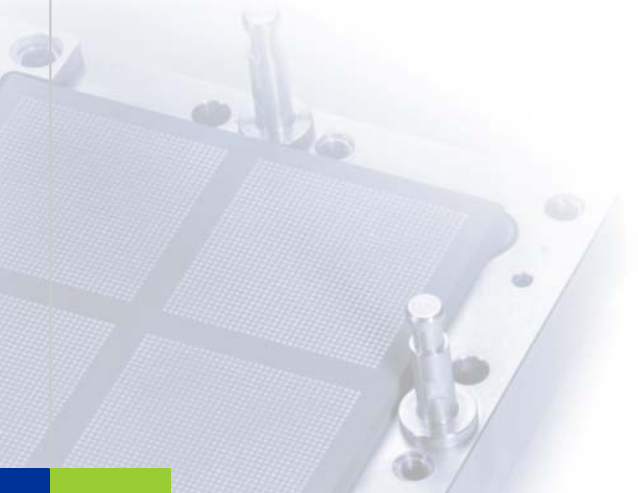
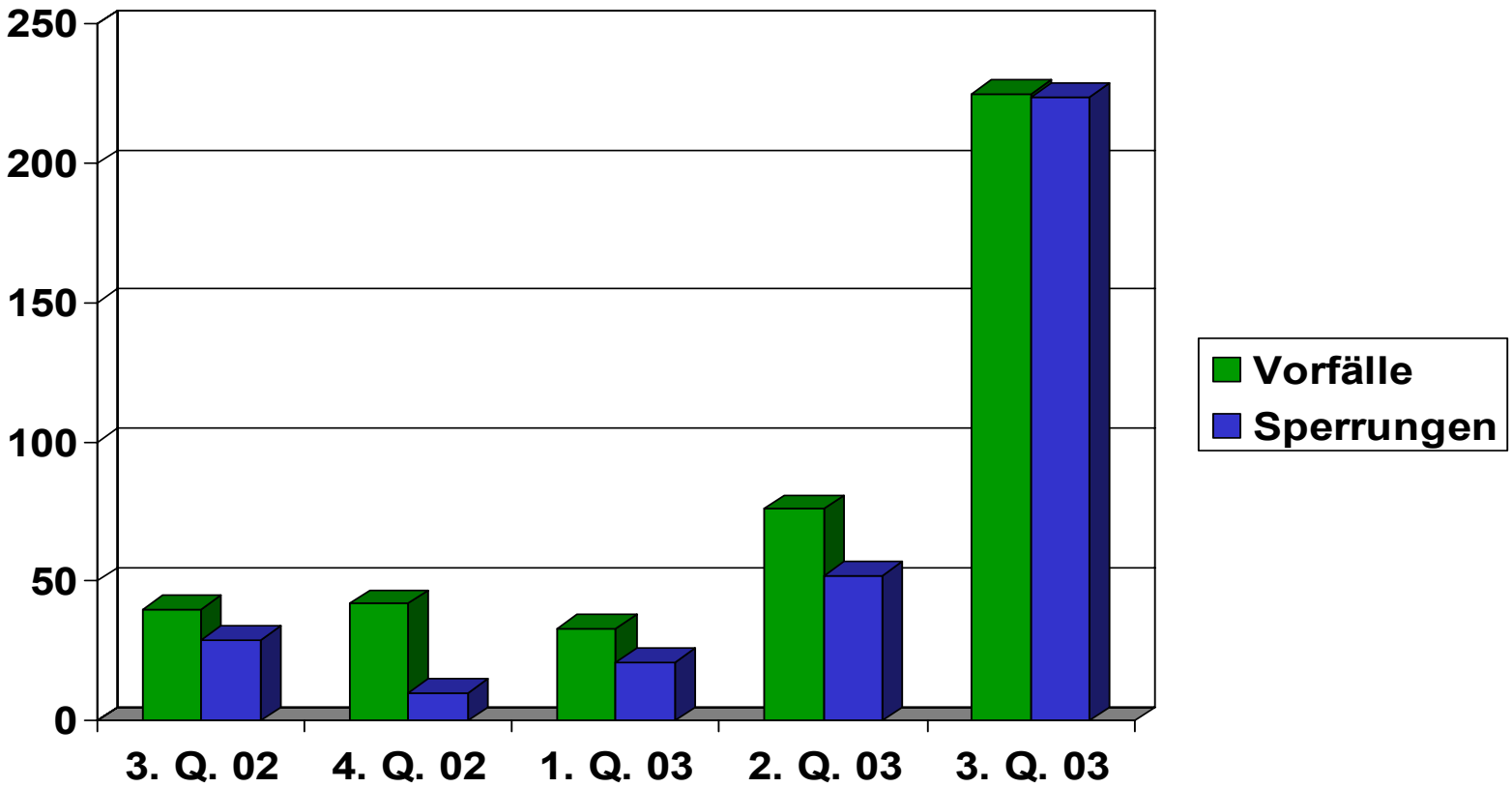
R|R|Z|N

Sicherheitstage WS 03/04

IT-Sicherheit in der Universität Hannover



Ein Bild sagt mehr als 1000 Worte…



Vom RRZN registrierte Sicherheitsvorfälle an der UH

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

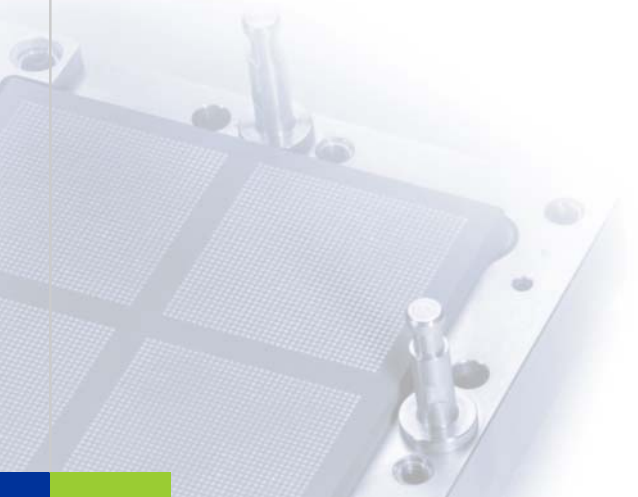
- besondere Herausforderung an einer Universität, da heterogene Systemlandschaften und Verantwortungsstrukturen.
- „Ordnung zur IT-Sicherheit…“ weist in die richtige Richtung

muss spezifische Belange berücksichtigen

- RRZN-Erfahrungen aus Institutskontakten (Sicherheitsvorfälle, Sicherheitsberatungen etc.)
- Mitwirkung der dezentralen IT-Sicherheitsbeauftragten an konzeptionellen Planungen

I.

Einige Grundlagen zur IT-Sicherheit



Begriffe

R|R|Z|N

Die folgenden, in Literatur/Dokumentationen häufig synonym gebrauchten Begriffe werden hier unterschieden:

- **IT-Sicherheit / Security:** Umfassender Sicherheitsbegriff
- **Netz(werk)-/ Computer-/ Systemsicherheit:**
  Teil-Aspekte (überwiegend technischer Art) der IT-Sicherheit
- **Datenschutz:**
  originär Schutz von Personen, nicht von IT-Systemen !
- **Datensicherheit:**
  begriffliche Einschränkung auf "Daten"? "Verwandschaft" zu Datenschutz? (nicht verwendet)

Ziele der IT-Sicherheit

Aufrechterhaltung bzw. Schutz vor Verlust der

- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

für Daten, Programme, Dienste

Zusätzlich

- **Authentizität / Unbestreitbarkeit**

für „Veranlasser“ von Vorgängen/Prozessen

Aus Sicherheitshandbuch des BSI:

R|R|Z|N

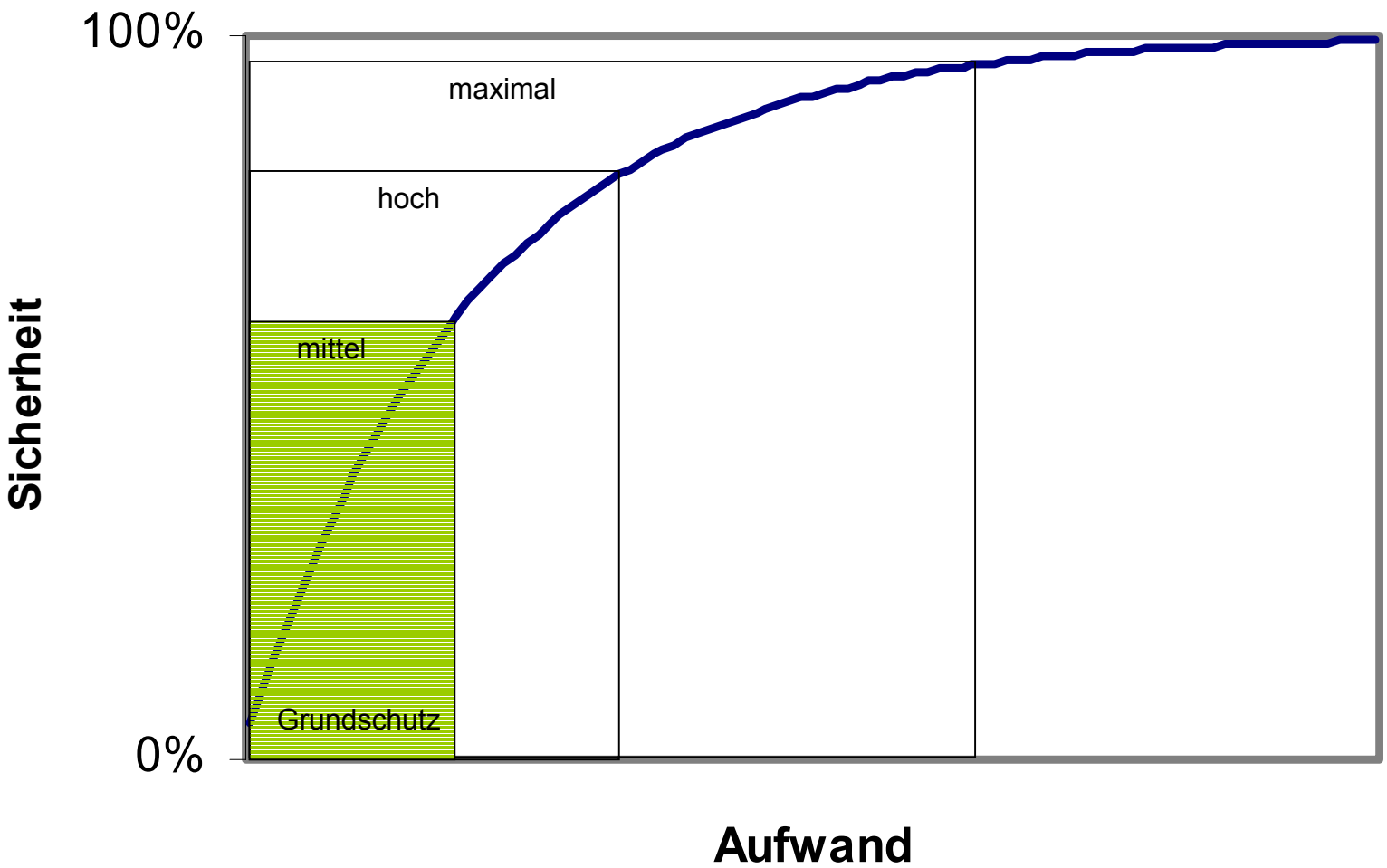
„**IT-Sicherheit** ist der Zustand eines IT-Systems, in dem die **Risiken**, die beim Einsatz dieses IT-Systems aufgrund von **Bedrohungen** vorhanden sind, durch **angemessene Maßnahmen** auf ein **tragbares Maß** beschränkt sind.“

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)**
- **technische Mängel / Versagen (Hardware, Software)**
- **organisatorische Mängel**
- **höhere Gewalt**

Aufwand - Nutzen- Relation *)



*) Nach Grundschutzhandbuch des BSI

Sicherheitsniveaus

R|R|Z|N

maximal/hoch:

- Schutz vertraulicher Informationen muss gewährleistet sein bzw. hohen gesetzlichen Anforderungen genügen
- Korrekte Verarbeitung, zeitkritische Vorgänge! Ausfallzeiten nicht akzeptabel!
- Schäden führen zum totalen Zusammenbruch bzw. zu erheblicher Beeinträchtigung der Institution (und auch Dritter) bzw. zu schwerwiegenden Folgen für breite gesellschaftliche oder wirtschaftliche Bereiche

mittel/niedrig:

- Vertraulichkeit interner Informationen gewährleistet bzw. nicht gefordert
- Kleinere Fehler und Ausfallzeiten in gewissen Umfang tolerabel
- Schäden haben geringe bzw. nur unwesentliche Beeinträchtigungen der Institution zur Folge

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

- absolute Sicherheit nicht möglich: **Welches Restrisiko tragbar?**

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)**

Einflußgrößen

- Sicherheitsziele
  - u. a. Festlegung der zu schützenden Werte
- Vorschriften / Richtlinien / gesetzliche Regelungen

Maßnahmen

- im technischen Bereich
- im nicht-technischen Bereich

Rückkopplung: Wirksamkeit / Effizienz der Maßnahmen?

Zu schützende Werte

R|R|Z|N

an Universität u. a.:

- **Ergebnisse von Forschungsarbeiten**
- **Vertragsinhalte**
- **personenbezogene Daten (auch Datenschutz!)**
- **finanzbezogene Daten**
- **effiziente Arbeitsabläufe**
  - Verlässliche Systeme bzw. Dienste!
- **Reputation**

System-/Netzsicherheit

- u. a.: Systempflege / Einstellungen / Security-Patches
- Einsatz Sicherheitsprodukte (z. B.: Antivirensoftware, Firewall-Systeme, Intrusion-Detection-Systeme)

Identifikation und Authentifikation

Zugriffskontrolle (Rechteverwaltung und -prüfung)

Verschlüsselung der Informationsübertragung

- Infrastruktur zur Schlüsselverwaltung erforderlich
- geeignet zu sicherer Authentifikation und Unbestreitbarkeit

Nichttechnische Maßnahmen

R|R|Z|N

organisatorischer, administrativer und personeller Art:

- **Zuständigkeiten, Rechte und Rollen festlegen**
  - Einweisung in Maßnahmen / Kontrolle der Wirksamkeit
- **Notfallvorsorge: Planung für den Eintritt von sicherheitsrelevanten Ereignissen**
  - Zuständigkeiten, Kontaktstellen
  - Schadensbegrenzung, Beseitigung der Ursachen, Beweissicherung
  - Wiederherstellung der Systemintegrität
- **Aufbau eines Sicherheitsbewusstseins**
  - Schulung der Anwender / Administratoren
- **Überwachung (Vorfälle häufig durch Innentäter!)**
- **Maßnahmen bei Einstellung und Ausscheiden von Personal**
  - insbesondere: bei Ausscheiden alle Rechte und Rollen löschen!

bauliche Aspekte, u. a.

- Wände, Decken, Türen, Fenster …
- Brand-/Rauchschutz
- Feuchtigkeitsschutz
- Versorgungszu- und ableitungen

räumliche Aspekte

- Zugangssysteme
- Diebstahlsicherung

Abhörmöglichkeiten ?

IT-Sicherheit ist *kein* fixierter Zustand.

Randbedingungen / Einflussgrößen dynamisch:

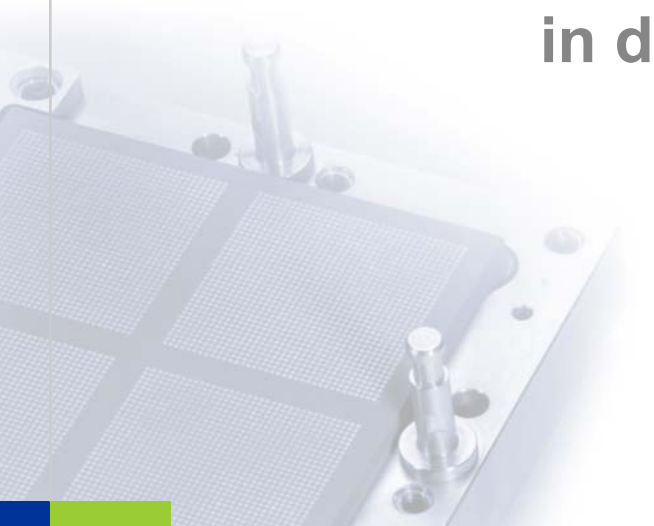
- Ziele / Aufgaben
- „Stand der Technik“
  - auch in Bezug auf Angriffs- / Verteidigungsmaßnahmen
- Vorschriften / Richtlinien / gesetzliche Regelungen

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

- Sicherheitsmanagement erforderlich
- auf Leitungsebene anzusiedeln!

II.

