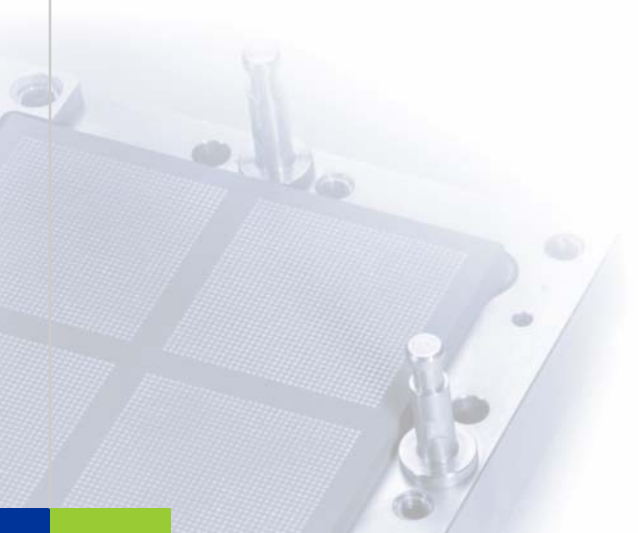
R|R|Z|N

Sicherheitstage WS 04/05

22.-24.11.2004



Die Sicherheitstage …

R|R|Z|N

bisher:

- einmal pro Jahr
- Dauer ca. 1 Woche
- möglichst umfangreiche Abdeckung der für die UH relevanten Themenbereiche
- Beteiligung auswärtiger Dozenten

ab jetzt:

- zweimal im Jahr bzw. einmal pro Semester
- Dauer ca. ½ Woche
- zusätzlich Einzelveranstaltungen
- Themenbereiche verteilt über mehrere Veranstaltungen
- Dozenten nur vom RRZN (ggfs. auch aus Uni)

Programm

R|R|Z|N

Montag

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

Dienstag

- **9:15 - 10:30** ***Sicherheit für Anwender*** — **Frau Gersbeck**
- **10:45 - 11:45** ***UH-CA: Zertifikate für digitale Signaturen und Verschlüsselung*** — **Frau Gersbeck**
- **12:00 - 13:00** ***Sicherheit für Windows-Workstations (1)*** — **Kaufmann**

Mittwoch

- **9:15 - 10:45** ***Sicherheit für Windows-Workstations (2)*** — **Obendorf**
- **11:00 - 12:30** ***Behandlung offener Fragen / Diskussion*** — **Hille et al.**

R|R|Z|N

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

IT-Sicherheit für die UH…

R|R|Z|N

hat signifikante Bedeutung

- einerseits etliche Sicherheitsvorfälle
- andererseits Projekte mit Sicherheitsrelevanz
- generell weiter zunehmende Vernetzung und Einbeziehung des Internets in Arbeitsabläufe

muss systematisch adressiert werden

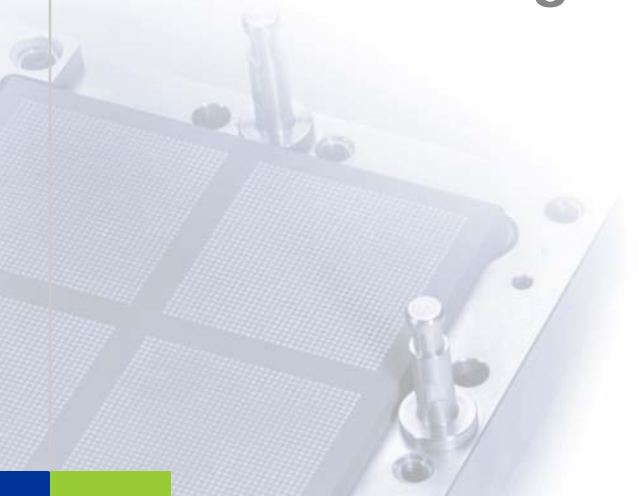
- besondere Herausforderung an einer Universität, da heterogene Systemlandschaften und Verantwortungsstrukturen.
- mit „Ordnung zur IT-Sicherheit…“ Basis vorhanden

muss spezifische Belange berücksichtigen

- RRZN-Erfahrungen aus Institutskontakten (Sicherheitsvorfälle, Sicherheitsberatungen etc.)
- Mitwirkung der laut Sicherheitsordnung am Sicherheitsprozess Beteiligten an konzeptionellen Planungen

I.

Einige Grundlagen zur IT-Sicherheit



Zum Begriff der IT-Sicherheit (1) *)

R|R|Z|N

Die öffentliche Diskussion der letzten Jahre zum Begriff der IT-Sicherheit konvergiert derzeit in folgende Richtung:

Die klassischen Sicherheitsziele **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** beschreiben aus technischer Sicht die Sicherheit von Systemen. Hierfür ist der zusammenfassende Begriff der **Verlässlichkeit** geprägt worden:

- **Verlässlichkeit** *(dependability)* – Sicherheit *der* Systeme
  - „Sachlage, bei der weder die **Systeme** noch die mit ihnen verarbeiteten **Daten** (Informationen) noch die Daten**verarbeitung** (Funktionen und Prozesse) in ihrem Bestand, ihrer Nutzung oder ihrer Verfügbarkeit unzulässig beeinträchtigt werden."

*) Nach „Sicherheit in der Informationstechnik – der Begriff IT-Sicherheit" von R. Dierstein, Informatik Spektrum Aug. 2004

Zum Begriff der IT-Sicherheit (2)

R|R|Z|N

Diese bisher vorherrschende Sicht der Verlässlichkeit wird ergänzt durch die Sicht der

- **Beherrschbarkeit** *(controllability)* – Sicherheit *vor dem* System – die Sicht der Betroffenen
  - Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden.

- **Verlässlichkeit** und **Beherrschbarkeit** sind als **komplementäre Sichten** des Begriffs IT-Sicherheit (”duale Sicherheit”) zu verstehen.

