

Sicherheitstage SS 05

6.-8.6.2005



Montag, 6.6.2005

- 9:15 - 10:45 *IT-Sicherheit in der Universität*
- 11:00 - 12:30 *Firewall-Schutz für Institute*

Hille
Prof. Breitner
Frau Peter

Dienstag, 7.6.2005

- 9:15 - 10:45 *Sichere Server unter Linux (1)*
- 11:00 - 12:00 *Digitale Signaturen in Theorie und Praxis*
- 12:00 - 12:30 *Zertifikate für Server*

Froriep
Frau Gersbeck
Froriep

Mittwoch, 8.6.2005

- 9:15 - 10:45 *Sichere Server unter Linux (2)*
inkl. *iptables* und *tripwire*
- 11:00 - 12:00 *Sicherheit von Anwendungen*
- 12:00 - 12:30 *Diskussion*

Froriep
Heisterkamp
Obendorf
Hille et al.

Sicherheitstage WS 04/05

IT-Sicherheit in der Universität Hannover

- I. **Einige Grundlagen zur IT-Sicherheit**
- II. **Zur Sicherheitslage in der Universität**
- III. **Neue RRZN-Angebote zur IT-Sicherheit**

Hacker: **Script Kiddies (Möchtegern-Hacker)**
 „Freaks“ (Hobby-Hacker)
 „professionelle Marktteilnehmer“

bevorzugte Angriffsziele:

Unis und Forschungseinrichtungen

Warum?

schlecht gesicherte Rechner
große Netz-Bandbreite

Interessenslage wandelt sich zunehmend:

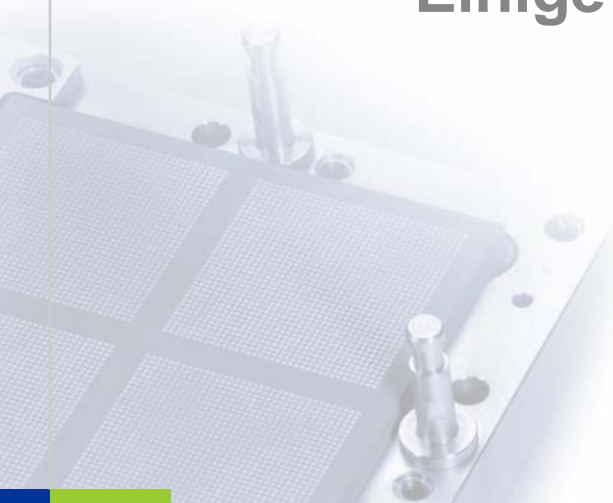
Bisher:

- intellektuelle Herausforderung (Freaks)
- „ausprobieren, was geht“ (Script Kiddies)
- **Heute: zunehmend gezielte wirtschaftliche und kriminelle Interessen der „professionellen Marktteilnehmer“, z. B.**
 - ein Virus richtet vieltausendfach Hintertüren ein, Netze aus derart unter Fremdkontrolle gebrachten Rechnern werden zentral auf Stundenbasis vermietet (SPAM-Versand, DoS-Angriffe etc.)
 - „erfolgreiche“ Industriespionage mittels speziell für diese Zwecke in Auftragsarbeit erstellte Trojaner, die durch standardmäßige Sicherheitssoftware nicht zu entdecken waren

- ➔ Sicherheitsvorfälle bekommen über die Störungen und Beeinträchtigungen hinaus zunehmend **qualitative Komponenten**
- **Zu schützende Werte an der Universität:**
 - Ergebnisse von Forschungsarbeiten
 - Vertragsinhalte
 - personenbezogene Daten (auch Datenschutz!)
 - finanzbezogene Daten
 - effiziente Arbeitsabläufe
 - Reputation
- **IT-Sicherheit an UH**
 - ➔ hat signifikante Bedeutung
 - ➔ muss systematisch adressiert werden
 - ➔ muss spezifische Belange berücksichtigen

I.

Einige Grundlagen zur IT-Sicherheit



- Teilbegriff der **Verlässlichkeit** (Sicherheit der Systeme) mit den semantischen Dimensionen
 - **Vertraulichkeit**
 - **Integrität**
 - **Verfügbarkeit**
- Teilbegriff der **Beherrschbarkeit** (Sicherheit vor den Systemen) mit den semantischen Dimensionen
 - **Zurechenbarkeit**
 - **Revisionsfähigkeit (oder Rechtsverbindlichkeit)**

Diese 5 Dimensionen gelten als **fundamental** und damit auch als **notwendig** für das Begriffsgebäude IT-Sicherheit. Sie müssen aus heutiger Sicht in jeder Zielsetzung mit Bezug zur IT-Sicherheit berücksichtigt werden (ggfs. durchaus mit unterschiedlichem Gewicht).

- **Grundbedrohungen sind Gefahren bezüglich der semantischen Dimensionen (Beeinträchtigung oder Verlust von Eigenschaften)**
- **Charakterisierung als Grundbedrohung ist unabhängig davon, ob Ursache oder Auslöser als**
 - willkürlich (beabsichtigt, intentional)**oder als**
 - unbeabsichtigt (zufällig, unvermeidbar, nichtintentional)**einzustufen sind**

- **vorsätzliche Handlungen (von Dritten, aber auch aus eigenen Reihen!)**
- **menschliche Fehlhandlungen (z. B. durch Fahr-/ Nachlässigkeit, mangelndes Sicherheitsbewusstsein)**
- **ungeeignete bzw. fehlende geeignete Verfahren**
- **technische Mängel / Versagen (Hardware, Software)**
- **organisatorische Mängel**
- **höhere Gewalt**

