

Electronic Mail - Gefahr für die Sicherheit?

Die Nutzung des Dienstes Electronic Mail geschieht heute in einer Vielfalt, die viele Nutzer zu einer „unkritischen“ Nutzung animiert. In dieser Beziehung kann man durchaus einen Vergleich mit dem Straßenverkehr wagen: Alle kennen neben Vor- und Nachteilen natürlich auch seine Risiken, sie können sich ihm aber nicht entziehen.

Wenn wir beim Mailing auch die Lebensgefahr ausschließen können, so gibt es doch eine Reihe von Ärgernissen, die den Nutzer direkt oder indirekt betreffen können. Insofern ist die Sicherheit des Mailedienstes ein breit gefächertes Thema, das sowohl die Betreiber von Mailediensten als auch die Endnutzer betrifft. Ich möchte mich in diesem Artikel an die Endnutzer wenden, die dieses Thema bisher noch nicht berührt hat.

Genauso wie im Straßenverkehr, um bei dem Vergleich zu bleiben, gibt es Regeln, deren Einhaltung erzwungen werden kann bzw. deren Einhaltung empfohlen wird, um einen erfolgreichen Mailaustausch erwarten zu können. Damit sind aber weder kapazitive Engpässe noch mißbräuchliche Nutzungen auszuschließen.

In unserem Heft Nr. 12 hat Herr Ohst den Artikel „Vertrauliche Kommunikation im Internet“ geschrieben, der nach wie vor aktuell ist (URL: <http://www.huberlin.de/inside/rz/rzmit/rzinhalt.html#nr.12>).

Darin wird u. a. darauf eingegangen, daß die am Mailaustausch beteiligten Server natürlich potentielle Angriffspunkte für Störungen oder Manipulationen sind. Genauso lauern Risiken in den PC-Pools, wenn bestimmte Programme zum Lesen und Verschicken von E-Mail (Mailtools) benutzt werden.

Herr Ohst setzt sich im wesentlichen mit folgenden Aspekten auseinander:

- *Vertraulichkeit* - nur der vorgesehene Empfänger soll in der Lage sein, die Mail zu lesen,
- *Authentizität* - der Absender soll überprüfen können, ob die Mail vom angegebenen Absender stammt und
- *Integrität* - der empfangene Mailinhalt soll mit dem abgeschickten identisch sein.

Diese Probleme lassen sich heute schon mit einem gewissen Aufwand durch sogenannte digitale Unterschriften und kryptografische Verschlüsselungen des Mailinhaltes lösen. Solche Methoden werden sich aber nur nach und nach durchsetzen, in vielen Fällen sind sie vielleicht gar nicht notwendig oder werden auch bewußt nicht eingesetzt. Eine illegal eingeschleuste Werbemail wird sicher nicht verschlüsselt sein, wenn sie ihren „Zweck“ erfüllen soll.

Unabhängig von diesem Problemkreis möchte ich Sie über weitere sicherheitsrelevante Konstellationen informieren.

Nutzung von Mailtools in PC-Pools

Ein PC in einem Rechner-Pool wird von vielen Mitarbeitern oder Studenten benutzt. Eine „personenbezogene“ Konfiguration, wie sie bei arbeitsplatzbezogenen PCs üblich ist, erfolgt dabei normalerweise nicht. E-Mail ist jedoch eine persönliche Angelegenheit, die sich oft mit den Nutzungsbedingungen in den PC-Pools beißt. Ein typisches Mailtool für MS-DOS, Windows NT- oder Mac-Rechner ist zum Beispiel „Eudora“ oder das in „Netscape“ enthaltene Mailtool. Diese Tools müssen konfiguriert werden. Wesentliche Angaben sind dabei:

- return address - der eigene Absender,
- SMTP-Server oder outgoing mail server - Rechner, über den E-Mail verschickt wird,
- POP-Account oder incoming mail server - Identifikation der Mailbox des Nutzers (auf einem UNIX-Rechner),
- mail directory - Verzeichnis für die lokale Speicherung von E-Mail auf dem PC.

Sehen wir uns diese Angaben etwas genauer an:

Der *eigene Absender* sollte es natürlich sein, wenn ich Antworten auf meine E-Mail erhalten möchte, er sollte auch stimmen! Ich kann auch einen falschen Absender angeben oder den benutzen, der zufällig in der Konfiguration steht (von einem vorhergehenden Nutzer?). Damit können die Angeschriebenen dann nicht antworten, oder ein anderer Nutzer erhält Antworten auf nicht von ihm geschriebene Mails. Die möglichen Reaktionen auf beiden Seiten möchte ich hier nicht ausmalen, es liegt jedenfalls ein Mißbrauch von E-Mail vor.