Zum Begriff der IT-Sicherheit (3)

R|R|Z|N

- **Semantische Dimensionen** des Begriffs IT-Sicherheit
  zur Verlässlichkeit:
  - **Vertraulichkeit**
  - **Integrität**
  - **Verfügbarkeit**

  zur Beherrschbarkeit:
  - **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 (1)

R|R|Z|N

- **der Verlässlichkeit:**
  - unbefugter Informationsgewinn
    - Beeinträchtigung oder Verlust der Vertraulichkeit von Ergebnissen oder Funktionen
  - unbefugte Modifikation
    - Beeinträchtigung oder Verlust der Integrität von Ergebnissen oder Funktionen
  - unbefugte Veränderung der Funktionalität
    - Beeinträchtigung oder Verlust der Verfügbarkeit des Funktionsablaufs oder der Ergebnisse
- **der Beherrschbarkeit:**
    - Beeinträchtigung oder Verlust Zurechenbarkeit
    - Verlust der Rechtsverbindlichkeit
    - unbefugte Manipulation von Betroffenen (?)

Grundbedrohungen (2)

R|R|Z|N

- **Charakterisierung als Grundbedrohung 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

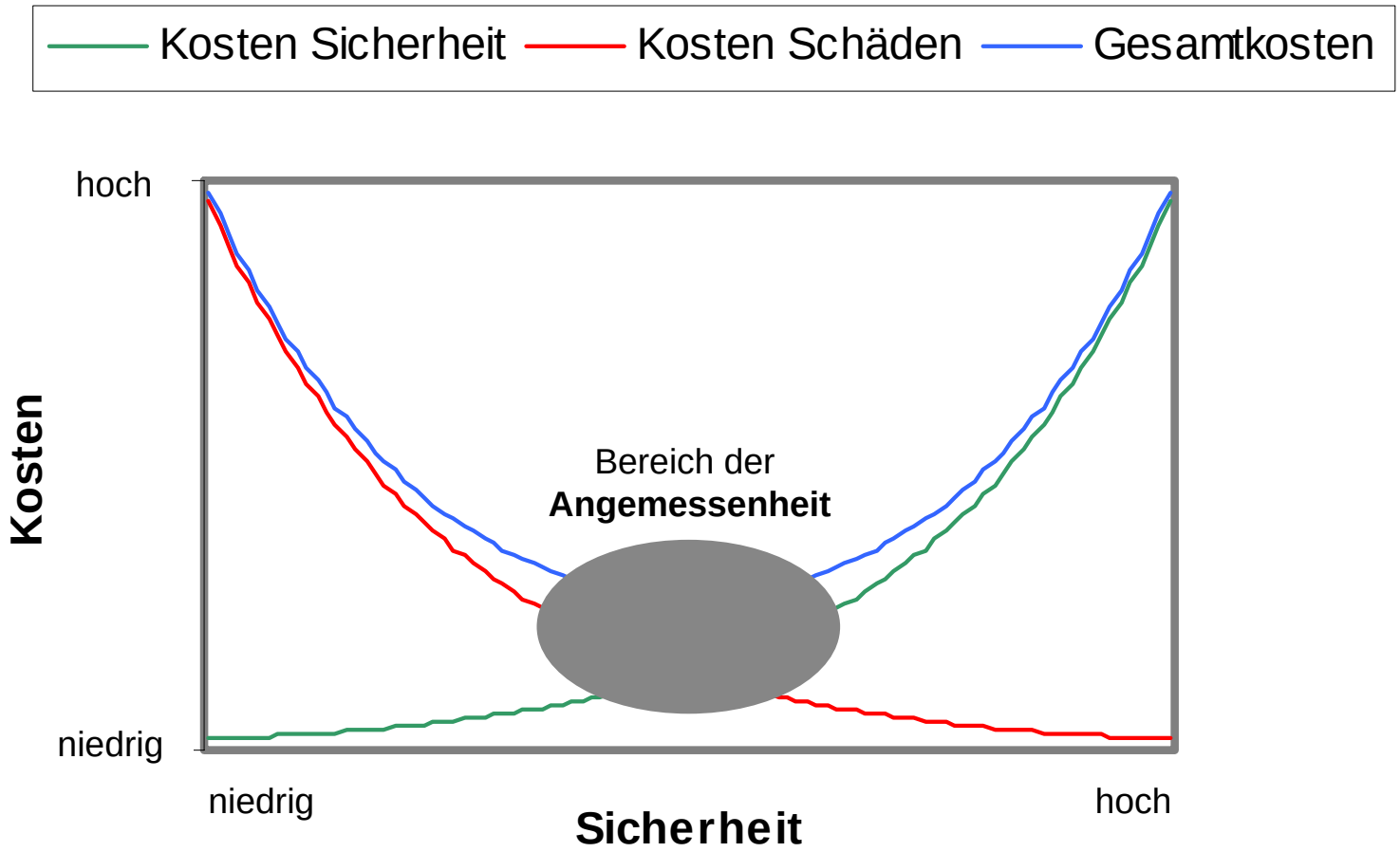
Hinweis: detailliertere Ausführungen im gleichnamigen Vortrag der Sicherheitstage November 2003