Technische Maßnahmen

- Bereich Hardware/Software/Konfiguration

Nichttechnische Maßnahmen

- Organisatorischer, administrativer und personeller Bereich

Infrastruktur-Maßnahmen

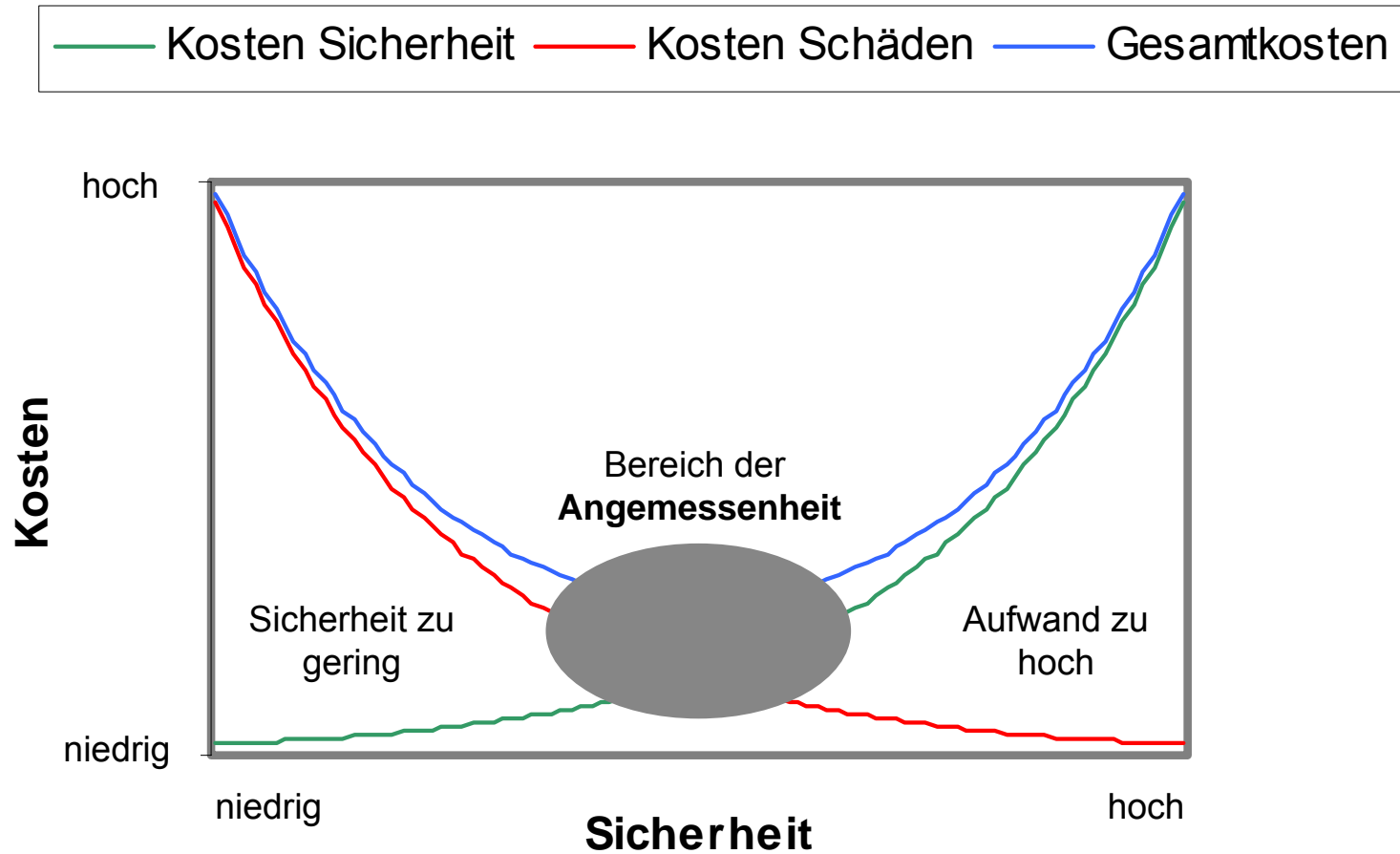
- bauliche und räumliche Aspekte
- Abhörsicherheit

Hinweis: detailliertere Ausführungen im gleichnamigen Vortrag der Sicherheitstage November 2003

http://www.rrzn.uni-hannover.de/fileadmin/it_sicherheit/pdf/Sich-in-UH_2003-11-14_10.pdf

IT-Sicherheit ist vergleichbar mit der Befriedung eines Areals durch einen Zaun:

- ***Der Zaun muss überall gleich hoch sein. (Ausgewogenheit)***
- ***Der Zaun muss vollständig sein, d.h. er muss das gesamte Areal umschließen. (Durchgängigkeit)***
- ***Die Qualität des Zauns muss dem Schutzziel entsprechen. (Angemessenheit)***

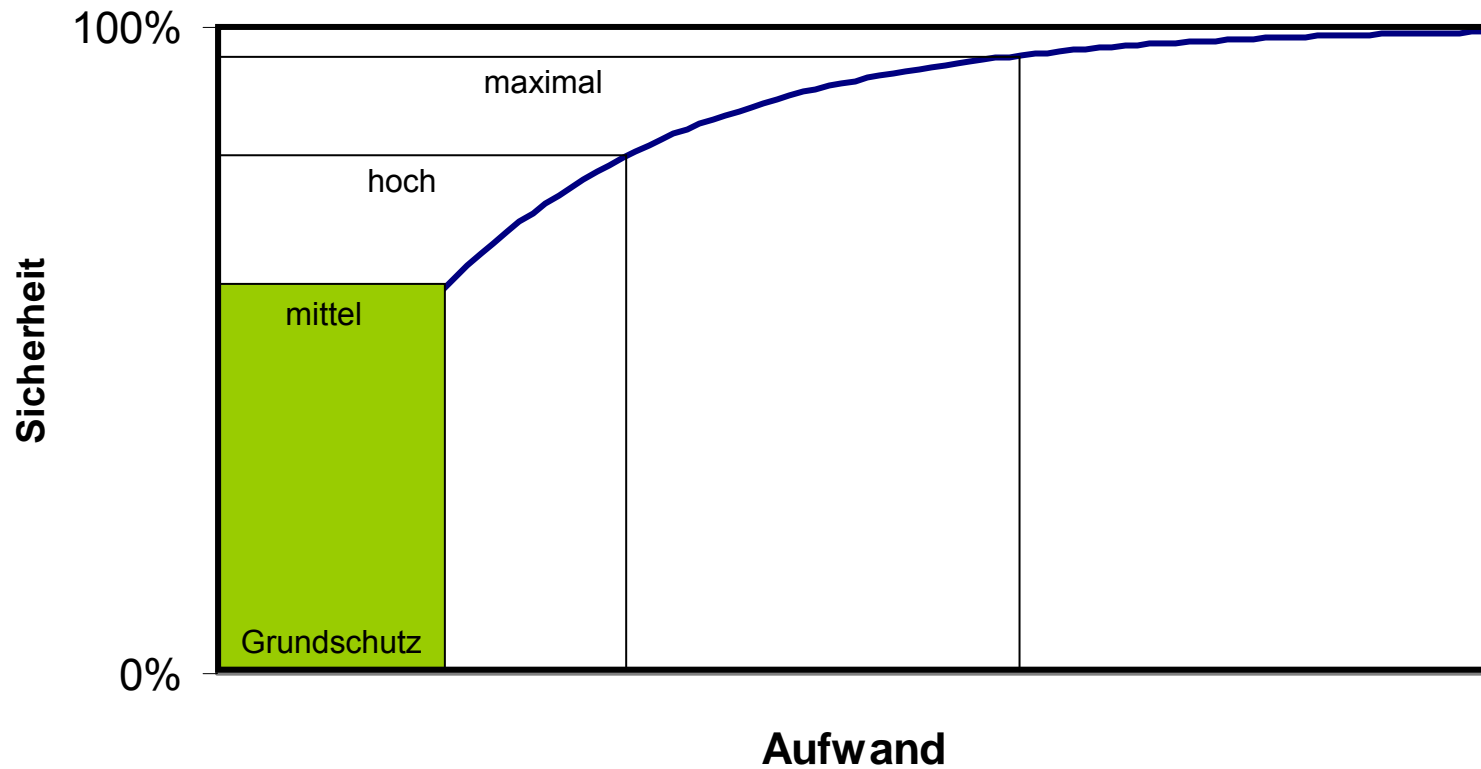


Klassifikation nach BSI:

- **Grundschutz: Durchführung von Standardmaßnahmen für den niedrigen bis mittleren Schutzbedarf**
 - detaillierte Analysen können entfallen

Hoher bis sehr hoher Schutzbedarf: detaillierte und aufwendige Einzel-Analysen erforderlich

- **welcher Aufwand ist erforderlich für ein tragbares Restrisiko?** (absolute Sicherheit nicht möglich!)
 - Frage der Angemessenheit
- **RRZN-Standarddienstleistungen liegen im Bereich des Grundschutzes**



*) Nach Grundschutzhandbuch des BSI

IT-Sicherheit ist *kein* fixierter Zustand.

Randbedingungen / Einflussgrößen dynamisch:

- Ziele / Aufgaben
- „Stand der Technik“
- Vorschriften / Richtlinien / gesetzliche Regelungen

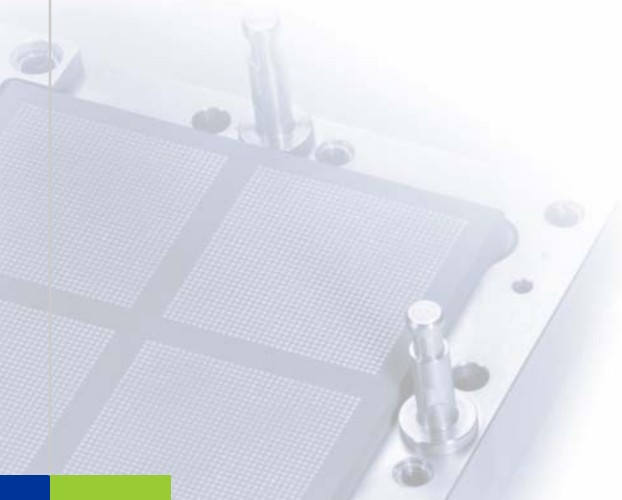
IT-Sicherheit muss als *Prozess* verstanden und organisiert werden

- Sicherheitsmanagement erforderlich
- auf Leitungsebene anzusiedeln!

Der IT-Sicherheitsprozess für die UH basiert auf der „Ordnung zur IT-Sicherheit in der Universität Hannover“
verfügbar u. a. auf Web-Seiten des Zentralen IT-Sicherheitsbeauftragten
<http://www.iwi.uni-hannover.de/it-sicherheit/Ordnung.pdf> bzw. über
http://www.rrzn.uni-hannover.de/it_sicherheit.html

II.

Zur Sicherheitslage in der Universität



Anmerkungen zu nachfolgenden Angaben:

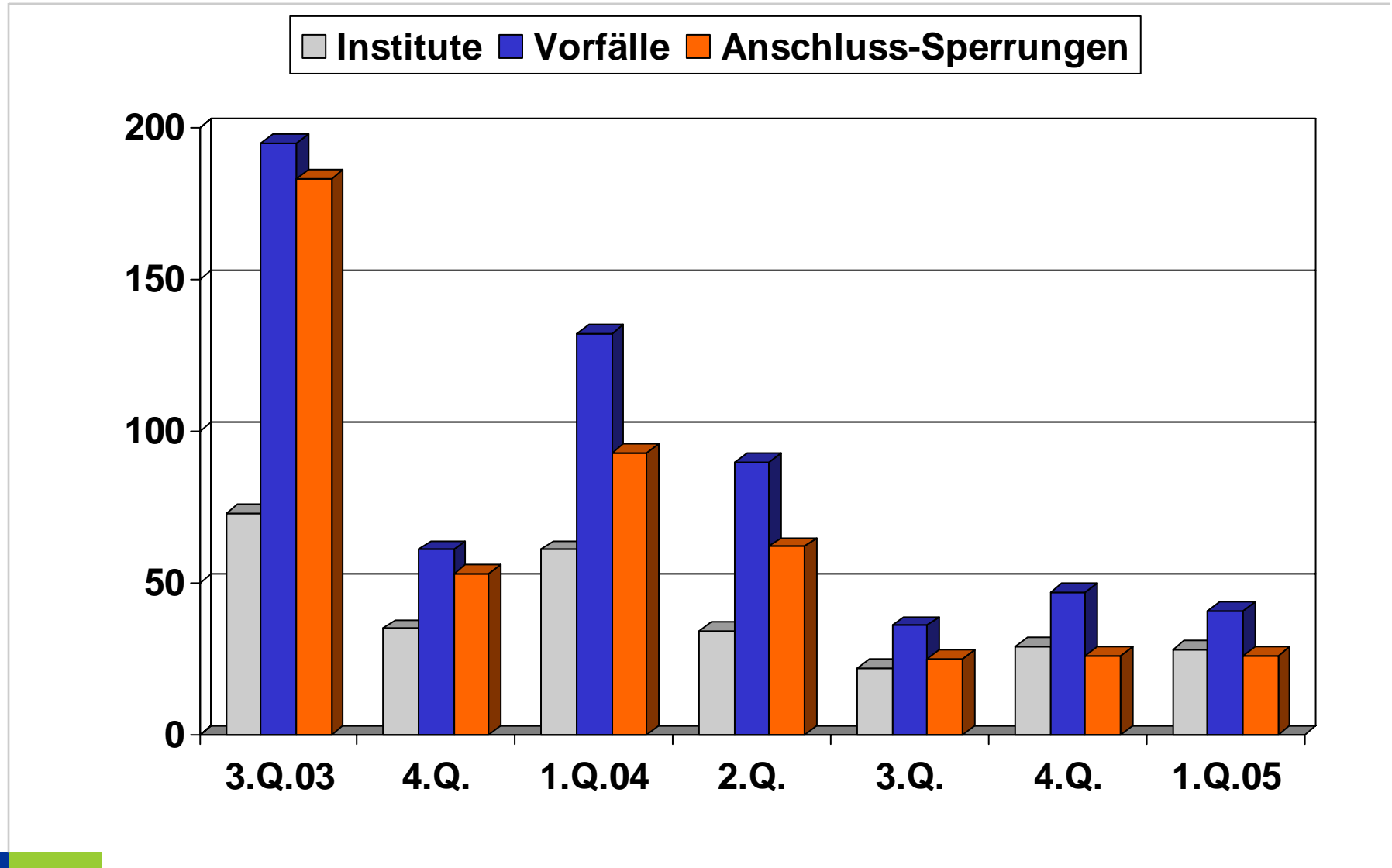
- **Im Gegensatz zu den bisherigen Sicherheitstagen werden Sicherheitsvorfälle im Bereich des Studentenwerks Hannover (StWH) nicht mehr berücksichtigt**

