R|R|Z|N

Sicherheitstage SS 05

6.-8.6.2005

Programm

R|R|Z|N

Montag, 6.6.2005

- **9:15 - 10:45** ***IT-Sicherheit in der Universität*** — **Hille, Prof. Breitner**
- **11:00 - 12:30** ***Firewall-Schutz für Institute*** — **Frau Peter**

Dienstag, 7.6.2005

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

Mittwoch, 8.6.2005

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

Prolog: „Was ist draußen los?“

R|R|Z|N

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

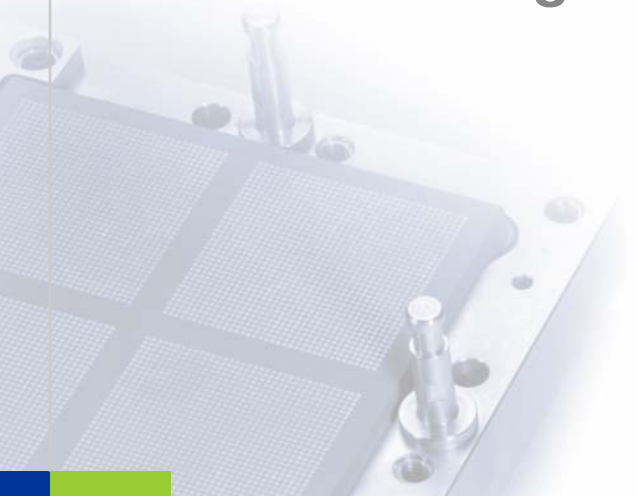
Konsequenzen

R|R|Z|N

- ➔ 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



Zum Begriff der 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

R|R|Z|N

- **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

Bedrohungen / Gefährdungen durch...

R|R|Z|N

- **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

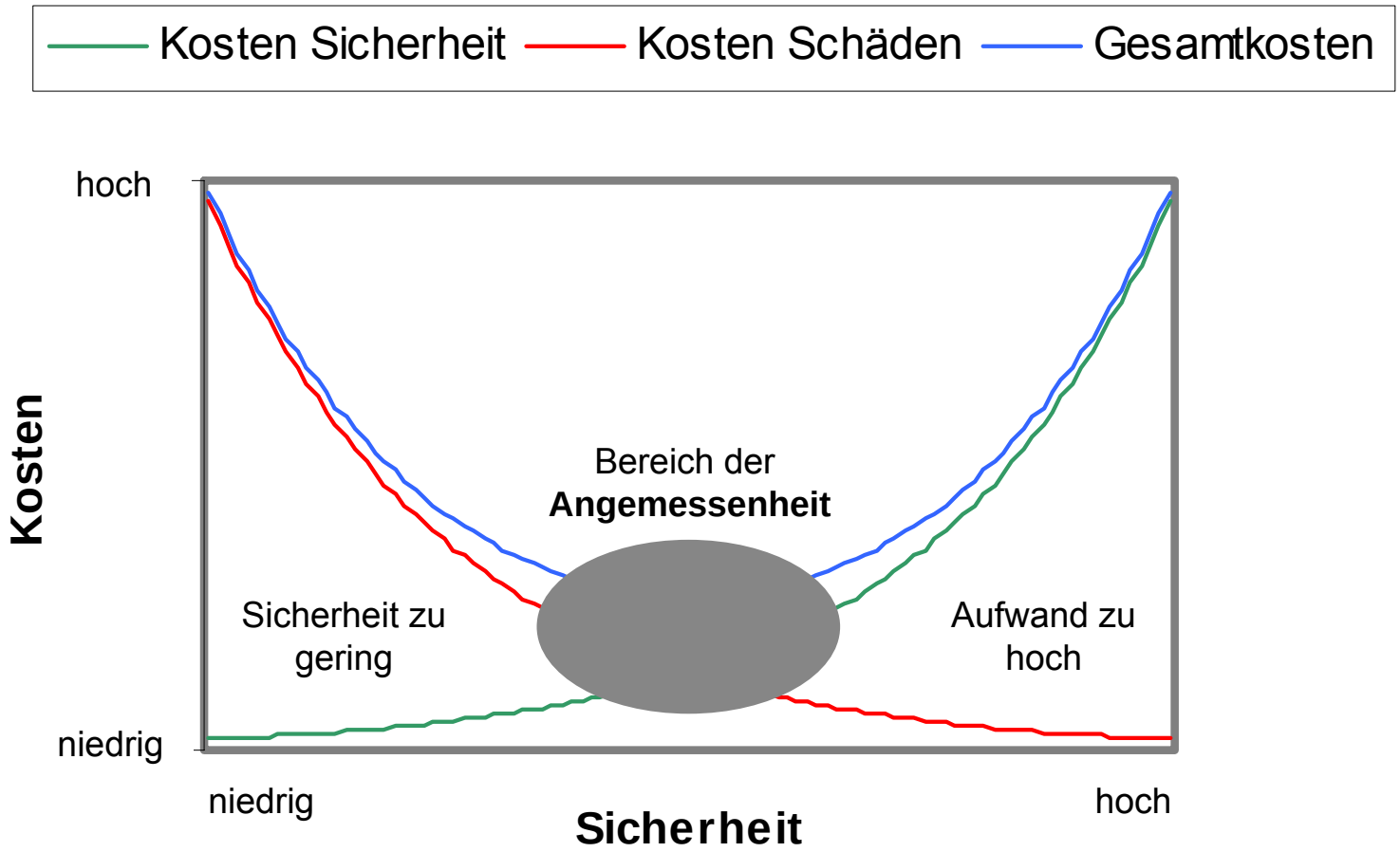
Hinweis: detailliertere Ausführungen im gleichnamigen Vortrag der Sicherheitstage November 2003

