SPAM-E-MAILS VERURSACHEN KOSTEN IN MILLIARDENHÖHE

Forschungsprojekt Securitas zur Sicherheit und Verfügbarkeit der Dienste „Telefonie über das Internet“ und „E-Mail“

>> Von Frank Niemann > In der Kommunikationstechnik existieren zwei wesentliche Prinzipien zur Übermittlung von Informationen:

- Die **Leitungsvermittlung**, wie sie in traditionellen Kommunikationsnetzen, z.B. dem analogen Telefonnetz (Plain Old Telephone System, POTS) oder dem digitalen Telefonnetz (Integrated Services Digital Network, ISDN) eingesetzt wird. In der Leitungsvermittlung werden drei Phasen unterschieden. Zu Beginn existiert eine Verbindungsaufbauphase (wählen), in der ein Kanal explizit für den Teilnehmer reserviert wird. Dann folgt eine Datenübertragungsphase, in der über den zuvor reservierten Kanal kommuniziert wird (telefonieren). Abgeschlossen wird mit einer Verbindungsabbauphase, in der die für den Teilnehmer reservierten Ressourcen im Netz wieder freigegeben werden (auflegen). Dem Teilnehmer steht somit ein durchgeschalteter, nur durch ihn nutzbarer Kanal zum Empfänger zur Verfügung.

- Die **Paketvermittlung**, wie sie z.B. im Internet oder besser ausgedrückt in auf dem Internet-Protokoll (IP)-basierten Kommunikationsnetzen verwendet wird. Hier werden die Informationen vom Sender in kleine Pakete verpackt, die mit einer Zielinformation (der IP-Adresse des Empfängers) versehen einzeln vom Sender zum Empfänger durch das Netz geleitet werden. Hierdurch wird eine bessere Auslastung einzelner Verbindungswege im Kommunikationsnetz erzielt, da sich Pakete mehrerer Teilnehmer eine Leitung teilen. Im Endkundenbereich finden sich häufig Ethernet-basierte lokale Netze (Local Area Network, LANs), in der sich alle an das LAN angeschlossene Teilnehmer das gemeinsame Übertragungsmedium teilen.

Die Entwicklung im Bereich der Kommunikationsnetze ist geprägt von einer Migration hin zu integrierten, auf dem Internet Protokoll (IP) basierenden Infrastrukturen, welche die Übertragung von Sprache und Daten ermöglichen. Dienste wie z.B. das World Wide Web (WWW), Datentransfer (File Transfer Protocol, FTP) oder elektronische Mail (E-Mail) sind Beispiele für Datendienste, Telefonie über das Internet (VoIP) ein Beispiel für einen Sprachdienst auf Basis des Internet Protokolls. IP-basierte Infrastrukturen sind von ihrer Konzeption her jedoch nicht auf Sicherheit und Robustheit gegen gezielte Angriffe ausgelegt. Für das Abhören und Manipulieren von ISDN-Telefonen ist teure Hardware und großes Wissen über die Protokollabläufe erforderlich. Werkzeuge zur Manipulation und zum Abhören IP-basierter Dienste wie z.B. Cain&Abel sind dagegen im Internet als Software frei verfügbar. Sie ermöglichen auch Angreifern mit relativ geringer Sachkenntnis erfolgreiches Abhören; beim Hochschulinformationstag 2008 zeigten z.B. zwei Studenten, die ihre Projektarbeit im Kommunikationstechnik-Labor absolviert hatten, wie einfach das Mitschneiden von Telefonaten über das Internet sein kann.

Vor diesem Hintergrund ist es das Ziel des Forschungsprojekts „Securitas“ des Kommunikationstechnik-Labors der Hochschule Pforzheim, Angriffsszenarien und Schutzmechanismen für den Sprachdienst „Telefonie über das Internet“ (Voice over IP, VoIP) und den Datendienst „E-Mail" zu entwickeln, und zwar unter besonderer Berücksichtigung der Spam-Problematik.