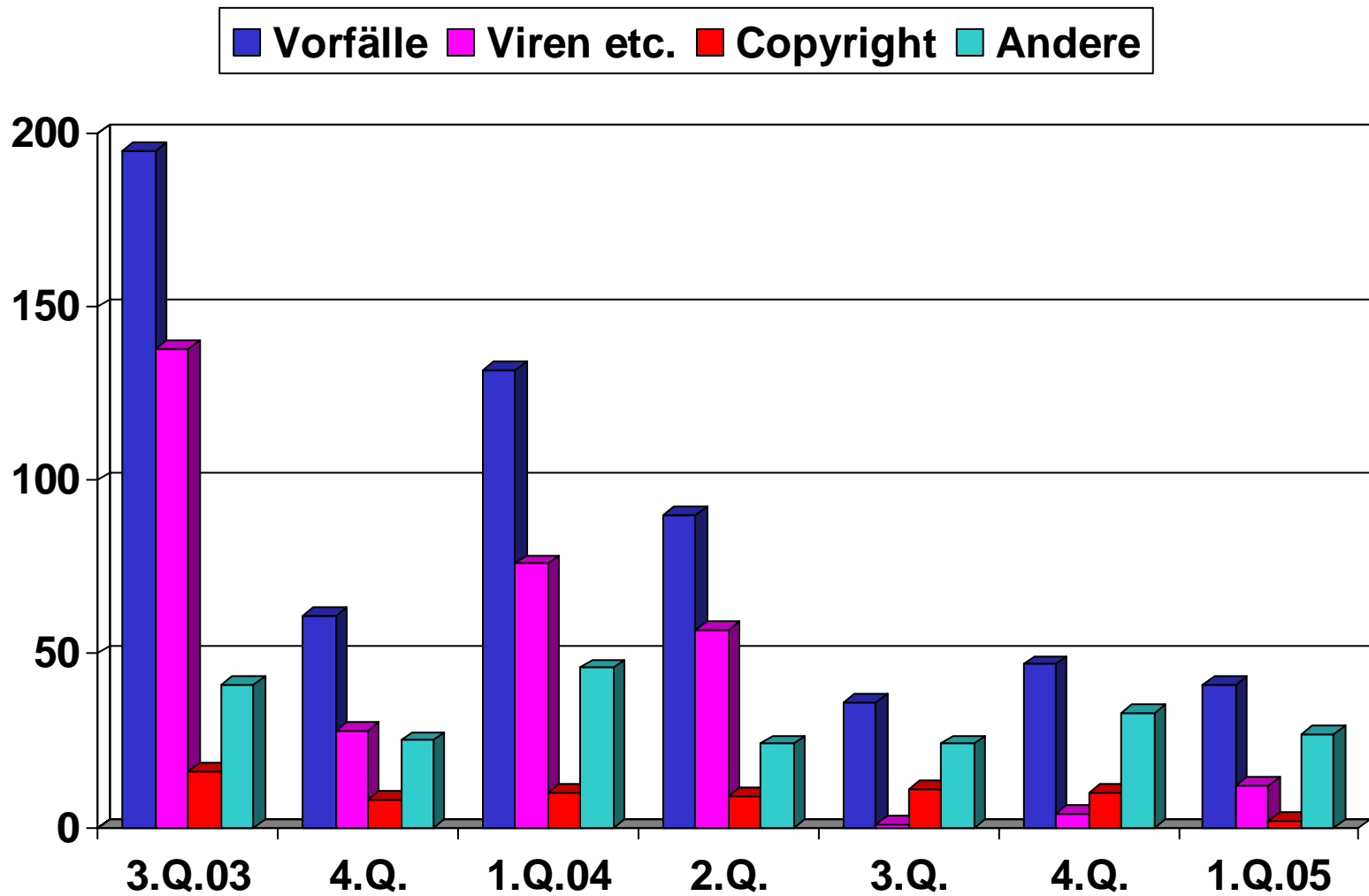
- Reduzierung auf die Vorgänge im „eigentlichen“ UH-Netz zeigt charakteristisches Bild der Sicherheitslage der UH (Vorfälle im Bereich des StWH weisen eine andere Verteilung auf.)
- die hier gegebenen Tabellen sind daher mit denen früherer Jahre nicht direkt vergleichbar bzw. enthalten andere Zahlen.

(Hinweis: Selbstverständlich werden Sicherheitsvorfälle im Bereich des Studentenwerks seitens des RRZN nach wie vor adäquat bearbeitet.)

Sicherheitsrelevante Vorfälle (2) ohne StWH

	Vorfälle insgesamt	Anzahl Institute	Anschluss-Sperrungen	davon Viren/Würmer	davon ©-Verstöße
3. Q. 2003	195	73	183	138	16
4. Q.	61	35	53	28	8
1. Q. 2004	132	61	93	76	10
2. Q.	90	34	62	57	9
3. Q.	36	22	25	1	11
4. Q.	47	29	26	4	10
1. Q. 2005	41	28	26	12	2
ganzes Jahr	214		139	74	32





Seit 3. Quartal 2004 deutlicher Rückgang der Virenvorfälle mit leichtem Wiederanstieg im 1. Q. 2005!

■ Vermutlich folgende Gründe beteiligt:

- im 2. Quartal 2004 wurde automatisches Sophos-Update bereitgestellt
 - inzwischen beziehen ca. 5600 Systeme in der UH von den Servern des RRZN automatisch Aktualisierungen
 - In etlichen Instituten erfolgt eine Unterverteilung, sodass die Zahl der automatisch geschützten Systeme noch größer sein wird.
- auf Anwenderseite mehr Sicherheitsbewusstsein beim Umgang mit Anhängen
- Leichter Wiederanstieg möglicherweise verursacht durch ungeschützte bzw. ungesicherte Notebooks

- **Fallzahlen quasi konstant in 2004 und Rückgang im 1.Q.05 (Zufall oder aufgrund der Maßnahmen?)**
- **Copyright-Verstöße werden von der Medienindustrie zunehmend rechtlich verfolgt**
 - Verurteilungen sind erfolgt
 - Rechte der UH können tangiert werden
- **darum weiterhin konsequentes Vorgehen notwendig:**
 - Rechner werden sofort vom RRZN gesperrt
 - die GL der betreffenden Einrichtung wird direkt benachrichtigt
 - Freischaltung nur nach schriftlicher Erklärung der Bereinigung des betreffenden Systems und auf ausdrücklichen Wunsch der GL