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)**

„Angemessenheit“



Klassifikation nach BSI:

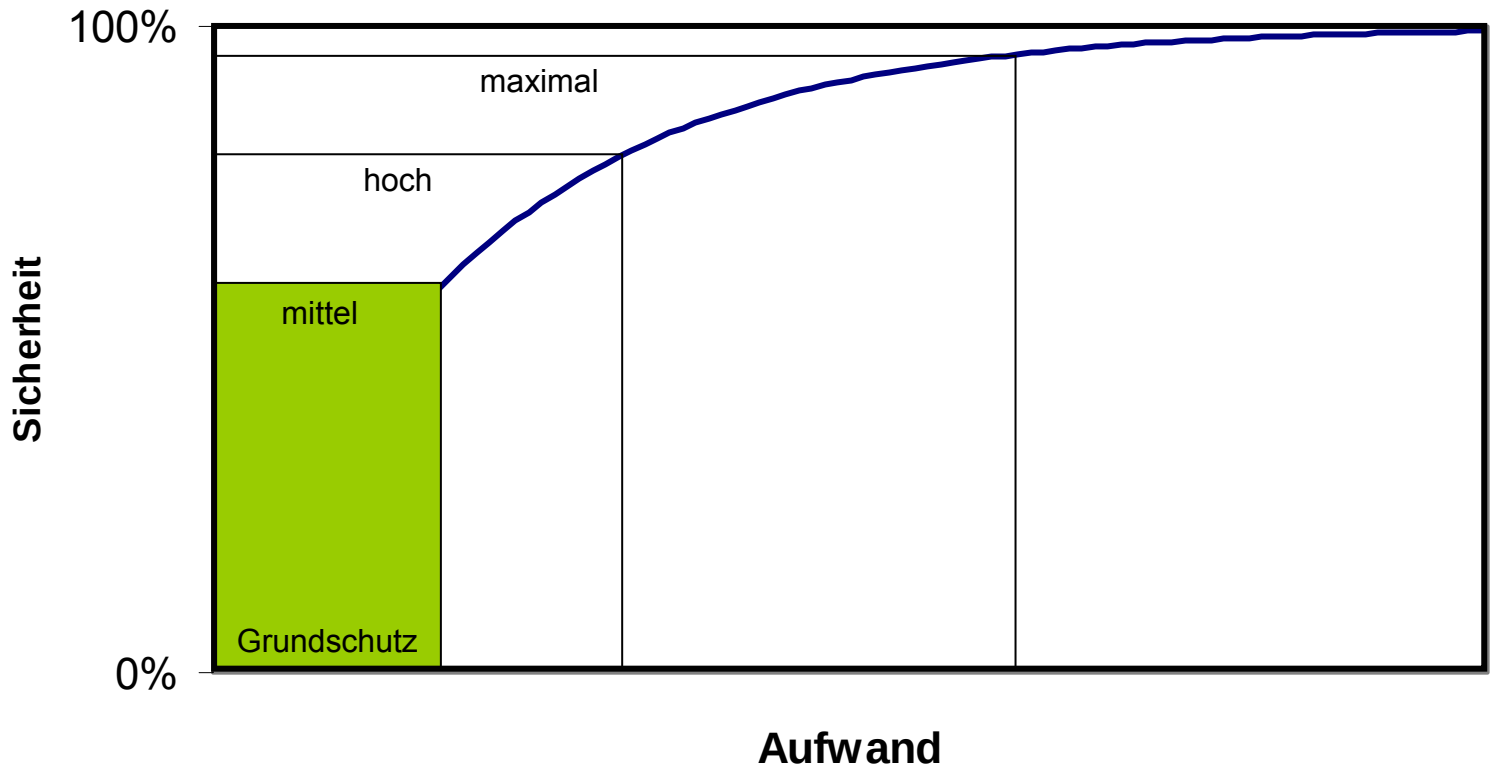
- **Grundschutz: Durchführung von Standardmaßnahmen für den niedrigen bis mittleren Schutzbedarf**
  - detaillierte Analysen können entfallen

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**

Aufwand-Nutzen-Relation *)



*) Nach Grundschutzhandbuch des BSI

IT-Sicherheit ist *kein* fixierter Zustand.