Der IT-Sicherheitsprozess in der Universität Hannover



Der IT-Sicherheitsprozess für die gesamte UH ist mit der „Ordnung zur IT-Sicherheit in der Universität Hannover“ in Gang gesetzt worden
(http://www.rrzn.uni-hannover.de/Security/Ordng_z_IT-Sicherht_Senat.pdf)

- IT-Sicherheit liegt im Gesamtinteresse der UH

Ziele der Ordnung

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

Beteiligte am IT-Sicherheitsprozess

R|R|Z|N

- der/die zentrale IT-Sicherheitsbeauftragte
- dezentrale IT-Sicherheitsbeauftragte
- der Sicherheitsstab
- das RRZN
- alle Einrichtungen der Universität

- Rechte und Pflichten der Anwender werden in separater Ordnung geregelt

Die IT-Sicherheitsbeauftragten (IT-SB)

R|R|Z|N

zentraler IT-SB wird vom Präsidenten eingesetzt

Stand: *Position durch Todesfall derzeit wieder vakant*

Benennung der dezentralen IT-SB durch Fachbereiche und zentrale Einrichtungen

Stand: *ist weitgehend erfolgt*

besondere Schulung der dezentralen IT-SB

Stand: *beginnt mit diesen Sicherheitstagen*

Ständige Mitglieder

- zentrale(r) IT-SB (Vorsitz)
- Vertreter(in) des RRZN (stellvertretender Vorsitz)
- Vertreter(in) des Rechtsdezernats
- der/die Datenschutzbeauftragte (ggfs. Vertretung)

weitere, von Präsident und Senat benannte sachverständige Mitglieder

Gesamtpersonalrat kann beratendes Mitglied benennen

Stand: *Vorschlagsliste beim Präsidenten*

- 7+1 Mitglieder inkl. der Vertreter der Wiss. Einrichtungen, der Verwaltung und der Studierenden

Benennung ausgesetzt, bis wieder ein zentraler IT-SB gefunden ist

Zentraler IT-SB und Sicherheitsstab:

- **Entwicklung/Fortschreibung**
  - der strategischen Planungen zur IT-Sicherheit
  - Entwicklung realisierbarer Sicherheitskonzeptionen (möglichst unter Beteiligung der dezentralen IT-SB)
  - der Leitlinien zur Ausbildung
- **Koordinationsgremium bei Sicherheitsvorfällen**
- **Beteiligung bei Projekten mit Sicherheitsbezug**
- **ggfs. Finanz- und Personalplanung**
- **Überwachung der Umsetzung inkl. Rückkopplung zu Planungen**

Der IT-Sicherheitsprozess

R|R|Z|N

- **Zentr. IT-SB initiiert, steuert und kontrolliert**
- **Sicherheitsstab unterstützt zentr. IT-SB**
- **IT-SBs nehmen sicherheitsbezogene Informationen entgegen und veranlassen Maßnahmen**
- **dez. IT-SBs überwachen die Sicherheit in ihrem Bereich. Sie informieren die Leitungen der betreffenden Einrichtungen und schlagen Lösungsmöglichkeiten bei Problemen vor. Ggfs. Bericht an zentr. IT-SB, dabei nicht an Weisungen gebunden.**
  - frühzeitige Beteiligung an sicherheitsrelevanten Projekten ihres Bereichs
  - Förderung des Sicherheitsbewusstseins in ihrem Bereich

Bei „Gefahr in Verzug“:

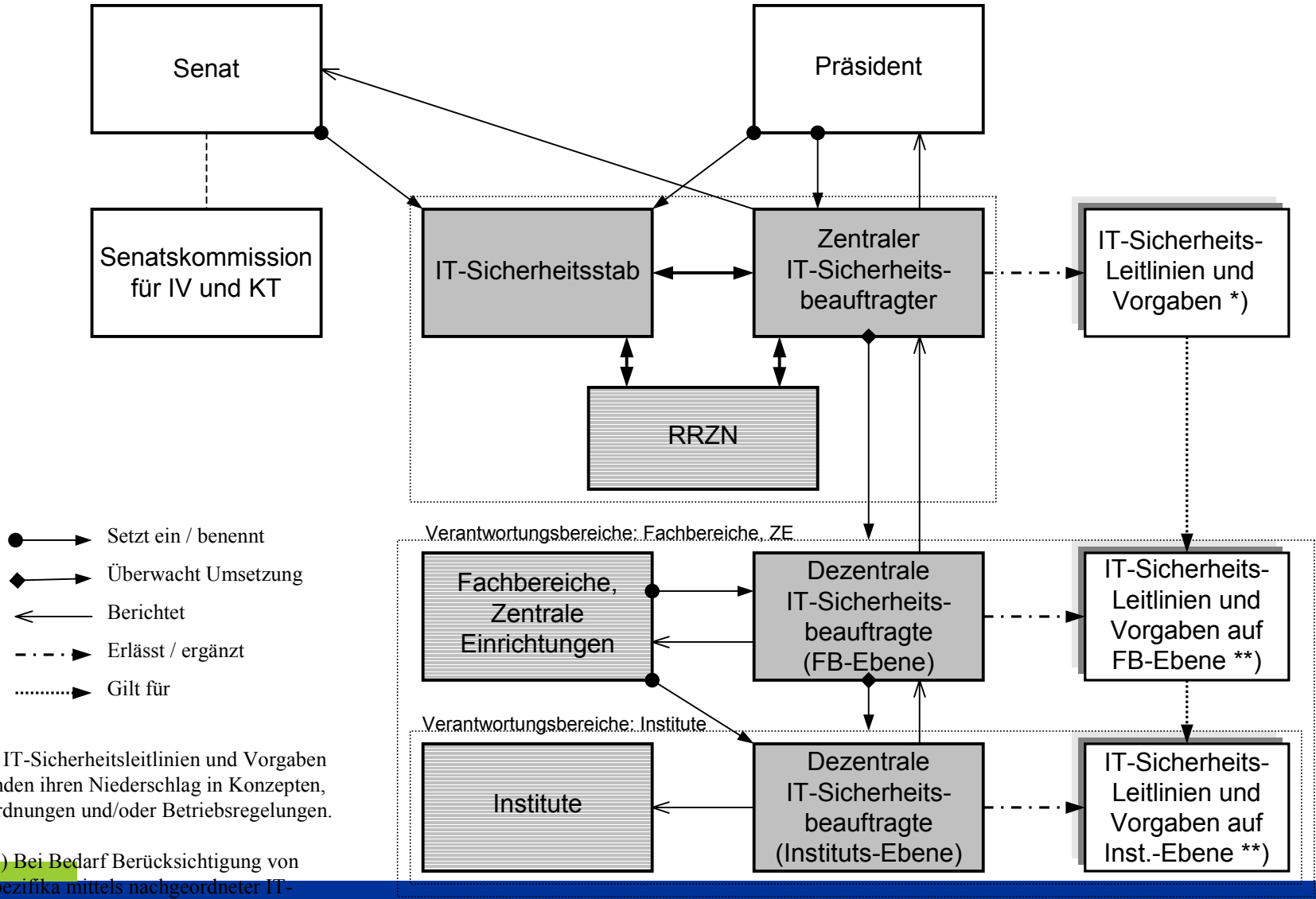
- Dezentrale IT-SB können Stilllegung von Rechnern/Systemen veranlassen
- RRZN kann Anschlüsse vorübergehend sperren
- Benachrichtigung ggfs. erst „danach“

Hinreichende Maßnahmen vor Wiederinbetriebnahme

- In Abstimmung mit dez. IT-SB bzw. RRZN
- Ggfs. Entscheidung des zentr. IT-SB

Stand: *gängige Praxis*

Verantwortungsstrukturen zur IT-Sicherheit an der UH



*) IT-Sicherheitsleitlinien und Vorgaben finden ihren Niederschlag in Konzepten, Ordnungen und/oder Betriebsregelungen.

**) Bei Bedarf Berücksichtigung von Spezifika mittels nachgeordneter IT-Sicherheitsleitlinien und Regelungen

Was ist mit der Ordnung erreicht?

R|R|Z|N

Rahmen für:

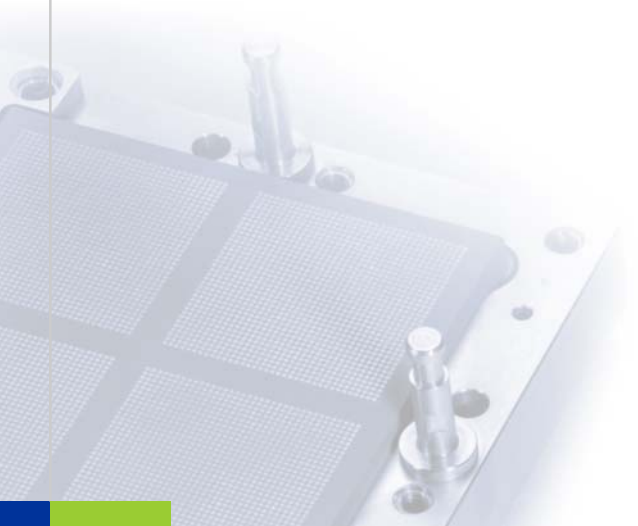
- Universitätsweiten IT-Sicherheitsprozess
- Entwicklung und Umsetzung eines realisierbaren Sicherheitskonzepts
- Vergleichbare Sicherheitsprozesse/-konzeptionen an anderen Hochschulen
  - TU Braunschweig hat Ordnung übernommen
  - An HMT Hannover bereitet Übernahme vor
  - Weitere ?

