Sicherheit im Rechnernetz DESY Zeuthen
Eine Anleitung für den Nutzer

Waltraut Niepraschk, DESY Zeuthen, 06.12.1999

---

1. Aktuelle Situation der System- und Netzwerkadministratoren

1.1 Entwicklung des Internets

60-er Jahre: Sicherheit der Daten und Rechner nebensächlich
Priorität: Funktionalität
Einsatz vor allem im wiss. Bereich
freier Austausch von Informationen

90-er Jahre: 70 Mill. Benutzer im Internet
kommerzielle Nutzung verstärkt
Sicherheit gewinnt an Bedeutung
Datenschutz

keine zentrale Kontrollinstanz
jeder entscheidet selbst über seine persönlichen Sicherheitsanforderungen - Risikoanalyse !

1.2 Hackerszene

Die Intelligenz der Tools, Frequenz, Typen und Hartnäckigkeit von Sicherheitsattacken nehmen ständig zu. Über Newsgruppen und Chat werden gehackte oder gesniffte Accounts ausgetauscht. Die Bereitstellung von "Hacker"-Tools erfolgt auf zahlreichen Webseiten. Die meisten Hacker sind keine Profis mehr, nur `make` genügt und die Tools können gestartet werden.

Die Hacker"profis" stellen immer ausgefeiltere Methoden zur Verfügung:

früher: Paßwort-Cracking, Suche nach offenen Accounts,
Konfigurationsfehlern und Protokollschwächen (NIS)
Attacken auf einzelne Hosts

heute: IP Spoofing
"Denial of Service" Attacken
Attacken auf ganze Internetdomänen
Mehrstufiges Vorgehen:

- Identifikation des Ziels
- Sammeln von Informationen
- Versuch einer Attacke -> neue Informationen
- weitere, gezielte Attacken
  Programmpakete RootKit/DaemonKit (troj. Programme)
  ls, ps, netstat, inetd, tcpd, ... werden modifiziert
  z.B. aktuell: Suche nach Sicherheitslücken im AFS

1.3 Gegenüberstellung Admins - Hacker

Admins	Hacker
zu wenig Zusammenarbeit	hervorragender Informationsaustausch
Abdeckung aller Lücken notwendig	Finden einer Sicherheitslücke
Schutz aller Maschinen	Finden einer Maschine
Überlastung	viel Zeit

1.4 Integrität und Vertraulichkeit im Internet

Vermeidung und Ersetzung veralteter, unsicherer Protokolle und Anwendungen.

Problem	Lösung
Abhören des Netzverkehrs, gefälschte IP Adressen	Zukunft: IP Version 6, ssh, ssl, https
gefälschte Nameservereinträge	DNS SEC, DNS Spoofing durch ssh verhindert
gefälschter Mailabsender	Mails signieren
Mitlesen von Mails	vercrypten mit PGP
gefälschte Identität	Verwendung von starken Authentisierungsmethoden: z.B. Kerberos

-> Für eine globale Kommunakation werden global kompatible Zertifizierungsinfrastukturen gebraucht!

Eine eindeutige Identifizierung der Teilnehmer, Benutzer und Rechner(Instanzen) und eine sichere Kommunikation wird gefordert.

1.5 Sicherheitsrisiken

Neben vorsätzlichen Handlungen gibts es zahlreiche weitere Gefährdungen, die Ursachen für unbeabsichtigte Schäden sein können:

- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Höhere Gewalt

Deshalb hat DESY beschlossen ein umfassendes Sicherheitskonzept zu erarbeiten. Es wurde ein IT-Sicherheitsbeauftragter und ein Rechnersicherheitsrat (RSR) berufen.