Der E-Mail-Dienst wird – noch vor dem World Wide Web – als wichtigster und meistgenutzter Datendienst auf Basis von IP angesehen. Die Hauptgefährdung für den E-Mail-Dienst liegt in dem immer weiter steigenden Aufkommen von Spam-E-Mails. Unter Spam-E-Mails oder kurz Spam werden unverlangt zugesandte Massen-E-Mails verstanden. Untersuchungen zeigen, dass auch bei konservativer Schätzung ca. 85% des weltweiten E-Mail-Aufkommens auf Spam zurückzuführen sind.

Der Begriff „Spam“ ist ursprünglich ein Markenname für Dosenfleisch gewesen. Seine heutige Bedeutung erlangte er durch einen Sketch der englischen Comedy-Serie „Monty Python’s Flying Circus“, bei dem der Witz darin besteht, dass auf der Speisekarte ausschließlich Gerichte mit „Spam“ stehen. Im Sketch wird

das Wort „Spam“ insgesamt 132 Mal erwähnt, daher wird „Spam“ als Synonym für eine nervende permanente Wiederholung (Massensendung) benutzt.

Die Gefährdung durch Spam-E-Mails lässt sich in zwei Teilbereiche untergliedern: Erstens muss sichergestellt werden, dass durch den schon heute sehr hohen Prozentsatz an Spam-E-Mails im Vergleich zu allen gesendeten E-Mails der Betrieb des E-Mail-Dienstes als Ganzes durch das Spam-Aufkommen nicht gefährdet wird. Zweitens gilt es zu berücksichtigen, dass durch Spam-Mails häufig Viren, Würmer und Trojaner übertragen werden (also Software), welche die Endsysteme und Daten von Anwendern bedrohen können.

Methoden zur Erkennung und Bekämpfung von Spam sind daher ein wichtiges Forschungsthema, um die Sicherheit und Verfügbarkeit des E-Mail-Dienstes zu gewährleisten. Ohne Spam-Erkennung und -Unterdrückung ist die weitere effiziente Nutzung des E-Mail-Dienstes in seiner jetzigen Form in Frage gestellt. Die Bedeutung dieser Aufgabe zeigt auch die Betrachtung der durch Spam entstehenden Kosten. Sie entstehen zunächst ganz banal durch Nutzung der Mailserver und die Bereitstellung von Speicher-Infrastruktur für unnütze Spam-E-Mails, die auch die Erreichbarkeit und Verfügbarkeit der Systeme insgesamt einschränken können. Weitere Kosten entstehen durch den Produktivitätsverlust der E-Mail-Empfänger, die Spam-Mail von relevanter Mail trennen müssen. Schließlich entstehen durch den unwissentlichen Versand von E-Mails und eventuell darin enthaltenen Viren durch ungeschützte E-Mail-Systeme schwer zu revidierende Imageschäden für Unternehmen.

Anhand von Fallbeispielen des Bundesamtes für Sicherheit in der Informationstechnik lässt sich zeigen, dass die Kosten pro Spam-Mail für ein mittelständisches Unternehmen ohne Schutzmaßnahmen ca. 18 Cent pro Mail betragen, mit Schutzmaßnahmen fallen Kosten von ca. 6 Cent pro Spam-Mail an. Seriöse Schätzungen beziffern die durch Spam verursachten Kosten in Deutschland für das Jahr 2005 mit 4,5 Milliarden US-Dollar. Prinzipiell gilt, dass eine frühzeitige Spam-Erkennung und -Unterdrückung kostengünstiger ist als eine Spam-Erkennung durch den Empfänger der E-Mail.

Spam tritt derzeit zwar hauptsächlich im Zusammenhang mit dem E-Mail-Dienst auf, für die Zukunft ist aber davon auszugehen, dass auch der Sprachdienst „Voice over IP“ zur Spam-Versendung missbraucht wird. Unter SPIT (Spam over Internet Telephony) werden unerwünschte Anrufe auf Basis von VoIP verstanden, die oftmals Werbebotschaften enthalten. Zwischen dem 4. und 9. September 2008 waren deutsche Voice-over-IP-Nutzer erstmals von SPIT-Attacken betroffen, teilweise klingelte zu nachtschlafender Zeit im Stundentakt das Telefon. Nach Informationen des „heise newstickers“ wandten sich einige Betroffene an die örtliche Polizei oder stellten gar Strafanzeige. Die Netzbetreiber waren diesen Attacken relativ hilflos ausgesetzt. In Zukunft ist davon auszugehen, dass SPIT-Anrufe überproportional zunehmen werden, da die Kosten für eine VoIP-Verbindung geringer ausfallen als für ein herkömmliches Telefonat. Zusätzlich können durch die Paketvermittlung im Gegensatz zur Leitungsvermittlung in ISDN-Netzen bei geeigneter Sprachcodierung viele parallele Spam-Nachrichten gesendet und so die Effizienz aus Sicht des Spamers deutlich erhöht werden.

