresse auf und legen Sie eine neue Adresse als Ersatz an.

6.1.3. Spam herausfiltern

Trotz aller Vorsicht kommt Spam bei Ihnen an. Mit Filtern können Sie einen Teil des Spams automatisch löschen (lassen).

Sogenannte Spam- oder Junk-Filter versuchen, den Spam auszusortieren. Diese Filter können beim Internetprovider, in der Firewall Ihrer Firma oder auf Ihrem PC betrieben werden. Dabei bleibt allerdings immer ein gewisses Restrisiko, dass auch einmal eine erwünschte Email falsch sortiert oder sogar gelöscht wird. Nachstehend sind einige Verfahren für die Filterung genannt. Beachten Sie, dass keins dieser Verfahren zuverlässig genug ist und deshalb mehrere Verfahren kombiniert werden sollten. Die erste und einfachste Gegenmaßnahme sollte sein: Wechseln Sie zu einem Provider, welcher SPAM automatisch löscht, in einen Spam-Ordner verschiebt oder zumindest markiert.

Die ersten vier genannten Filter werden auf Servern angewandt, die restlichen vorwiegend auf dem PC des Anwenders.

Blacklisting

Unliebsam bekannte Mailserver von Marketingfirmen und andere Absender, die eine längere Zeit den gleichen Absendernamen verwenden, werden in einer schwarzen Liste auf einem Blacklist-Server erfasst. Ihr Mailserver fragt beim Empfang jeder Mail nach, ob der Absender dort gelistet ist. Wenn ja, wird die E-Mail als verdächtig markiert oder abgewiesen. Das Problem dabei: Die Blacklists sind unzuverlässig. Die Einträge lassen sich manipulieren. T-Online und andere seriöse Firmen landen öfter automatisch in so einer Liste. Alle E-Mails von T-Online-Kunden abzuweisen, wäre nicht ratsam.

Greylisting

Der Server wertet drei Kennzeichen aus, die in jeder Mail enthalten sind: Mail-Adresse von Absender, Empfänger sowie IP-Adresse des Absenders. Hat der Server noch nie eine Mail mit dieser Daten-Kombination erhalten, schickt er eine Antwort an den Absender-Server: „Bin überlastet, kann E-Mail jetzt nicht annehmen, versuch es später noch mal“. Erfahrungsgemäß unternehmen Spammer meist nur einen Zustellversuch pro Adresse und versuchen es dann mit dem nächsten potentiellen Opfer. Seriöse Server unternehmen meist nach einigen Minuten oder Stunden (üblich sind 15 Minuten) einen zweiten Zustellversuch. Dieser wird durchgelassen. Leider kann man sich weder darauf verlassen, dass der Mailserver jedes seriösen Absenders einen weiteren Zustellversuch macht, noch darauf, dass die Spammer nichts dazulernen.

Tarpitting

Die Bezeichnung kommt von Tarpit = Teergrube. E-Mails von verdächtigen Absendern werden mit zunehmender Verzögerung bestätigt. Der Spam-Versender bricht vermutlich die Verbindung ab. Selbst wenn nicht, wird er ausgebremst und es kommen weniger Spam-Mails an.

IP-Screening

Spammer probieren oft willkürliche Adressen aus, beispielsweise eine Liste aller häufigen Vornamen. Wenn der empfangende Mailserver entdeckt, dass eine hohe Anzahl Mails eines bestimmten Absenders nicht zustellbar ist, wird die Verbindung gesperrt oder „in die Teergrube geschickt“.

Landes- oder Sprachfilter

Sie könnten einstellen, dass Sie Mails mit englischem Text oder einem asiatischen Absender nie annehmen wollen.

Heuristische Filter

Eine Vielzahl von Regeln wird auf die Mail angewandt. Der Grad der Übereinstimmung mit bestimmten Wörtern, Ähnlichkeiten und Zusammenhängen wird mit Punkten bewertet. Ist die Summe der Punkte zu hoch, wird die Mail als Spam markiert. Allerdings erfordert diese Methode ein Feintunig beim Festlegen der Punktzahl, ab wann eine Mail als Spam gilt. Der Grat zwischen erwünschten und unerwünschten Mails ist schmal.