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

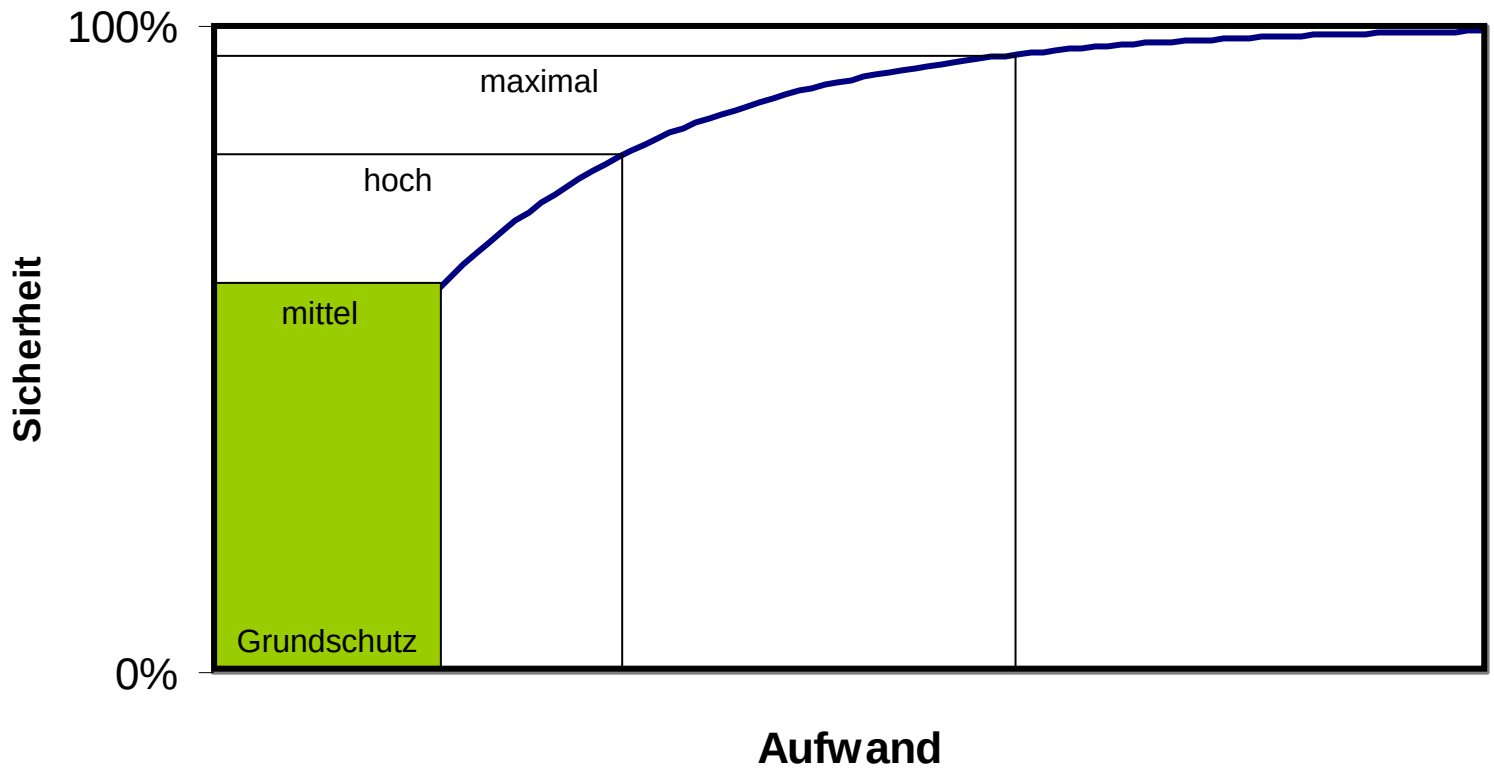
IT-Sicherheit ist vergleichbar mit der Befriedung eines Areals durch einen Zaun:

- *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“



Aufwand-Nutzen-Relation *)



*) Nach Grundschutzhandbuch des BSI

R|R|Z|N

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**

R|R|Z|N

IT-Sicherheit ist *kein* fixierter Zustand.

Randbedingungen / Einflussgrößen dynamisch:

- Ziele / Aufgaben
- „Stand der Technik“
  - auch in Bezug auf Angriffs- / Verteidigungsmaßnahmen
- 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 Sicherheitsbeauftragten
http://www.iwi.uni-hannover.de/it-sicherheit/Ordnung.pdf bzw. über
http://www.rrzn.uni-hannover.de/it_sicherheit.html

Ziele der Ordnung

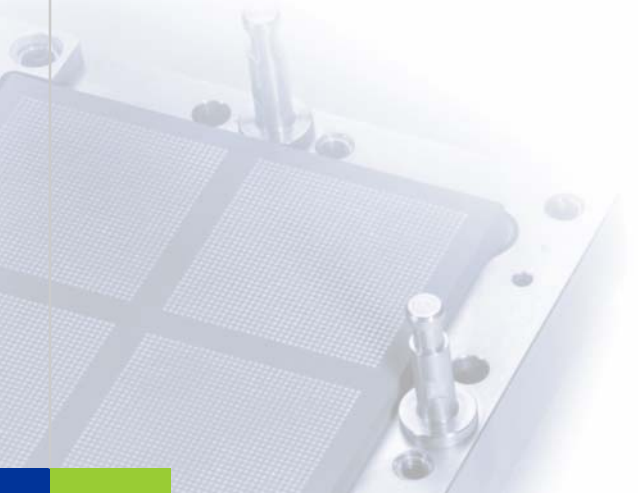
- Festlegung der Verantwortungsstrukturen
- Verbindlichkeit und weitgehende Rechtssicherheit für alle Beteiligten
- Orientierung an „Standards“