2. Statistik von Sicherheitsvorfällen im DESY Zeuthen

Im Dezember 1997 bemerkten wir lange unentdeckt gebliebene Häckeraktivitäten auf einem wenig administrierten Rechner. In den letzten Jahren wurden zahlreiche Sicherheitsmaßnahmen realisiert, z.B. TCP Wrapper, Login von Remoterechnern nur über SecureShell oder Einmalpaßwörter, Installation eines zentralen Loghosts und Auswertung der Logfiles. Wer zu diesem Thema mehr wissen möchte, kann sich an security@ifh.de wenden.
Seit Dezember 1997 bemerkten wir keinen weiteren Hackereinbruch.

Sicherheitsvorfälle:

Portscans: sendmail, popper, imap, telnet, ftp, ssh !
die zum Teil einzelne Maschinen, aber auch die ganze Domäne ifh.de betrafen.

1999

Januar	21
Februar	8
März	12
April	9
Mai1	1
Juni	10
Juli	13
August	9
September	11

WWW Service	Suche nach cgi-bin Scripten: webdist.cgi, phf.cgi, php.cgi, Count.cgi
	selten
News Service	Hackeraktivitäten verringert
	1997 2-3 Attacken/Woche
ftp Service	Suche nach Konfigurationsfehlern
	3-4 Attacken/Monat

3. Hinweise für den Nutzer

3.1. Warum muß auch der Nutzer auf Sicherheit achten ?

Nutzer hat unterschrieben, daß er seinen Account schützt.

DESY Zeuthen ist nicht isoliert. In der HEP Gemeinde sind nicht überall die gleichen Sicherheitsmaßnahmen realisiert. Zum Teil arbeiten Benutzer, die auch einen Account in Zeuthen haben, auf nicht zentral oder gar nicht administrierten Rechnern. Hackern kann der Zugang zu DESY Zeuthen ermöglicht werden.

Nach einem Hackereinbruch in einem anderem LAB werden meist Sniffer installiert, die die Paßwörter abgehören.
Ist einer dieser gesnifften Accounts durch einen Benutzer getrustet zu einem Account in ifh.de ist für den Hacker auch der Zugang zu ifh.de gesichert. Die Hacker wissen auch, daß die Benutzer oft die gleichen Paßwörter in verschiedenen LABs benutzen. So hangeln sich die Hacker zu einem Rechner des anderen LABs.

Die Hacker suchen wiederum auf diesem Rechner nach Sicherheitslücken. Die Administratoren versuchen, die Rechner auf dem neuesten Patchstand zu halten, aber es gibt Situationen, wo ein Rootzugang nicht verhindert werden kann (z.B. vom Hersteller kann noch kein Patch zur Verfügung gestellt werden).

Files können modifiziert oder gelöscht werden. Informationen können mißbraucht werden. Der Account kann mißbraucht werden für Attacken gegen andere Einrichtungen. Damit wird der Ruf von DESY geschädigt.

Achtung: Auch HomePCs werden gescannt, wenn sie per Modem/ISDN am Netz sind !

3.2. Wie kann sich der Nutzer schützen

3.2.1. Gute Paßwörter

Gute Passwörter sollten:

- nur dem Accountinhaber bekannt sein
- nie im Klartext in einem File oder Programm oder auf einem Zettel am Terminal erscheinen
- zwar leicht zu merken sein, aber nicht leicht zu erraten
- nicht in Wörterbüchern stehen
- zusammengesetzt sein aus Zahlen, Sonderzeichen,Groß- und Kleinbuchstaben
- möglichst lang sein: 6 - 8 Zeichen lang
- kein CTRL, #, @, \ enthalten

Paßwörter altern nach 180 Tagen und können nicht wiederverwendet werden. Der Account wird gesperrt, wenn das Paßwort nicht geändert wird.
Man sollte nicht überall das gleiche Paßwort verwenden ! Besonders Rechnern, die wenig administriert werden, sollte man nicht trauen, also nicht in .rhosts oder .shosts eintragen und man sollte dort ein anderes Paßwort verwenden.