Bayesische Filter

Diese Filter untersuchen zuerst eine große Anzahl bereits in Spam und Nicht-Spam sortierter Mails. Anhand bestimmter Charakteristika wird eine statistische Auswertung erstellt, die dann auf neue Mails angewandt wird. Das Programm berechnet die prozentuale Wahrscheinlichkeit, ob es sich um Spam handelt. Wenn der Anwender eine falsch eingeordnete Mail findet, teilt er dies dem Programm mit, welches daraufhin seine Treffergenauigkeit verbessert. Bayes-Filter erfordern ein ständiges Training, sonst entwickeln sie sich in die falsche Richtung. Im Email-Programm „Thunderbird“ beispielsweise ist ein SPAM-Filter integriert, der als JUNK-Filter bezeichnet wird. Dieser Bayes-Filter muss von Ihnen lernen, woran eine Spam-Mail erkannt werden kann.

Filterregeln beim Anwender

Jeder E-Mail-Client bietet Ihnen die Möglichkeit, Filterregeln zu erstellen – allerdings nur, wenn Sie das POP3-Protokoll verwenden. In Outlook Express beispielsweise können Sie über „Extras“ → „Nachrichtenregeln“ → „Filterregeln“ eigene Regeln erstellen. Sie könnten alle E-Mails, in denen das Wort „Viagra“ vorkommt, automatisch löschen lassen. Allerdings bringt das nicht viel, denn die Spam-Versender berücksichtigen das und variieren die Reizworte. Vi-agra, Viagrra, V1agra, Fiagra – ein Mensch versteht das, ein Computer erkennt das nicht. Wenn Sie alle E-Mails löschen, die das Wort „Sex“ enthalten, würden sie auch „Sex and the City“ blockieren sowie „Sextant“, „Sextett“, „Sicherheit**sex**perte“, Abschluss**sex**amen, Sonntag**sex**kursion und Schiff**sex**plosion.

Am Beispiel von Windows Live Mail: Unter dem Menüpunkt „Ordner“ finden Sie die „Nachrichtenregeln“. Mit Regeln kann man z. B. Newsletter in Unterordner verschieben.

Die im Beispiel gezeigte Regel färbt alle E-Mails grün, bei denen im Text oder im Betreff das Wort „Bestellung“ vorkommt.

Wer allerdings schreibt „hiermit bestelle ich“ oder „schicken Sie mir“, fällt durch das Filter. Dann muss die Filterregel angepasst werden oder es müssen weitere Regeln hinzugefügt werden.

