Sicherheitstage RRZN Universität Hannover SS 2005

6. Juni 2005

Prof. Dr. Michael H. Breitner
(breitner@iwi.uni-hannover.de)

Übersicht dieses Vortrages

- **Persönliches**
- **Informationssysteme**
- Einführung in die **Informations- und Datensicherheit** und die zugehörigen **Strukturen** an der **Universität Hannover**
- **Probleme** und **Maßnahmen** an der **Universität Hannover**

www.iwi.uni-hannover.de/professor.html

Institut für Wirtschaftsinformatik der wirtschaftswissenschaftlichen Fakultät der Universität H - Microsoft Internet Explorer

Institut für Wirtschaftsinformatik
der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

- Home
- Wir
  - Mitarbeiter
  - Adresse/ Anfahrt
- Lehre
- Forschung
- Publikationen
- Tagungen
- Service
- IT-Sicherheits-beauftragter
- Sitemap
- Impressum

Suchen

Forschungsschwerpunkte · Publikationen · Curriculum Vitae

Prof. Dr. Michael H. Breitner

Telefon: (0511) 762 4901 oder 0173 3895801 (mobil)
Raum: I-453
Sprechstunde: Dienstag 15 - 18 Uhr und gerne auch nach Vereinbarung (Email)
Email: **breitner@iwi.uni-hannover.de**
Anschrift: Institut für Wirtschaftsinformatik, Universität Hannover, Königsworther Platz 1, D-30167 Hannover

Forschungs- und Beratungsschwerpunkte:

- Geschäftsmodelle und Kosten/Nutzen-Analysen im E- und M-Business, z. B. für E- und M-Learning und Preisvergleichsdienste
- Künstliche Intelligenz, insbes. Künstliche Neuronale Netze und Neurosimulator FAUN
- Softwareengineering und Rapid Application Development (RAD)
- Intra- und Internetanwendungen, z. B. Software-Agentensysteme
- Hoch- und Höchstleistungsrechnen (HPC)
- E-Learning Anwendungen und Multimedia, insbes. UbiLearn System
- Informations- und Kommunikationssysteme, z. B. WARRANT-PRO 1 und 2 für Finanzdienstleister
- Ubiquitous Computing ("allgegenwärtiges" Rechnen)
- Operations Research, z. B. Optimierung und dynamische Spiele, sowie mathematische Modellierung und Simulation
- Wissenschaftsgeschichte, -theorie und -ethik sowie Futurologie und Technologiefolgenabschätzungen

Werdegang: Geboren 1963 in **München**; Abitur 1983; Nach der Bundeswehr (Z2 und RO) 1984 bis 1990 Studium der Mathematik mit Wirtschaftswissenschaften an der **TU München**; Diplomarbeit im **Deutschen Zentrum für Luft- und Raumfahrt (DLR), Oberpfaffenhofen** 1989 bis 1990; 1990 bis 1995 wissenschaftlicher Mitarbeiter an der TU München; 1995 Wechsel an die **TU Clausthal** und Promotion zum Dr. rer. nat. (Mathematik); 1996 - 2002 Lehrbeauftragter für **Mathematik** und **Informatik**; 1997 bis 2002 Akad. Rat; 2001

www.iwi.uni-hannover.de/it-sicherheitsbeauftragter.html

Institut für Wirtschaftsinformatik der wirtschaftswissenschaftlichen Fakultät der Universität H - Microsoft Internet Explorer

Institut für Wirtschaftsinformatik
der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

- Home
- Wir
- Lehre
- Forschung
- Publikationen
- Tagungen
- Service
- IT-Sicherheits-beauftragter
- Sitemap
- Impressum

Suchen

Zentraler IT-Sicherheitsbeauftragter

Aktuelles

Sicherheitstage im WS 2004/2005, 22.-24. November 2004, RRZN: Download **Vortragsfolien Breitner (PDF-Datei color, 5,2 MB)** und **Vortragsfolien Breitner (PDF-Datei sw, 3,3 MB)**.

Prolog

Am 10. Juli 2002 beschliesst der Senat der Universität Hannover die

Ordnung zur IT-Sicherheit in der Universität Hannover.

"IT" steht für Informationstechnologie, d. h. technische Komponenten sowohl in Informations- als auch in Kommunikationssystemen aller Art. Anfang 2003 ernennt der Präsident der Universität Hannover **Herrn Prof. Dr.-Ing. Rudolf Damrath** zum ersten zentralen IT-Sicherheitsbeauftragten, dessen Aufgaben und Befugnisse in der Ordnung zur IT-Sicherheit festgelegt sind. Am 26.11.2003 ernennt der Präsident der Universität Hannover **Herrn Prof. Dr. Michael H. Breitner** zum neuen zentralen IT-Sicherheitsbeauftragten. Alle **zentralen Beauftragten** unterstützen die Hochschulleitung direkt, z. B. durch Empfehlungen oder/und regelmäßige Berichte oder/und unregelmäßige Berichte im Bedarfsfall.

