FORSCHUNGSZENTRUM JÜLICH GmbH
Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61–6402

Beratung und Betrieb, Tel. (02461) 61–6400

Technische Kurzinformation

FZJ-ZAM-TKI-0394
B. Mertens, M. Sczimarowsky, R. Theisen, Th. Eickermann
17.09.2004
Eine Englische Übersetzung dieser TKI ist als TKI-0395 erschienen

Umgangsregeln bei der elektronischen Kommunikation

Für Mitarbeiter des Forschungszentrums sind in der Betriebsvereinbarung Informations- und Kommunikationssysteme [1] verbindliche Regeln für die Nutzung der elektronischen Datenkommunikation (e-Kommunikation) festgelegt. Das vorliegende Dokument enthält dazu erläuternde und ergänzende Informationen zu Risiken und Verhaltensregeln bei der e-Kommunikation.

Für das Forschungszentrum ist die elektronische Kommunikation (z.B. E-Mail, Zugriff auf Web-Seiten, Teilnahme an Diskussionsforen, Zugang zu entfernten Datenbanken, Videokonferenzen, Grid-Computing) und deren ständige Verfügbarkeit eine strategische Notwendigkeit. Wie andere Betriebsmittel muss auch die elektronische Kommunikation verantwortungsvoll und wirtschaftlich genutzt werden. Höflichkeit, Aufrichtigkeit, das Vermeiden jeglicher Verstöße gegen Anstand, Recht und Gesetz sind wie bei jeder Art von Kommunikation selbstverständlich.

Das Internet weist aber besondere Eigenschaften und Risiken auf, die oft nicht unmittelbar zu erkennen sind. Daher sind zusätzliche Verhaltensregeln erforderlich, die von allen Teilnehmern beachtet werden müssen.

1 Gefahren bei der Nutzung des Internet

Die ersten Ursprünge des Internet stammen aus einem Forschungsprojekt der amerikanischen Regierung Ende der 60er Jahre; das Entwicklungsziel war damals eine möglichst robuste und zuverlässige Vernetzung zwischen relativ wenigen Universitätsrechenzentren herzustellen. Sicherheit und Vertraulichkeit der Kommunikation spielten damals eine untergeordnete Rolle. Dies wirkt sich noch heute im Internet mit seinen vielen hundert Millionen Nutzern weltweit aus. Besonders schwerwiegend sind folgende Risiken:

1. Ausspähen von Informationen

   Informationen werden in der Regel über viele Netzknoten und Übertragungsstrecken im Internet transportiert; dort können sie relativ einfach von Dritten mitgelesen werden.

2. Verfälschen von Informationen, Vortäuschen einer fremden Identität

   Während des Transports durch das Internet können Daten verändert werden, ohne dass der Empfänger dies bemerkt. Auch Absenderangaben von E-Mails sowie Rechneradressen können gefälscht werden. Man hat also keine Sicherheit über die Identität des Kommunikationspartners und die Authentizität der Information.

3. Einschleusen schädlicher Programme

   Manchmal werden im Internet zusammen mit scheinbar harmlosen Informationen (E-Mail,

Web-Seiten) schädliche Programme (Viren, Würmer, Trojanische Pferde, ...) verschickt oder angeboten, die sich meist unbemerkt auf Ihrem Rechner einnisten und dort Schaden anrichten können.

4. Unbefugtes Eindringen in Rechner

   Auch ohne eigene aktive Kommunikation ist Ihr Rechnersystem in Gefahr, von unbefugten Dritten ('Hackern') missbraucht zu werden, sofern eine Verbindung zum Internet besteht. Hacker nutzen oft Fehler in der Betriebs- und Anwendungs-Software aus, um heimlich über das Netz schädliche Programme einzuschleusen, die oft eine völlige Kontrolle des Rechners ermöglichen. Über solche Trojanischen Pferde können beispielsweise auch Tastaturanschläge protokolliert und an den Hacker verschickt werden, der damit auch höchst schützenswerte Informationen (z.B. Passwörter, PIN) in Erfahrung bringen kann.