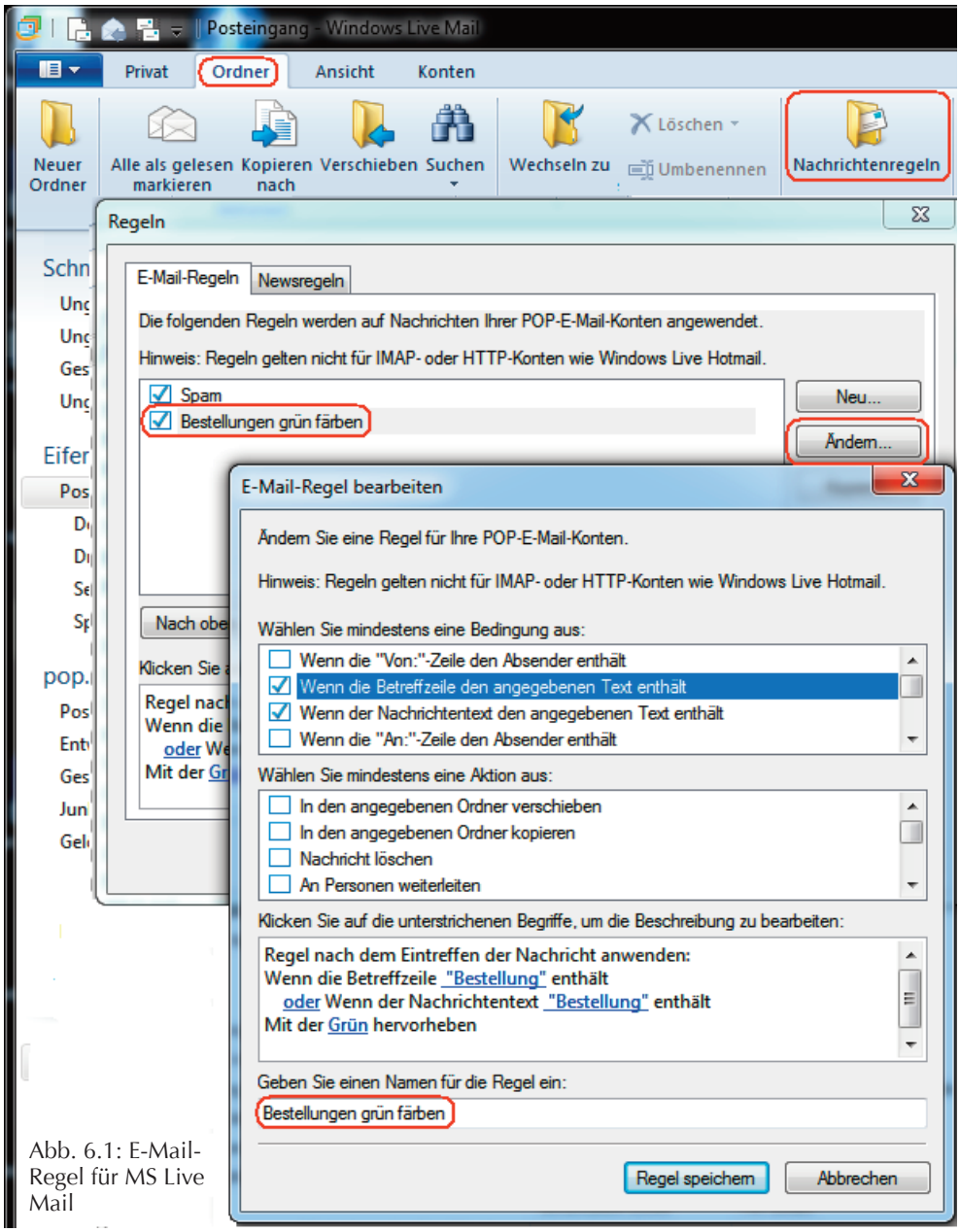

Abb. 6.1: E-Mail-Regel für MS Live Mail

Lokale Whitelist

Sie erstellen eine Liste der Adressen, von denen Sie Emails entgegennehmen wollen. E-Mails von diesen Absendern werden auf jeden Fall akzeptiert. Manche E-Mail-Programme werten Ihre Kontakte-Liste automatisch aus: Mails von Adressen, die in Ihrer Adressliste stehen, werden immer durchgelassen.

Lokale Blacklist

Sie erstellen eine Liste der Adressen, von denen Sie Emails nicht entgegennehmen wollen. E-Mails von diesen Absendern werden blockiert. Wenn es Ihnen beispielsweise nicht gelungen ist, einen lästigen Newsletter abzubestellen, können Sie dessen Absender in diese Liste eintragen.

Bei Windows Live Mail finden Sie die White- und Blacklist in „Menü“ → „Optionen“ → „Sicherheitsoptionen“ → „Sichere bzw. Blockierte Absender“.

Eine Restmenge Spam wird es trotzdem bis in Ihr Postfach schaffen. Lesen Sie nun, was Sie mit diesem Rest machen können oder nicht machen dürfen.

6.1.4. Umgang mit Spam

Es ist passiert. Trotz aller Vorsicht und trotz des E-Mail-Filters kommen noch einige Spam-Mails an. Was nun?

Spam abbestellen

Unerwünschte Abos von Firmen, deren Kunde Sie sind, können Sie in der Regel abbestellen. Die versendende Firma anzurufen, wäre die sicherste Möglichkeit, ist aber ungebräuchlich. Wenn Sie ein Impressum mit Anschrift und Telefonnummer finden können, ist der Versender höchstwahrscheinlich seriös und Sie werden in der E-Mail einen „Remove me“ oder „Unsubscribe“-Link finden, mit dem Sie sich selbst aus dem E-Mail-Verteiler der Firma streichen können. Das funktioniert meist einwandfrei.

Was sollte man nie tun?

- Antworten Sie niemals auf unerwünschte Emails. Wenn Sie in einer Spam-Mail einen Link zum Abbestellen finden, benutzen Sie ihn nicht! Das Abbestellen wird nicht funktionieren. Die angezeigte Absender-Adresse ist entweder gefälscht, oder – schlimmer noch – der Versender weiß nun, dass Ihre Adresse in Benutzung ist. Der Wert ihrer E-Mail-Adresse im Spam-Geschäft steigt, und Sie werden noch mehr Spam erhalten.
- Sehen Sie sich den Betreff genau an! Viele Emails können Sie löschen, ohne sie zu öffnen. Selbst das Öffnen einer Spam-Mail aus Neugier kann bereits Schäden verursachen!
- Links in Spam-Emails führen häufig auf Internetseiten, die mit Schädlingen oder Spionagetools präpariert sind. Allein durch das Öffnen, Anschauen und Schließen einer solchen Seite kann Ihr PC bereits infiziert werden!
- Klicken Sie keine Links in E-Mails an, sondern machen Sie sich die Mühe, die Webadresse Zeichen für Zeichen abzutippen. Der Grund: Können Sie zwischen dem ersten und dem zweiten „a“ in

