

Spam-Abwehr und sichere PCs

Burckhard Schmidt | Computer- und Medienservice, Systemsoftware und Kommunikation | bschmidt@cms.hu-berlin.de

Kaum jemand spricht mehr von Viren. Spam oder auch Junk sind in aller Munde und in den Postfächern. Viren wurden, wie Sie sich erinnern werden, vielfach per E-Mail verschickt, oft als Anhang. Insofern war das Medium E-Mail nur das Transportmedium für einen Schädling. Daran hat sich eigentlich nichts geändert, außer dass die Anzahl der verschickten E-Mails enorm gestiegen ist.

Was transportieren E-Mails, wenn wir mal vom ursprünglichen Anliegen einer „vernünftigen“ Kommunikation absehen? Es sind Viren wie bisher und Werbung, immer wiederkehrend und scheinbar nutzlos. Letzteres hat den Begriff Spam geprägt.

Eine weitere Variante, „Phishing“ genannt, versucht, Sie unter dem Vorwand eines wie auch immer gearteten Sicherheitsproblems auf nachgemachte Webseiten von Dienstleistern (z. B. Banken) zu führen. Dort sollen Ihnen dann persönliche Zugangsdaten entlockt werden.

Oder es werden Mitgefühl, Hilfsbereitschaft oder auch nur die Neugier geweckt. Sie folgen mit einem Klick der dargebotenen URL und finden eigentlich nichts Unlauteres. Das ist meistens der Einstieg in präparierte Web-Seiten, die versuchen, nicht behobene Sicherheitslücken Ihrer Software aufzuspüren und auszunutzen. Davon merken Sie wahrscheinlich erst einmal gar nichts.

Spam-E-Mails stellen unabhängig von ihrem Inhalt eine ziemliche Belästigung dar. Neben der Gefahr, wichtige E-Mails zwischen dem Spam zu übersehen, können sie auch die Sicherheit des PCs beeinträchtigen. Die Kennzeichnung von E-Mails als Spam und darauf aufbauende Filter können den Überblick wieder herstellen.

Was kann passiert sein?

Das Ausnutzen von Sicherheitslücken in Betriebssystemen und Programmen hat eigentlich immer das Ziel, Schadsoftware (Malware) zu installieren, über die es dem Initiator möglich wird, unbemerkt

durch die „Hintertür“ (Backdoor) Ihren PC fernsteuerbar zu machen. Sofern Ihr PC online ist, kann das die Software dem Initiator signalisieren. Dieser kann nun beliebige Aktionen auf Ihrem PC ausführen, z. B. weitere Schadsoftware installieren, mit der er Spam versenden kann! Der Initiator kann natürlich nun auch Ihre „üblichen“ Arbeiten am PC verfolgen, z. B. Tastatureingaben, wenn Sie sich bei einem Dienstleister anmelden. Er wird aber versuchen, Ihre Arbeitsfähigkeit nicht allzu sehr einzuschränken, denn er will Ihren PC weiterhin mitbenutzen.

Bot-Netze

Sie bezweifeln sicher, dass ein PC, wenn dieser zum Spammen benutzt wird, so wichtig sein soll? Der oben beschriebene Vorgang spielt sich permanent im Internet ab, so dass Ihr fernsteuerbarer PC nur einer von Millionen ist. International geht man von wenigen Personen aus, die die von ihnen beherrschten PCs, allgemein als Bot-Netz (von engl. robot: Roboter) bezeichnet, kommerziell vermarkten. Diese nehmen von „Vermittlern“ Aufträge an, z. B. zum Versenden von Werbe-E-Mails.

Mit dem Betrieb dieser Bot-Netze lässt sich Geld verdienen (das ist Realität). Sie können dazu gehören – zum Bot-Netz meine ich natürlich – sofern Sie sich nicht um die Sicherheit Ihrer PCs kümmern oder bestimmte Sorgfaltspflichten ignorieren. Weil in diesem „Markt“ Geld verdient wird, wird sich das Spam-Problem nicht von allein erledigen. Im Gegenteil, es wird weiter „investiert“, um die Bot-Netze

auszubauen (Ausnutzung von Sicherheitslücken) und auch neue Möglichkeiten für den Spam-Versand zu finden. Spam-Versender und Mailserver-Betreiber stehen sozusagen in einem ständigen „Wettkampf“, Spam-Versand kontra Spam-Abwehr.

Was kann man noch mit Bot-Netzen machen? Wenn Sie einen Konkurrenten behindern möchten, geben Sie an seine Adressen gerichtete E-Mails in Auftrag, so dass die E-Mail-Flut über mehrere Tage die gesamte E-Mail-Kommunikation des Konkurrenten (darunter vielleicht Bestellungen, Auftragsbestätigungen, Rechnungen) lahmlegt. Oder Sie lassen permanent Anfragen an seinen Web-Server richten, so dass der im Prinzip nicht mehr erreichbar ist.

Zurück zum Ausgangspunkt: Das alles fängt mit einer E-Mail an und setzt unsichere PCs voraus. Wenn es gelingen würde, die Spam-E-Mails zu „unterdrücken“, dann würden Sie als Empfänger nicht auf diese E-Mail reagieren, also auch nichts falsch machen können. Das ist auch ein oft geäußerter Wunsch unserer E-Mail-Nutzer. Um es gleich vorweg zu sagen: Die Unterdrückung von E-Mails durch uns ist strafbar nach § 206 Abs. 2 Nr. 2, Strafgesetzbuch (StGB), wobei auch das Telekommunikationsgesetz (TKG) bzgl. des Fernmeldegeheimnisses (§ 88) zu beachten ist.