Randbedingungen / Einflussgrößen dynamisch:

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

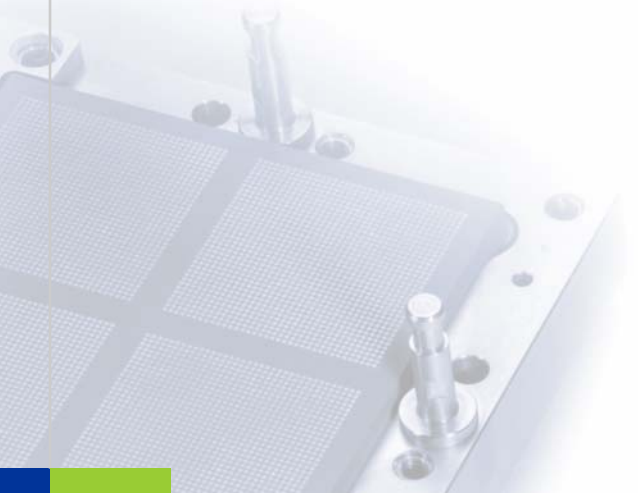
IT-Sicherheit muss als *Prozess* verstanden und organisiert werden

- 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 gegeben Tabellen sind daher mit denen früherer Jahre nicht direkt vergleichbar bzw. enthalten andere Zahlen.

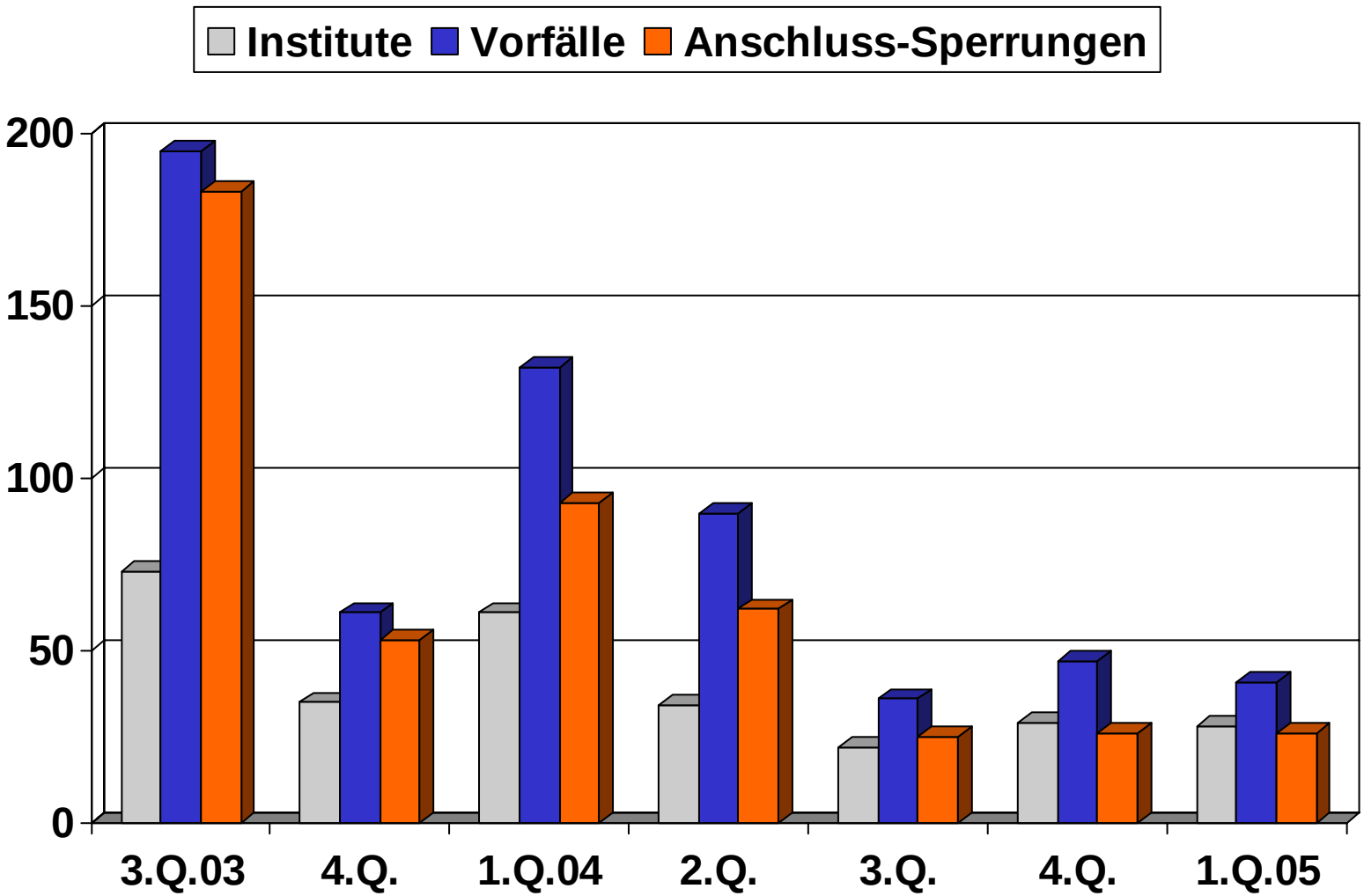
(Hinweis: Selbstverständlich werden Sicherheitsvorfälle im Bereich des Studentenwerks seitens des RRZN nach wie vor adäquat bearbeitet.)