5. Preisgabe persönlicher Informationen

   Bei der Kommunikation im Internet hinterlassen Sie zum einen stets an unterschiedlichen Stellen Informationen, die Rückschlüsse auf Ihre Person und ihr Kommunikationsverhalten erlauben (Name, Internet-Adresse, Uhrzeit, Art und Menge der abgerufenen Information usw.). Zum anderen wird man oft aktiv zur Eingabe sensibler Informationen aufgefordert. Dabei ist zu beachten, dass nicht in allen Ländern ausreichende Datenschutzbestimmungen greifen, die einen Missbrauch personenbezogener Daten unter Strafe stellen.

2 Grundsätzliche Verhaltensregeln bei der Nutzung des Internet

Zum Schutz vor Gefahren der elektronischen Kommunikation hat der Vorstand des Forschungszentrums eine Richtlinie zur IT-Sicherheit erlassen, deren Beachtung für alle Mitarbeiter verbindlich ist [2]. Insbesondere müssen damit auch die Sicherheitsregeln für den IT-Grundschutz [3] beachtet werden (z.B. Betriebssystem und Viren-Scanner aktuell halten). Diese Sicherheitsregeln bieten ausreichenden Schutz gegen die oben genannten Risiken.

Es versteht sich von selbst, dass von den Mitarbeitern des Forschungszentrums selbst keine Bedrohung der IT-Sicherheit anderer ausgehen darf, dass von ihnen alle einschlägigen rechtlichen Bestimmungen zu beachten sind und dass von ihnen die elektronische Kommunikation nicht absichtlich behindert oder beeinträchtig werden darf.

Insbesondere sind nicht zulässig:

- jegliche Internet-Nutzung, die geeignet ist, den Interessen des Forschungszentrums oder dessen Ansehen in der Öffentlichkeit zu schaden
- das Abrufen oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,
- das Abrufen oder Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen oder pornografischen Äußerungen oder Abbildungen,
- unbefugtes Abhören von Datenübertragungen,
- unbefugtes Eindringen in Rechnersysteme anderer,
- das absichtliche Verbreiten von Viren oder anderen schädlichen Programmen,
- fahrlässige oder gar vorsätzliche Störungen oder Unterbrechungen des laufenden Netzbetriebs.

Darüber hinaus sind durch die Betriebsvereinbarung für die private Nutzung ausdrücklich untersagt:

- das Verfolgen kommerzieller oder sonstiger geschäftlicher Zwecke,
- das Abrufen kostenpflichtiger Informationen,
- der Download von Musik- oder Videodateien,

- die aktive Beteiligung an Tauschbörsen, Internet-Auktionen, Online-Spielen oder ähnlichen Angeboten.

3 Regeln und Empfehlungen bei der Nutzung von E-Mail

Wegen der besonderen Eigenschaften der Kommunikation über E-Mail sind noch weitere Umgangsregeln und Empfehlungen zu beachten. Sie gelten gegebenenfalls auch für andere Kommunikationsformen. Online-Informationen zum Thema E-Mail und zu Sicherheitseinstellungen befinden sich auf den Web-Seiten des ZAM [4].

Die folgenden Regeln müssen beachtet werden:

Rechtliches

- Versenden Sie niemals E-Mail mit gesetzwidrigem, beleidigendem, diskriminierendem, belästigendem, abfälligem, diffamierendem, drohendem oder obszönem Inhalt.
- Täuschen Sie niemals beim Versenden von E-Mail einen falschen Absender vor (spoofing).
- Leiten Sie niemals Kettenbriefe weiter.

