"Security Policy" für das Institut der theoretischen Physik und den Computerraum Physik — Entwurf

Andreas Hirczy <http://fubphpc.tu-graz.ac.at/~ahi/> $Date: 2000-02-13$

Inhaltsverzeichnis

1 Allgemeines

Mit der Verwendung der Accounts erklären sich alle Benutzer der Computer bereit, die Regeln dieses Textes zu akzeptieren.

Diese Regelungen werden bei Bedarf an veränderte technische Rahmenbedingungen oder geändertes Benutzerverhalten angepaßt.

Zu jedem Computer am Institut gibt es eine verantwortliche Person (*Betreuer, Administrator*). Sie finden am Webserver eine *Liste* <http://www.itp.tu-graz.ac.at/Lokales/Computer/Liste/finder.pl> mit dieser Zuordnung.

2 Rechte und Pflichten aller Benutzer

2.1 Lesen der Electronic Mail

Jeder Benutzer soll seine EMail lesen, weil \dots

2.2 Accountdisziplin

Geben Sie Ihr Passwort **keinesfalls** an andere Personen weiter. Auch die Betreuer der Computer werden Sie niemals nach ihrem Passwort fragen. Sollten Sie Ihr Passwort vergessen haben, wird es auf Anfrage neu gesetzt.

Wählen Sie gute Passworte!

Der Algorithmus zur Passwortprüfung verwendet eine nicht umkehrbare Hashfunktion, um aus Ihrem Passwort und einer zufälligen Zahl eine weitere Ziffernfolge zu generieren. Die einzige Möglichkeit, ihr Passwort im Klartext lesbar zu machen, besteht im systematischen Probieren aller möglichen Passworte. Wegen der hohen Anzahl der Möglichkeiten (alle Permutation von 8 Zeichen aus [a-z][A-z][0-9][.,:;-_#´*+] und einigen weiteren Zeichen) ist es nicht sinnvoll, den Passwortraum vollständig abzusuchen. Die klassischen Crackprogramme stützen sich daher auf Wörterbücher, deren Einträge auf verschiedene Arten kombiniert und permutiert werden. Ergänzt werden diese Daten durch Kenntnisse über das soziale Umfeld (*social engineering*).

Passworte, die nicht verwendet werden sollen, umfassen:

- englische und deutsche Worte sowie deren Flexionen
- Wörter, die in der Passwortdatei selbst stehen (alle lokal bekannten Namen)
- Muster (123456, abc123, qwertz)
- geographische Bezeichnungen
- Telephonnummern, Raumnummern, Autonummern und der Geburtstag der Freundin oder Ehefrau (Daten mit irgendeiner Beziehung zu einer bestimmten Person)
- Variationen von obigem

Gute Passworte

- bestehen aus sechs bis acht Zeichen
- enthalten gemischte Groß und Kleinschreibung
- enthalten Buchstaben und Ziffern
- enthalten nicht alphanmerischen Zeichen
- sind leicht zu merken, damit die Versuchung, sie aufzuschreiben, minimiert wird.

Ich verwende meist eines der folgenden Verfahren, um eine sicheres, aber trotzdem leicht zu merkendes Passwort zu finden:

- Wählen sie einen Satz, der für sie leicht zu merken, aber nicht zu geläufig ist. (Beispielsweise den ersten Satz ihrer Diplomarbeit/Habilitierungsschrift.) Nehmen sie jeweil den ersten (oder dritten, letzten) Buchstaben jedes Wortes und setzen sie daraus das Passwort zusammen. Achten Sie auch hier auf Sonderzeichen und Ziffern. Beispiel: "Warum ein Passwort, ich mag keines!" wird zu "WeP,imk!" oder "WeP,1mk!".

- Stellen Sie ein Folge von jeweils einem Konsonanten und einem oder mehreren Vokalen hintereinander. Worte, die auf diese Art generiert werden, können im Allgemeinen ausgeprochen werden und werden deshalb leichter behalten. Beispiel: “KoDouPae”

Die als Beispiel angeführten Passworte sind selbstverständlich kein guten Passworte mehr.

2.3 Crackversuche

Versuche, Computer außerhalb des lokalen Netzes in ihrer Funktion zu beeinträchtigen oder systematisch nach möglichen Angriffspunkten zu untersuchen, werden von den zuständigen Administratoren meist auf recht harsche Weise dem Institut gemeldet. Vorgänge dieser Art müssen daher **unbedingt unterlassen** werden.

Innerhalb des lokalen Netzes soll diese Regelung nicht so streng ausgelegt werden. Vermweiden Sie unbedingt, Schaden jeder Art anzurichten. “Erfolge” melden sie bitte umgehend Ihren zuständigen *Betreuern* `<mailto:edv@itp.tu-graz.ac.at>`.