Bedeutung der IT-Sicherheit bzw. Informations- und Datensicherheit

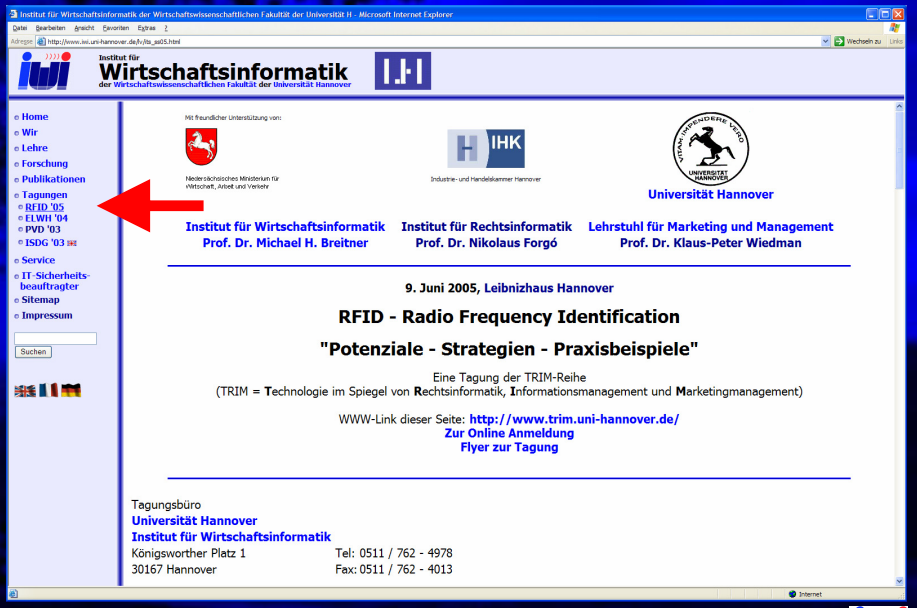
Statt der IT-Sicherheit sollte besser ganzheitlich die "Sicherheit von Informationssystemen" bzw. kurz die "Informations- und Datensicherheit" adressiert werden. Informationssysteme sind soziotechnische Systeme, zu deren Komponenten einerseits technische Geräte (z. B. Rechner und Netzwerke) zählen, zu denen andererseits aber auch die Menschen gehören, die diese Geräte nutzen. Zu den Informationssystemen werden heute meist auch die Kommunikationssysteme gezählt, da eine rapide technologische Konvergenz zu beobachten ist (z. B. IP-Telefonie, Internet-Videokonferenzen, MDAs und Smartphones usw.). Informations- und Datensicherheit bedeutet allgemein die Sicherstellung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Nachrichten, von Programmen sowie von Diensten. Einen guten Überblick über Informations- und Datensicherheit liefert der

Leitfaden IT-Sicherheit: IT-Grundschutz kompakt

des **Bundesamtes für Sicherheit in der Informationstechnik (BSI)**, vgl. auch ein **Interview mit dem BSI-Präsidenten Dr. Udo Helmbrecht** der Zeitschrift **Wirtschaftsinformatik** und die **European Network and Information Security Agency (ENISA)**. Alternativ

www.iwi.uni-hannover.de/lv/its_ss05.html

www.iwi.uni-hannover.de/trim



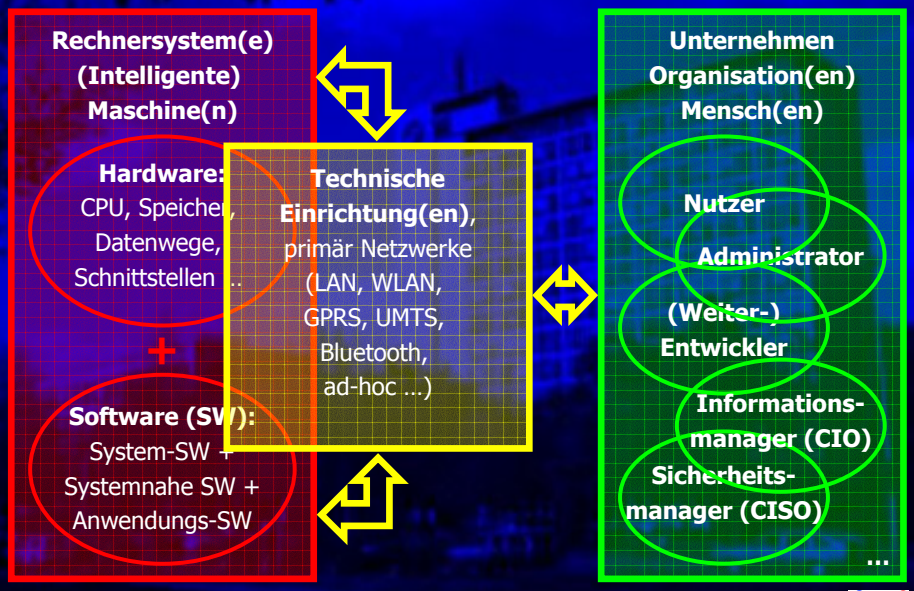
Übersicht dieses Vortrages

- **Persönliches**
- **Informationssysteme**
- Einführung in die **Informations- und Datensicherheit** und die zugehörigen **Strukturen** an der **Universität Hannover**
- **Probleme** und **Maßnahmen** an der **Universität Hannover**

Prolog

- Deutschland ist heute eine **Informationsgesellschaft** (und **Dienstleistungsgesellschaft**), d. h. **Informationen** sind zum **Produktionsfaktor Nummer 1** geworden
- Die Universität Hannover muß sich heute an privaten Unternehmen messen lassen, u. a. muß über „**Outsourcing**" und „**Outtasking**" im Großen und Kleinen nachgedacht werden:
  - Wichtigstes Ziel erfolgreicher Unternehmen ist heute **Kundenzufriedenstellung** und **Kundengewinnung**
  - **Kunden** sind Studierende, öffentliche Einrichtungen, privatwirtschaftliche Unternehmen und „die Gesellschaft"
  - Es resultieren sekundäre Ziele wie **Qualitätssicherung** und **-verbesserung**, **gutes Aufwand-/Ertrags-** bzw. **Kosten/Nutzen-Verhältnis**, **Effizienz**, **Effektivität**, ...