Sicherheit

- Benutzen Sie die aktuelle Version Ihres Mail-Programms und nutzen Sie dessen Sicherheitseinstellungen [4].
- Seien Sie misstrauisch und nutzen Sie im Zweifel alle Ihnen zur Verfügung stehenden Mittel (z.B. Telefon), um sich von der Authentizität des Absenders zu überzeugen — insbesondere bevor Sie E-Mail-Anhänge öffnen oder Internet-Links anklicken. Die Information im Mail-Kopf kann leicht gefälscht werden.
- Gehen Sie sehr sorgfältig mit Ihrem Passwort um (Auswahl, regelmäßige Änderung, Geheimhaltung). Eine Mail, in der Sie nach Ihrem Passwort gefragt werden, verfolgt mit Sicherheit keinen legitimen Zweck und darf daher niemals beantwortet werden. Das gleiche gilt sinngemäß für andere sensitiven Daten wie z.B. Kreditkartendaten, PINs, TANs (phishing).
- Unverschlüsselte Mail ist im Internet nicht vor Abhören durch Unbefugte geschützt. Senden Sie nichts unverschlüsselt per E-Mail, was Sie nicht auch auf einer Postkarte mitteilen würden. Zur Verschlüsselung bietet das ZAM Hilfsmittel (z.B. X.509-Zertifikate, GnuPG).
- Benutzen Sie die für Ihren Rechner angebotenen Antiviren-Programme, um Ihre Mails zu prüfen. Deren Viren-Muster müssen täglich aktualisiert werden. Trotz des zentralen Viren-Scanners ist diese Schutzmaßnahme unabdingbar.
- Nutzen Sie die vom ZAM angebotenen Vorkehrungen gegen Spam (unverlangt eingehende Werbung oder Schlimmeres) und löschen Sie die dann noch eintreffende Spam-Mail möglichst umgehend. Von jeder Reaktion auf Spam-Mail, auch auf Aufforderungen der Art: 'To unsubscribe, please ...' ist dringend abzuraten, da Sie damit dem Spammer die Funktionsfähigkeit Ihrer E-Mail-Adresse mitteilen.

Hoaxes

- Ignorieren Sie offensichtliche Falschmeldungen (Hoaxes, Schwindel, Veralberungen). Meist wird man vor einem neuen Computer-Virus gewarnt und aufgefordert, irgendwelche Systemeinstellungen zu ändern und alle Freunde und Bekannten vor der neuen Gefahr zu warnen. Wenn Sie unsicher sind, ob es sich um einen Hoax handelt, fragen Sie im ZAM nach oder schauen Sie im Internet bei [5] nach.

Die folgenden Empfehlungen sollten beachtet werden:

Höflichkeit

- Bei wichtigen Angelegenheiten frage man sich vor Verschicken einer E-Mail, ob nicht ein persönliches Gespräch die angemessenere Kommunikationsform ist.
- Versehen Sie Ihre E-Mail vor dem Versenden mit einem aussagekräftigen Betreff (Subject).
- Um sicherzustellen, dass der Empfänger weiß, wer der Absender ist, hängen Sie Ihrer Mail Ihre Kontaktinformation (Anschrift, Tel./Fax-Nr., E-Mail-Adresse) an. Die meisten Mail-Programme können automatisch den Inhalt einer vorbereiteten (signature-) Datei anhängen. Halten Sie eine solche Datei kurz.
- Wenn Sie eine Nachricht weiterleiten, verändern Sie den Inhalt nicht. Wenn es sich um eine persönliche Mail handelt, bitten Sie zuvor den Autor um Erlaubnis.
- Prüfen Sie Ihr Postfach regelmäßig auf neu eingegangene Nachrichten. Häufig ist ein wesentlicher Grund für die Nutzung von E-Mail die Annahme einer kurzen Reaktionszeit. Wenn die Bearbeitung der E-Mail länger dauert, hilft dem Absender eine kurze Rückmeldung von Ihnen dabei, zu erkennen, dass seine E-Mail angekommen ist und zur Kenntnis genommen wurde.
- Sorgen Sie umgekehrt im Falle einer längeren Abwesenheit dafür, dass der Absender über den Verbleib seiner E-Mail informiert wird. Der Mail-Server bietet die Möglichkeit der automatischen Benachrichtigung der Absender.

Technik

- E-Mail sollte aus einfachem Text bestehen. Neuere Mail-Programme bieten zwar die Möglichkeit, E-Mail im HTML-Format zu erzeugen, und damit z.B. Zeichensatz oder Farbe des Mail-Textes zu variieren. Dieses Format wird jedoch auch zur Verbreitung schädlicher Software missbraucht, und sollte deshalb vermieden werden. Darüber hinaus unterstützen auch nicht alle Mail-Programme HTML, was das Lesen zur Zumutung machen kann.
- Verwenden Sie im Kopf der E-Mail (Header) keine Umlaute, sondern loesen Sie diese auf.
- Wenn Sie Anhänge (Attachments) verschicken, vergewissern Sie sich, dass der Empfänger diese auch interpretieren kann.
- Seien Sie sich dessen bewusst, dass das Mail-System für die Übermittlung kurzer Textnachrichten konzipiert wurde. Für große Datenmengen ($>$ 10 MByte) sollten andere Techniken (z.B. Secure File Copy) benutzt werden. Sehr große E-Mails können, sofern sie überhaupt transportiert werden, die Funktion der beteiligten Mail-Server stark beeinträchtigen.
- Überprüfen Sie regelmäßig Ihr Postfach, ob der Ihnen zugewiesene Speicherplatz mit Nachrichten nicht schon weitgehend belegt ist. Verlagern Sie ggf. Ihre Nachrichten auf Ihren lokalen Rechner und löschen Sie nicht mehr benötigte Mail, damit genügend Speicherplatz für Ihr Postfach frei ist und Sie weiterhin E-Mail empfangen können.