„Andere“ (= „Vorfälle“ - „Viren“ - „Copyright“) **enthält u. a.**

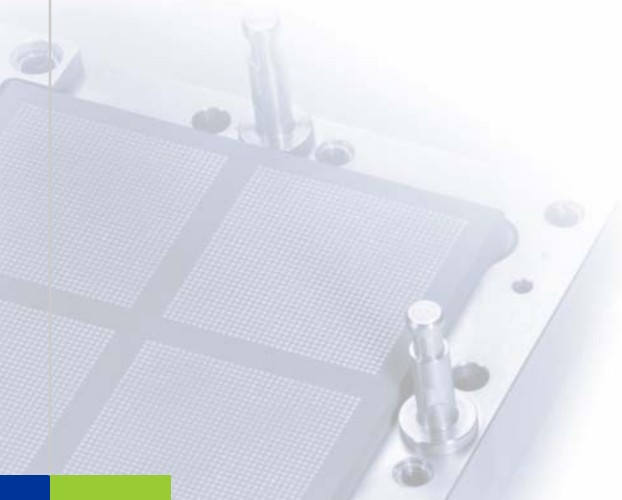
- Einbrüche (gehackte Systeme)
- Einrichtung/Betrieb suspekter FTP-Server (z. B. durch Einbruch oder durch nicht sachgerechte Administration)
 - Einsatz z. B. für Angebot zweifelhaften Materials
- Scan-Vorfälle (ggfs. verursacht durch nicht erkannte Schadsoftware)
- Einrichtung/Betrieb von SPAM-Relays

Auffällig:

- relativ konstant über den Betrachtungszeitraum
- nach Rückgang der Virenvorfälle nunmehr signifikant (u. a. Besserung durch Einsatz von Firewalltechnik und durch sachgerechte Administration möglich)

III.

Neuere RRZN-Angebote zur IT-Sicherheit



verfügbar:

1. zentraler Netzschutz / Logdatenserver
2. Zertifizierungsdienst der UH-CA
3. automatische Sophos-Aktualisierung
4. SPAM-Abwehr (inkl. weiterer Maßnahmen zur Viren-Abwehr)
5. Abonnieren von Security-Meldungen des DFN-CERT
6. Info zu gesperrten Anschlüssen
7. neue Handbücher zur IT-Sicherheit

in Arbeit / demnächst verfügbar:

8. Untersuchung/Empfehlung bzgl. PFW

in Planung:

9. Maßnahmen für Notebooks / Anschluss ans UH-Netz

- **Möglichkeiten zum Schutz von Institutsnetzen durch zentrales Firewallsystem im RRZN**
 - Alternative zu institutseigenen Firewallsystemen
- **Status**
 - Produktionsbetrieb mit 31 Instituten hinter 21 vom RRZN administrierten FW-Systemen
 - 10 weitere Institute in konkreter Vorbereitung, 7 interessiert
 - Neu: separater Logserver zur Bereitstellung der Logdaten
- **nähere Behandlung im nachfolgenden Vortrag „Firewallschutz für Institute“ (Frau Peter), u. a.:**
 - Darstellung der zentralen RRZN-Lösung („Netzschutz“)
 - Möglichkeiten für institutseigene Firewalls
 - Vergleich der Lösungen (Vor-/Nachteile)

- **Ziel: Aufbau einer Infrastruktur zur Zertifizierung von öffentlichen Schlüsseln mit Einbindung in DFN-Hierarchie**
- **Motivation**
 - Unterstützung von
 - gesicherte E-Mail-Kommunikation
 - Digitale Signatur
 - Verschlüsselung möglich, wenn auch der Adressat ein Zertifikat besitzt
 - eigenes Zertifikat umso „nützlicher“, je mehr Zertifikate im Feld sind
 - gesicherte Klient-/Server-Verbindungen auf Basis von SSL
 - Code Signing
 - Einstieg in den Aufbau einer Public Key Infrastructure (PKI)
 - zunehmende Bedeutung von PKI-basierten Verfahren zu erwarten (Sicherheitsaspekte der Zurechenbarkeit und Revisionsfähigkeit)
 - Know-How-Gewinn
 - Voraussetzung für künftig zu erwartende „große Anforderungen“

■ Status:

- Zertifizierung seitens der DFN-PCA im Mai 2004 erfolgt
- Seit November 2004 für Benutzer freigegeben (Pilotbetrieb)
- Betrieb als Service-Angebot (freiwillige Nutzung)
- Insgesamt bisher mehr als 110 Zertifikate ausgestellt
- Selbstentwickeltes Web-Interface mit dem Ziel der einfachen Nutzbarkeit

- **Näheres zum Zertifizierungsdienst der UH-CA im Vortrag
„Digitale Signaturen in Theorie und Praxis“
(Frau Gersbeck)**

■ Inzwischen

- DFN bietet unter dem Namen „DFN-PKI“ Zertifizierungsdienste für Mitgliedsorganisationen (u. a. Hochschulen) an
 - neue Policy, mehrere Betriebsmodelle
- RRZN wird technischen CA-Betrieb an die DFN-PKI geben, organisatorischer CA-Betrieb sowie die RA verbleiben im RRZN

■ Vorteile:

- Entlastung vom relativ aufwendigen Betrieb der CA-Server
- „bessere“ Zertifikate
 - „fortgeschrittene elektronische Signatur“
 - Gültigkeitsdauer kann auf zwei Jahre erhöht werden (Fortfall der Hierarchie-Ebene der UHtopCA)

■ Planung:

- RRZN steigt demnächst in Probebetrieb der DFN-PKI ein
- Produktionsbetrieb seitens DFN ab 1.1.2006 geplant

■ Auswirkungen für Benutzer

- Bisher ausgestellte („alte“) Zertifikate können bis zu ihrem Ablaufdatum uneingeschränkt verwendet werden
- Bei Bedarf werden auch weiterhin alte Zertifikate ausgestellt, jedoch Ablaufdatum beschränkt auf den 24.5.2006 (limitiert durch Ablaufdatum des jetzigen UH-CA-Zertifikats)
- Sobald Probetrieb der neuen UH-CA stabil läuft, können Benutzer teilnehmen und „neue“ Zertifikate nach der neuen Policy erhalten
- Bezüglich des Antragverfahrens und der Handhabung des Web-Interfaces sind keine nennenswerten Änderungen zu erwarten

➔ **Der Vortrag von Frau Gersbeck ist unabhängig von „alt“ oder „neu“ bzw. gilt für beide Fälle**