Prinzipieller Aufbau eines Informationssystems



Prolog

- **Permanente** und **hochzuverlässige**, **leistungsfähige Kommunikation** und **Informationsverarbeitung** (Beschaffung, Verarbeitung, Verbreitung und Speicherung) ist kein Wettbewerbsvorteil mehr sondern eine „**Conditio sine qua non**", um Informationen als Produktionsfaktor bei der **Leistungserbringung** (Lehre, Forschung und „Beratung") der Universität Hannover bereitzustellen
- **Informationsverarbeitungs-** und **Kommunikations-systeme wachsen zusammen**, vgl. z. B. globale IP-Telefonie neben Chats und Email, Videokonferenzen, MS Messenger oder Daten-übertragung mit GPRS, UMTS, ...

Trends & Technologiefolgenabschätzung:

Mobile IP-Telefonie durch weitverbreitete WLANs

COMPUTER ZEITUNG

Die Website für die Informationsgesellschaft

Elektroingenieur — Finden Sie den Job Ihres Lebens.

Über uns | Kont

Suchen

[Home] - [Artikelsuche] - [IP-Telefonie kommt mit Bildübertragung] [Fachartikel]

Home

CZ Aktuelle Ausgabe
Aktuelle Meldungen
Thema dieser Woche
Kommentar der Woche
Highlights
Heftinhalt
Leserbriefe

Serie: Rentabilität der IT-Ausgaben

CZ im Internet
Audio-Beiträge
Artikelsuche
Web-Tipp
Marktübersichten

Schrittweise Migration etabliert sich bei der Netzkonvergenz

IP-Telefonie kommt mit Bildübertragung

Voice over IP gewinnt an Akzeptanz: Bis 2007 soll dieser Markt laut Infonetics Research um jährlich über 40 Prozent wachsen. Mit Video-funktionalität werden die-se Kommunikationssysteme künftig multimedial.

Mit Nokias Communicator 9500 kann man per per GSM und WLAN surfen. Foto: Nokia

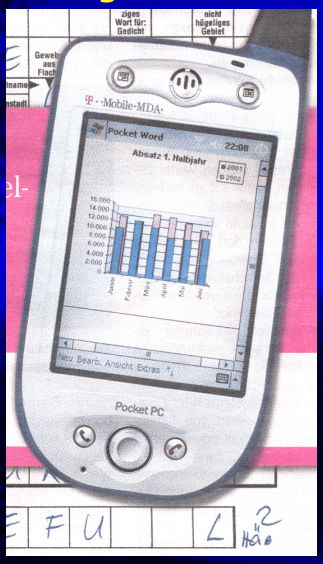
Auch die Integration der Telefonie in die wie Pilze aus dem Boden sprießenden WLANs dürfte die Verbreitung von Voice over IP unterstützen. Mit dem Communicator 9500, dem ersten Handy-Organizer, der über Funk-netztechnik verfügt, springt Nokia (Halle 26, Stand E68) jetzt auf diesen Zug.

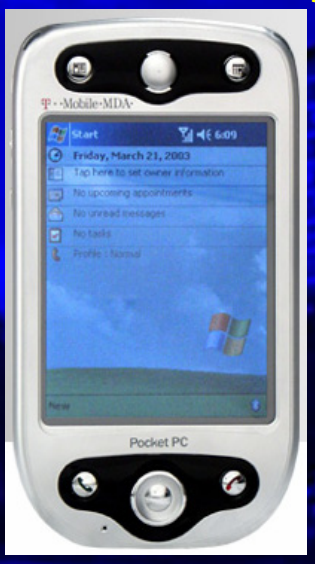
Quelle: Computerzeitung 12, 2004, Seite 18

Trends & Technologiefolgenabschätzung:

Mobile IP-Telefonie durch weitverbreitete WLANs

Trends & Technologiefolgenabschätzung:
Integration Telefonie & PDA: Mobile Digital Assistent





Trends & Technologiefolgenabschätzung:
Integration Telefonie & PDA: Mobile Digital Assistent

Trends & Technologiefolgen:
„Der PC in zehn Jahren"