Positive Auswirkungen:

- Sicherheitsbewusstsein verbessert
- Mehr Sicherheit durch vorbeugende Maßnahmen
- bessere Arbeitsbasis für Mitarbeiter im Bereich der IT-Sicherheit

III.

Maßnahmen zur IT-Sicherheit



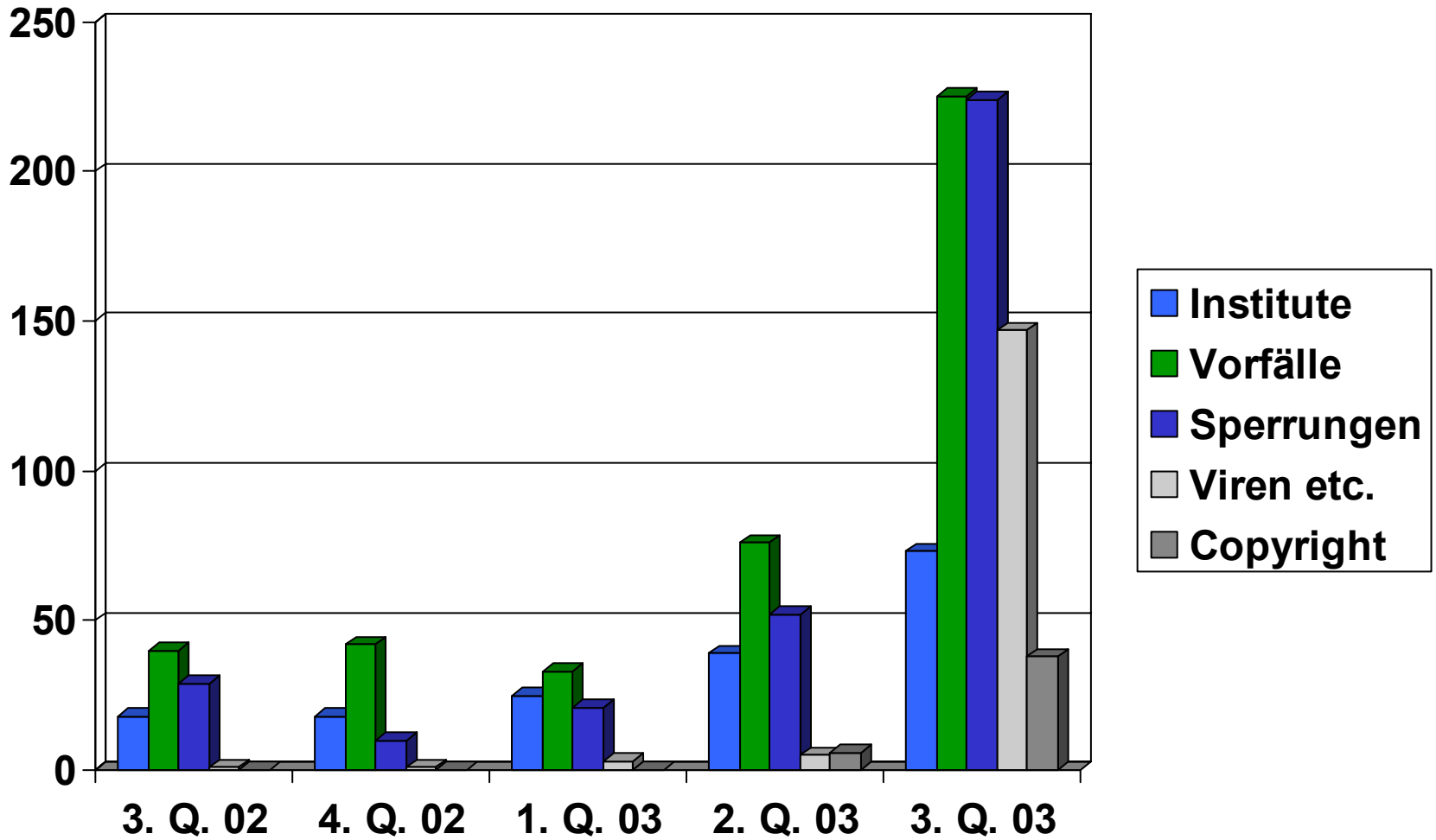
Gliederung

R|R|Z|N

1. **Sicherheitsrelevante Vorfälle**
2. **Zur Situation in Instituten**
3. **Schutz von Institutsnetzen**
   - Firewalls im Institut
   - Zentraler Netzschutz durch RRZN
4. **Weitere technische Maßnahmen**
5. **Aufbau einer Zertifizierungsinstanz**
6. **Sonstige Hilfsmittel zur IT-Sicherheit**

1. Sicherheitsrelevante Vorfälle (1)

R|R|Z|N



Sicherheitsrelevante Vorfälle (2)

R|R|Z|N

	Vorfälle insgesamt	Anzahl Institute	Anschluss-Sperrungen	davon Viren/ Würmer	davon ©-Verstöße
3. Q. 2002	40	18	29	1	
4. Q. 2002	42	18	10	1	
1. Q. 2003	33	25	21	3	
2. Q. 2003	76	39	52	5	6
3. Q.2003	225	73	224	147	38
insgesamt	**416**	**109**	**336**	**157**	**44**

Einige charakteristische Fälle

R|R|Z|N

im 2. Quartal

- Einrichtung (und Entdeckung) unauthorisierter aftp-Server
  - Einsatz für Angebot zweifelhaften Materials
- Einrichtung von Spam-Versendern
- Erste Mahnungen bezüglich Copyright-Verletzungen

im 3. Quartal

- Blaster-Epidemie ab 18.8.
- Sobig-F-Epidemie ab 25.8.
- Starke Zunahme der Mahnungen bzgl. Copyright-Verletzungen

generell

- Immer wieder flackert Code Red II auf, obwohl Epidemie schon mehr als zwei Jahre zurückliegt.

Ursachenforschung (1)

R|R|Z|N

- **Ursachen der starken Blaster-Verbreitung:**
  - Blaster verbreitet sich **nicht** über Mail-Mechanismen, kann daher auch nicht an zentralen Mail-Relays zurückgehalten werden.
  - Blaster verbreitet sich über Port 135. Da Port 135 jedoch am Übergang zwischen UH-Netz und Internet gesperrt ist, muss Blaster eingeschleppt worden sein (vermutlich über ein infiziertes Notebook).
- **Lehren:**
  - Erfordert Überlegungen, wie sich das UH-Netz vor Notebooks, die sicherheitsgefährdende Komponenten enthalten, schützen lässt.

Ursachenforschung (2)

R|R|Z|N

- **Ursachen der starken Sobig-F-Verbreitung:**
  - Sobig-F verbreitet sich über eine eigene smtp-engine, dadurch sehr rasant!
  - Vermutlich hat die Verwendung von Webmail-Accounts und damit der direkte Bezug von Mails von anderen Providern virenbehaftete Mails hereingeholt. Wenn der lokale Virenschutz nicht up-to-date ist, wird beim Öffnen der Anhänge die Verbreitung in Gang gesetzt.
- **Lehren:**
  - Lokaler Virenschutz eminent wichtig!
  - RRZN wird prüfen, ob weitere Maßnahmen möglich bzw. sinnvoll sind.
  - Anwender: Noch kritischerer Umgang mit E-Mail-Anhängen bei Mails zweifelhafter Herkunft!

Zu Copyright-Verletzungen

R|R|Z|N

Seit 2. Q. d. J. laufen Beschwerden amerikanischer Medien-Institutionen ein mit Angaben zum „wann-wie-wo“.

Da Rechte Dritter betroffen sind, drohen möglicherweise Schadenersatzansprüche gegen Verursacher sowie ggfs. auch gegen Institutsleitungen und Uni-Leitung.