■ **Status**

- Derzeit aktualisieren sich automatisch ca. 5600 Rechner direkt von den RRZN-Servern
- Zusätzlich aktualisiert wird eine (unbekannte) Anzahl von Rechnern durch eine Unterverteilung in etlichen Instituten

■ **Neue Sophos Version Anti-Virus 5.0 in Vorbereitung**

- Neues Design: Benutzeroberfläche „Windows-like“
- Kein separater Update-Klient mehr erforderlich
- Update läuft im Hintergrund (u. a. kein Pop-up-Fenster mehr)

■ **Nach Sicherheitstagen Freigabe der Version 5 mit Veröffentlichung als Top-Thema**

- Bisherige Version 4 wird von Sophos noch bis Februar 2006 unterstützt
- Bis dahin beide Versionen auf Download-Server verfügbar

- **Zur Konfiguration der automatischen Aktualisierung:**
 - Eine wesentliche Sicherheitslücke besteht zwischen Hochfahren eines Rechners und der ersten Aktualisierung
 - Darum: im Konfigurationsmenü entsprechendes Häkchen setzen, damit der Rechner im Rahmen des Hochfahrens aktualisiert wird und an der möglichen Entwicklung während der Abschaltzeit partizipiert.
 - Es vermittelt trügerische Sicherheit, den Virenschutz tagsüber stündlich zu aktualisieren, wenn der Rechner morgens auf dem Stand von 14 oder 16 Stunden zurück in Betrieb genommen wird!
- **Hinweis:**
ein eintägiger Workshop (mit praktischen Arbeiten) zum Thema „Virenbeseitigung bei Windows-Systemen“ findet am 24.6. statt. Einige Plätze sind noch frei. Anmeldung ist erforderlich.

***PureMessage* von Sophos als E-Mail-Managementlösung für Mail-Server und Gateways, u. a.:**

- Quarantäne möglich für
 - SPAM
 - Viren-Mails nach Bereinigung (Rest-Mail als SPAM behandelt)
 - „verdächtige“ Mails (ausführbare Anhänge)
- Benutzer hat Kontrollmöglichkeiten über den Quarantäne-Manager bzw. kann die Ausnutzung der Features individuell regeln
- automatische Antiviren- und **Antispam-Updates**

- **Zur Inbetriebnahme: im Prinzip weicher Übergang zu PureMessage**
 - Inbetriebnahme mit Veröffentlichung als Top-Thema (2/05)
 - Einzelne Institute/Domänen sind bereits umgeschaltet (default: alle Filterungen aktiv)
 - Weitere Institute können sich melden bzw. RRZN tritt auch an Institute heran
 - Ziel: Umstellung bzw. Umleitung aller Domänen über das Sophos-Gateway

- **Nähere Informationen unter <http://www.rrzn.uni-hannover.de/puremessage.html>**

Ziel: Meldungen zur IT-Sicherheit können in Abhängigkeit von standardisierten Schlüsselwörtern abonniert werden

- **Web-Interface steht zur Verfügung**
 - Meldungen zu Schlüsselwörtern können durch Anklicken abonniert oder abbestellt werden
- **Zugriff nur aus UH-Netz (130.75.x.x) möglich**
- **zunächst nur für Meldungen des DFN-CERT realisiert, prinzipiell aber auch erweiterbar auf andere Quellen**

RRZN -Netscape
Datei Bearbeiten Anzeigen Gehe Lesezeichen Extras Fenster Hilfe

Zurück Weiterleiten Neu laden Stop Drucken

eMail Anfang Radio Netscape.de Suche Shop@Netscape Lesezeichen The Mozilla Or... Latest Builds

R|R|Z|N

Regionales Rechenzentrum für Niedersachsen

Universität Hannover

[A-Z](#) [Hotline](#) [Kontakt](#) [Sitemap](#) [Intern](#)

RRZN >

Veranstaltung 2.06.2005 03.06.: Niedersächsisches Telekolloquium zum Lernmanagementsystem Stud.IP	Organisation Über uns Mitarbeiter Nutzungsregelungen Stellenangebote Dienstleistungskatalog	Forschung & Lehre Rechnernetze Forschung Lehre Publikationen Software	Suche <input type="text"/> erweiterte Suche... Suchmaschinenlabor
Veranstaltung 30.05.2005 6. – 8.6.: Sicherheitstage im RRZN	Netz Datennetz Mail-Service Netzdienste Netzzugang	Zentrale Server Betriebskonzept Anwendungen Hochleistungsrechnen Archiv/Backup SAP	IT-Sicherheit Antivirensoftware Anwenderinfos Administratoreninfos Zertifizierung (UH-CA)
Virenmeldung 23.05.2005 Sober.P lädt heute neue Programmteile aus dem Internet nach	Arbeitsplatzrechner PC/Workstation Server Anwendersoftware Software-Info DB Gerätebeschaffung	Angebote Handbücher Kurse Druckausgabe Softwareverteilung Verkauf & Verleih	Multimedia Audio/Video 3D/Visualisierung Digital Imaging CD/DVD-Authoring TYPO3
18.05.2005 Stellenangebot Fachleitung IT-Sicherheit			RRZN-Service: Abo der Security-Warnungen des DFN-CERT Archiv

[News-Liste](#)

Letzte Änderung: 03. Jun 2005 [Anne-Kathrin Iltmann](#) [Impressum](#)

Start DE 15:10

Abo Security Mails - Netscape

http://www.rrzn.uni-hannover.de/abo_sec_mails.html

Regionales Rechenzentrum für Niedersachsen | Universität Hannover

Navigation: A-Z, Hotline, Kontakt, Sitemap, Intern

RRZN > IT-Sicherheit > Abo Security Mails >

Organisation
Forschung und Lehre
Netze
Zentrale Server
IT-Sicherheit
Antivirensoftware
Anwenderinfos
Administratoreninfos
Abo Security Mails
IT-Sicherheitsbeauftragte UH
Zertifizierung (UH-CA)
Arbeitsplatzrechner
Angebote
Multimedia
News
Suche

Abo-Service: Security-Warnungen des DFN-CERT

Der DFN-CERT verschickt regelmäßig und aktuell die neuesten verfügbaren Sicherheitsmeldungen der verbreitetsten Hersteller. Diese Meldungen können Sie hier abonnieren, und erhalten somit frühzeitig Nachricht von den gerade aktuellen Sicherheitsproblemen.

Die Warnungen sind durch Stichworte in einzelne Themengebiete geordnet, für jedes Themengebiet gibt es eine eigene Mailing-Liste. Sie können eine beliebige Auswahl an Listen abonnieren, je nach dem, welche Thematik für Sie von Belang ist.

DFN CERT

Wie können Sie abonnieren?