Sicherheitsrelevante Vorfälle (2) ohne StWH

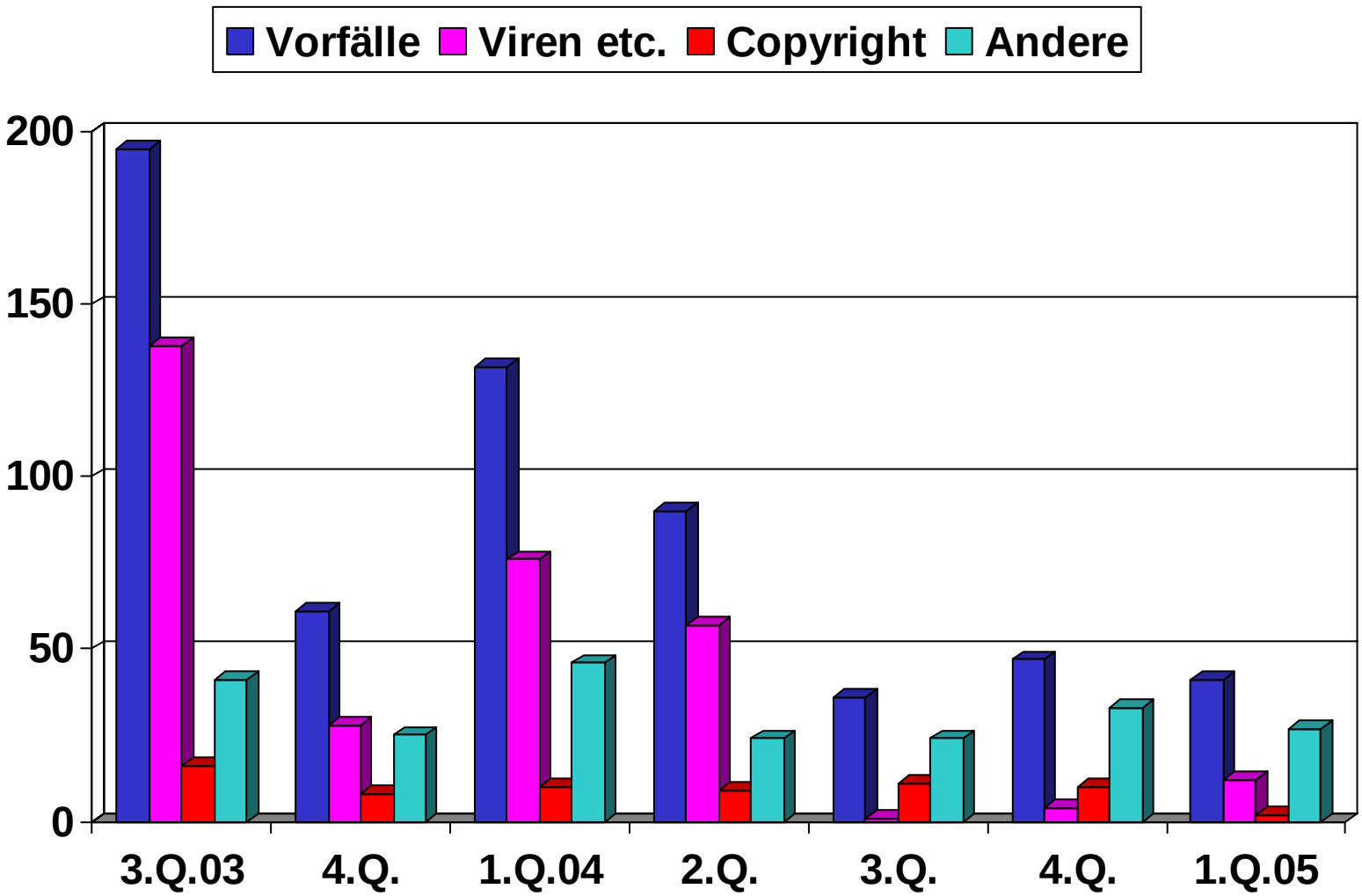
R|R|Z|N

	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**

Sicherheitsrelevante Vorfälle (3) ohne StWH



Sicherheitsrelevante Vorfälle (4) ohne StWH



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

Anmerkungen zu „Copyright-Verstößen“

R|R|Z|N

- **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

Anmerkungen zu „Andere“

R|R|Z|N

„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

Neuere RRZN-Angebote zur IT-Sicherheit

R|R|Z|N

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

R|R|Z|N

- **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 Bereitgestellung 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)

2. Zertifizierungsdienst der UH-CA (1)

R|R|Z|N

- **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 Infrastucture (PKI)
    - zunehmende Bedeutung von PKI-basierten Verfahren zu erwarten (Sicherheitsaspekte der Zurechenbarkeit und Revisionsfähigkeit)