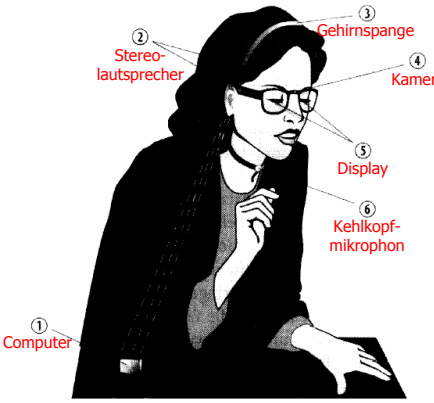


Abb. 1

hohen Tönen, manche – wie Delete-, Enter- oder

mit Zoomfunktion wie mit einem Feldstecher, oder im Makromodus wie mit Lupe), deren Bilder aber auch vom Computer über Bildverarbeitungsprogramme verwendet werden können. Die Kamera hat auch einen Kompass, d.h. der PC14 weiß über GPS, wo man sich befindet und auch in welche Richtung und mit welcher Kopfneigung man blickt. (6) ist ein Kehlkopfmikrophon, das gesprochene Worte (nach einiger Übung auch solche, die mit geschlossenem Mund gesprochen werden) aufnehmen kann: sei es zum Telefonieren, oder zur Auswertung durch den Computer. Hier ist auch ein kleiner Lautsprecher eingebaut, damit fallweise andere Menschen mithören können, selbst wenn sie gerade keine PC14-Brille tragen. (3) ist eine Spange, die unter den Gehirnaktivitäten einige wenige erkennen kann, etwa jene, die entstehen, wenn man an eine Bewegung einer Hand oder

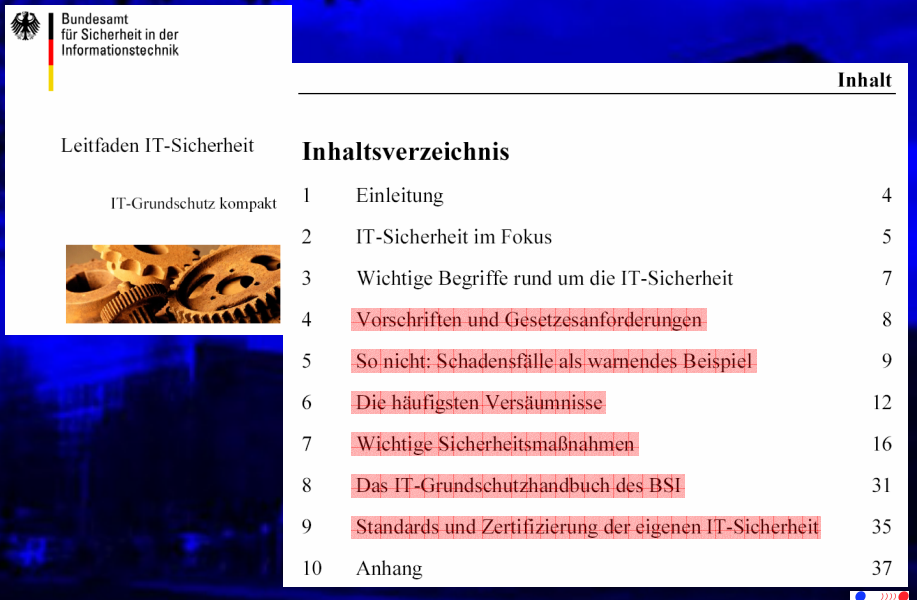
Quelle: Futurologe Prof. Dr. Hermann Maurer (TU Graz), Der PC in zehn Jahren, Informatik-Spektrum, Band 27, Nummer 1, Februar 2004, Seiten 44 – 50, download gescannt von meiner WWW-Vorlesungsseite „Grundlagen der Wirtschaftsinformatik"

Übersicht dieses Vortrages

- **Persönliches**
- **Informationssysteme**
- Einführung in die **Informations- und Datensicherheit** und die zugehörigen **Strukturen** an der **Universität Hannover**
- **Probleme** und **Maßnahmen** an der **Universität Hannover**

www.iwi.uni-hannover.de/it-sicherheitsbeauftragter.html

Leitfaden IT-Sicherheit des BSI



5 So nicht: Schadensfälle als warnendes Beispiel

Szenario 1: "Kein Backup"

Eine Anwaltskanzlei betreibt ein kleines Netz mit einem zentralen Server, auf dem alle Daten gespeichert werden. Der Server enthält ein Bandlaufwerk, auf das in regelmäßigen Abständen eine Sicherungskopie gespeichert wird. Der Administrator bewahrt die Sicherungsbänder in einem verschlossenen Schrank in seinem Büro auf. Als eines Tages der Server durch einen Festplattendefekt ausfällt, sollen die Daten vom Sicherungsband wieder eingespielt werden. Dabei stellt sich jedoch heraus, dass das Bandlaufwerk offenbar bereits längere Zeit defekt war und gar keine Daten auf die Sicherungsbänder geschrieben hatte. Das einzige noch funktionstüchtige Sicherungsband ist mehr als fünf Jahre alt. Alle Daten der letzten Jahre sind damit verloren.

Der Administrator hat bei der Planung der Datensicherung eine weitere potentielle Gefahr übersehen: Selbst wenn das Bandlaufwerk funktioniert hätte, wären bei einem Feuer oder ähnlichen Katastrophen neben den Originaldaten auch die Sicherungsmedien in seinem Schrank mit vernichtet worden!