  www.sparkasse.de

  einen Unterschied erkennen? Das erste „a“ ist ein kyrillischer Buchstabe, das zweite „a“ ein lateinischer. Beide haben einen unterschiedlichen Zeichencode. Das sieht man nicht, nur der Computer kennt den Unterschied. So einfach kann man Sie auf eine betrügerische Domain lenken.
- Banken, Versicherungen, Arbeitsamt oder Behörden würden Ihnen nur dann eine E-Mail schicken, wenn Sie das vorher ausdrücklich erlaubt haben. Niemals würde eine solche Institution Sie auffordern, Ihr Passwort zu bestätigen oder persönliche Daten einzugeben.
- Mit manchen Firmen, vor allem mit Telekommunikationsfirmen, kann man den Online-Versand der Rechnung vereinbaren und damit meist Geld sparen. Ohne eine ausdrückliche Vereinbarung wird eine seriöse Firma keine Rechnung per E-Mail schicken. Wenn Sie eine unerwartete Rechnung bekommen, ignorieren Sie diese. Sollte diese wider Erwarten kein Spam sein, ist das nicht schlimm. Seriöse Anbieter wissen, dass E-Mails gelegentlich verloren gehen oder in Spamfiltern hängen bleiben, und sie schicken irgendwann eine Zahlungserinnerung mit der Briefpost.

- Wenn Sie eine Mahnung per E-Mail erhalten und sich nicht auf Anhieb ertappt fühlen, nutzen Sie im Zweifelsfall die Telefon-Hotline des Unternehmens, um sich Gewissheit zu verschaffen.
- Manche E-Mails sind denen einer Bank oder seriösen Firma sorgfältig nachgemacht und leiten Sie auf gefälschte Seiten weiter. Sehen Sie sich die Adresse in der Adressleiste ihres Browsers genau an!
- Wenn Sie von einem Anbieter, wo Sie tatsächlich Kunde sind, aufgefordert werden, Ihre Kundendaten erneut einzugeben, steckt eine Betrugsabsicht dahinter. Warum sollte der Shop-Betreiber die Daten erneut anfordern, die er bereits bei Ihrem ersten Einkauf erhalten hat? Wenn Sie Zweifel haben, öffnen Sie die Internetseite dieses Anbieters im Browser, melden Sie sich wie gewohnt an und schauen Sie dort nach Hinweisen. Möglicherweise werden Sie schon auf der Startseite vor solch einer E-Mail gewarnt. Wenn dort dann alles wie immer ist, handelt es sich bei der fraglichen E-Mail um Spam.
- Überweisen Sie kein Geld ins Ausland, und mit Western Union schon gar nicht! Aus den AGB: *„Auszahlung erfolgt an die Person, die Western Union nach Prüfung eines Identifikationspapiers als empfangsberechtigt ansieht."* Die Art des Ausweises ist nicht vorgeschrieben. Die „**M**oney **T**ransfer **C**ontrol **N**umber" soll für Sicherheit sorgen, doch in manchen Ländern bekommt man das Geld auch ohne die MTCN ausgezahlt. In den AGB steht *„Die MTCN hat eine reine Steuerungsfunktion."* In einigen Gegenden werden die Angestellten der Western Union von Gangstern besser bezahlt als von ihrem Arbeitgeber.

Umgang mit Anhängen

Dateianhänge in Spam-Emails enthalten oft Trojaner, Hijacker oder andere Malware. Deshalb gilt:

- Wenn der Text einer geöffneten E-Mail ihnen nichts sagt, dann öffnen Sie angehängte Dateien nicht.
- Öffnen Sie nur Email-Anhänge, bei denen Sie den Absender der Email kennen und Sie den Erhalt eines Anhangs erwartet haben.
- Achtung, auch E-Mails von Bekannten können Schädlinge enthalten! Wenn deren PC befallen ist, verschickt sich der Schädling möglicherweise automatisch an alle Adressbucheinträge. Symantec meint, dass bereits 18 % des Spams mit einer Absenderadresse eines tatsächlich existierenden Kontos auf die Reise geschickt wird. Bei Mails mit ungewöhnlichem Inhalt oder unangekündigten Anhängen zur Sicherheit nachfragen!
- Anhänge, die schädliche Programme enthalten, enden oft auf „`.pif`", „`.exe`", „`.scr`", „`.bat`" (eine vollständige Liste ist unter „4.2.2. Versand mit SMTP" zu finden).
- Deaktiveren Sie im E-Mail Programm das automatische Laden von Bildern in einer HTML-Email.
- Besser noch: Deaktiveren Sie im E-Mail-Programm generell die Darstellung von E-Mails im HTML-Format und versenden Sie nur Mails im Textformat. Ob auf einer Webseite oder in einer Mail – im HTML-Text kann Schadcode eingebettet sein, im Textformat niemals. Allerdings hat das Textformat auch Nachteile: Einige Sonderzeichen, z. B. das Euro-Zeichen, können nicht dargestellt werden.