Unter folgenden Voraussetzungen können Sie Abonnent der Sicherheits-Warnmeldungen des DFN-CERT werden:

- Ihr Rechner hat eine IP aus dem Bereich der Universität Hannover.
- Auf Ihrem Rechner befindet sich ein konfigurierter Mail-Klient.

Zum Abonnieren oder Abbestellen einer Liste wählen Sie den entsprechenden Link hinter der Liste aus. Es öffnet sich ein bereits fertig ausgefülltes Mail-Fenster, welches Sie bloß noch absenden müssen.

Sicherheitsabfrage

Um zu vermeiden, dass Irgendjemand ohne Ihren Einfluss, mit gefälschtem

Hinweis auf aktuelle Veranstaltung im RRZN:

[Sicherheitstage im RRZN vom](#)

Taskbar: Start, ZoneAlarm, Sophos Anti-Virus, Vortrag_ego, Microsoft PowerPoint, Check for Updates, Abo Security Mails, DE, ZA, 15:12

Abonnierbare Listen:

ADMIN-SEC-RRZN	Wichtige Meldungen für Administratoren, auch Hinweise auf DFN-Veranstaltungen.	abonnieren abbestellen
ADVISORY-SEC-RRZN	Advisories des Cert Coordination Centers.	abonnieren abbestellen
CALDERA-SEC-RRZN	Warnungen der SCO Group (ehemals Caldera Systems).	abonnieren abbestellen
CISCO-SEC-RRZN	Warnungen von Cisco's Product Security Incident Response Team (PSIRT).	abonnieren abbestellen
COMPAQ-SEC-RRZN	Warnungen des Compaq Security Response Teams.	abonnieren abbestellen
DEBIAN-SEC-RRZN	Warnungen des Debian-Teams.	abonnieren abbestellen
FEDORA-SEC-RRZN	Advisories des Fedora-Teams. Betrifft die älteren RedHat-Versionen. Aus Gründen der Übersichtlichkeit hat das DFN-CERT diese Meldungen mit dem eigenen Stichwort "Fedora" versehen und von den RedHat-Meldungen separiert.	abonnieren abbestellen

Fragestellung:

Liegt Fehlfunktion oder RRZN-seitige Sperrung vor, wenn ein Rechner bzw. Netzanschluss keine Verbindung mehr zum Netz bekommt:

Anwort:

- über spezielles Web-Interface kann Sperr-Status zu einzelnen IP-Adressen abgefragt werden
- den IT-Sicherheitsbeauftragten und Security-Admins in den Instituten sind spezielle URLs bekannt gegeben worden (Aufruf nur aus UH-Netz bzw. 130.75.x.x möglich)
 - IT-Sicherheitsbeauftragte: Status, ggfs. Grund der Sperrung
 - Security-Administratoren: nur Status (Grund bei zuständigem IT-Sicherheitsbeauftragten oder im RRZN erfragen)
 - diese URLs sollen nicht weitergegeben werden

Gesperrte IP-Adressen

Auf dieser Seite haben die dezentralen Sicherheitsbeauftragten der Universität Hannover die Möglichkeit abzufragen, ob und warum bestimmte IP-Adressen gesperrt wurden. So können Sie als dezentraler Sicherheitsbeauftragter Administratoren aus Ihrem Zuständigkeitsbereich erste Hinweise geben, welche Gründe zur Sperrung führten. Für weitere Informationen verweisen Sie die Administratoren bitte an das Security-Team des RRZN:

- Andreas Anft Tel. 19792
- Birgit Gersbeck-Schierholz Tel. 19789
- Christine Peter Tel. 8021

E-Mail: security@rrzn.uni-hannover.de

Hinweis: Trotz unseres Bemühens, diese Auskunft so aktuell wie möglich zu halten, kann es vorkommen, dass gesperrte IP-Adressen manchmal erst mit einer gewissen Verzögerung hier abzufragen sind.

Tragen Sie die IP, zu der Sie eine Sperrungsauskunft wünschen, in das Eingabefeld ein und betätigen Sie den Button „Abfrage“.

130.75 Abfrage

uni-hannover.de (130.75.) ist gesperrt
FTP-Server unter TCP-Port 444;
2004-07-22 16:04:22

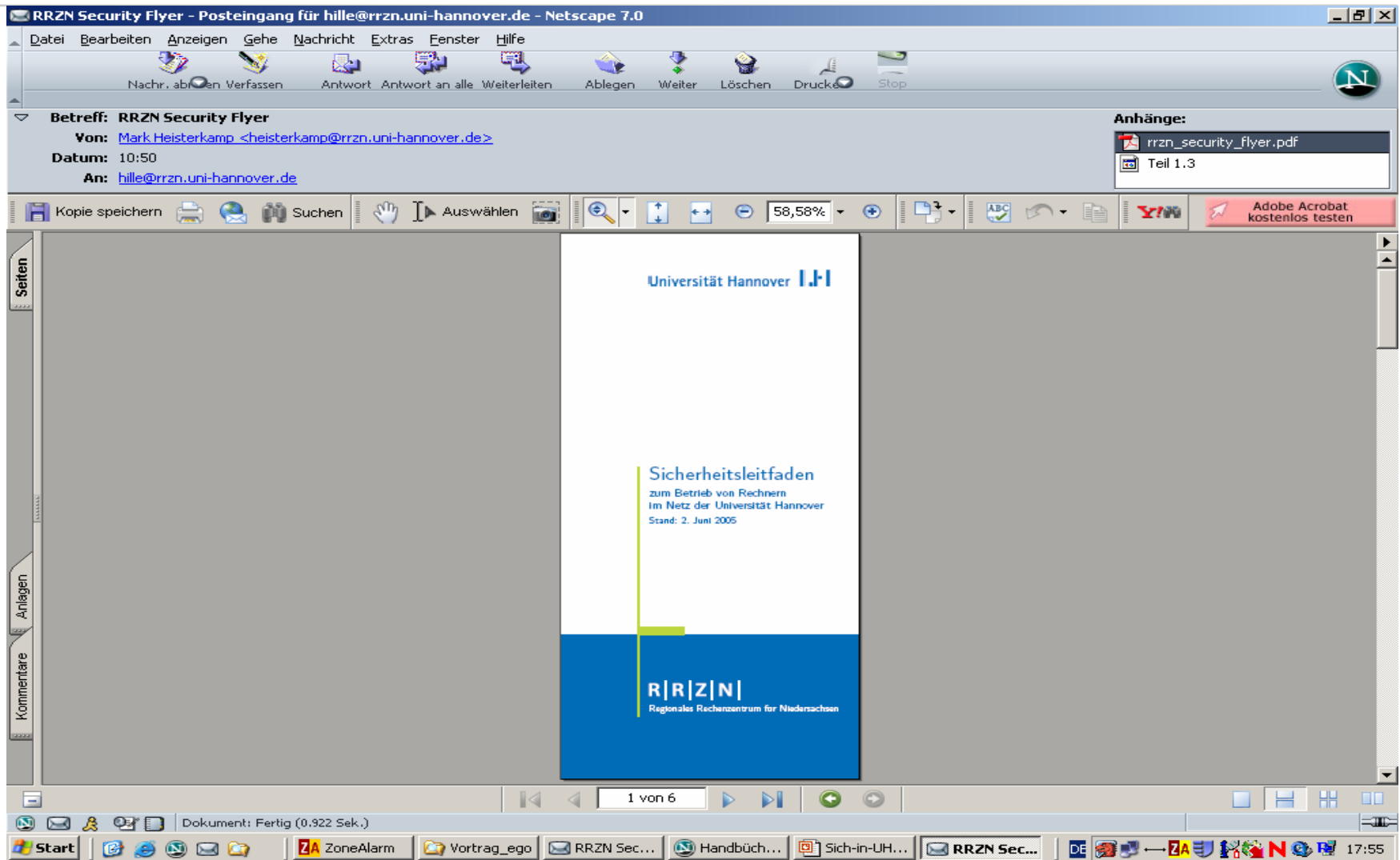
Nach Behebung der Ursachen, die zur Sperrung geführt haben, können die Administratoren die vollständige Wiederfreischaltung per E-Mail beantragen.