Maßnahmen
regelmäßige Überprüfung der Backup-Bänder
Rücksicherung prüfen und üben
Lagerung von Sicherungsbändern außerhalb der eigenen Büroräume, beispielsweise in einem Bankschließfach

Leitfaden IT-Sicherheit des BSI

Szenario 2: "Befall durch Computer-Viren"

Ein Unternehmen setzt flächendeckend Virenscanner ein. Eine Aktualisierung der Virenscanner findet jedoch nur sporadisch statt, beispielsweise im Rahmen von Betriebssystem-Updates. Eines Tages erhält die IT-Abteilung eine Virenwarnung bezüglich eines neuen E-Mail-Virus, das sich in Windeseile über das Internet an immer mehr Empfänger verbreitet. Das Unternehmen verfügt jedoch über keinen automatisierten Update-Mechanismus, mit dessen Hilfe im Eilverfahren die Virenscanner auf allen Rechnern mit der neuen Virendefinition aktualisiert werden könnten. Im Rahmen einer Notfallmaßnahme werden die Mailserver vom Internet getrennt. Der Virus hat sich aber bereits ins interne Netz eingeschlichen und kann nicht an der weiteren Ausbreitung gehindert werden. Da der Virus Office-Dokumente zerstört, müssen alle Rechner vom Netz genommen und heruntergefahren werden, bis die IT-Verantwortlichen nach und nach alle PCs mit einem aktuellen Virenscanner-Update versehen und bereits befallene Rechner mühevoll “gesäubert” haben. Der gesamte IT-Betrieb ist für mehrere Tage nahezu stillgelegt. Durch zerstörte Daten, Verspätungen bei der Auftragsabwicklung und verlorene Arbeitszeit entsteht ein beträchtlicher Schaden. Kurz nach Abschluss dieser Arbeiten tauchen erste Varianten des Virus im Internet auf, die von der zuvor mühevoll aktualisierten Scanner-Version noch nicht erkannt werden. Die gesamte Arbeit muss nochmals wiederholt werden.

Maßnahmen
Update-Konzept für Sicherheits-Updates erstellen
“IT-Inseln” innerhalb des Unternehmens nicht vergessen (z. B. Notebooks und Testrechner)

Leitfaden IT-Sicherheit des BSI

6 Die häufigsten Versäumnisse

Bei einer Analyse der typischen Fehler und Versäumnisse finden sich nur geringe Abhängigkeiten von Unternehmensgröße und Branche. Anhand der dargestellten Liste können Sie überprüfen, welche spezifischen Versäumnisse in Ihrem Umfeld eine Rolle spielen und wie dieser Sachverhalt zu bewerten ist. Das nächste Kapitel greift die geschilderten Defizite nochmals auf und zeigt anhand konkreter Maßnahmen, wie Sie diesen mit angemessenem Aufwand begegnen können.

6.1 Unzureichende IT-Sicherheits-Strategie

❒ **Sicherheit hat einen zu geringen Stellenwert**

IT-Sicherheit hat im Vergleich mit anderen Anforderungen (Kosten, Bequemlichkeit, große Funktionalität, ...) häufig einen zu geringen Stellenwert. Stattdessen wird IT-Sicherheit lediglich als Kostentreiber und Behinderung gesehen. Besonders bei Neuanschaffungen werden Sicherheitseigenschaften einer Anwendung oder eines Systems häufig vernachlässigt oder gar nicht bedacht. Dafür gibt es verschiedene Gründe: Mangelnde Managementunterstützung für IT-Sicherheit, ungenügende Recherche über Sicherheitsaspekte, neue Trends in der Branche, Marketinggesichtspunkte oder knappe Budgets etc. Sicherheitsmängel treten zumeist nicht unmittelbar zu Tage. Stattdessen erhöht sich "nur" das aus diesen Defiziten erwachsende Risiko! Im ungünstigsten Fall werden notwendige Sicherheitsmaßnahmen immer wieder auf unbestimmte Zeit verschoben, da sie jedes Mal niedriger priorisiert sind als zwischenzeitlich neu hinzu kommende andere Aufgaben.

Ein Beispiel in diesem Zusammenhang ist die rasant wachsende Zahl völlig ungesicherter drahtloser

Leitfaden IT-Sicherheit des BSI

I. Systematisches Herangehen an IT-Sicherheit

1) IT-Sicherheitsaspekte müssen bei allen Projekten frühzeitig und ausreichend berücksichtigt werden
2) Im Falle mangelnder Ressourcen sollten alternative Lösungsansätze in Erwägung gezogen werden
3) Die IT-Sicherheitsziele müssen festgelegt werden, damit angemessene Maßnahmen definiert werden können
4) Zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme sollten geeignete Regelungen getroffen werden
5) Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden **(Beispiel)**
6) Besonders umständliche Sicherheitsanforderungen sollten vermieden werden **(Beispiel)**
7) Zuständigkeiten müssen festgelegt werden
8) Bestehende Richtlinien und Zuständigkeiten müssen bekannt gemacht werden
9) Die IT-Sicherheit sollte regelmäßig überprüft werden
10) Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien sollten regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft werden
11) Langfristig sollte ein umfassendes Sicherheitsmanagement aufgebaut werden
12) Alle bestehenden Sicherheitsrichtlinien sollten schriftlich in einem Sicherheitskonzept dokumentiert werden

Leitfaden IT-Sicherheit des BSI

5. Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden

Wer eine Weile über sinnvolle Schritte zur Erhöhung der eigenen IT-Sicherheit nachgedacht hat, wird sich bald vor mehr Aufgaben gestellt sehen, als er zeitlich und finanziell bewältigen kann. Daher ist eine geeignete Priorisierung identifizierter Sicherheitsziele und -maßnahmen erforderlich. Diese Priorisierung sollte auch unter Abwägung des Kosten-Nutzen-Verhältnisses getroffen werden.