Strikte Reaktion in Übereinstimmung mit dem zentralen IT-SB und in Analogie zu §8 der Sicherheitsordnung:

- betroffene Rechner/Anschlüsse werden unverzüglich gesperrt
- die Geschäftsleitung betroffener Einrichtung wird benachrichtigt u. a. mit der Bitte, die „Bereinigung“ der Rechner zu veranlassen.
- Wiederfreigabe gesperrter Rechner/Anschlüsse erfolgt nur auf ausdrücklichen Wunsch der Geschäftsleitung.

- **Die Anzahl der Fälle hat inzwischen wieder abgenommen!**

Im Falle eines Falles…

R|R|Z|N

Ruhe bewahren – und keine Zeit verlieren !

Wenn möglich: Aktuelle Informationen auf Security-Seiten des RRZN prüfen (http://www.rrzn.uni-hannover.de/Security/)

zuständigen IT-Sicherheitsbeauftragten benachrichtigen

RRZN benachrichtigen (kurze E-Mail an security@rrzn.uni-hannover.de)

ggfs. betroffenes System vom Netz trennen

Typische Sicherheitsmängel:

- **Einsatz veralteter Betriebssoftware**
- **Einsatz von Betriebssystemen ohne Benutzer-Administration**
- **Rechner laufen ohne Betreuung**
- **Rechner bieten nicht benötigte Dienste**
- **Rechner/Dienste, die nur intern verwendet werden, sind von außen zugänglich**
- **Gefahrenträchtige Softwarekonstellation**

Empfehlungen zur Abhilfe

R|R|Z|N

Umsetzung der Sicherheitsordnung im Institut:

IT-Sicherheit ist Chefsache**!**

Mitarbeiter(inne)n muss bekannt sein, wer zuständiger dezentrale IT-SB ist

für jede IT-Komponente muss Betreuer/in und zuständige/r dez. IT-SB festgelegt sein

- es darf keine nicht-zugeordneten und „unbewachten“ Komponenten geben!

Netzstruktur: Konfigurationsskizze!

Tabelle der IT-Ausstattung, für jedes System:

- Hardware- / Software- / Netzkomponenten
- Aufgabenstellung / erforderliche Dienste
- Kommunikationsbeziehungen / Erreichbarkeit:
  - Institutsintern / UH-Netz / Internet
- Betreuer

Schutzbedarf, Schutzziele

Verbesserungsmöglichkeiten

R|R|Z|N

Rechner-/Netzkonfiguration / Aufgabenspektrum / Softwarekonstellation prüfen und ggfs. ändern:

- **Nur Betriebssysteme mit Benutzer-Administration und in aktueller Version einsetzen! (A-Rundschreiben der UH)**
  - Sicherheitsproblematische Systeme ausschließlich intern bzw. ohne Verbindung zum UH-Netz einsetzen
- **interne Aufgaben nur auf Rechnern, die von außen nicht zugänglich sind**
- **Alle nicht benötigten Dienste abschalten (kein „automatische“ Installation)**
- **Unterstützungsmöglichkeit durch RRZN berücksichtigen (derzeit Solaris, Linux, Windows NT/2000/XP)**
  - ggfs. auf Servern, die von außen erreichbar sein müssen (WWW, Mail), Systeme einsetzen, für die RRZN im Ernstfall Unterstützung leisten kann.

Backup-Konzept

- Regelmäßige Datensicherung!
- individuelle Sicherung auf Datenträger vs. auf Server
  - Datenträger nicht im Rechner lassen! (Verlustgefahr!)
- ggfs. Sicherung von Servern auf RRZN-Archivsystem

Für Ernstfall *vorab* u. a. klären:

Wer/wie ist zu benachrichtigen?

Konsequenzen einer (massiven) Störung?

Datenträger mit Original-Software verfügbar?!

Restore-Prozedur praktisch(!) bekannt?

Aufklärung / Sensibilisierung der Anwender

R|R|Z|N

Sicherheit kann nicht ohne sicherheitsbewusstes Verhalten der Anwender erreicht werden!

Verhaltensempfehlungen für Anwender erforderlich, z. B.

- zum Passwortgebrauch
- zu Einsatz und Update von Anti-Viren-Software
- zum Internet-Gebrauch (u. a. Web, Mail)
- "Werbung": nur die Regeln greifen, die akzeptiert werden!
- Wer zu benachrichtigen bei auffälligen Vorkommnissen?

darum auch RRZN-Kurs „Sicherheit für Anwender“

- Verbreitung der Informationen in den Fachbereichen durch dezentrale IT-SB als Multiplikatoren vorgesehen
- Vermittlung von Institutsspezifika ist naturgemäß Sache der Institute!

Möglich durch Einsatz von Firewall-Technik

- Erlauben/Verbieten von Kommunikation
- durch Regeln verbindlich für das gesamte Institutsnetz und alle angeschlossenen Rechner

Realisierung durch den Einsatz von Firewall-Systemen (FWS)

- FWS im Institut
- Personal Firewall ?
- zentraler Netzschutz (FWS im RRZN)

Systeme zum Erlauben/Ablehnen von Kommunikationsverbindungen

Steuerung durch Regelsätze u. a.

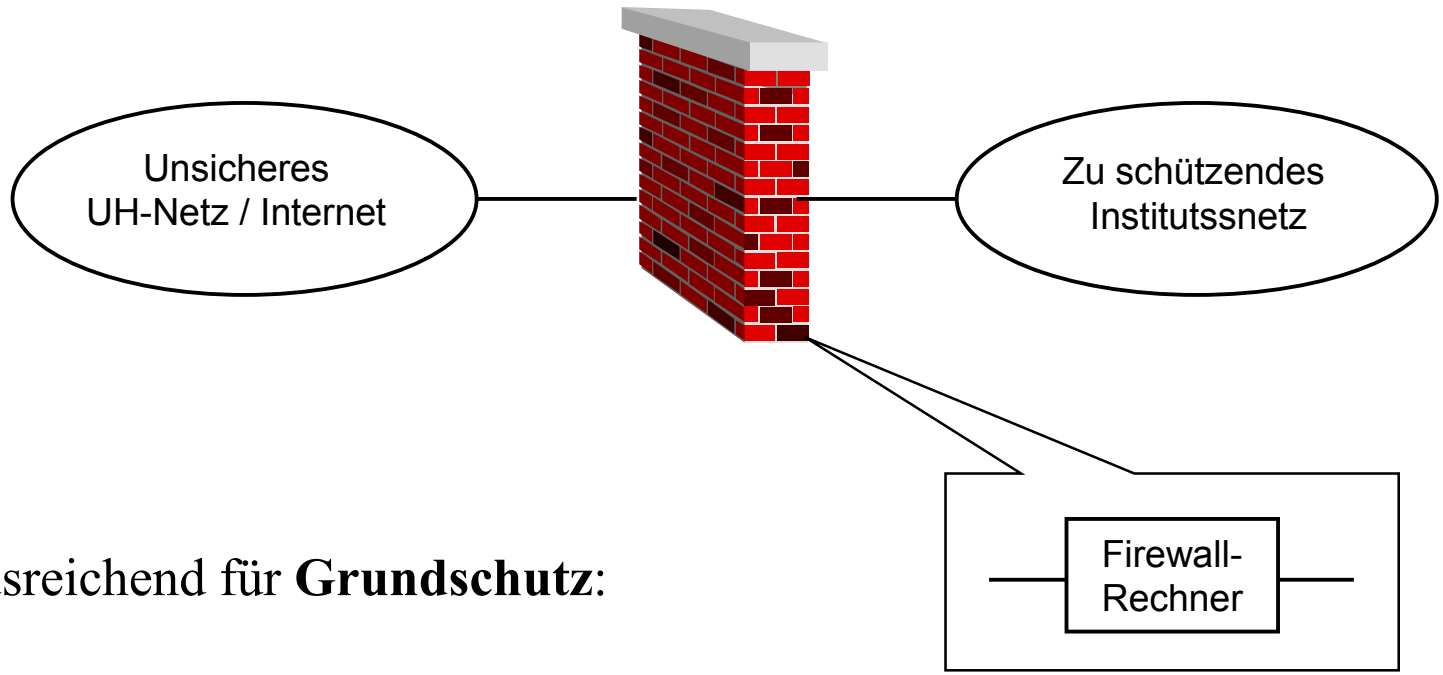
- verbindungsbasiert (IP-Adressen, Ports, Richtung)
- dienstebasiert (z. B. telnet, http, smtp, ftp)
- benutzerbasiert
- zeitbasiert

Maxime: „Es ist alles verboten, was nicht explizit erlaubt ist“

Viele unterschiedliche Firewall-Systeme (FWS):