3.2.2. Keine abhörbaren Paßwörter übertragen, abhörsichere Verbindungen aufbauen

Durch geswitchte Netzwerktechnologie und strukturierte Verkabelung wird die Möglichkeit des Abhörens des Netzwerkes deutlich eingeschränkt.
Die Übertragung unverschlüsselter Paßwörter kann ``nur'' beim Zugang vom Xterminal zum Zielrechner nicht verhindert werden. Bei Verwendung der empfohlenen Software ist die Verbindung ansonsten verschlüsselt: Statt rsh, rlogin, rcp, telnet und ftp sollten
`ssh, scp, xssh` verwendet werden.

`man ssh`: *"encrypted communications between two untrusted hosts over an insecure network"*

Viele nützliche Hinweise findet man in den FAQ's: http://www.employees.org/~satch/ssh/faq

ssh

und Zubehör sind auf allen UNIX Rechnern installiert. Sie können aber nur verwendet werden, wenn auf dem Zielrechner der sshd Daemon läuft.

Auch auf WindowsNT wird ein NetInstall Paket zur Verfügung gestellt, in dem ein ssh Client enthalten ist: Teraterm.
Das X11 Forwarding kann eingeschaltet werden.

In DESY Zeuthen und Hamburg wird als Authentisierungsmethode neben Kerberos die Rhost-Methode (/etc/hosts.equiv, .rhosts) + RSA-basierte Hostauthentisierung verwendet.
Auf jedem Rechner werden 2 Keys generiert: ein public und ein private Key. Die public Keys werden in /etc/ssh_known_hosts gesammelt.
Auch der Benutzer kann diesen Machanismus nutzen. Er wird gefragt (bei default Konfiguration), ob der public Key des Zielrechners eingetragen werden soll in sein `~/.ssh/known_hosts` (auf dem Startrechner).
Wenn sein Startrechner vertrauenswürdig ist, und der Benutzer den Startrechner in seinem `~/.rhosts` oder besser `~/.shosts`
auf dem Zielrechner eingetragen hat, dann kann er sich auch ohne Paßwort einloggen.

Beispiele:
```
ssh machine.domain command
ssh -l user machine.domain
scp * user@host.domain:directory
scp user@host.domain:directory/'*' .
```

Einloggen mit Einmalpaßwörtern S/KEY (telnet und ftp)

Eine kurze Anleitung findet man unter http://www.ifh.de/computing/projects/security/SKEY/skey.html

`keyinit`	Erzeugen von Einmalpaßwörtern an Konsole
`keyprint | lpr`	Ausdrucken der Einmalpaßwörter in Kreditkartenform

Einmalpaßwörter sind nur sinnvoll, wenn danach keine weiteren Paßwörter angegeben werden müssen, z.B. für AFS oder Kerberos Authentisierung, da diese sonst doch abgehört werden könnten.

Zur Zeit sind die S/KEYs der einzigste sichere Zugang, wenn die ssh nicht zur Verfügung steht.

Zukunft: ssh Client über Webbrowser (Java-Applet)

Mailservice

Protokolle: `imap4` und `pop`

`pop`	Protokoll vermeiden, wird nur noch innerhalb von ifh.de unterstützt Paßwörter werden häufig im Klartext im Netz übertragen
`imap4`	mit Kerberosauthentisierung
`imap4`	mit Kerberosauthentisierung und SSL (Secure Socket Layer)

Der imap Zugang ist jetzt so konfiguriert, daß eine Kerberos Authentisierung verlangt wird. Damit ist der rsh Zugang zum Mailserver nicht mehr notwendig.

Achtung: wenn der Benutzer von imap z.B. über pine kein Kerberos Ticket hat, wird das Paßwort im Netz im Klartext übertragen.

Wie können Klartextpaßwörter vermieden werden?

- Kerberos Ticket vorher besorgen
- wenn das nicht möglich ist, z.B. bei Windows PC Nutzern, sollte man eine sichere Verbindung über SSL aufbauen.
- SKEY Benutzer: kein Kerberos Ticket erzeugen, man will ja in diesem Fall jedes wiederverwendbare Paßwort vermeiden. Deshalb ist imap auf dem Mailserver so installiert, daß von der zngate/znmbr1 noch ein rsh möglich ist, d.h. pine kann auf dieser Maschine immer ohne Eingabe eines Paßwortes eine Verbindung zum Mailserver aufbauen.