7. Dokumentation zur IT-Sicherheit (1)

Handbücher -Netscape
Datei Bearbeiten Anzeigen Gehe Lesezeichen Extras Fenster Hilfe
Zurück Weiterleiten Neu laden Stop http://www.rrzn.uni-hannover.de/buecher.html
eMail Anfang Radio Netscape.de Suche Shop@Netscape Lesezeichen The Mozilla Or... Latest Builds
R|R|Z|N
Regionales Rechenzentrum für Niedersachsen
Universität Hannover
A-Z Hotline Kontakt Sitemap Intern
RRZN > Angebote > Handbücher >
Organisation Themenbereich/Kategorie alle Themen
Forschung und Lehre Status am RRZN verfügbar
Netze Titel Sicherheit
Zentrale Server
IT-Sicherheit
Arbeitsplatzrechner
Angebote
Handbücher
Kooperation Betriebssysteme
Infos Windows Server 2003 Sicherheit Sicherheit im Netzwerk neu
Neue Titel in 2005/04 Netze/Internet
Bezugsquellen Netzwerke Sicherheit
Pressepiegel Internet & Co
Kommentare Computersicherheit im Internet für Anwender
Lektoren gesucht Internetworking: Sicherheit
Erfolgsstory
Kurse
Druckausgabe
Softwaredistribution
Verkauf & Verleih
Multimedia
News
Dokument: Done (0.546 Sek.)
Start ZoneAlarm Vortrag_ego Re: Sicherheit... Handbücher... Sich-in-UH_20... DE 17:46

Flyer „Sicherheitsleitfaden“ als Orientierungshilfe zur IT-Sicherheit für Anwender und Administratoren.

- enthält: Kurzbeschreibungen zu Sicherheitsthemen mit Links auf die entsprechenden Web-Seiten.
- Status: Entwurfssfassung liegt vor u. a. mit folgenden Themen:
 - Antiviren-Software / Viren, Würmer etc.
 - Firewalls / Netzschutz / Personal Firewalls
 - Funkvernetzung
 - VPN-Nutzung
 - Passwörter
 - Digitale Signaturen
- Entwurf wird nach Sicherheitstagen den IT-Sicherheitsbeauftragten zugesandt mit Bitte um Kommentierung
- anschließend endgültige Version



- **RRZN untersucht derzeit Personal Firewalls (PFW) mit dem Ziel, eine konkrete Produktempfehlung auszusprechen bzw. eine Campus-Lizenz zu erwerben.**
- **wesentliche Entscheidungskriterien werden sein:**
 - Vorkonfigurierbarkeit
 - Handhabbarkeit im Feld seitens der Anwender
 - technische „Finessen“ erscheinen demgegenüber als weniger relevant

Bis zur konkreten Empfehlung (Termin noch unklar)
Orientierung an unseren Webseiten zu Personal Firewalls

Problem:

Freizügiger Anschluss von Rechnern (Notebooks) an das UH-Netz kann den Feind in die eigenen Linien bringen.

- als Mindestsicherheitsmaßnahmen sind erforderlich (ähnlich wie bei „normalem“ PC am Netz):
 - professionelles Betriebssystem mit aktuellen Patches
 - aktuelle Anti-Virensoftware
 - aktuelles Personal Firewall-System
- Besondere Gefährdung durch „eben mal“-Anschluss von privaten Notebooks und Gäste-Notebooks

Lösung schwierig:

- Die Einhaltung notwendiger Sicherheitsmaßnahmen kann derzeit technisch nicht hinreichend überwacht werden
- Cisco hat erste Komponenten für „self-defending networks“ angekündigt, RRZN verfolgt

The screenshot shows the RRZN website in a Netscape browser window. The browser's address bar displays `http://www.rrzn.uni-hannover.de/`. The website header includes the RRZN logo and the text 'Regionales Rechenzentrum für Niedersachsen' and 'Universität Hannover'. A navigation menu contains links for 'A-Z', 'Hotline', 'Kontakt', 'Sitemap', and 'Intern'. The main content area is organized into several columns:

- Veranstaltung**: Lists events such as '2.06.2005' (Telekolloquium) and '30.05.2005' (Sicherheitstage).
- Organisation**: Includes links for 'Über uns', 'Mitarbeiter', and 'Dienstleistungskatalog'.
- Forschung & Lehre**: Lists 'Rechnernetze', 'Forschung', 'Lehre', and 'Software'.
- Suche**: A search bar with a 'Suchmaschinenlabor' link.
- Netz**: Lists 'Datennetz', 'Mail-Service', and 'Netzzugang'.
- Zentrale Server**: Lists 'Betriebskonzept', 'Anwendungen', and 'SAP'.
- IT-Sicherheit**: This menu item is circled in red. It includes 'Antivirensoftware', 'Anwenderinfos', 'Administratoreninfos', and 'Zertifizierung (UH-CA)'.
- Arbeitsplatzrechner**: Lists 'PC/Workstation', 'Server', and 'Gerätebeschaffung'.
- Angebote**: Lists 'Handbücher', 'Kurse', and 'Verkauf & Verleih'.
- Multimedia**: Lists 'Audio/Video', '3D/Visualisierung', and 'TYPO3'.

At the bottom of the page, there is a footer with the text: 'Letzte Änderung: 03. Jun 2005 Anne-Kathrin Iltmann Impressum'.