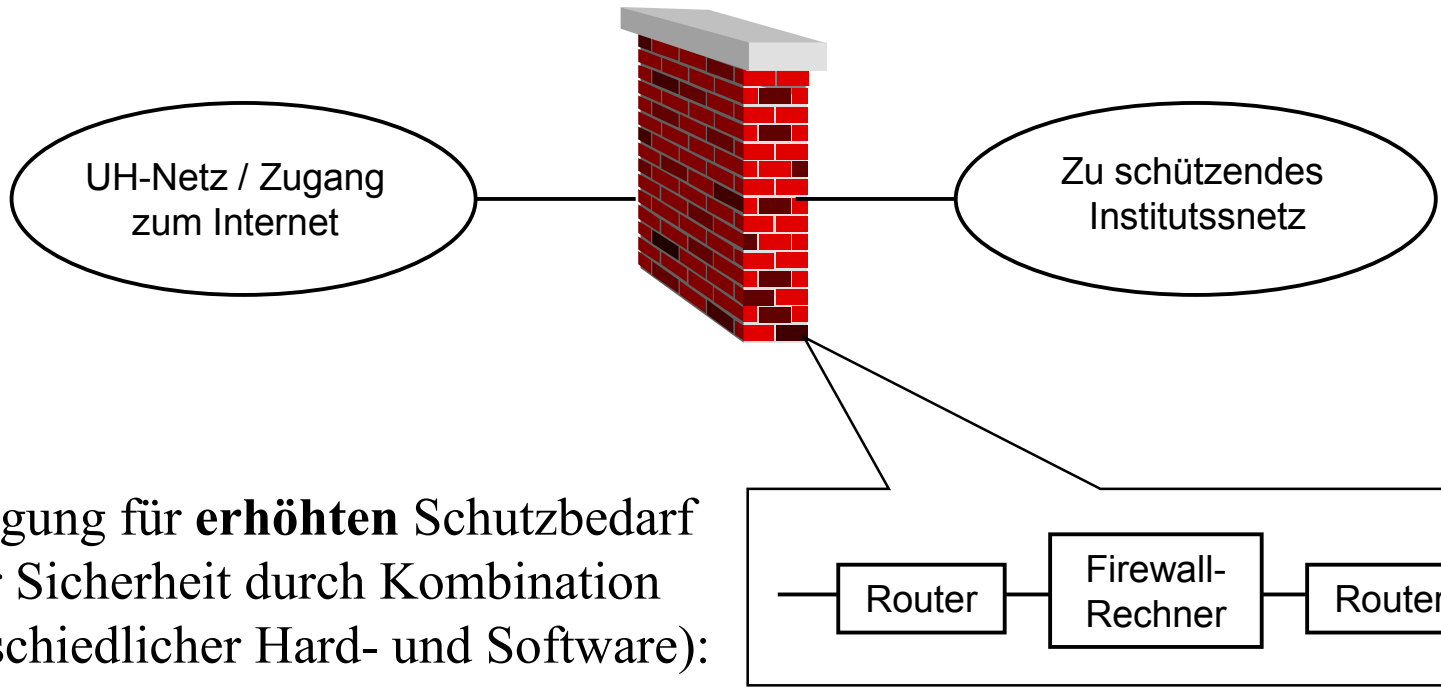
- **Proprietäre Hardware/Software, beispielsweise**
  - Router mit Firewall Feature Set (Cisco)
  - PIX-Firewall (Cisco)
- **Standard-Hardware (PC oder Unix-Workstation) mit Firewall-Software, beispielsweise**
  - Linux-PC mit Linux-FW-Software (iptables)
  - Solaris-WS mit Firewall-Software von Checkpoint

Einstufiges FWS



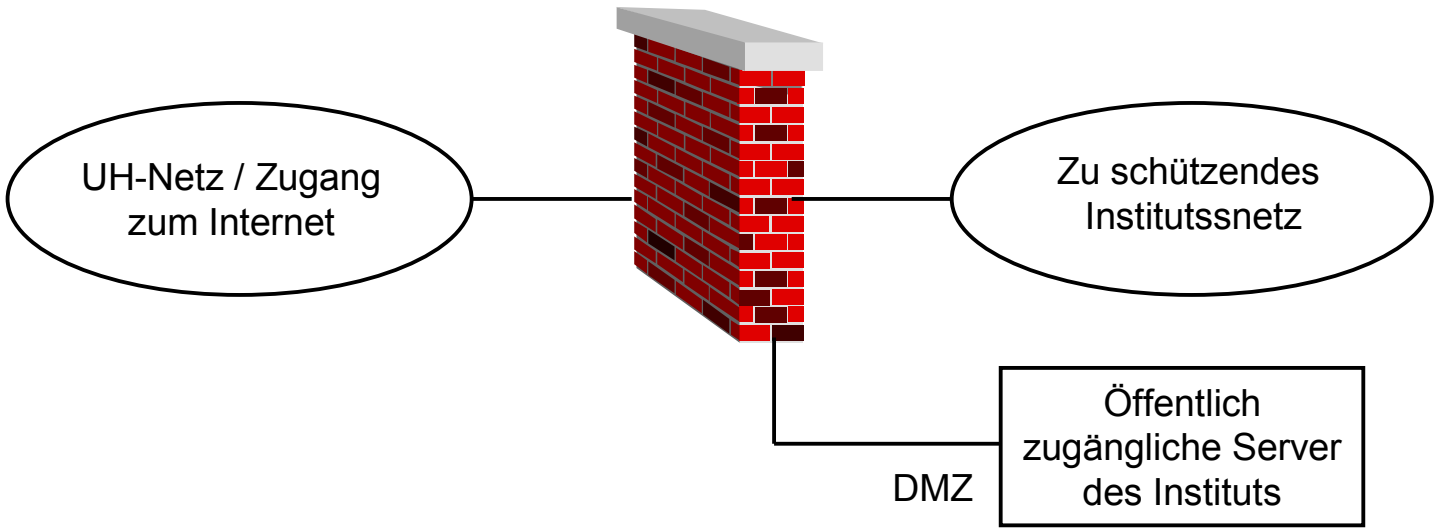
Ausreichend für **Grundschutz**:

Zweistufiges FWS



Auslegung für **erhöhten** Schutzbedarf (mehr Sicherheit durch Kombination unterschiedlicher Hard- und Software):

FWS mit DMZ (demilitarisierte Zone)



Möglichkeit zum Fernhalten des öffentlichen Verkehrs vom „eigentlichen“ Institutsnetz

FWS: Pflege erforderlich!

R|R|Z|N

Regeln sind auf aktuellem Stand zu halten bzw. sich ändernden Konstellationen anzupassen!

- Regelsatz muß „widerspruchsfrei“ sein!
  - Sorgfältige Administration erforderlich!

Firewall-Software muss aktuell gehalten werden

regelmäßige Log-Analyse erforderlich (täglich?!)

- „Firewall kann keine Angriffe verhindern, aber dazu beitragen, daß sie nicht unerkannt bleiben“

ohne Pflege kann FWS Schutzwirkung verlieren

Wovor kann FWS **nicht** schützen?

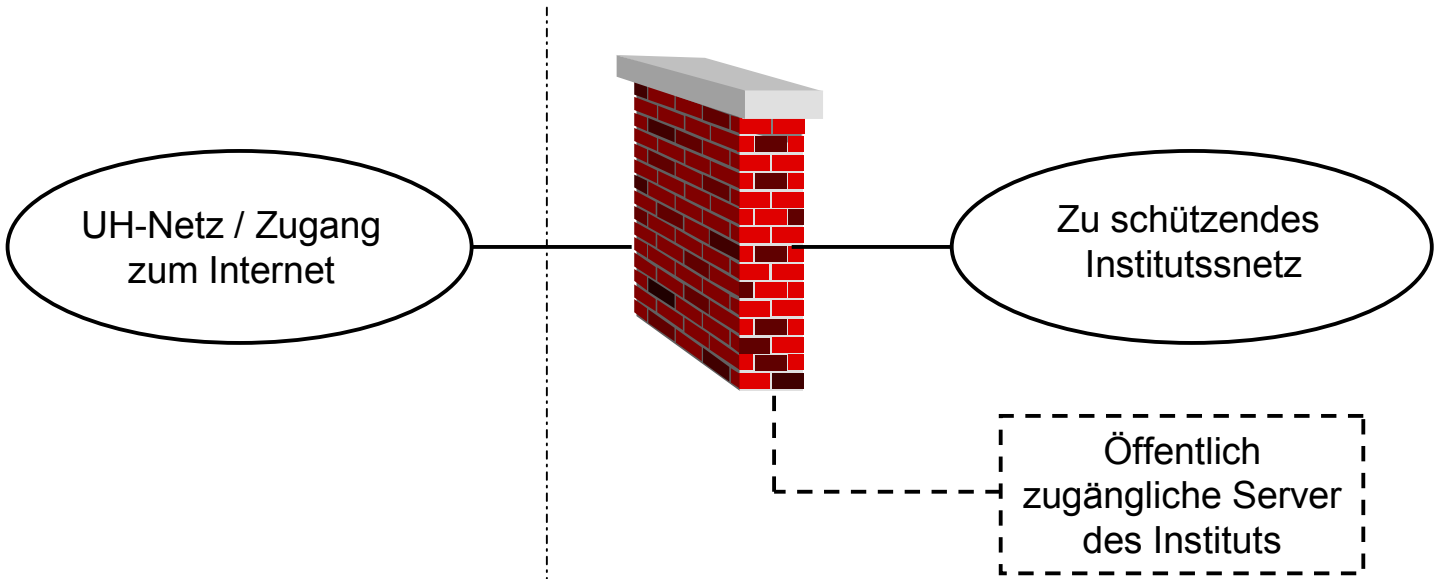
R|R|Z|N

Keinerlei Schutz vor „importierten“ Angriffen!