Demnächst wird eine modifizierte Version von pine zur Verfügung gestellt, die eine abhörsichere, zertifizierte Verbindung zum Mailserver aufbaut: `pine-ssl`

Bei Verwendung von `netscape`
als Mailreader sollte man, wenn möglich, das Protokoll imap4 einschalten. Das ist erst ab Version 4 möglich. Wir wollen auf allen Plattformen netscape4 zur Verfügung stellen (bis auf IRIX).
Da der Resourcenverbrauch sehr groß ist, haben wir lange gezögert. Auf den PCs (Windows und Linux) ist netscape4 der Standard.

Bei WindowsNT wird das Protokoll imap4 bei allen gängigen Mailreadern unterstützt.
imap4 in Verbindung mit SSL wird von netscape4 und InternetExplorer zur Verfügung gestellt.

3.2.3. Bildschirm schützen

Es gibt folgende Möglichkeiten, seinen Bildschirm zu schützen:

`xlock` (-> `/products/security/athena/bin/xnlock`)
Locken des Bildschirmes
in HEPiX X11 Umgebung eingebunden

`xscreensaver` Bildschirm wird nach vorgegebener Zeit automatisch gelockt
Bildschirm kann vom Nutzer gelockt werden
nicht standardmäßig eingerichtet
aber empfohlen!

Die Einbindung von xscreensaver als X11 Client in die HEPiX X11 Umgebung erfolgt beim `fvwm2` (Standard Windowmanager in DESY Zeuthen) wie folgt:

editieren Sie das File `~/.hepix/xclients`
und fügen Sie folgende Zeile hinzu:

```
/usr/local/bin/X11/xscreensaver -lock-mode &
```

Damit wird der Daemon gestartet, der dafür sorgt, daß ein automatisches Locken des Bildschirmes erfolgt. Um auch per Kommand den Bildschirm zu locken, muß das Kommando

```
/usr/local/bin/X11/xscreensaver-command -lock
```

ausgeführt werden. Dieses sollte in das File `~/.hepix/wm/fvwm2_user_menu` eingefügt werden, wenn das Kommando im Usermenu des Windowmanagers erreichbar sein soll:

```
#and now your own User-menu
AddToMenu UserPopup "User menu" Title
...
+ "Loc\&k Screen\%small.lock.xpm\%" \
Exec /usr/local/bin/X11/xscreensaver-command -lock
...
```

Nach einem neuen Login ist der Bildschirmschutz aktiv. Wenn Sie Probleme haben sollten, wir helfen

Ihnen gern (Bitte Mail an uco).

3.2.4. Kerberos, AFS

Wir haben im Sommer 1999 auf Kerberos Authentisierung umgestellt. Damit werden über NIS (Network Information Service - ein Dienst, der genutzt wird, um Informationen im LAN zu verteilen) keine Paßwörter mehr (zwar vercryptet, aber mit crack Programmen knackbar) im Netz verteilt.

Nach der jetzt installierten Authentisierungmethode erhält der Benutzer ein Kerberos Ticket und ein AFS Token, das der Benutzer benötigt, um sich gegenüber AFS zu authentisieren, damit er also Zugriffsrechte für sein AFS Homedirectory erhält. Zwar haben die Benutzer nur auf Linux standardmäßig das AFS Homedirectory als Homedirectory, aber auch bei den anderen UNIX Rechnern wird das AFS Homedirectory in Zukunft eingeführt und ist jetzt schon erreichbar.

Hilfsprogramme:

`tokens` (Links auf `/usr/afsws/bin/tokens.krb`) dient zur Kontrolle von Existenz und Lebensdauer von Kerberos Ticket und AFS Token, Gültigkeit von 25 Stunden (Standard im CERN und DESY)

`tklife` warnt eine Stunde vor Ablauf, ist in den Shellprofiles eingebaut.

