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-0395
B. Mertens, M. Sczimarowsky, R. Theisen, Th. Eickermann
17.09.2004
The German version of this TKI is available as TKI-0394

Handling rules for electronic communication

For staff members of the Research Centre, binding rules for the use of electronic data communication (e-communication) are laid down in the Internal Agreement on Information and Communication Systems [1]. The present document contains explanatory and complementary information on the risks and rules of conduct in e-communication.

For the Research Centre, electronic data communication (e.g. e-mail, access to websites, participation in discussion forums, access to remote databases, video conferences, grid computing) and its constant availability are a strategic necessity. In the same way as other resources, electronic communication must be used responsibly and economically. Politeness, sincerity, the avoidance of any offences against decency, rights and laws are a matter of course as in any other kind of communication.

The Internet, however, displays special features and risks, which often cannot be directly identified. It is therefore necessary that all participants observe additional rules of conduct.

1 Dangers in using the Internet

The Internet has its origins in a research project of the American administration in the late sixties; the development goal was to establish the most robust and reliable networking possible between relatively few university computer centres. The security and confidentiality of communication played a minor role at that time. This still has an effect on the Internet today with its hundreds of millions of users worldwide. The following risks are particularly grave:

1. Spying out information

   Information is generally transported across a large number of network nodes and transmission links on the Internet, where it can be read relatively easily by third parties.

2. Corrupting information, pretending a false identity

   During their transport through the Internet data can be modified unnoticed by the recipient. Sender details in e-mails and computer addresses can also be falsified. You thus cannot be sure of the identity of your communication partner and the authenticity of the information received.

3. Implanting harmful programs

   Together with seemingly harmless information (e-mail, websites) harmful programs (viruses, worms, Trojan horses, ...) are sometimes sent or offered on the Internet, which in most cases can implant themselves unnoticed on your computer and cause damage there.

4. Unauthorized penetration into computers

   Even if you do not actively communicate yourself, your computer is in danger of being misused by unauthorized third parties ('hackers'), if there is a connection to the Internet. Hackers often exploit faults in the operating and application software to clandestinely implant harmful programs through the network, which often enable complete control of the computer. Via such Trojan horses it is also possible, for example, to log keyboard strokes and send them to the hacker, who can thus obtain information extremely worth being protected (e.g. passwords, PIN).

5. Disclosure of personal information

   In communicating on the Internet, on the one hand, you always leave information at different places, which allows conclusions to be drawn concerning your person and your communication behaviour (name, Internet address, type and amount of retrieved information etc.). On the other hand, you are often actively requested to enter sensitive information. It should be noted here that adequate data protection provisions penalizing a misuse of personal data are not effective in all countries.

2 Fundamental rules of conduct in using the Internet

In order to protect against the dangers of electronic communication, the Board of Directors of the Research Centre has issued a guideline on IT security, which must be observed by all members of staff [2]. In particular, the security rules for IT baseline protection [3] must thus also be observed (e.g. updating operating systems and virus scanners). These security rules provide sufficient protection against the above risks.

It goes without saying that the Research Centre's staff on their part must not threaten the security of others, that they must observe all relevant legal provisions and that they must not intentionally impede or impair electronic communication.

In particular, the following is not permitted:

- any Internet use that is suitable to harm the interests of the Research Centre or its reputation among the general public
- retrieving or disseminating contents that violate legal provisions on data protection, personal rights, copyright or criminal law
- retrieving or disseminating insulting, defamatory, anti-constitutional, racist or pornographic utterances or illustrations
- unauthorized bugging of data transmissions
- unauthorized penetration into computer systems of others
- intentionally spreading viruses or other harmful programs
- negligent or even wilful disturbances or interruptions of running network operation

Furthermore, the internal agreement expressly prohibits the following for private use:

- pursuing commercial or other business purposes
- retrieving information on a fee-paying basis
- downloading music or video files
- actively participating in swap shops, Internet auctions, on-line games or similar offers

3 Rules and recommendations for using e-mail

Due to the special features of e-mail communication, further handling rules and recommendations are to be observed, which may also apply to other forms of communication. On-line information on the topic of e-mail and on security settings can be found on the web pages of ZAM [4].

The following rules must be observed:

Legal

- Never send e-mail with illegal, insulting, discriminatory, annoying, disparaging, defamatory, threatening or obscene contents.
- Never pretend to be somebody else in sending e-mail (spoofing).
- Never forward chain letters.