- Gefahr durch E-Mail-Attachments
- Gefahr beim „Surfen“ durch „aktive“ Web-Inhalte
  - Java, Javascript und Active-X deaktivieren!
- Unkontrollierte Änderungen an Systemen vermeiden!
- Disziplin der Anwender erforderlich!

➔ Aktivitäten, die **scheinbar legal** erfolgen (inkl. Manipulationen am FWS selbst) können vom FWS nicht verhindert werden!

FWS im Institut



sichert Rechner**, kein Netz**

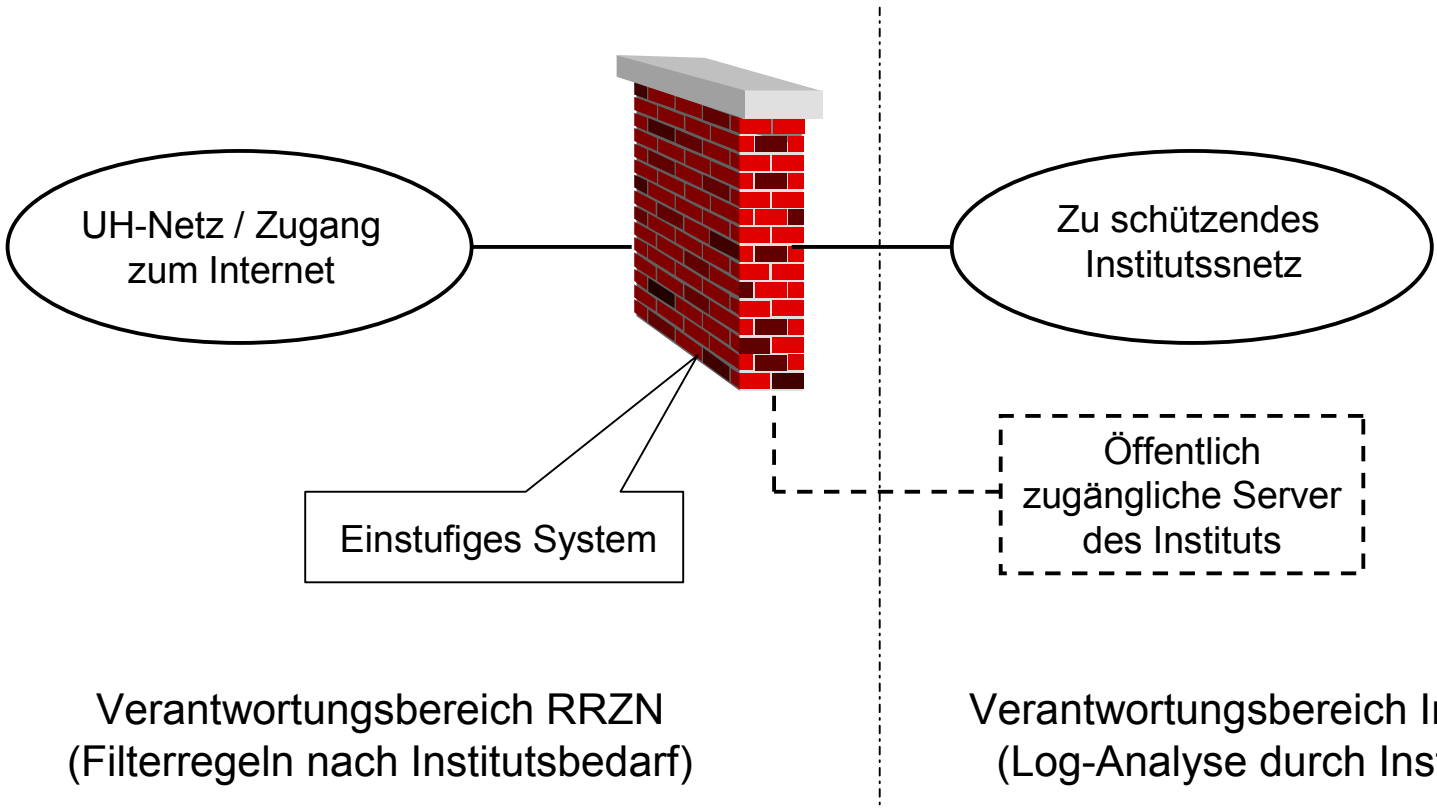
zur Sicherung eines Institutsnetzes **daher nicht geeignet**

- allenfalls professionelle Versionen mit zentraler Administration verwenden, damit die Regeln institutsweit unter Kontrolle sind
- aber **zusätzlich** zu bestehendem FWS nützlich

als Sofortmaßnahme **geeignet („besser als nichts“)**

gut geeignet für häusliche PCs

Zentraler Netzschutz durch RRZN (1)



Zentraler Netzschutz durch RRZN (2)

R|R|Z|N

RRZN betreibt einstufiges FWS im RRZN

Institut kann sich hinter FWS schalten lassen

- Institut definiert Anforderungen
- RRZN überträgt dies in Regeln und administriert
  - zukünftig ev. Auswahl aus „Standard-Regelsätzen“
- Institut kontrolliert Logs

Vereinbarung mit Institut

Kostenlos für Institute der UH

Vergleich der Alternativen

R|R|Z|N

	FWS im Institut	Zentraler Netzschutz
Schutz-niveau	■Grundschutz oder höher ■FWS: Auswahl d. Institut	■Grundschutz ■FWS: „RRZN-Standard“
Vorteile	■Schutz individueller ■flexibler bei Änderungen	■Aufwand für Institut geringer ■Kostenlos
Nachteile	■Know How erforderlich ■Administrationsaufwand ■finanzieller Aufwand	■Änderungen: weniger flexibel ■Regeln eher pauschal

Derzeitiger Status

- **In Betrieb bei 7 Instituten**
- **In Arbeit mit 11 weiteren Instituten**
- **Nach einem noch für 2003 zugesagtem Software-Update steht für den zentralen Netzschutz ein leistungsfähigeres und flexibleres Firewall-Modul zur Verfügung.**

- **bei Interesse Mail an security@rrzn.uni-hannover.de unter folgenden Randbedingungen:**
  - Der zentrale Netzschutz ist derzeit noch kein Standard-Service
  - Ihr Wunsch wird entgegen genommen, und Realisierungsmöglichkeiten werden geprüft (eine Bearbeitung „in Reihenfolge der Eingänge“ kann nicht zugesichert werden).
  - In jedem Fall ist Mitwirkung des Instituts erforderlich

Sicherheitsbewusste Systemadministration

Virenschutz

Verschlüsselung

- für Dialogzugriff und Dateiübertragung
- in Kommunikationsnetzen

Systeme „härten“

- keine „automatische“ Installation
- alle unbenötigte Dienste entfernen
- alle Guest-Accounts sperren
- etc. etc.
- auf RRZN-Securityseiten einschlägige Hinweise für Windows XP

Systempflege

- Systeme auf aktuellem Level halten
- Security patches einbringen
- RRZN prüft derzeit Möglichkeiten für einen zentralen Update-Service

Antiviren-Software

R|R|Z|N

- **Auf zentralen Mailgateways Antivirensoftware von McAfee**
  - Täglich vollautomatisches Update
- **Für PCs in Instituten**
  - Neuer Landeslizenzvertrag mit Fa. Sophos bis 31.10.2006
  - Erweiterung der Produktpalette (wird automatisches Update auch für Arbeitsplatzrechner ermöglichen)
  - Kostenlose Nutzung für Angehörige der UH
  - Einsatz auf häuslichen Rechnern für nicht kommerzielle Zwecke erlaubt
- **Lokaler Schutz auf PCs dringend erforderlich, da sonst kein Schutz insbesondere vor Viren, die sich nicht über Mails verbreiten (siehe Blaster & Co).**

Neues Vorgehen bezüglich E-Mails?