Status

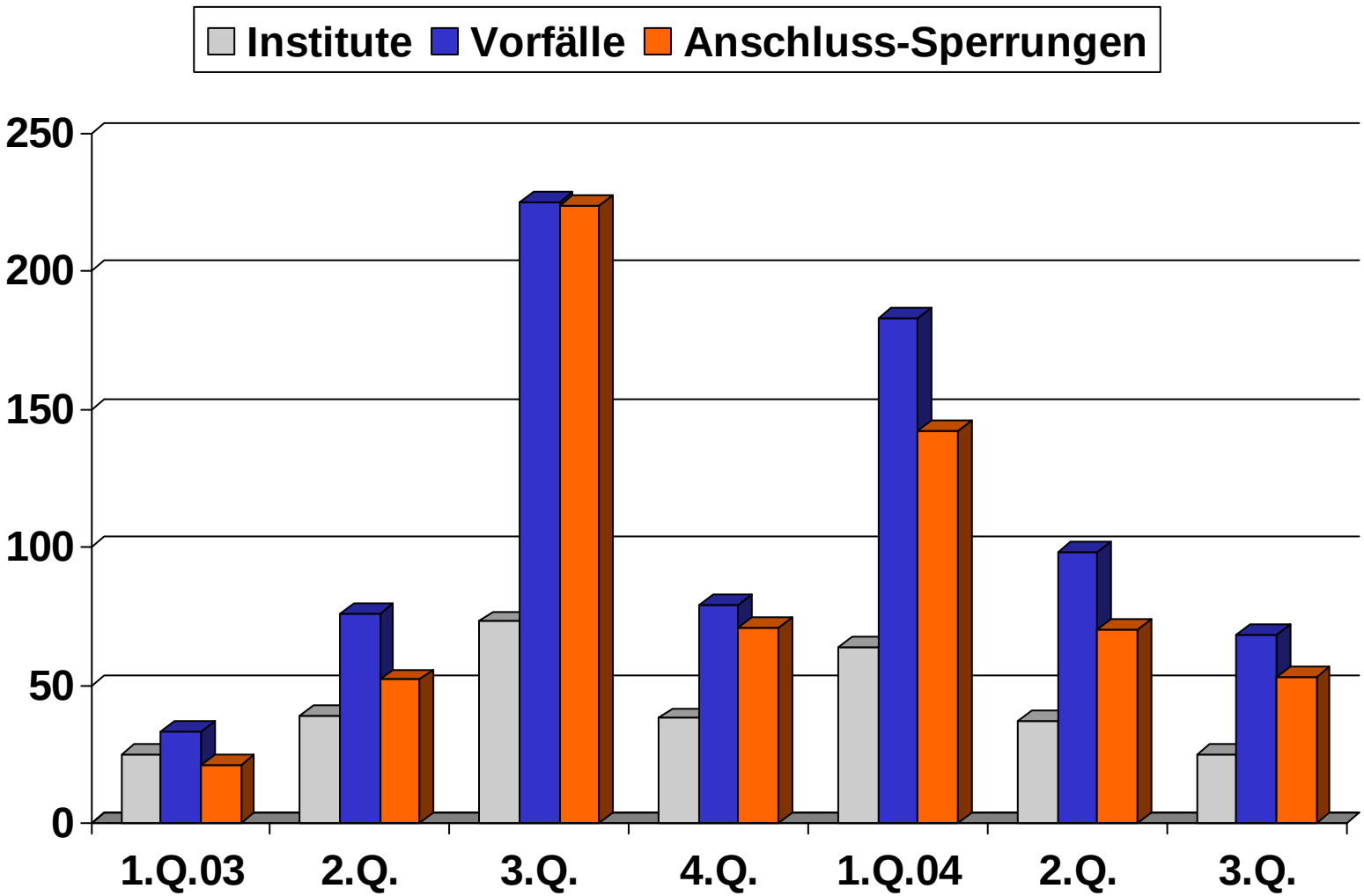
- Seit Ernennung von Prof. Breitner zum Zentralen IT-Sicherheits-beauftragten und der „weiteren Mitglieder“ des Sicherheitstabs Ende 2003 seitens des Präsidenten ist die Ordnung „in Betrieb“.

II.