6. Besonders umständliche Sicherheitsanforderungen sollten vermieden werden

Es sollten möglichst nur solche Sicherheitsvorgaben gemacht werden, deren Einhaltung praktikabel ist und die nicht von einem Großteil der Betroffenen als realitätsfremd oder gar schikanös erachtet werden. Zudem versteht sich von selbst, dass zur Umsetzung von Vorgaben und Maßnahmen auch die technische und organisatorische Infrastruktur bereitgestellt werden muss. Anderenfalls besteht die Gefahr, dass die Richtlinien in ihrer Gesamtheit nicht mehr ernst genommen und zunehmend missachtet werden. Im Zweifelsfall sollten die Anforderungen eher etwas heruntergeschraubt werden und dafür strenger auf deren Einhaltung geachtet werden. Es empfiehlt sich auch, alle Maßnahmen, die besonders tief in die gewohnte Arbeitsweise eingreifen, mit betroffenen Anwendern vorher zu besprechen.

Leitfaden IT-Sicherheit des BSI

I. Systematisches Herangehen an IT-Sicherheit

1) IT-Sicherheitsaspekte müssen bei allen Projekten frühzeitig und ausreichend berücksichtigt werden
2) Im Falle mangelnder Ressourcen sollten alternative Lösungsansätze in Erwägung gezogen werden
3) Die IT-Sicherheitsziele müssen festgelegt werden, damit angemessene Maßnahmen definiert werden können
4) Zu jedem vorhandenen Sicherheitsziel und jeder zugehörigen Maßnahme sollten geeignete Regelungen getroffen werden
5) Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden
6) Besonders umständliche Sicherheitsanforderungen sollten vermieden werden
7) Zuständigkeiten müssen festgelegt werden
8) Bestehende Richtlinien und Zuständigkeiten müssen bekannt gemacht werden
9) Die IT-Sicherheit sollte regelmäßig überprüft werden
10) Vorhandene Arbeitsabläufe und Sicherheitsrichtlinien sollten regelmäßig hinsichtlich Zweckmäßigkeit und Effizienz überprüft werden
11) Langfristig sollte ein umfassendes Sicherheitsmanagement aufgebaut werden
12) Alle bestehenden Sicherheitsrichtlinien sollten schriftlich in einem Sicherheitskonzept dokumentiert werden

II. Sicherheit von IT-Systemen

13) Vorhandene Schutzmechanismen sollten genutzt werden
14) Virenschutzprogramme müssen flächendeckend eingesetzt werden
15) Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden
16) Allen Systembenutzern sollten Rollen und Profile zugeordnet werden
17) Administratorrechte sollten auf das erforderliche Maß eingeschränkt werden
18) Programmprivilegien sollten begrenzt werden
19) Die Standardeinstellungen gemäß Auslieferungszustand sollten geeignet angepaßt werden
20) Handbücher und Produktdokumentationen sollten frühzeitig gelesen werden
21) Ausführliche Installations- und Systemdokumentationen müssen erstellt und regelmäßig aktualisiert werden

Leitfaden IT-Sicherheit des BSI

III. Vernetzung und Internet-Anbindung

22) Zum Schutz von Netzen muß eine Firewall verwendet werden
23) Eine sichere Firewall muß bestimmten Mindestanforderungen genügen
24) Nach außen angebotene Daten sollten auf das erforderliche Mindestmaß beschränkt werden
25) Nach außen angebotene Dienste und Programmfunktionalität sollten auf das erforderliche Mindestmaß beschränkt werden
26) Beim Umgang mit Web-Browsern ist besondere Vorsicht geboten, riskante Aktionen sollten unterbunden werden
27) Bei E-Mail-Anhängen ist besondere Vorsicht notwendig
28) Ein gesonderter Internet-PC zum Surfen ist eine kostengünstige Lösung für die meisten Sicherheitsprobleme bei der Internet-Nutzung

IV. Faktor Mensch: Kenntnis und Beachtung von Sicherheitserfordernissen

29) Sicherheitsrichtlinien und -anforderungen müssen beachtet werden
30) Am Arbeitsplatz sollten Ordnung herrschen und keine sensitiven Informationen frei zugänglich sein
31) Bei Wartungs- und Reparaturarbeiten sind besondere Vorsichtsmaßnahmen zu beachten
32) Mitarbeiter müssen regelmäßig geschult werden
33) Nur eine ehrliche Selbsteinschätzung hilft weiter: Manchmal muß Expertenrat eingeholt werden
34) Für alle bestehenden Sicherheitsvorgaben sollten Kontrollmechanismen aufgebaut werden
35) Konsequenzen für Sicherheitsverstöße sollten festgelegt und veröffentlicht werden
36) Erkannte Sicherheitsverstöße sollten auch tatsächlich sanktioniert werden

Leitfaden IT-Sicherheit des BSI

V. Wartung von IT-Systemen: Umgang mit sicherheitsrelevanten Updates

37) Sicherheits-Updates müssen regelmäßig eingespielt werden
38) Zu den Sicherheitseigenschaften verwendeter Software sollten in regelmäßigen Abständen ausführliche Recherchen durchgeführt werden
39) Es sollte ein Aktionsplan zum Einspielen erforderlicher Sicherheits-Updates erstellt werden
40) Softwareänderungen sollten getestet werden