Besondere Regeln gelten für den privaten E-Mail-Verkehr:

- Dieser ist grundsätzlich über externe Mail-Dienste abzuwickeln. Mit dieser Regelung soll zum einen erreicht werden, dass Sie (beim Versenden privater E-Mail) nicht mit Ihrer dienstlichen E-Mail-Adresse auftreten. Zum anderen soll so verhindert werden, dass sich (durch das Empfangen privater E-Mail) in Ihrem dienstlichen Postfach private E-Mails befinden können, was zu rechtlichen Probleme führen könnte (Telekommunikationsgesetz, Briefgeheimnis, ...).
- Wenn Sie einen externen E-Mail-Dienst nutzen, sind Sie nicht mehr durch den zentralen Viren-Scanner des ZAM geschützt (wie Sie es wären, wenn Sie die Mail per 'forward' an Ihre dienstliche Adresse weiterleiten würden). Es ist daher absolut notwendig, dass auf dem Rechner, auf dem Sie diese Mails lesen, ein sich automatisch aktualisierender Viren-Scanner läuft.
- Zusätzlich empfehlen wir dringend, einen Mail-Dienstleister zu nutzen, der seinerseits einen Viren-Scanner einsetzt. Nach einem Test der Stiftung Warentest im August 2003 bieten die kostenlosen E-Mail-Angebote von web.de und hotmail.com den besten Virenschutz. Diese

Dienste bieten jedoch häufig nicht das Sicherheitsniveau des zentralen Viren-Scanners des ZAM und machen keinesfalls einen eigenen Viren-Scanner überflüssig.

4 Regeln und Empfehlungen zur Nutzung von Internet-Informationsdiensten (WWW, NetNews usw.)

Die folgenden Regeln müssen beachtet werden:

- Suchen Sie keine Web-Dienste auf und beteiligen Sie sich nicht an Diskussionsforen usw., wenn diese offensichtlich gesetzwidrige Inhalte oder Ziele haben. Rufen Sie keine gesetzwidrigen Inhalte ab.
- Suchen Sie keine Web-Server oder Diskussionsforen mit fragwürdigen Inhalten auf. Hier lauern oft verborgene Gefahren, die die Sicherheit Ihres Systems bedrohen. Beachten Sie, dass Sie mit Ihrer Internet-Adresse als Mitarbeiter des Forschungszentrums ausgewiesen sind.

Die folgenden Empfehlungen sollten beachtet werden:

- Benutzen Sie möglichst sichere Einstellungen des Betriebssystems und der Anwendungen (z.B. des Web-Browsers). Bitten Sie ggf. den IT-Ansprechpartner in Ihrer Organisationseinheit um entsprechende Hilfe.
- Es ist nicht zu verhindern, dass bei der Kommunikation im Internet an unterschiedlichen Stellen gewisse Datenspuren zurückbleiben. Man sollte aber möglichst vermeiden, selbst noch zusätzliche personenbezogene Daten zu liefern. Somit ist große Zurückhaltung geboten, wenn man von einem fremden Rechnersystem nach Namen, E-Mail-Adresse, Wohnort usw. gefragt wird.

Links

[1] www.fz-juelich.de/gr/intern/e-kommunikation

[2] www.fz-juelich.de/internes/IR/IT-Sicherheitsrichtlinie_der_Forschungszentrum_Juelich_GmbH_(IR_119-1).pdf

[3] www.fz-juelich.de/internes/IR/IT-Sicherheitsregeln_fuer_den_Grundschutz_(IR_119-1).pdf

[4] www.fz-juelich.de/MAIL

[5] www.tu-berlin.de/www/software/hoax.shtml