Warum wird keine automatische Verlängerung angestrebt?

- Diese wäre nicht im Sinne des Erfinders.
- Tickets/Tokens könnten mißbraucht werden.
- Passwörter nicht im Klartext abspeichern.

Wenn Sie Prozesse automatisieren möchten und keine Lösung finden, wenden Sie sich bitte an uco@ifh.de. Vielleicht können wir weiterhelfen.

Wozu brauche ich Tokens/Tickets

- für den Zugriff auf die AFS Homedirectories
  Auf den Linux Rechnern sind die AFS Homedirectories Standard.
- in pine (mit Kerberos Authentisierung) für den Zugang auf den Mailserver
  Bitte vor Aufruf mit `tokens` überprüfen, ob ein Kerberos Ticket vorhanden ist.
  Es ist ein Unterschied, ob man sich vorher ein Ticket besorgt, oder ob es beim Verbindungsaufbau zum imap-Server im Klartext übers Netz übertragen wird!

Wann bekomme ich ein neues Token/Ticket?

- beim Einloggen über X11 (XDM) (außer Digital UNIX, SunOS4)
- beim Einloggen über telnet, ftp und rsh (außer Digital UNIX)
  nur innerhalb ifh.de zulässig und NICHT empfohlen, da Paßwörter im Klartext übertragen werden
- beim Einloggen über ssh/xssh/xrsh (DESY Zeuthen spez.) wenn eine Paßwortauthentisierung erfolgt, d.h. die Rhost-RSA Methode nicht verwendet wird
- durch Ticket-/Tokenforwarding durch ssh/xssh/xrsh (DESY Zeuthen spez.)
- durch Reaktivierung der Session, die durch xscreensaver geschützt ist
  Ein neues Token/Ticket erhält man aber nur auf dem Loginrechner.
  Es gibt noch kein Kommando, um überall die Tokens/Tickets zu verlängern

Wie besorge ich mir neue Tokens/Tickets, wenn sie abgelaufen sind ?

mit `klog` (-> `/usr/afsws/bin/klog.krb`)

(/usr/afsws/bin/klog erzeugt nur AFS Token)

`klog`	Token für den aktuellen Account in der lokalen AFS Zelle besorgen
`klog -cell desy.de`	Token in der Zelle desy.de erzeugen
`klog nieprask@cern.ch`	Token für nieprask in der Zelle cern.ch erzeugen

Bemerkung: in jeder Zelle nur einen Token

3.2.5. Sicherheitsrelevante Files schützen und richtig installieren

Unberechtigter Zugriff auf Directories und Files kann verhindert werden durch Setzen von ACLs bzw.UNIX Zugriffsrechten.

UNIX Filesystem: Zugriffsrechte für Files und Directories

Rechte für User/Group/Other	read/write/execute
`chmod`	Änderung der Rechte
`umask`	entscheidund für neue Files/Directories

Sicherheitsrelevante Files:

.netrc, .rhosts	in Nutzerverantwortung
.Xauthority	X11 Authentisierung mit xauth
Login profiles	
Startupfiles und Konfigurationsfiles der Applikationen .pinerc, .emacs, ...	
Directories: .ssh, .ssl, .pgp, ...	werden automatisch von den entsprechenden Applikationen und bei Einrichtung des Accounts richtig angelegt

AFS Filesystem: Zugriffsrechte NUR für Directories

-> zu schützende Files müssen in entsprechend gesicherte Directories

von den UNIX Zugriffsrechten hat nur noch das x-Bit (Execute) des Eigentümers Bedeutung.
! Alle anderen Rechte werden durch ACLs festgelegt.

Die Zugriffsrechte werden auf Subdirectories beim Erzeugen vererbt, aber nicht bei Änderung der ACLs in den darüberliegenden Directories.