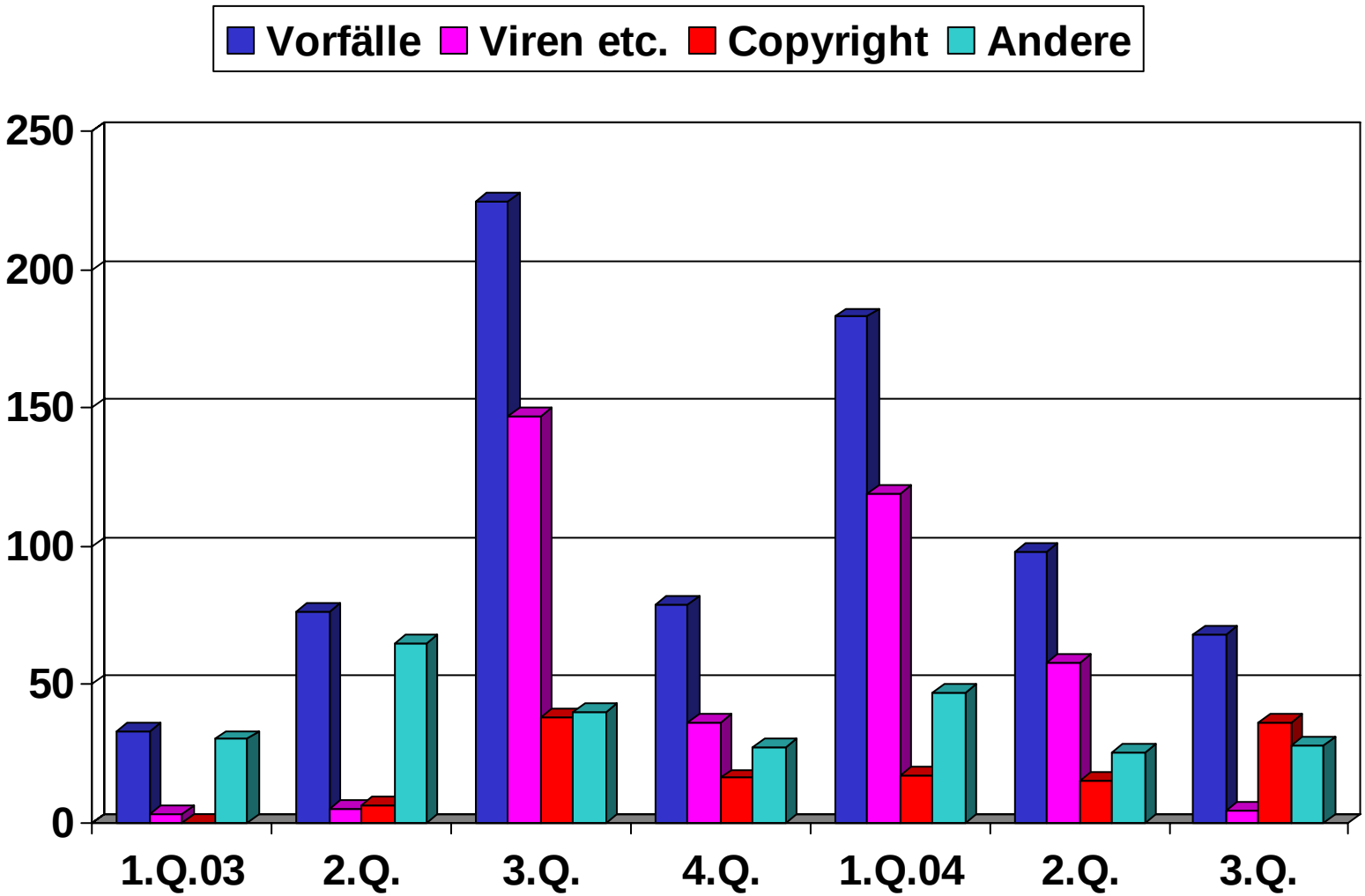
Zur Sicherheitslage in der Universität



Sicherheitsrelevante Vorfälle (1)



Sicherheitsrelevante Vorfälle (2)



Sicherheitsrelevante Vorfälle (3)

R|R|Z|N

	Vorfälle insgesamt	Anzahl Institute	Anschluss-Sperrungen	davon Viren/ Würmer	davon ©-Verstöße
1. Q. 2003	33	25	21	3	
2. Q.	76	39	52	5	6
3. Q.	225	73	224	147	38
4. Q.	**79**	**38**	**71**	**36**	**16**
1. Q. 2004	**183**	**64**	**142**	**119**	**17**
2. Q.	**98**	**37**	**70**	**58**	**15**
3. Q.	**68**	**25**	**53**	**4**	**36**
12 Monate	**428**	**96**	**336**	**217**	**84**

Anmerkungen zu „Viren/Würmer“

R|R|Z|N

Im 1. Q. 04 viele Virenvorfälle, u. a.

- Agobot, Bagle, MyDoom und Netsky inkl. div. Varianten
- immer wieder noch Code Red/Nimda-Ableger

im 2. und 3. Quartal Rückgang bis auf den (niedrigen) Stand vom 1. Q. 2003! Vermutlich folgende Gründe beteiligt:

- weniger gefährliche Viren „unterwegs“
  - z. B. keine schwerwiegenden Warnungen des BSI eingegangen
- auf Anwenderseite mehr Sicherheitsbewusstsein beim Umgang mit Anhängen
- im 2. Quartal wurde automatisches Sophos-Update bereitgestellt
  - derzeit werden ca. 4500 Systeme in der UH automatisch aktualisiert

Anmerkungen zu „Copyright-Verstößen“

R|R|Z|N

- **Nach Häufung der Fälle im 3.Q.03 und konsequentem Vorgehen in Übereinstimmung mit dem zentralen IT-Sicherheitsbeauftragten und in Analogie zu §8 der Sicherheitsordnung zunächst wieder Rückgang der Anzahl der Fälle.**
- **Fallzahlen quasi konstant bis 2.Q.04 einschließlich.**
- **Im 3.Q.04 haben Fälle wieder deutlich zugenommen (überwiegend in Studentenwohnheimen).**

  Bemerkenswert:

  - die Anzahl der beanstandenden Organisationen hat sich im 3. Q. 04 gegenüber dem 2. Q. 04 von 3 auf 9 erhöht!
    - deswegen nicht notwendigerweise eine absolute Zunahme der Fälle, sondern möglicherweise eine höhere Entdeckungsquote

Anmerkungen zu „Andere“

In der Graphik ergeben sich die Werte zu „Andere“ aus „Vorfälle“ abzgl. „Viren“ abzgl. „Copyright“

„Andere“ enthält u. a.

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

Auffällig: relativ konstant über den Betrachtungszeitraum

III.

Neue RRZN-Angebote zur IT-Sicherheit

1. **Verfügbar**
2. **In Arbeit / demnächst verfügbar**
3. **In Planung**

Neue RRZN-Angebote zur IT-Sicherheit

R|R|Z|N

verfügbar:

1. automatische Software-Aktualisierung
2. zentraler Netzschutz
3. Zertifizierungsdienst
4. Abonnieren von Security-Meldungen des DFN-CERT
5. Info zu gesperrten Anschlüssen
6. neue Handbücher zur IT-Sicherheit

in Arbeit / demnächst verfügbar:

7. verbessertes Benachrichtigungswesen
8. Anti-SPAM-Maßnahmen

in Planung:

9. Sicherheitsmaßnahmen für Notebooks / Anschluß ans UH-Netz
10. Weitere Maßnahmen zur Viren-Abwehr

1. automatische Software-Aktualisierung

R|R|Z|N

- **automatisches Sophos-Update**
  - bisher notwendige manuelle Aktualisierung mit IDE-Dateien sowie turnusmäßige Sophos-Neuinstallation entfällt ersatzlos
  - leistungsfähige redundante Server installiert
  - Derzeit partizipieren ca. 4500 Rechner

- **Software Update Service (SUS)**
  - automatische Aktualisierung für Systeme Windows 2000 und Windows XP

- **beide Themenbereiche werden im Vortrag „Sicherheit für Windows-Workstations (1)“ (Kaufmann) ausführlicher behandelt**