6.1.5. Automatische Vorschau abschalten

Viele Clients sind so „freundlich", die zuletzt eingegangene Mail in einem Vorschaufenster automatisch zu öffnen. Das Problem: Falls die zuletzt eingegangene Mail rein zufällig eine bösartige ist, kann durch deren Öffnen der PC sekundenschnell vollautomatisch infiziert werden.

Der Anteil von Spam ist in vielen Postfächern erheblich größer ist als der nützliche Anteil. Da ein nennenswerter Teil der Spam-Mails nicht nur lästig, sondern auch bösartig ist, besteht eine hohe Wahrscheinlichkeit der Ansteckung durch die automatische Anzeige. Es ist klüger, auf die automatische Anzeige zu verzichten. Bei den meisten Mail-Clients können Sie über „Layout" oder „Anzeige" → „Layout" die Anzeige ausschalten.

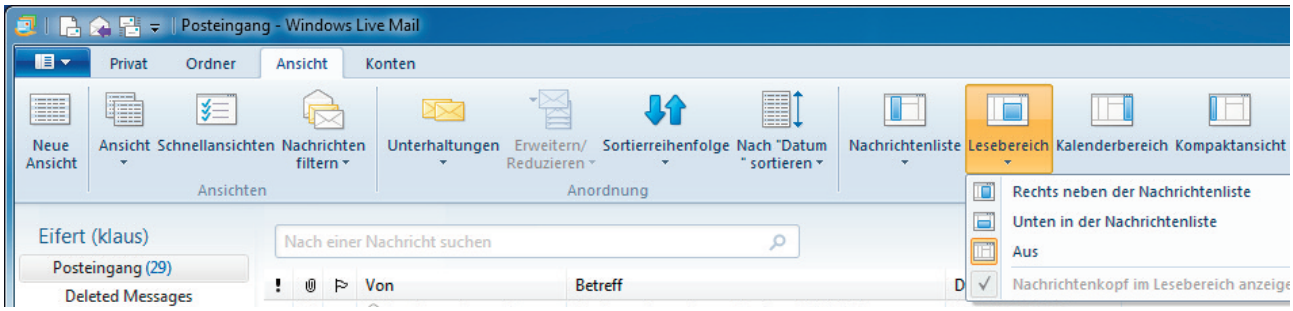

Abb. 6.2: Vorschau ausschalten bei Windows Live Mail: Klicken Sie auf „Aus".

6.1.6. Verdächtige Mail gefahrlos prüfen

Eine Mail von einem unbekannten Absender ist eingegangen. Sie wüssten gern, was darin steht, aber Sie trauen sich nicht, die Datei zu öffnen? Es gibt zwei ungefährliche Möglichkeiten:

- Schauen Sie die E-Mail im „Textmodus“ an (siehe 8.9.1. E-Mail absichern).
- Schauen Sie den Quelltext an. Leider funktioniert diese Methode nicht mit allen Mail-Clients.

Klicken Sie mit der rechten Maustaste auf die verdächtige Mail, dann im Kontextmenü auf „Eigenschaften“ → Registerkarte „Details“ → „Quelltext“. In der Abb. 6.3 sehen Sie ein Beispiel einer Spam-Mail.

Beurteilen Sie:

- **`From:`** ist eine „vernünftig aussehende“ Absenderadresse erkennbar? Könnte es wohl eine Organisation oder Firma geben, die sich „du-wurdest-verlinkt“ nennt? Es sollte wohl besser „du-wurdest-gelinkt“ heißen.
- **`To:`** Ist Ihre Adresse korrekt oder steht vor dem „@“ ein falscher „local-part“?
- **`Subject:`** Ist der Betreff plausibel?
- Können Sie im „Body“ der Mail einen sinnvollen Text erkennen?
- Sind Betreff und Body in korrekter deutsche Sprache verfasst?
- Ist der Inhalt so interessant, dass Sie bereit sind, ein Infektionsrisiko einzugehen?