AFS Doku: http://www.desy.de/usg/docs/ps/afs.html.de

Listen der ACLs:

```
fs listacl path
fs la path
```

Beispiel Homedirectory von Account winzig:

```
fs la /afs/ifh.de/user/w/winzig
Access list for /afs/ifh.de/user/w/winzig is
Normal rights:
system:administrators rlidwka
system:anyuser l                    NUR Lookup Rechte
                                    keine Lese/Schreibrechte
winzig rlidwka
```

Files schützen:

- wenn Files nur für den Benutzer erreichbar sein sollen, kann er diese nach ~/private kopieren.

Sollen diese außerdem in anderen Directories verfügbar gemacht werden, sind 2 Schritte notwendig:
Moven nach ~/private
Link auf das entsprechende File

Beispiel:

```
mv $AFSHOME/geheim $AFSHOME/private/geheim
ln -s $AFSHOME/private/geheim $AFSHOME/geheim
```

- wenn der Benutzer Rechte entfernen möchte, muß er die entsprechenden ACLs entfernen

  Beispiel: anyuser soll keine Rechte mehr haben

  ```
  fs sa path system:anyuser none
  ```

- Rechte in einem Verzeichnisbaum ändern:

  Beispiel 1: Alle Subdirectories erhalten die ACLs der angegebenen Directory.

  ```
  cd /afs/ifh.de/user/w/winzig/mcdir
  find . -type d -exec fs copyacl /afs/ifh.de/user/w/winzig/mcdir {} \;
  ```

  Beispiel 2: Bei allen Subdirectories werden die Rechte für den Account albert entfernt.

  ```
  find . -type d -exec fs sa albert none {} \;
  ```

3.2.6. X11 Security beachten

Auf Zielrechner läuft sshd: ssh/xssh

Die ssh bietet die Möglichkeit des X11 Tunneling, so daß der gesamte X11 Traffic verschlüsselt wird. Ist X11-Forwarding eingeschaltet, kann der Benutzer auf dem Zielrechner X11 Applikationen starten, ohne sich um X11 Authentisierung zu kümmern. Die DISPLAY Variable wird generiert von der ssh und zeigt auf den Zielrechner. Die ssh erzeugt einen Proxy Xserver, verwendet dabei einen Zufallsauthorisierungskey. Der richtige Authorisierungskey wird nicht im Netzwerk verwendet.

`ssh -f host xterm` xterm wird nach Authentisierung (wenn notwendig in der Shell) im Hintergrund gestartet

`ssh -n host emacs` Applikation wird im Hintergrund gestartet, funktioniert nur, wenn keine Paßwortabfrage notwendig ist

Beispiele:

```
xssh machine.domain
xssh -l user machine.domain
xssh machine command
```

Vorteile:

- kein pseudo-tty blockiert
- kein zusätzlicher Prozeß
- wenn Paßwortabfrage notwendig, wird kleines zusätzliches Fenster (`ssh-askpass`) gestartet

Zielrechner hat keine ssh

Die User basierte X11 Zugriffskontrolle ist beim XDM Login eingeschaltet. Das File .Xauthority enthält den MIT-MAGIC-COOKIE Key, der vom XDM generiert wird. Der für diesen Display erzeugte Key wird von `xauth extract` extrahiert und kann mit `xauth merge` auf dem Zielrechner eingebunden werden.

`xrsh` realisiert automatisch die Übertragung des Keys.

xrsh (-> xssh in DESY Zeuthen)

`xrsh -rsh -auth xauth machine.domain` (DESY Zeuthen spezifisch)
(`xrsh -auth xauth machine.domain` MIT)

Voraussetzung für diese Methode ist, daß kein Paßwort eingegeben werden muß (rhost-Methode).

Zielrechner hat keine User basierte X11 Zugriffskontrolle

Display schützen!