Security

- Use the latest version of your mail program and utilize its security settings [4].
- Be mistrustful and when in doubt use all available means (e.g. telephone) to convince yourself of the sender's authenticity - especially before you open e-mail attachments or click on Internet links. The information in the mail header can be easily falsified.
- Handle your password very carefully (selection, regular change, secrecy). An e-mail in which you are asked for your password certainly does not pursue a legitimate purpose and must therefore never be answered. The same applies analogously to other sensitive data such as credit card data, PINs, TANs (phishing).
- Unencrypted mail on the Internet is not protected against bugging by unauthorized persons. Do not send anything unencrypted by e-mail which you would not also communicate on a postcard. ZAM can provide encryption aids (e.g. X.509 certificates, GnuPG).
- Use the antivirus programs available for your computer to check your mails. Their virus patterns must be updated daily. Despite the central virus scanner this protective measure is indispensable.
- Make use of the precautions against spam (junk advertising or worse) offered by ZAM and immediately delete any spam mail nevertheless received. You are urgently advised not to respond to spam mail, including requests of the type 'To unsubscribe, please ...', since you thus communicate the functionability of your e-mail address to the spammer.

Hoaxes

- Ignore obvious false messages (hoaxes, fraud, pranks). In most cases you are warned of a new computer virus and requested to change certain system settings and to alert all your friends and acquaintances. If you are not sure whether it is a hoax, ask ZAM or look on the Internet at [5].

The following recommendations should be observed:

Politeness

- For important matters you should ask yourself before sending an e-mail whether a personal conversation would not perhaps be more appropriate.
- Prior to sending provide your e-mail with an informative subject.
- In order to ensure that the recipient knows who is the sender, attach your contact information (postal address, tel./fax no., e-mail address) to your mail. Most mail programs can automatically attach the contents of a prepared (signature) file. Keep such a file short.
- If you forward a message do not modify the contents. If it is a personal mail obtain the author's permission before.

- Regularly check your mailbox for newly received messages. An essential reason for using e-mail is frequently the assumption of a short response time. If it takes longer to deal with the e-mail, a short message to the sender will help him to be aware that his e-mail has been received and taken notice of.
- Conversely, in the case of prolonged absence take care that the sender is informed about the fate of his e-mail. The mail server provides the possibility of automatically notifying the sender.

Technology

- E-mail should consist of simple text. Recent mail programs provide the possibility of generating e-mail in HTML format and thus varying e.g. the character set or colour of the e-mail text. However, this format is also misused for disseminating harmful software and should therefore be avoided. Furthermore, not all mail programs support HTML, which can make reading a nuisance.
- Do not use umlauts in the e-mail header, but resolve them into two vowels.
- If you send attachments, make sure that the recipient can interpret them.
- You should be aware of the fact that the e-mail system was designed for transmitting short text messages. For large data volumes (> 10 Mbytes) other techniques should be used (e.g. file transfer). Very large e-mails - if transported at all - can greatly impair the function of the mail servers involved.
- Regularly check your mailbox to ascertain whether the storage space allocated to you is not already largely occupied by messages. If necessary, relocate your messages to your local computer and delete any mail no longer needed, so that sufficient storage space is available for your mailbox and you can continue to receive e-mail.

Special rules are applicable to private e-mail traffic:

- In principle, this should be handled via external mail services. This is to ensure, on the one hand, that you do not appear with your official e-mail address (when sending private e-mail). On the other hand, this is to prevent private e-mails being contained in your official mailbox (due to receiving private e-mail), which could lead to legal problems (Telecommunications Act, secrecy of correspondence, ...).
- If you use an external e-mail service, you are no longer protected by the central virus scanner of ZAM (as you would be if you forwarded the mail to your official address). It is therefore absolutely necessary that an automatically updated virus scanner is running on the computer on which you read these mails.
- In addition, we urgently recommend that you should use a mail provider employing a virus scanner on his part. According to a test by Stiftung Warentest (consumer goods testing foundation) in August 2004, the free e-mail services of web.de and hotmail.com provide the best virus protection. However, these services frequently do not provide the security level of ZAM's central virus scanner and do by no means make a virus scanner of your own superfluous.

4 Rules and recommendations for using Internet information services (WWW, NetNews etc.)

The following rules must be observed:

- Do not visit any web services and do not participate in discussion forums etc., if these obviously have illegal contents or goals. Do not retrieve any illegal contents.

- Do not visit any web servers or discussion forums with questionable contents. These often contain hidden dangers threatening the security of your system. Be aware that your Internet address identifies you as a staff member of the Research Centre.

The following recommendations should be observed:

- Use the safest possible settings of the operating system and the applications (e.g. of the web browser). Where necessary, ask the IT contact person in your unit of organization for help.
- It cannot be avoided that certain data traces are left somewhere on the Internet due to communication. However, you should not furnish additional personal data yourself. You should therefore be very hesitant if you are asked for your name, e-mail address, place of residence etc. by an external computer system.

Links

[1] www.fz-juelich.de/gr/intern/e-kommunikation (currently only in German)

[2] www.fz-juelich.de/zam/security/principles/IT-Security-Guideline_IR119-1_040317.pdf

[3] www.fz-juelich.de/zam/security/principles/IT_Security_Rules_for_Baseline_Protection_031209.pdf

[4] www.fz-juelich.de/zam/mail_en

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