R|R|Z|N

Die Anzahl virenbehafteter Mails wächst ständig. Viele Mails bestehen ausschließlich aus dem verseuchten Anhang. Nach dessen Entfernung ist die Mail inhaltslos.

Bisher:

- Virenbehaftete Anhänge werden gelöscht, die modifizierte Mail zugestellt

Derzeit Überlegungen:

- Mails, die Viren enthalten, werden komplett abgewiesen (d. h., es folgt auch keine Benachrichtigung mehr)
- Mails mit Anhängen, deren Extensions darauf hindeuten, dass es sich um direkt ausführbare Programme handelt, werden komplett abgewiesen

- **RRZN wird konkreten Vorschlag erstellen, Hochschulleitung wird entscheiden**

Verschlüsselung

R|R|Z|N

Zur Sicherung von Daten gegen Einsichtnahme und/oder Manipulation seitens Unbefugter

Die insgesamt erreichbare Sicherheit hängt (neben Algorithmen und Schlüssellängen) ab von der Ebene, auf der verschlüsselt wird:

- über Verschlüsselungsebene hinaus kein Schutz
- Maximaler Schutz auf Anwendungsebene (setzt entsprechende Anwendungsprodukte voraus!)

Verschlüsselung kann für andere Sicherheitsmaßnahmen kontraproduktiv sein (z. B. für zentrale Viren- oder Content-Prüfungen)

Verschlüsselungsverfahren (1)

R|R|Z|N

Symmetrisch

- Ein **Schlüssel zum Ver- und Entschlüsseln**
- **Schlüssellänge derzeit ca. 128 – 196 bit**
- **Problem: Schlüsselübertragung über „unsicheres Gelände“**

Asymmetrisch

- **Ein** Paar **von Schlüsseln („privat“ und „öffentlich“), die über eine „Einwegfunktion“ zusammenhängen**
  - Nur zwei relevante Einwegfunktionen bekannt:
    - Faktorisierung von Primzahlen
    - Diskreter Logarithmus ($g^x \equiv M \pmod p$)
- **Verschlüsselte Nachrichten können nur mit dem „anderen“ Schlüssel entschlüsselt werden**
- **Aufgrund größerer Schlüssellängen (derzeit 1024 – 2048 bit) vergleichsweise langsam**

Hybride Verfahren

- Verschlüsselte Verbindung wird mit asymmetrischem Verfahren aufgebaut
- es folgt Vereinbarung bzw. verschlüsselte Übertragung eines Schlüssels für symmetrische Verfahren („session key“)
- anschließend symmetrisch und damit wesentlich performanter weiter

Einsatz verschlüsselter Verbindungen

R|R|Z|N

Dialogzugriff zu RRZN-Compute-Servern nur über *ssh* (secure shell) möglich

- ssh-Einsatz wird auch für Institutssysteme empfohlen (Kurs am 21.11.)

Dateiübertragung von/zu RRZN-Servern weitgehend nur per *sftp* möglich

- Bei Performanceproblemen können auch Spezialentwicklungen eingesetzt werden (beispielsweise nur Passwortverschlüsselung)

im Kommunikationnetz bei Aufbau von VPN- und WLAN-Verbindungen

Zur flexiblen Nutzung auf Anwendungsebene muss die Zugehörigkeit eines Schlüsselpaares zum Schüsselinhaber (Person oder Rechner) von einer Zertifizierungsstelle bestätigt sein.

5. Aufbau einer Zertifizierungsinstanz (1)

Dient der Zertifizierung von Schlüsseln für asymmetrische Verschlüsselungsverfahren

- **Damit zwei grundsätzliche Anwendungsmöglichkeiten**
  - Digitale Signatur: Die Authentizität eines Dokuments kann sichergestellt werden
  - Verschlüsselte Übertragung von Dokumenten: Es kann sichergestellt werden, dass ausschließlich der Besitzer des privaten Schlüssels das Dokument entschlüsseln kann.
- **Erforderlich: Bestätigung der zweifelsfreien Zuordnung einer Person oder eines Rechners zu einem Schüsselpaar**
- **Dies leistet eine „CA“ (Certification Authority)**

Aufbau einer Zertifizierungsinstanz (2)

R|R|Z|N

An RRZN für UH im Aufbau

Web-Interface für Benutzer

- Antragsstellung inkl. Schlüsselerzeugung
- Schlüsselverwaltung (z. B. Zertifikatswiderruf)

Persönliche Identifizierung notwendig

Zertifikate nach X.509

Bis auf weiteres Dienst-“Angebot“

- Moderate Nutzung erwartet (Erfahrung an anderen Unis)

Aufbau einer Zertifizierungsinstanz (3)

R|R|Z|N

Status:

- **CA-Rechnerkonfiguration läuft**
- **Policy demnächst in UH verabschiedet**
- **Dann Zertifizierung durch DFN-PCA (in Hamburg)**
- **Anschließend Betriebsaufnahme (möglichst noch im Frühjahr 04)**
- **Spezielle Veranstaltung zur Einführung vorgesehen**

Security-Seiten des RRZN

http://www.rrzn.uni-hannover.de/Security/

- aktuelle Warnhinweise
- Informationen für Anwender u. Administratoren
- div. Downloads (Antivirensoftware, ssh)
- Sicherheits-Checks bzw. Selbsttests
- sonstige Tools, z. B. TCP-Wrapper für Unix-Systeme
- Anleitung „Maßnahmen nach einem Hacker-Einbruch“
  - für Unix-Systeme (für Windows geplant)
- Papiere der Sicherheitstage
- Hinweise für häusliche PCs
- wichtige Links
- etc. etc.

Nachdruck von sicherheitsbezogenen Büchern des Herdt-Verlags

- Internetworking: Sicherheit
- Computersicherheit im Internet für Anwender
- Windows 2000 – Sicherheit im Netzwerk

Für UH-Angehörige in der Auskunft des RRZN erhältlich

Dienstleistungskatalog (1)

R|R|Z|N

- **Im Dienstleistungskatalog des RRZN**
  http://www.rrzn.uni-hannover.de/dienstleistungskatalog/dlk.pdf
  sind die Dienstleistungen des RRZN aufgeführt
- **Einträge enthalten eine Kurzbeschreibung des Angebots, das angestrebte Ergebnis sowie die entsprechenden Kontaktpersonen**
- **Dienstleistungen zur IT-Sicherheit:**
  - 1051: Beratung zum Einsatz von Sicherheitsmaßnahmen
  - 1052: Beratung zur Analyse und Behebung von sicherheitsbezogenen Störfällen
  - 1053: Beratung zum Einsatz von Verschlüsselungssoftware

Dienstleistungskatalog (2)

R|R|Z|N

- 1054: Beratung zu Planung und Einsatz von Firewall-Maßnahmen
- 1055: Installation und Konfiguration von Sicherheitsmaßnahmen
- 1056: Unterstützung bei Analyse und Behebung von sicherheitsbezogenen Störfällen
- 1057: Durchführung von externen Sicherheitsüberprüfungen
- 2078: Entwicklung eines Sicherheitskonzepts für ein Funknetz nach IEEE 802.11

Web-Adressen zur IT-Sicherheit

R|R|Z|N

www.rrzn.uni-hannover.de/Security/: Security-Seiten des RRZN, darüber auch:

www.bsi.bund.de: Bundesamt für Sicherheit in der Informationstechnik (u. a. Grundschutzhandbuch!)

www.cert.dfn.de: DFN-CERT (Dokumente, Tools)

www.cert.org: CERT Coordination Center (CCC)

www.lfd.niedersachsen.de: Landesbeauftragter für Datenschutz Niedersachsen (u. a. Checklisten)

www.ietf.org/rfc/rfc2196.txt: "Site Security Handbook"

Security-Seiten der Hersteller

Rückkopplung erbeten !

- zur Weiterentwicklung des Sicherheitsprozesses
- zur Erstellung praxisnaher Dokumente
- zur Optimierung künftiger Veranstaltungen

Programm Sicherheitstage WS 03/04

R|R|Z|N

Fr: - **IT-Sicherheit in der Universität Hannover**

Mo: - **Sicherheit in Unix-Systemen**

Di: - **Sicherheit in Windows-Systemen**

Mi+Do:

- **Sicherheit von Netzwerkservern in heterogenen Umgebungen**

Fr: - **Sicherheit für Anwender**

- **ssh etc.**