Der *SMTP-Server* ist sozusagen das nächstgelegene „Postamt“, über das ich die Mail verschicken kann. Dieser Server gehört normalerweise zur eigenen Einrichtung und identifiziert eine Mail u. a. mit Angaben dieser Einrichtung. Es gibt zur Zeit massive Versuche von „Internet-Piraten“, massenhaft Mail mit dubiosen Angeboten über solche SMTP-Server fremder Einrichtungen weltweit zu verbreiten, spamming genannt.

Benutzen Sie also auch den SMTP-Server der Einrichtung, mit der Sie einen entsprechenden Nutzungsvertrag haben (am Rechenzentrum z. B. mailhost.rz.huberlin.de). Ansonsten setzen Sie sich dem Verdacht des Mißbrauchs aus und bringen zudem Ihr Institut oder Ihre Universität in Mißkredit.

Mit dem *POP-Account* geben Sie den Account und damit den Namen Ihrer Mailbox an, die Sie lesen möchten.

Sie werden dabei nach einem Paßwort gefragt, das nur Ihnen bekannt sein darf. Die Nutzungsbedingungen in PC-Pools sind erfahrungsgemäß nicht immer so aus-

gelegt, daß einem Dritten das Ausspähen von Account und Paßwort nicht gelingen würde. Damit wäre dann der Zugriff auf Ihre Mail auch für einen Dritten möglich. Falls Sie Ihren Platz am PC zwischendurch einmal verlassen, ohne Ihr Mailtool zu schließen, bieten Sie auch gute Möglichkeiten für einen Mißbrauch.

Schließlich müssen Sie daran denken, daß Ihre Mail im eventuell nicht bewußt konfigurierten *mail directory* auf der Platte des PC abgespeichert werden kann. Damit kann ein nachfolgender Nutzer Ihre Mail einsehen oder Informationen für das Fälschen von E-Mail gewinnen. Sie gehen sicher davon aus, daß Sie in Ihrer Mail nichts „zu verbergen“ haben, aber das ist für den potentiellen Mißbrauch auch nicht entscheidend.

Diese wenigen Beispiele zeigen, daß in einem PC-Pool Bedingungen für das Mailing als persönliche Angelegenheit nicht so ohne weiteres vorliegen. In diesem Falle ist der Betreiber des PC-Pools gefordert. Das kann, bedingt durch die Unzulänglichkeit von Betriebssystemen oder Mailtools, auch den Verzicht auf „komfortable“ Tools bedeuten.

Im PC-Saal des Rechenzentrums wird der Maildienst über das System Banyan VINES angeboten, zu dem von vornherein ein eigenständiges Mailtool gehört, das diese Probleme nicht aufweist. Der Zugang zu Mailboxen, die auf einem UNIX-Server des Rechenzentrums liegen, ist innerhalb von „telnet-Sitzungen“ mit dem Mailtool „pine“ möglich. Das ist vielleicht nicht so bequem wie beispielsweise mit „Eudora“, zieht aber insgesamt weniger Konflikte nach sich.

Mailmißbrauch

Die Nutzung eines PC in häuslicher (studentischer) Umgebung ist genaugenommen unter gleichen Kriterien zu betrachten. Leider hat uns speziell der Mißbrauch von E-Mail für kommerzielle (Werbe-) Zwecke schon zu Nutzungseinschränkungen für Studenten gezwungen. Teilweise war eine gewisse (gespielte) Naivität gegenüber „Freunden“ dafür die Ursache.

Ich bin hier eigentlich, ausgehend von unzureichenden oder ungeschützten Mailkonfigurationen, schon bei dem Thema „*Mailmißbrauch*“ angelangt. In der Tat kann man durch Unkenntnis solcher Zusammenhänge dem Mißbrauch sehr leicht Vorschub leisten. Solange dabei „nur“ der Nutzer selbst betroffen wäre, könnte man darüber fast hinwegsehen. In Wirklichkeit ziehen aber solche Nachlässigkeiten oder auch der bewußte Mißbrauch von E-Mail eine Reihe von Folgen für alle nach sich.

Ein Nutzer, der beispielsweise Werbemails massiv verschickt oder in Newsgruppen verteilt, erzeugt eine Protestflut von erbosten Nutzern, die normalerweise die Postmaster der betroffenen Einrichtungen zu bearbeiten haben, was natürlich unnötig Kapazitäten bindet.