Aber Sie haben ja nun den Inhalt der E-Mail erfahren, ohne sie geöffnet zu haben.

Bei E-Mails in einem IMAP-Postfach funktioniert das nicht. Sie müssen die verdächtige Mail zuerst in ein lokales Postfach verschieben oder weiterleiten, z. B. in Ihr Postfach „Entwürfe“.

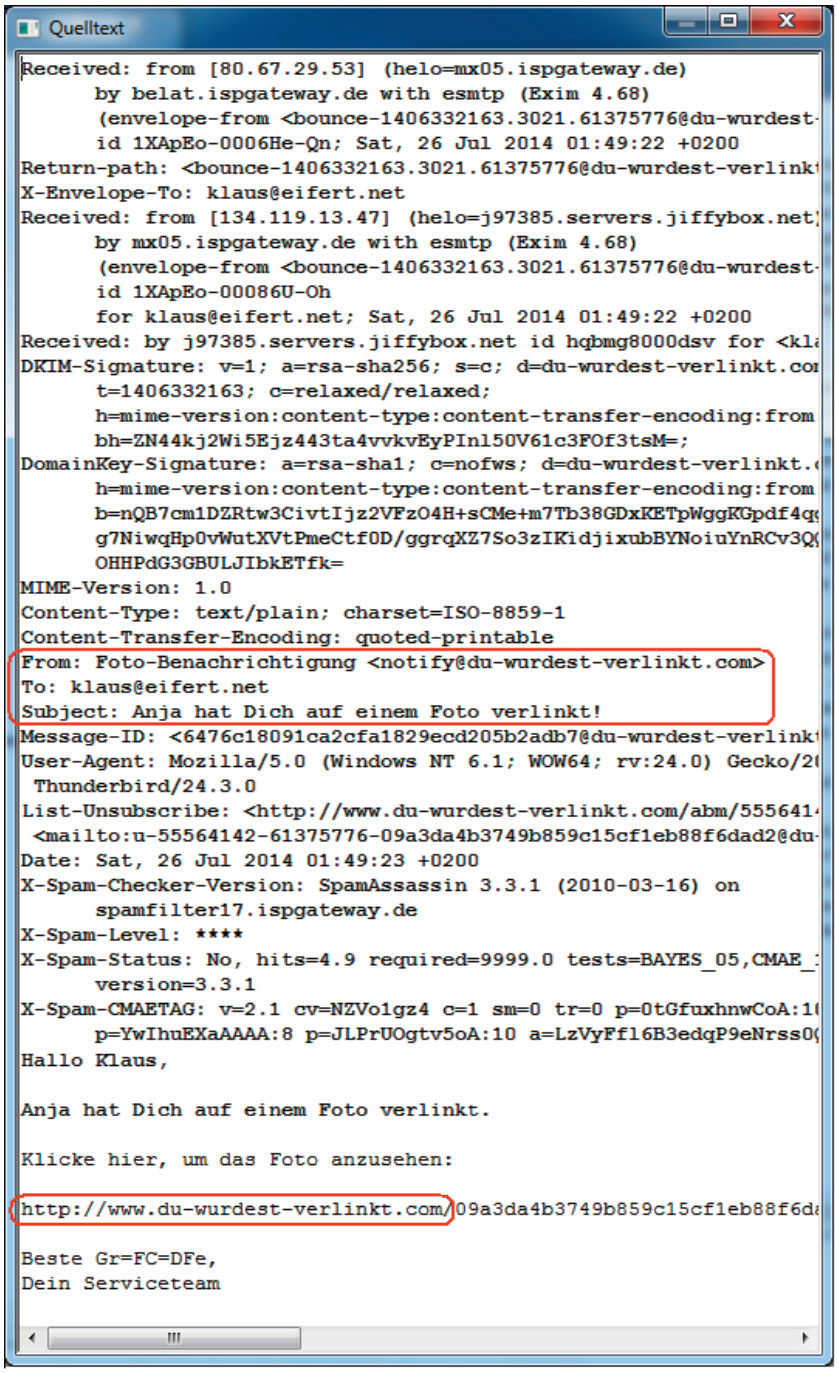

Abb. 6.3: Quelltext einer Spam-Mail

Beispiele aus meinem Postfach

Bei den nächsten Beispielen genügt ein Blick auf die wahre Absenderadresse, um zu erkennen, dass keine seriöse Firma dahinter steht. Im Postfach sehen Sie z. B. „Paypal“ als Absender, und in den Eigenschaften sehen Sie, dass der tatsächliche Absender „jermann@jkr.ch“ ist und dass er einen Server in der Schweiz benutzt.