Im Rahmen des Forschungsprojekts Securitas werden an der Hochschule Pforzheim im Labor für Kommunikationstechnik innovative Lösungsansätze zur Spam- und SPIT-Erkennung und zum Umgang mit Spam-E-Mails bzw. SPIT-Telefonanrufen erforscht und entwickelt. Hierzu wurde eine E-Mail-Umgebung auf Basis der im Internet frei verfügbaren Software „exim“ realisiert, in der verschiedene Prüfungen zur Spam-Erkennung implementiert worden sind. Derzeit werden weitere Verfahren entwickelt und bewertet.

Telefonie ist im Gegensatz zum E-Mail-Dienst ein Echtzeitdienst. Dies bedeutet, dass an die Methoden zur SPIT-Erkennung größere Anforderungen in Bezug auf eine kurze Prüfphase zu stellen sind als zur Spam-Erkennung. Es wurde eine Laborumgebung zum Testen von VoIP im Kommunikationstechnik-Labor aufgebaut, in der SPIT-Anrufe generiert werden, mit denen die vorhandenen VoIP-Telefone unterschiedlicher Hersteller lahm gelegt werden können. Auf Basis bisheriger Technik hilft dann nur noch, die Telefone vom Stromnetz zu trennen und neu zu booten. Gleichzeitig werden auf Basis der ebenfalls im Internet frei verfügbaren Telekommunikations-Anlage (TK) „Asterisk“ Methoden zur SPIT-Erkennung erarbeitet. Erste Tests zeigen auch hier die Wirksamkeit der angewandten Methoden.

In Zukunft sollen weitere Dienste in die Betrachtungen einbezogen werden. Unter dem Oberbegriff „Unified Communications“ wird die Integration von Sprache, E-Mail, Instant Messaging, SMS, Fax und weiteren Diensten verstanden. Dies erweitert nicht nur die Möglichkeiten, unter denen ein Teilnehmer erreicht werden kann, gleichzeitig werden hiermit auch die Möglichkeiten zur Spam-Versendung vergrößert. Ziel ist es daher, einen einheitlichen Ansatz zur Spam-Erkennung für alle Dienste zu entwickeln.

Das Projekt wird vom Bundesministerium für Bildung und Forschung (BMBF) mit knapp 260 T € über eine Laufzeit von drei Jahren im Rahmen der Förderlinie „IngenieurNachwuchs“ unterstützt. In der Ausbildung des ingenieurwissenschaftlichen Nachwuchses nehmen die Fachhochschulen mit rd. 192.000 Studierenden und 26.000 Absolventen jährlich eine zentrale Rolle ein. Ziel der Förderlinie „IngenieurNachwuchs“ ist es daher, neben der Forschung auch der Nachwuchsproblematik im Ingenieurbereich zu begegnen. Es werden im Projekt auf vielen Ebenen junge Menschen an den Ingenieurberuf im Bereich der Kommunikationstechnik herangeführt. Neben drei fest angestellten wissenschaftlichen Projektmitarbeitern, einer studentischen Hilfskraft, „Projekt-, Bachelor- und Masterarbeitern“ unterschiedlicher Studiengänge arbeiten auch eine Schülerin und ein Schüler im Rahmen der Berufsorientierung am Gymnasium (Bogy) in dem Projekt mit. Projektstart war der 1. Juni 2008. Kooperationspartner sind die Drachenfels GmbH aus Pforzheim, das Hochschulrechenzentrum und die Universität Hannover

Dr.-Ing. Frank Niemann
ist Professor und Studiendekan der Studiengänge Elektrotechnik/Informationstechnik und Technische Informatik.