  - Know-How-Gewinn
    - Voraussetzung für künftig zu erwartende „große Anforderungen“

Zertifizierungsdienst der UH-CA (2)

R|R|Z|N

- **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)**

Zertifizierungsdienst der UH-CA (3)

R|R|Z|N

- **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

Zertifizierungsdienst der UH-CA (4)

R|R|Z|N

- **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 Probebetrieb 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**

3. automatische Sophos-Aktualisierung

R|R|Z|N

- **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

automatische Sophos-Aktualisierung (2)

R|R|Z|N

- **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.

R|R|Z|N

***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**

SPAM-Abwehr (2)

R|R|Z|N

- **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**

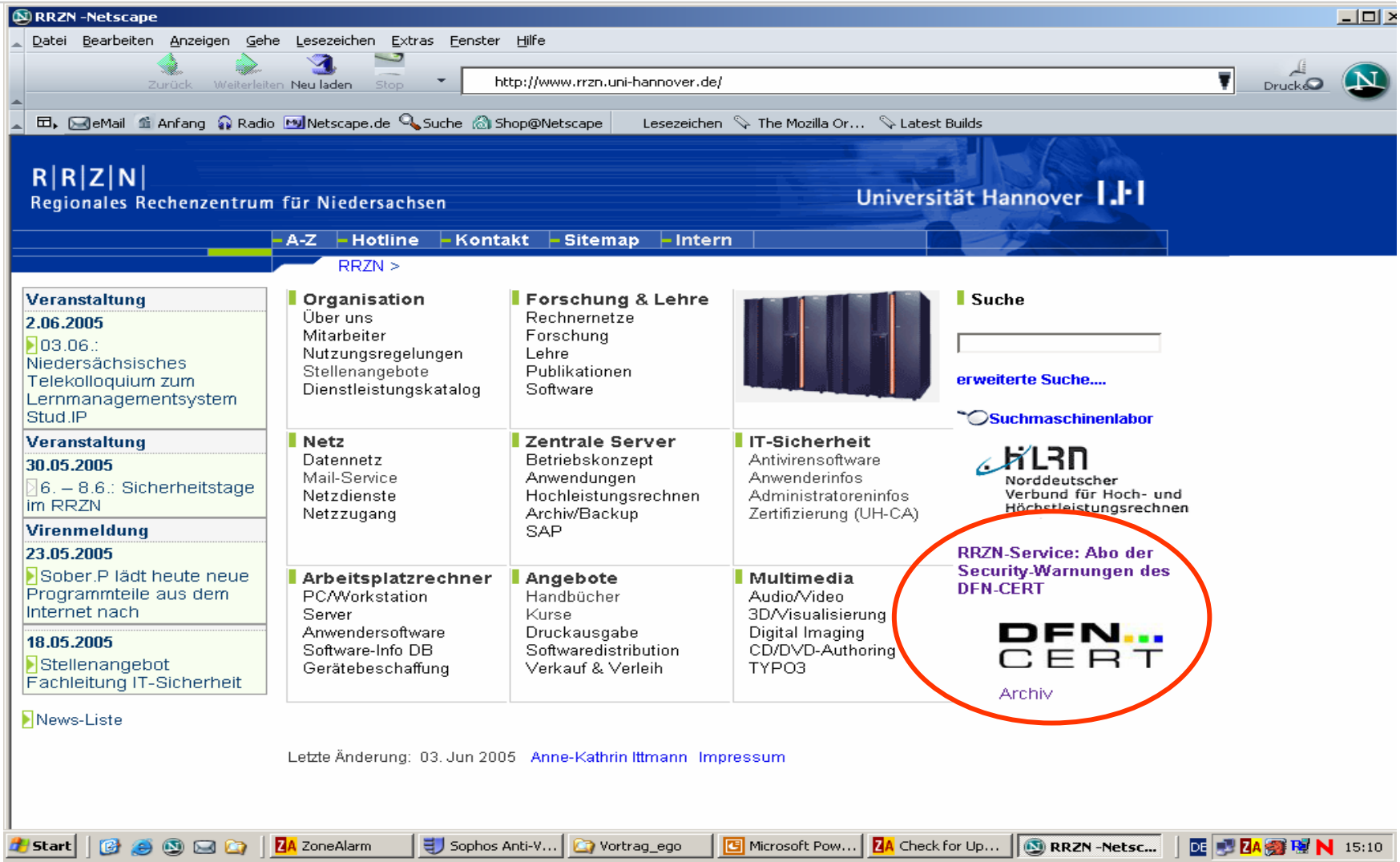
5. Abonnieren von Security-Meldungen (1)