Haben Sie noch Zweifel? Die Betrüger machen sich fast nie die Mühe, eine Webseite anzulegen. Lassen Sie Google nach „direkt-fotos.com“, „freierstick8gb.com“ oder „keinvertag39euro.com“ suchen. In der Regel finden Sie nichts. Falls doch – besser nicht anklicken, die Seite könnte infiziert sein. Wenn Sie auf `http://www.denic.de` ins Feld „Domainabfrage - whois“ den Domainnamen eingeben, wird Ihnen der Eigentümer der Webseite angezeigt. Bei Domains, die nicht auf .de enden, verwenden Sie `http://whois.domaintools.com` für die Recherche.

- Von: „Paypal“ jermann@jkr.ch
  Betreff: Nicht vergessen: Bitte bestätigen Sie Ihre Konteninformationen!
- Von: „PayPal“ <wwwrun@vs151071.vserver.de>
  Betreff: Ihr PayPal-Konto ist eingeschränkt – Ihre Mithilfe ist gefragt!
- Von: „Foto-Benachrichtigung“ <notify@direkt-fotos.com>
  Betreff: Steffi hat Dich auf einem Foto verlinkt!
- Von: „Gratis-Tipp“ <gratistipp@freierstick8gb.com>
  Betreff: Re: Versand Ihres 8GB USB Sticks
- Von: „Klaus Schmidt“ <info@keinvertag39euro.com> (Beachten Sie den Schreibfehler!)
  Betreff: [Erinnerung] Das neue iPhone ohne Vertrag für 39,00 Euro
- Von: „Telekom Leiter Kundenservice“ <ozgencatalay@dortelgiyim.com>
  Betreff: Neue Mobilfunk-Rechnung KP706800476965

IP Address	64.74.223.32
IP Location	- Georgia - Atlanta - Enom
Whois Server	whois.enom.com
Website Title	SEX FACEBOOK (18+)

Abb. 6.4: whois-Abfrage nach „direkt-fotos.com“

Eine Benachrichtigung über einen misslungenen Zustellversuch ist ein freundlicher Service. Aber kennen Sie eine Firma „wa-zustellung“? Müsste dort nicht ein Firmenname wie debitel, kongstar oder telekom stehen?

- Von: "Serviceteam" <delivery@wa-zustellung.com>
  Betreff: Zustellung auf Mobiltelefon nicht möglich

Was ist am folgenden Beispiel auffällig? Die Firma nennt sich zweimal „Download Center GmbH“, einmal „Center GmbH Download“, einmal „Giropay Office GmbH“, und keiner der Namen passt zum französischen Domain-Namen „sfr.fr“. Außerdem: Kündigung innerhalb von 7 Tagen? Stornieren innerhalb von 2 Wochen? Mahnverfahren nach 7 Tagen? Na was denn nun? Im angeblich alles erklärenden Anhang lauerte ein Trojaner.

> Von: "Center GmbH Download" <pgk13@sfr.fr>
> Betreff: Download Center Online Rechnung für Eifert
>
> Sehr geehrter Nutzer Eifert,
>
> wir sind sehr erfreut Sie als unseren neuen Kunden zu begrüßen.
>
> Die monatliche Beitragszahlung beträgt 49,90 €. Die Laufzeit Ihres Vertrags beträgt 12 Monate und kann jeweils zum Monatsende gekündigt werden. Wir weisen Sie freundlich darauf hin, dass durch die Bestätigung der AGBs von Download Center GmbH ein gültiger Vertrag abgeschlossen wurde.
>
> Anbei im Anhang finden Sie nochmal die Kostenaufstellung mit unseren Kontodaten. Die Rechnung ist innerhalb von 7 Tagen zu begleichen. Sollten Sie unser Angebot nicht annehmen, können Sie bequem innerhalb von 2 Wochen mit Hilfe des Schreibens im Anhang den Vertrag stornieren. Sollten wir weder eine Zahlung, noch eine Kündigung innerhalb von 7 Tagen erhalten, werden wir die Gebühren des Mahnverfahrens und Verzugszinsen Ihnen in Rechnung stellen müssen.
>
> Wir wünschen Ihnen weiterhin gute Unterhaltung auf unserer Plattform.
>
> Mit freundlichen Grüßen.
>
> Giropay Office GmbH Florian Eckhart
>
> Download Center GmbH

So klar wie in dem folgenden Beispiel ist es leider nur selten: Ein Absender aus der Slowakei arbeitet für die deutsche Sparkasse? Dass der Sparkasse das Geld für einen besseren Übersetzer gefehlt hat, ist extrem unwahrscheinlich.