R|R|Z|N

- **Möglichkeiten zum Schutz von Institutsnetzen durch zentrales Firewallsystem im RRZN**
  - Alternative zu institutseigenen Firewallsystemen
  - bereits seit längerer Zeit in Erprobung
    - **derzeit Pilotbetrieb mit 17 Instituten, 8 weitere in konkreter Vorbereitung**
- **jetzt Standard-Angebot**
  - die dafür benötigten Firewall-Features sind herstellerseits erst in jüngerer Zeit zur Verfügung gestellt worden
- **nähere Behandlung im nachfolgenden Vortrag „Firewallschutz für Institute“ (Frau Peter), u. a.:**
  - Möglichkeiten für institutseigene Firewalls
  - Darstellung der zentralen RRZN-Lösung („Netzschutz“)
  - Vergleich der Lösungen (Vor-/Nachteile)

3. Zertifizierungsdienst (1)

R|R|Z|N

- **Unter den Namen UHtopCA und UH-CA ist am RRZN eine Zertifizierungsinfrastruktur für die Universität Hannover aufgebaut worden zur Zertifizierung von öffentlichen Schlüsseln unter Einbindung in DFN-PCA-Hierarchie**
- **Motivation**
  - Konkrete Nachfragen aus Instituten nach bzw. RRZN-Unterstützung von
    - gesicherte E-Mail-Kommunikation
    - gesicherte Klient-/Server-Verbindungen auf Basis von SSL
    - Code Signing
  - Einstieg in den Aufbau einer Public Key Infrastucture (PKI), da zunehmende Bedeutung von PKI-basierten Verfahren zu erwarten (Sicherheitsaspekt der „Beherrschbarkeit“)
  - Know-How-Gewinn

Zertifizierungsdienst (2)

R|R|Z|N

- **Status:**
  - Zertifizierung seitens der DFN-PCA im Mai 2004 erfolgt
  - Seit Ende Mai Testbetrieb mit „vollwertigen“ Zertifikaten
    - Bisher 40 Zertifikate ausgestellt für Personen und Server, davon ca. 1/3 für Personen und Server in UH-Instituten
- **ab sofort: mit Aktivierung der Web-Seiten „Zertifizierung“ Pilotbetrieb für Benutzer freigegeben**
  - Betrieb als Service-Angebot (freiwillige Nutzung, Ausstellung einiger hundert Zertifikate zu erwarten)
  - skalierbare Struktur
- **Näheres im Vortrag „UH-CA: Zertifikate für digitale Signaturen und Verschlüsselung“ (Frau Gersbeck)**

4. Abonnieren von Security-Meldungen (1)

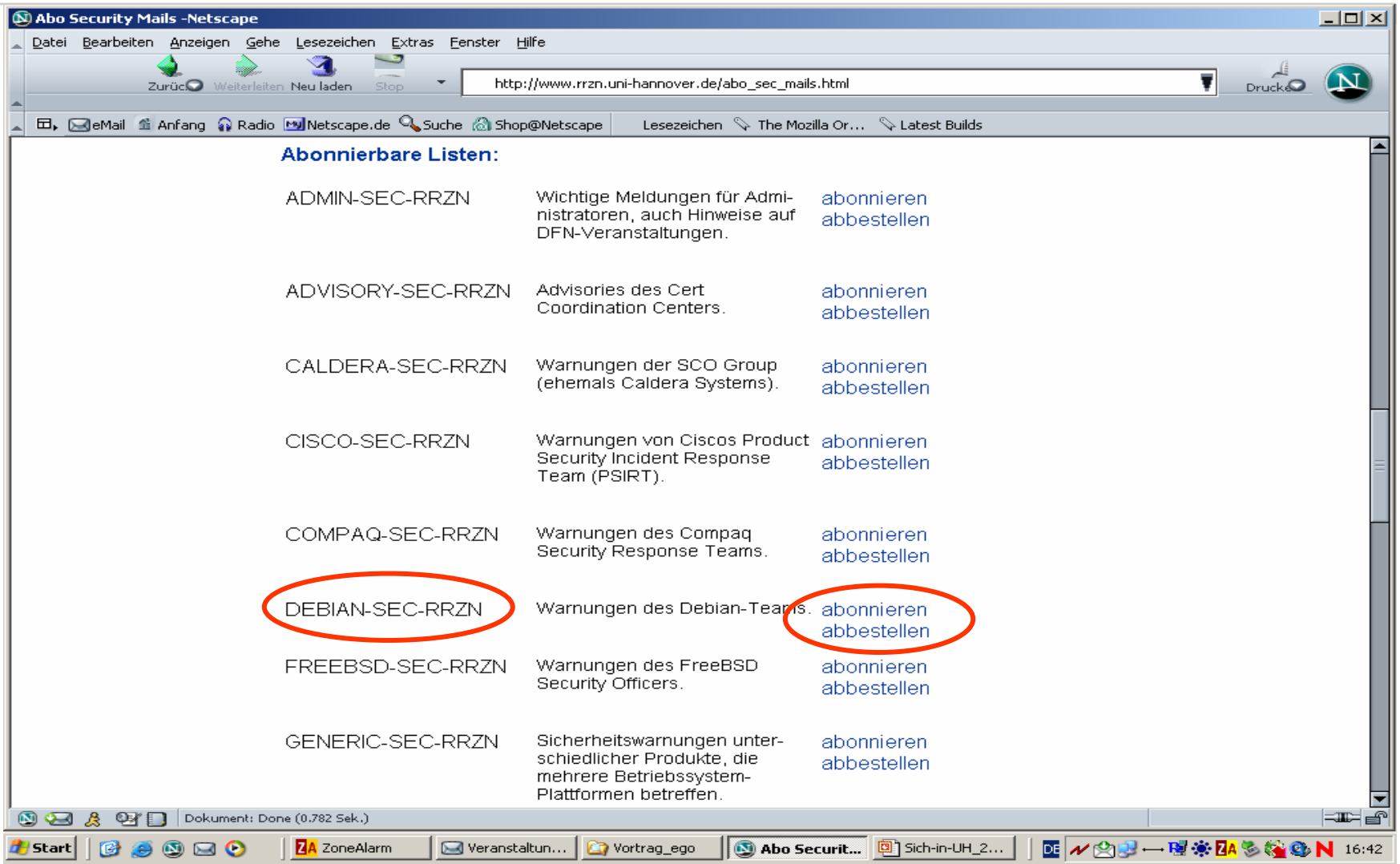
R|R|Z|N

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**

Abonnieren von Security-Meldungen (2)