Wenn Sie selbst etwa Mails mit Werbecharakter oder dubiosen Angeboten erhalten (auch Kettenbriefe

gehören dazu!), werden Sie sich sicher auch ärgern. Das Auslesen der E-Mail über eine Telefonverbindung verursacht ja unnötige Telefonkosten und bedeutet Zeitverschwendung für die Analyse der E-Mail oder mitunter eine volle Platte im PC.

Aber wie verhalten Sie sich in einem solchen Falle?

Erste Reaktion: Da schicke ich aber gleich eine Beschwerdemail hin! - Normalerweise falsch! -

Damit geben Sie dem Absender die Bestätigung, daß er eine gültige Mailadresse gefunden hat, sofern der Absender eine gültige Mailadresse angegeben hat.

Zweite Reaktion: Dem schicke ich mehrfach irgendeine große Datei! - Auch wieder falsch! -

Dabei verschwenden Sie selbst Ressourcen (Telefonkosten, Belastung des Mailhosts und der Internetverbindungen, die die Universität ja zu bezahlen hat!). Außerdem stellen Sie dann sicher fest, daß der Absender gefälscht war, Sie eine Benachrichtigung „user unknown“ und – wenn Sie Pech haben – auch die gesendeten Daten zurück erhalten. Zu allem Übel wird dann auch der Postmaster mit einer Mail über die mißlungene Zustellung informiert. Ganz nebenbei begeben Sie sich mit diesem Verhalten auf das gleiche Niveau wie der Verursacher der E-Mail! Sie betreiben Mailmißbrauch.

Was können Sie effektiv machen: Diese Mail löschen, bei wiederholtem Auftreten ist eine Information an Ihren Postmaster sinnvoll.

Die oben genannte Methode, Mail über den SMTP-Server einer fremden Einrichtung zu verschicken, macht es schwierig, den wahren Absender herauszufinden. Da solche Attacken oft das massenhafte Verschicken von E-Mail beinhalten, sind SMTP-Server mitunter so überlastet, daß der Mailbetrieb für die eigenen Nutzer zum Erliegen kommt. Da liegt die eigentliche Gefahr, der wir begegnen müssen! Die Betreiber von Maildiensten (also auch das Rechenzentrum) sind dann gezwungen, durch den Einsatz geeigneterer Software (sofern überhaupt beschaffbar) solche Mißbräuche möglichst zu verhindern.

Andererseits können auch Sie uns durch umsichtiges Verhalten in dem Bestreben unterstützen, einen stabilen Mailbetrieb zu gewährleisten,

Wie gelangt Ihre Mailadresse ungewollt auf Mailinglisten?

Da ist es eigentlich so wie im täglichen Leben, wenn Sie Ihr „Gewinnzertifikat“ (persönlich an Sie gerichtet) voller Hoffnung an die angegebene Adresse zurückschicken: Gewonnen haben Sie bestimmt nichts, aber Sie erhalten als Belohnung noch mehr Werbeschriften!

Als seriöser Nutzer sind Sie sicher oft erfreut, die Mailadresse eines Partners auf dem WWW-Server zu finden, also richten Sie auch so etwas ein. Damit ist Ihre Mailadresse natürlich auch für andere verfügbar! Das gezielte Suchen von Informationen läßt sich mittels

Suchmaschinen im Internet bereits automatisieren. Warum also nicht nach Mailadressen suchen?

Surfen Sie gerne im Internet? Haben Sie schon „heiße“ Server besucht (ja, aber nur kurz)? Haben Sie für eine „freie Mailbox“ bei x.y einen Fragebogen ausgefüllt? Sie ahnen es, damit ist Ihre Mailadresse bekannt, eventuell auch etwas zu Ihren beruflichen Absichten, Betätigungsfeldern usw. Von dort ist es eigentlich nur noch ein kleiner Schritt, daß diese Informationen vermarktet werden können.

Nutzen und Mißbrauch der elektronischen Kommunikation liegen dicht beieinander, den perfekten Schutz wird es nicht geben. Das kommt mir irgendwie bekannt vor, haben Sie etwas anderes erwartet?