VI. Verwendung von Sicherheitsmechanismen: Umgang mit Paßwörtern und Verschlüsselung

41) Sicherheitsmechanismen sollten sorgfältig ausgesucht werden
42) Es müssen gut gewählte (sichere) Paßwörter eingesetzt werden
43) Voreingestellte oder leere Paßwörter sollten geändert werden
44) Arbeitsplatzrechner sollten bei Verlassen mit Bildschirmschoner und Kennwort gesichert werden
45) Sensitive Daten und Systeme müssen geschützt werden

VII. Schutz vor Katastrophen und Elementarschäden

46) Notfallchecklisten sollten erstellt werden und jedem Mitarbeiter bekannt sein
47) Alle wichtigen Daten müssen regelmäßig gesichert werden (Backup)
48) IT-Systeme müssen angemessen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt sein
49) Maßnahmen zum Zutrittsschutz und zum Schutz vor Einbrechern müssen umgesetzt werden
50) Der gesamte Bestand an Hard- und Software sollte in einer Inventarliste erfaßt werden

Leitfaden IT-Sicherheit des BSI

8 Das IT-Grundschutzhandbuch des BSI

In den vorhergehenden Kapiteln wurden verschiedene Aspekte der IT-Sicherheit beleuchtet und erläutert, warum sich eine angemessene Sicherheit nicht allein durch technische Mechanismen und Funktionen erreichen lässt. Vielmehr müssen die technischen Sicherheitsfunktionen durch organisatorische, personelle und baulich-physische Maßnahmen flankiert werden. Wer jetzt systematisch und umfassend seine IT-Sicherheit verbessern möchte, steht vor der Herausforderung, eine möglichst optimale Sicherheitsfunktionalität bei vertretbaren Kosten zu erreichen. Dazu kommt: Die umgesetzten Lösungen müssen praxistauglich und ausreichend komfortabel sein, damit sie von den Betroffenen auch in der täglichen Arbeit akzeptiert werden. Dieses Kapitel zeigt prinzipielle Vorgehensweisen bei der Erstellung professioneller IT-Sicherheitskonzepte auf und erklärt Ihnen, wie das IT-Grundschutzhandbuch des BSI dabei helfen kann.

8.1 Das IT-Grundschutzhandbuch des BSI als Grundlage eines professionellen IT-Sicherheitskonzeptes

Umfassend aber teuer: Die Risikoanalyse

Eine Möglichkeit, ein Sicherheitskonzept zu erstellen, ist die traditionelle Risikoanalyse. Dabei werden individuelle Sicherheitsmaßnahmen für eine vorliegende IT-Landschaft erarbeitet. Die zu schützenden Werte (IT-Systeme, Daten, Know-how etc.) werden ermittelt und genau untersucht,

Management der Informations- und Datensicherheit (www.iwi.uni-hannover.de/it-sicherheitsbeauftragter.html)

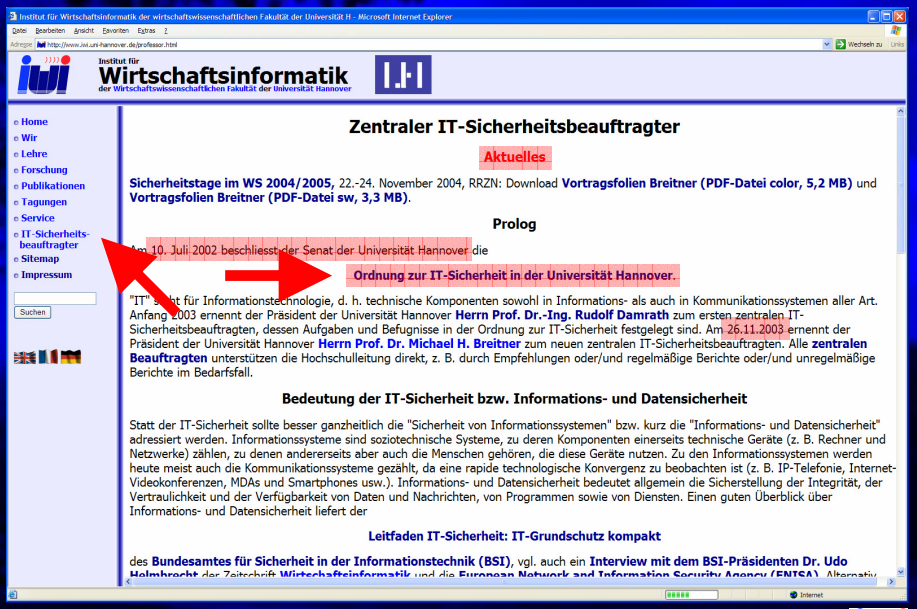
- Sowohl die
  - **Verbesserung** als auch nur die
  - **Erhaltung** der **aktuellen Informations-** und **Datensicherheit**

  bedarf permanenter Anstrengungen. Notwendig sind z. B. sowohl ein
  - **durchdachtes Sicherheitskonzept**, als auch ein
  - **gut strukturierter Sicherheitsprozeß**,

  die beide Teile eines **umfassenden Sicherheitsmanagements** sein müssen. Aufgaben des Sicherheitsmanagements sind die
  - **Planung**, die
  - **Realisierung** und die
  - **Kontrolle** der **Informations-** und **Datensicherheit**,

  wobei jeweils **strategische**, **taktische** und **operative** Aufgaben zu erledigen sind. Wichtig ist, nicht nur auf
  - **Krisen** und akute **Bedrohungen** angemessen zu **reagieren**, sondern auch
  - **präventiv** und **vorausschauend** zu **agieren**.