Abonnierbare Listen (Auszug)



5. Info zu gesperrten Anschlüssen (1)

R|R|Z|N

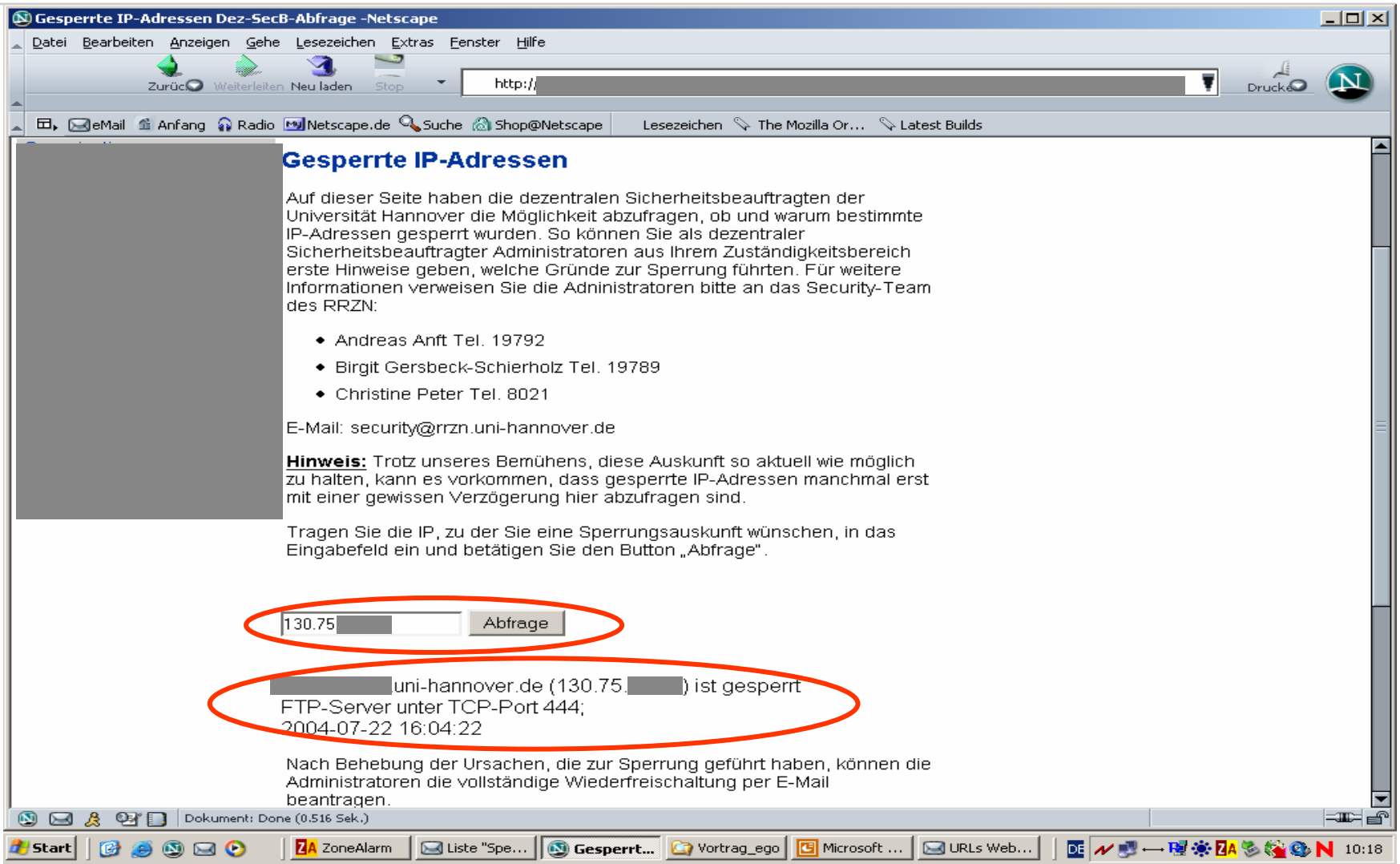
Fragestellung:

Ein Rechner bzw. Netzanschluss bekommt keine Verbindung mehr zum Netz:
Liegt Fehlfunktion oder RRZN-seitige Sperrung vor?