Burckhard Schmidt

Umgang mit Paßwörtern Die Sorgen der Benutzerberatung

In diesem Artikel sollen einige Aspekte der Arbeit der Benutzerberatung des Rechenzentrums hinsichtlich der Thematik dieses Heftes beschrieben werden. Gerade wir als Benutzerberatung sind in den meisten Fällen der erste Ansprechpartner der Benutzer, haben die oft undankbare Aufgabe, Sicherheitsanforderungen durchzusetzen und sind nicht selten dem verständnislosen Zorn eines Mitarbeiters oder Studierenden der HU ausgesetzt, dessen Account wegen einer nicht durchgeführten Paßwortänderung oder eines anderen „Vergehens“ gesperrt wurde. Wir müssen jedoch immer wieder feststellen, wie erschreckend groß die Defizite im Sicherheitsbewußtsein vieler Benutzer sind, wie unbekümmert Paßwörter an andere weitergegeben werden (Teilweise werden sie sogar per E-Mail verschickt!) und wie wenig Klarheit darüber herrscht, welche Folgen ein derart leichtfertiger Umgang mit dem eigenen Account haben kann.

Als wir zum Sommersemester 1995 begannen, für Studierende einen im Vergleich zu den vorangegangenen Jahren erheblich vereinfachten persönlichen Zugang zum Internet über einen UNIX-Account anzubieten¹, waren Probleme hinsichtlich der Sicherheit des Netzes in diesem Umfang noch kein Thema für uns. Als einzige Sicherheitsmaßnahme wurde die Änderung des Paßwortes beim ersten Login erzwungen, was durch das Kommando *passwd* in der Datei *.login* realisiert war. Die zunächst überschaubar geringe Zahl der eingetragenen Benutzer stieg erwartungsgemäß rasant an (gegenwärtig liegt sie bei ca. 12.000), und auch die ersten massiven Hacker-Attacken ließen nicht lange auf sich warten.

Die Angriffe konzentrierten sich u. a. auf das Entschlüsseln von Paßwörtern. Diese werden im Betriebssystem UNIX chiffriert gespeichert. Durch eine

Schwäche des bei uns eingesetzten Account-Verwaltungssystems NIS (Network Information System) ist es jedoch relativ einfach möglich, die chiffrierte Form eines Paßwortes zu lesen. Hacker benutzen sog. Crack-Programme, die mit umfangreichen Wörterbüchern arbeiten, jedes darin enthaltene Wort verschlüsseln und mit den im NIS gespeicherten Einträgen vergleichen. So können Paßwörter herausgefunden werden, die z. B. nur aus einem Wort der englischen oder deutschen Sprache bestehen. Um dem zu begegnen, begannen wir, selbst solch ein Crack-Programm laufen zu lassen. Zunächst wurden die Benutzer, deren Paßwort von diesem Programm ermittelt werden konnte, per E-Mail gebeten, ihr Paßwort zu ändern. Das hat sich bald als unzureichend erwiesen. Sehr viele Benutzer lesen ihre Mails nur in größeren Abständen, so daß wir uns gezwungen sahen, derart unsichere Accounts mit sofortiger Wirkung zu sperren. Die Benutzer wurden auf diese Art veranlaßt, sich mit uns in Verbindung zu setzen. „Sperren“ hieß dabei, dem Benutzer (und dem Hacker!) jeglichen Zugang zu dem Account zu verwehren. Gespeicherte Daten wurden davon nicht berührt, auch Mails konnten weiterhin empfangen werden. Die Sperre konnte durch das Rechenzentrum jederzeit wieder aufgehoben werden, wobei ein neues, sicheres Paßwort gesetzt wurde.

Im Herbst 1996 ersetzten wir das UNIX-Standard-Kommando *passwd* durch das Programm *anpasswd*, das bereits beim Ändern des Paßwortes durch den Benutzer das neue Paßwort auf seine Sicherheit testet. Seitdem können zu einfach strukturierte Paßwörter gar nicht mehr in das System gelangen. Da es darüber hinaus viele Möglichkeiten gibt, ein Paßwort – mit oder ohne Absicht – in fremde Hände geraten zu lassen, kann auch ein relativ sicheres Paßwort nach einer gewissen Zeit nicht mehr als sicher gelten. Daher führten wir gleichzeitig die Regelung ein, daß jedes Paßwort halbjährlich zu ändern ist. Zusätzlich verlangten wir nach dem Einrichten neuer Accounts die Änderung des

¹ Wendland, B.: Mit „amor“ ins Internet
RZ-Mitteilungen, Nr. 11, 1995, S. 23f.
http://www.hu-berlin.de/rz/rzmit/rzm11/rzm11_9.html