> Von: "Sparkasse Online" <miroslava.juskova@truni.sk>
> Betreff: Sicherheitshinweis!!!
>
> Sehr geehrter Kunde,
>
> Im vergangenen Jahr Sparkasse, zusammen mit vielen anderen deutschen Banken wurde das Ziel einer weit verbreiteten Internet-Betrug. Deshalb haben wir ein Projekt, dies zu verhindern Zukunft gestartet.
>
> Alle Online-Bankkonten zu einem neu entwickelten Safety-System, das überwacht und verdächtige Aktivitäten in unserem Online-Bankkonto verbunden werden. Wir können sehen, dass Ihrem Online-Bankkonto ist noch nicht mit dem neu entwickelten Sicherheitssystem ausgestattet. Daher bitten wir für 5-10 Minuten Ihrer Zeit, um dieses Sicherheitsupdate installieren. Nach der Aktualisierung dieses Sicherheitsupdate wird einer unserer Mitarbeiter mit Ihnen Kontakt aufnehmen, um den gesamten Prozess abzuschließen. Wenn der Prozess abgeschlossen ist, können Sie weiterhin Ihre Online-Banking mit der Sparkasse zu nutzen.
>
> Wir danken Ihnen für Ihre Kooperation. Freundlichen Grüßen,
> Sparkasse.

Die folgende raffinierte Mail war bereits vom Provider als „Spam“ markiert worden. Den 1&1 De-Mail-Kundenservice gibt es wirklich, und die für Rückfragen angegebene Telefonnummer ist korrekt. Nur: Ich habe mit 1&1 keine Geschäftsbeziehung. Und wer ist eigentlich <web7p1>? Die angegebene Kundennummer war den Mitarbeitern der Rechnungsstelle unbekannt. Die werden wohl in den nächsten Tagen ziemlich unter Anrufen ächzen. Als 1&1 Kunde würde ich mich vielleicht über den hohen Rechnungsbetrag wundern und den bösartigen Anhang anklicken. Und auch wenn ich mich nicht wundere, erfolgt die Abbuchung. Einige Tage später erfolgt dann eine zweite, die „echte“ Abbuchung und es ist vielleicht schon zu spät, der ersten Abbuchung zu widersprechen.

> From: "1&1 De-Mail-Kundenservice" <web7p1>
>
> To: <klaus@eifert.net>
>
> Ihre Kundennummer: 201383599
>
> Guten Tag, anbei erhalten Sie Ihre Rechnung vom 19.11.2014.
> Der Rechnungsbetrag in Höhe von 199,94 EUR wird am 19.11.2014 von Ihrem Konto abgebucht.
>
> Haben Sie Fragen zu Ihrer Rechnung? Gerne sind unsere Mitarbeiter der Rechnungsstelle für Sie da.
>
> Mit freundlichen Grüßen
> Ihre 1&1 De-Mail GmbH
> Telefon: +49 721 960 97 85 Festnetztarif

Eine Bestellung über 200 Bücher? Prima! Beinahe wäre ich auf die folgende Mail hereingefallen:

> Sehr geehrte Damen und Herren,
>
> Ich interessiere mich sehr für Ihre Angebote auf Amazon. Bitte lassen Sie mich wissen, welchen Rabatt Sie geben, wenn ich mehr als 200 Stücke des Produkts: http://www.amazon.de/A3JWKR8XB7XF bestelle.
>
> Mfg, thomas.lippemeier@gmx.de

Doch im Quelltext war „hinter“ dem sichtbaren Link eine Adresse aus Südafrika (.za) versteckt:

> ... des Produkts: http://www.amazon.de/A3JWKR8XB7XF bestelle.

Man muss sehr vorsichtig sein, fast schon paranoid, und ganz genau hinschauen, um derart gefährliche Mails zu erkennen. Bei so vielen raffinierten Angriffen staune ich immer wieder, dass nicht 90 % aller deutschen PC infiziert sind, sondern „nur“ etwa ein Drittel.

Übrigens: Es ist unwahrscheinlich, dass ein Software-Anbieter Sie über das Vorliegen eines Updates benachrichtigt. Und dass Ihnen ein Software-Anbieter unaufgefordert ein Update per E-Mail zuschickt, ist ausgeschlossen.