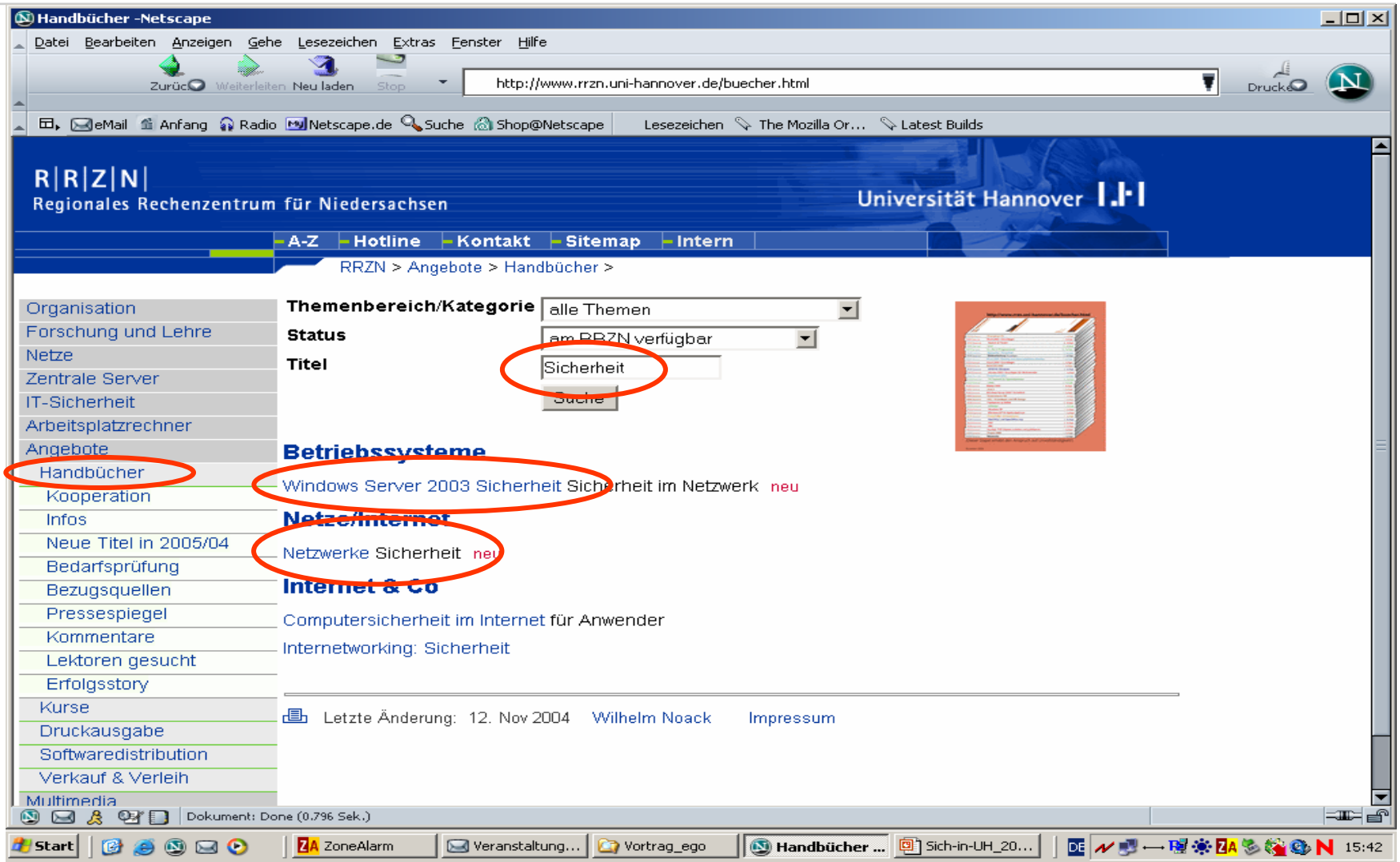
Anwort:

- 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)



6. Neue Handbücher zur IT-Sicherheit



7. Verbessertes Benachrichtigungswesen

R|R|Z|N

- **Security-Mailbox für jedes Institut der UH**
  - Adress-Muster: security-<Inst>@<sec-domain> o. ä
  - Einrichtung in spezieller Domain seitens RRZN
  - Administration seitens der Einrichtung (mittels Kurzanleitung)
    - Eintragung der „Zieladressen“, bei Bedarf Aktualisierung
  - benötigt vom RRZN für Institutsbenachrichtigungen
  - Nutzung seitens dez. IT-Sicherheitsbeauftragter
- **Security-Verteiler für gesamte UH (vom RRZN betrieben)**
  - Security-UH@listserv.uni-hannover.de
    - Basierend auf o. a. Security-Mailboxen
    - vom RRZN und zentralem IT-Sicherheitsbeauftragten genutzt
- **Security-Verteiler für Fachbereiche/Fakultäten möglich**
- **Näheres zu gegebener Zeit schriftlich**

RRZN ist Landeslizenz für Produkt „PureMessage“ von Sophos beigetreten

- **E-Mail-Managementlösung für Mail-Server und Gateways, u. a.:**
  - integrierter Viren- und Spam-Schutz
  - Quarantäne-Manager
  - Kontrollmöglichkeiten auch für Endbenutzer
  - automatische Antiviren- und **Antispam-Updates**

- **PureMessage wird derzeit auf den Einsatz am RRZN vorbereitet, demnächst Betriebsaufnahme vorgesehen.**

9. Sicherheitsmaßnahmen für Notebooks

R|R|Z|N

Problem:

Der freizügige Anschluss von Rechnern (Notebooks) an das UH-Netz bringt die Gefahr des Einbringens von Schadsoftware mit sich.

- Mindestsicherheitsmaßnahmen wie etwa
  - professionelles Betriebssystem mit aktuellen Patches
  - aktuelle Anti-Virensoftware

  können zwar empfohlen, aber derzeit nicht wirksam durchgesetzt werden

Lösung: „self-defending networks“ (Firmenentwicklung)

- bei Aufschaltung erfolgen Sicherheitsüberprüfungen
  - ggfs. muss vor Zugangsfreigabe beispielsweise Update erfolgen

➢ **RRZN verfolgt Entwicklung und wird bei Verfügbarkeit Lösung auf Eignung für Einsatz in der UH prüfen**

10. Weitere Maßnahmen zur Viren-Abwehr

R|R|Z|N

Standardmäßig erfolgt zentrale Viren-Prüfung von E-Mails mit Antiviren-Software von McAfee

Bisher:

- Virenbehaftete Anhänge werden gelöscht (RRZN Hinweis)
- Modifizierte Mail wird zugestellt (dann meist „SPAM-Mail“)

Weitere denkbare Möglichkeiten:

- **alle** virenbehafteten E-Mails löschen?
- **ausführbare Anhänge** generell löschen (**ohne** Virenprüfung)?
- **E-Mails mit ausführbaren Anhängen** generell löschen (ohne Virenprüfung)?

➢ **Da die Virenproblematik in der UH im letzten dreiviertel Jahr stark rückläufig gewesen ist, wurden diese Fragen vorerst nicht weiter verfolgt. (Ev. künftig individuelle Lösungen mittels PureMessage möglich)**

Zu guter Letzt:

Die Fundgrube…