R|R|Z|N

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**

… derzeit als Top-Thema



Abonnieren von Security-Meldungen (2)

Abonnierbare Listen (Auszug)

6. Info zu gesperrten Anschlüssen (1)

R|R|Z|N

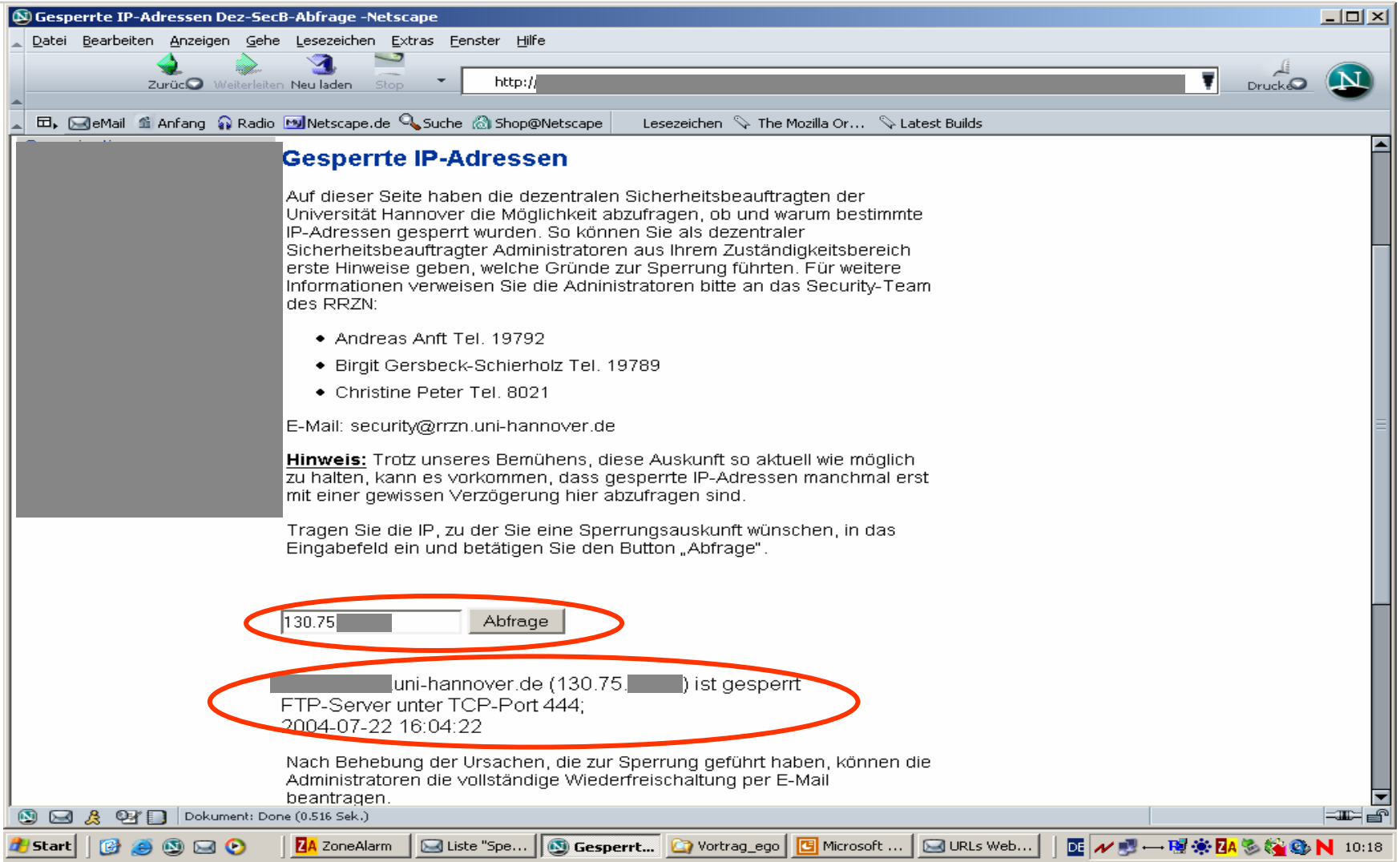
Fragestellung:

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

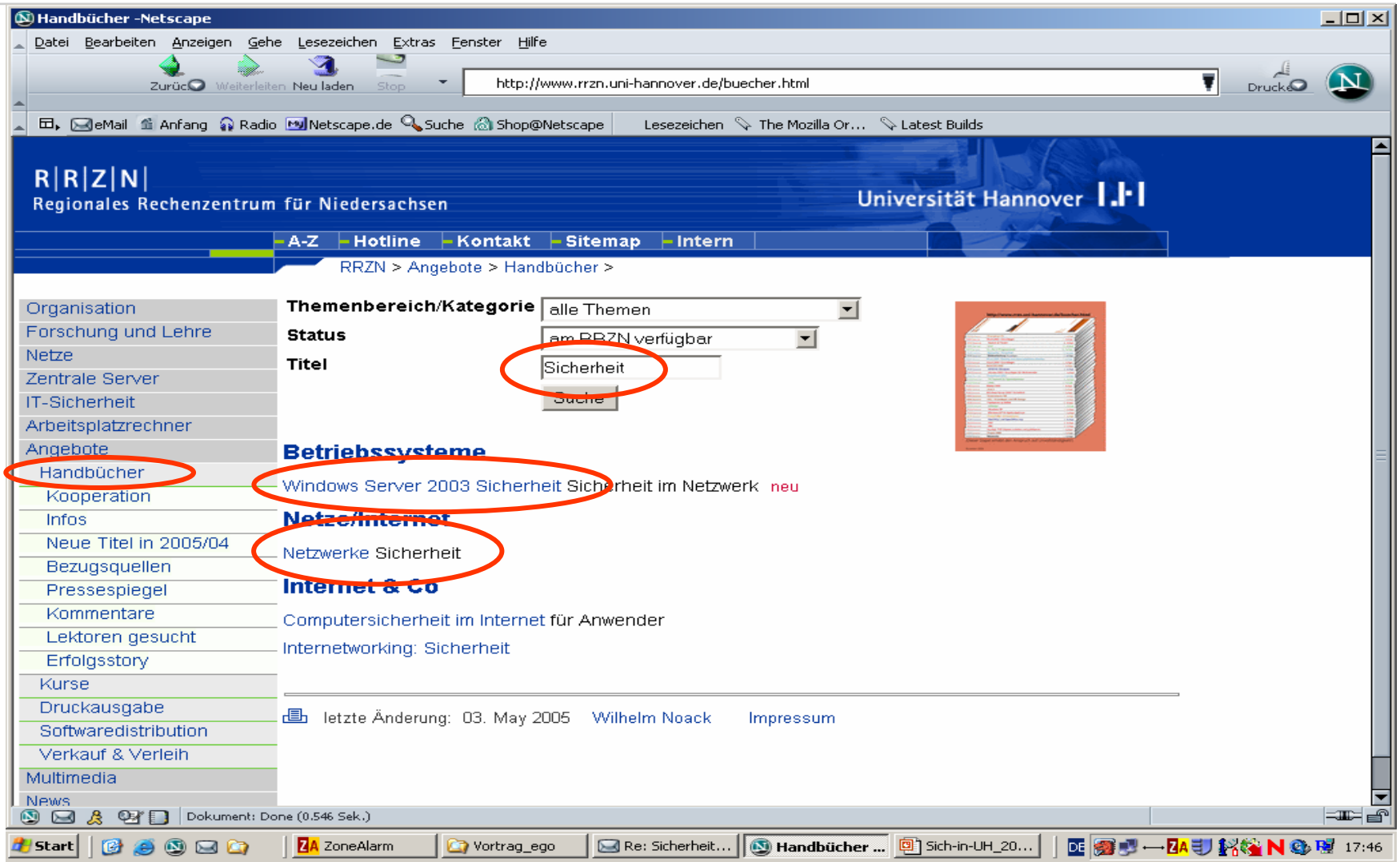
Anwort:

- 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-Administatoren: nur Status (Grund bei zuständigem IT-Sicherheitsbeauftragten oder im RRZN erfragen)
  - diese URLs sollen nicht weitergegeben werden

Info zu gesperrten Anschlüssen (2)



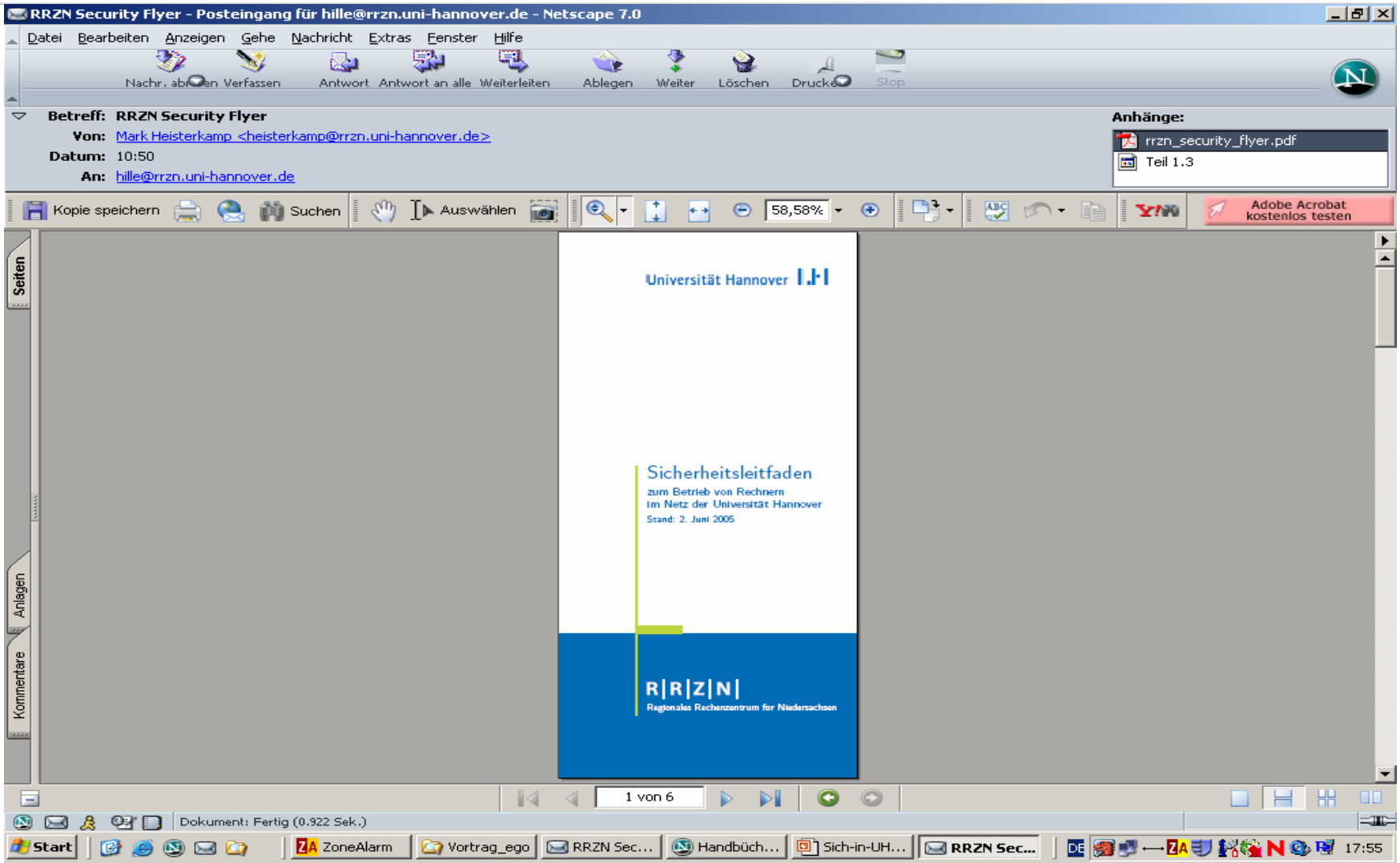
7. Dokumentation zur IT-Sicherheit (1)



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

- enthält: Kurzbeschreibungen zu Sicherheitsthemen mit Links auf die entsprechenden Web-Seiten.
- Status: Entwurfsfassung 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

Dokumentation zur IT-Sicherheit (3)



8. Personal Firewalls

R|R|Z|N

- **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

Zu guter Letzt:

… die Fundgrube