Bitte bedenken sie, daß “Denial of Service”-Attacken durch Überlastung von Systemresourcen bei allen Unix-Varianten durch Benutzer mit gültigem Password möglich sind. Sollten derartige Versuche unternommen werden, muß durch Setzen beziehungsweise Verschärfen von Limits (Speicher, CPU-Zeit usw.) Abhilfe geschaffen werden.

Altbekannte Angriffe werden im Allgemeinen nicht erfolgreich sein; die Verfolgung zum Urheber erfordert für die Administration aber häufig erheblichen Aufwand. Unmutsreaktionen könnten nicht ausbleiben. Wenn sie Versuche in dieser Richtung planen, können Sie sich vorher mit den *Betreuern* `<mailto:edv@itp.tu-graz.ac.at>` der Computeranlage absprechen.

2.4 Reboot / Abschaltung von Computern

Neustart oder Abschalten von laufenden PCs ohne dringenden Grund ist nicht statthaft. Als dringender Grund wird zum Beispiel Rauchentwicklung im Gehäuse des Rechners oder Ähnliches akzeptiert werden.

Das Stillegen von Computern, um die IP-Adresse anderweitig zu verwenden, ist explizit nicht erlaubt.

2.5 Installation von Hard- und Software

Die Installation von Hard- und Software ist den Administratoren der Computer vorbehalten. Das Öffnen der Computergehäuse ist nicht erlaubt. Externe Geräte wie zum Beispiel Modems oder ISDN-Adapter fallen ebenfals unter diese Regelung.

Ausnahmen:

- Programme, die im Rahmen von Forschung und Lehre benötigt werden und im Homedirectory des Benutzers bleiben.
- Drucker, sofern bereits ein passender Treiber installiert war.

2.6 Starten eigener Netzwerkservices

Proxy-Server:

Proxy-Server werden grundsätzlich nicht verwendet. Die Installation von Proxy-Servern macht Zugriffskontrollen, die auf Überprüfung der IP-Adressen des Absenders basieren, wirkungslos.

Selbstständige Server:

Eigene Server dürfen nur nach Abstimmung mit **allen EDV-Beauftragten und dem Institutsvorstand** und **nur auf eigenen Geräten** eingerichtet werden. Dabei ist auch besonderes Augenmerk auf gesetzliche Regelungen, insbesondere im Bereich des Urheberrechtes zu legen.

2.7 Anschluß eigener PCs an das Netz der TU Graz

Eigene PCs dürfen nur nach Anmeldung bei den *EDV-Beauftragten* `<mailto:edv@itp.tu-graz.ac.at>` an das Netzwerk angeschlossen werden.

Bei der Inbetriebnahme des Computers gibt es keinen Anspruch auf Unterstützung. Eventuell finden Sie Lösungen zu Ihren Problemen im *Handbuch für Administratoren* `<http://www.itp.tu-graz.ac.at/Lokales/Computer/man-admi.html>`. Bei Fehlfunktionen, die die Integrität der übrigen Installation gefährden, kann der Netzwerkanschluß ohne Vorwarnung deaktiviert werden.

2.8 Dringende Empfehlungen

- Verwenden Sie `ssh` anstelle von `telnet` oder `rsh`.
- Kontrollieren Sie vor dem Belegen von Speicherplatz auf den Festplatten, ob diese dem Bedarf genügen können. Legen sie Daten, die nur kurzfristig (zum Beispiel Zwischenergebnisse im Rahmen einer Simulation) benötigt werden, nicht in ihrem Homedirectory, sondern unter `/tmp` oder `/var/tmp` ab. Weil diese Verzeichnisse immer lokal zum Rechner stehen, ist der Zugriff schneller und sowohl das Netzwerk als auch die Fileserver und das Backup-System werden entlastet. Bitte entsorgen sie diese Dateien, sobald sie nicht mehr gebraucht werden.
- Belegen Sie nicht exzessiv Speicherplatz durch das Horten von `mp3`-Audiodaten oder Bildern und Filmen mit Witzchen und dergleichen.
- Sammeln sie kein alten Quelltexte von fremden Programmen.

3 Rechte und Pflichten der Administratoren

Durchsetzen der in diesem Dokument angeführten Regeln mit technische Mitteln

3.1 regelmäßige Upgrades

täglich, bei Erscheinen neuer sicherheitsrelevanter Patches

3.2 Scannen des Netzes nach nicht autorisierten Services

regelmäßig, mindestens 1 mal pro Monat

3.3 Sichten der Log-Dateien

alle Log-Einträge umleiten auf FAEPPC23/32; dort regelmäßig (mindestens 1 mal pro Woche) überprüfen (derzeit realisiert mit `wots`)

3.4 Kontrolle der Integrität einzelner Knoten im Netz

Prüfen der installierten Software und Configuration mit Hashsummen

(derzeit realisiert mit `Cfengine`, alternativ `tripwire`)

3.5 Suche nach leicht zu erratenden Passworten

1 mal pro Semester, (derzeit realisiert mit `John the Ripper`)