Spam-Filter

An dieser Stelle ist jeder E-Mail-Benutzer selbst gefordert. So lassen sich die in den aktuellen E-Mail-Programmen vorhandenen Spam-Filter erfolgreich zum Aus-sortieren von Spam-E-Mails nutzen. Sie müssen diese lediglich aktivieren und Ihren Bedürfnissen anpassen.

Eine weitere Möglichkeit besteht darin, dass wir jede E-Mail bereits bei der Einlieferung einer Spam-Bewertung unterziehen und im „positiven“ Fall eine zusätzliche Kopfzeile „Spam“ in die E-Mail einfügen. Eine E-Mail mit diesem Merkmal kann in jedem E-Mail-Programm herausgefiltert werden. Sie müssen dann wieder selbst entscheiden, wie Sie mit den aussortierten Spam-E-Mails umgehen.

Die genannte Spam-Bewertung haben wir bereits über mehrere Jahre durchge-

führt und publiziert. Die Spam-Erkennung verschlechterte sich im Laufe des Jahres 2007 zusehens und wäre nur mit permanentem personellen Aufwand stabilisierbar gewesen. Darum wurde eine kommerzielle Lösung der Firma IronPort (Cisco Systems) im November 2007 zum Einsatz gebracht. Die Spam-Bewertung erfolgt seitdem wieder auf hohem Niveau und sehr zuverlässig. Unsere E-Mail-Nutzer, die sich ursprünglich entsprechende Filterregeln in ihren E-Mail-Programmen eingerichtet hatten, konnten nun sofort Nutzen aus dieser neuen Technik ziehen. Wir mussten leider feststellen, dass viele E-Mail-Nutzer die einfachen Filtermöglichkeiten ihrer E-Mail-Programme gar nicht kennen bzw. nicht einsetzen und dann vereinzelt Beschwerden bezüglich des Spams an uns richten.

Darum wollen wir noch einen Schritt weitergehen und aufgrund der zuverlässigen Spam-Bewertung die Kopfzeile „Spam“ ausnutzen, um Spam-E-Mails direkt in einen separaten „Spam-Ordner“ zuzustellen. Damit werden im Posteingang nahezu keine Spam-E-Mails mehr erscheinen. Bei Bedarf oder zur Überprüfung sind sie aber weiterhin einsehbar. Dieses zuletzt beschriebene Verfahren, verbunden mit einem zyklischen Löschen der ältesten E-Mails aus diesem Spam-Ordner, ist an eine Vereinbarung zwischen dem Betreiber des E-Mail-Dienstes und den E-Mail-Nutzern gebunden. Dazu ist eine Dienstvereinbarung mit dem Gesamtpersonalrat in Vorbereitung.

Zur Spam-Bewertung muss man feststellen, dass es immer ein Restrisiko geben wird, eine E-Mail fälschlicherweise als Spam zu bewerten. Nicht zuletzt deshalb sollten Sie die Spam-Ordner regelmäßig durchsehen und die E-Mails kritisch betrachten bzw. einige Vorsichtsmaßnahmen walten lassen:

- Kenne ich den vermeintlichen Absender? Aber Vorsicht, E-Mails können unter falschem Namen verschickt werden!
- Ist die eigene E-Mail-Adresse in der Adressenzeile sichtbar?
- Oder erhalten Sie üblicherweise E-Mails mit versteckter Adresse (Bcc-Feld)?
- Lassen sich aus dem Betreff schon Rückschlüsse auf den Inhalt ziehen?
- In welcher Sprache ist der Betreff verfasst, ist er verständlich?

- Seriöse Dienstleister schicken sicherheitsrelevante Informationen nicht per E-Mail.
- Enthält die E-Mail Anhänge, die ich erwarte?
- Vergewissern Sie sich zur Not beim Absender, was der Anhang enthalten soll.
- Lassen Sie nicht prinzipiell Anhänge automatisch öffnen.
- Folgen Sie nicht jeder URL, die in einer E-Mail genannt wird.
- Steht die E-Mail im Zusammenhang mit einem aktuell massiv publizierten Ereignis, das auf Ihr Mitgefühl oder auch nur auf Ihre Neugierde setzt? Vorsichtig und sachlich bleiben!

Im Vorfeld der beschriebenen Spam-Bewertung werden eine Reihe weiterer Verfahren zur generellen Reduzierung des Spam-Aufkommens angewendet, die ebenfalls auf den eingesetzten Servern der Firma IronPort zur Verfügung stehen. Es ist jeweils zu entscheiden, ob von einem externen Server oder PC überhaupt E-Mails angenommen werden sollen. Dazu gehört die Auswertung einfacher Sperrlisten (oft als Blacklist bezeichnet), die Adressen von PCs und Servern im Internet enthalten, die üblicherweise keine E-Mails versenden oder durch den Versand von Spam-E-Mails aufgefallen sind. Erheblich fundiertere Aussagen enthält die Reputationsdatenbank der Firma IronPort zu solchen Adressen. So können vorab schon über 95% aller Verbindungen zur Übergabe von E-Mails an uns abgelehnt werden (unter Angabe einer Fehlerinformation). Von den „restlichen“ zugestellten E-Mails werden immerhin auch noch über 60% als Spam bewertet!

Zusammenfassend lässt sich sagen, dass neben anderen Möglichkeiten das Medium E-Mail dazu benutzt wird, direkt oder indirekt Schwächen in den von Ihnen verwendeten Programmen auszunutzen, mit dem Ziel, Ihren Rechner zukünftig missbräuchlich benutzen zu können. Insofern trägt die Vermeidung von Spam und der kritische Umgang damit letztlich zur Sicherheit des eigenen PCs bei. Die Zustellung in einen separaten Spam-Ordner oder die Nutzung eigener Filter im E-Mail-Programm unterstützen Sie dabei.