Niemals `xhost +` weltweite Schreib-und Leserechte

Abhören von Paßwörtern möglich, in Hacker-Tools eingebunden

Host basierte Zugriffskontrolle:

`xhost + machine.domain` wenn die Domäne nicht angegeben wird, kann jeder Host, der diesen Namen hat, die X11 Verbindung abhören

Aufruf:

```
xrsh -rsh -auth xhost machine.domain
```

xrsh mit rsh kann nur verwendet werden, wenn die DISPLAY Variable auf den Xserver zeigt und nicht durch ssh erzeugt wurde, d.h. also nicht auf den Proxy-Xserver zeigt

Achtung:

Beim Einloggen in WinCenter muß die DISPLAY Variable auf den Xserver zeigen!

3.2.7. Signieren von Mails und Verschlüsselung von Files

Bei uns ist `pgp` version 2.6.3i installiert. `pgp` ist in `pine` eingebaut.
`pgp` ist geeignet zum Signieren und Verschlüsseln von Mails.

Weitere Informationen findet man unter:

http://www.ifh.de/computing/services/software/unix-tools/pgp_doc.html

http://www.pgp.net/pgpnet/pgp-faq/

`pgp-public-keys@keys.pgp.net` ist die email - Kontaktadresse für den Key-Service

Die Kommandos für die Key-Service findet man erläutert unter
http://www.de.pgp.net/pgpnet/email-help-de

http://www.uk.pgp.net/pgpnet/pks-commands.html ist ein Webinterface für den Key-Service.

pgp kann auch nur zur Verschlüsselung verwendet werden.

```
pgp -e textfile
pgp textfile
```

`crypt` ist ein Programm, mit dem der Inhalt eines Files verschlüsselt werden können.

`crypt key < clear.file > encrypted.file` Das File wird mit Hilfe des Keys (Paßwort) verschlüsselt.

`crypt key < encrypted.file > clear.file` Das File wird entschlüsselt.

3.2.8. Schutz vor Datenverlust

nur Homeverzeichnisse sind standardmäßig im Backup (AFS und NFS).

Eine Anleitung zum Rückspeichern von Daten aus dem Backup findet man unter:
http://www.ifh.de/computing/services/backup/backup.html

Wenn Bedarf an der Aufnahme weiterer UNIX Verzeichnisse (begrenzte Datenmenge) besteht, schicken

Sie bitte eine Mail an uco@ifh.de

3.2.9. Zahlreiche weitere Sicherheitsprobleme

Hier können nur ein paar weitere Hinweise angegeben werden. Die Liste ist nicht vollständig.

- Code nicht von unbekannten ftp Servern Code installieren, nur authorisierte Server verwenden. Check-Summen überprüfen (MD5).
- Ausführbarer Code kann in PostScript Dateien versteckt sein. PosstScript-Viewer sind standardmässig so konfiguriert, daß sie das Ausführen von Kommandos nicht zulassen.
- Bitte beachten Sie die Hinweise zum Virenschutz.
- Websecurity
    - Webserver Securityprobleme (cgi-bin)
    - aktive Webinhalte
      vom Webserver heruntergeladener und in seinem Kontext ablaufender ausführbarer Code
      Java, ActiveX, JavaScript

3.3 Weitere Informationsquellen

Die DFN CERT Webseite: http://www.cert.dfn.de/infoserv/

Die CERN Security Seite: http://wwwinfo.cern.ch/dis/security/

Bundesamt für Sicherheit in der Informationstechnik: http://www.bsi.bund.de/

3.4 Wachsamkeit

Es gab in der Vergangenheit zahlreiche Hackereinbrüche in Labs, mit denen zusammengearbeitet wird, z.B.
in DESY HH mehrere Einbrüche, auch im ZIB und SLAC, ...

Bitte achten auf:

- beim Einloggen auf ``Last login from ..."
- auf obscure File ``.. ." oder ähnliches
- auf fehlerhafte Zugriffsrechte
- auf modifizierte Files

Bitte alle Unstimmigkeiten melden an security@ifh.de !