www.iwi.uni-hannover.de/it-sicherheitsbeauftragter.html



Institut für Wirtschaftsinformatik der Wirtschaftswissenschaftlichen Fakultät der Universität Hannover

- Home
- Wir
- Lehre
- Forschung
- Publikationen
- Tagungen
- Service
- IT-Sicherheits-beauftragter
- Sitemap
- Impressum

Suchen

Zentraler IT-Sicherheitsbeauftragter

Aktuelles

Sicherheitstage im WS 2004/2005, 22.-24. November 2004, RRZN: Download **Vortragsfolien Breitner (PDF-Datei color, 5,2 MB)** und **Vortragsfolien Breitner (PDF-Datei sw, 3,3 MB)**.

Prolog

Am 10. Juli 2002 beschliesst der Senat der Universität Hannover die

Ordnung zur IT-Sicherheit in der Universität Hannover.

"IT" steht für Informationstechnologie, d. h. technische Komponenten sowohl in Informations- als auch in Kommunikationssystemen aller Art. Anfang 2003 ernennt der Präsident der Universität Hannover **Herrn Prof. Dr.-Ing. Rudolf Damrath** zum ersten zentralen IT-Sicherheitsbeauftragten, dessen Aufgaben und Befugnisse in der Ordnung zur IT-Sicherheit festgelegt sind. Am 26.11.2003 ernennt der Präsident der Universität Hannover **Herrn Prof. Dr. Michael H. Breitner** zum neuen zentralen IT-Sicherheitsbeauftragten. Alle **zentralen Beauftragten** unterstützen die Hochschulleitung direkt, z. B. durch Empfehlungen oder/und regelmäßige Berichte oder/und unregelmäßige Berichte im Bedarfsfall.

Bedeutung der IT-Sicherheit bzw. Informations- und Datensicherheit

Statt der IT-Sicherheit sollte besser ganzheitlich die "Sicherheit von Informationssystemen" bzw. kurz die "Informations- und Datensicherheit" adressiert werden. Informationssysteme sind soziotechnische Systeme, zu deren Komponenten einerseits technische Geräte (z. B. Rechner und Netzwerke) zählen, zu denen andererseits aber auch die Menschen gehören, die diese Geräte nutzen. Zu den Informationssystemen werden heute meist auch die Kommunikationssysteme gezählt, da eine rapide technologische Konvergenz zu beobachten ist (z. B. IP-Telefonie, Internet-Videokonferenzen, MDAs und Smartphones usw.). Informations- und Datensicherheit bedeutet allgemein die Sicherstellung der Integrität, der Vertraulichkeit und der Verfügbarkeit von Daten und Nachrichten, von Programmen sowie von Diensten. Einen guten Überblick über Informations- und Datensicherheit liefert der

Leitfaden IT-Sicherheit: IT-Grundschutz kompakt

des **Bundesamtes für Sicherheit in der Informationstechnik (BSI)**, vgl. auch ein **Interview mit dem BSI-Präsidenten Dr. Udo Helmbrecht** der Zeitschrift **Wirtschaftsinformatik** und die **European Network and Information Security Agency (ENISA)**. Alternativ

Ordnung zur IT-Sicherheit der Uni H

Ordnung zur IT-Sicherheit in der Universität Hannover

(vom Senat beschlossen am 10.7.2002)

Präambel

Ein leistungsfähiger Universitätsbetrieb erfordert in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf Informationstechnik (IT) und hierbei insbesondere auf vernetzte IT-Systeme stützen. Dafür ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich. Insbesondere die Anbindung der IT-Systeme an das weltweite Datennetz erfordert wirksamen Schutz gegen Eingriffe von außen. Die Thematik der "Sicherheit in der Informationstechnik" ("IT-Sicherheit") bekommt damit für die Universität Hannover eine grundsätzliche Bedeutung, die die Entwicklung und Umsetzung eines einheitlichen Sicherheitskonzepts für die Universität erforderlich macht. Dieses kann wegen der komplexen Materie, der sich weiterentwickelnden technischen Bedingungen und der begrenzten finanziellen Mittel nur in einem kontinuierlichen Sicherheitsprozess erfolgen, der den besonderen Bedingungen der Universität Hannover mit ihren vielen dezentralen Einrichtungen gerecht wird. Dazu empfiehlt es sich, diesen Sicherheitsprozess an Prinzipien zu orientieren, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im *IT-Grundschutzhandbuch*[1], einem - auch international - anerkannten de-facto-Standardwerk zur IT-Sicherheit, niedergelegt sind.

§ 1

Ordnung zur IT-Sicherheit der Uni H

§ 3
Beteiligte am IT-Sicherheitsprozess

Im Sinn dieser Ordnung sind am IT-Sicherheitsprozess der Universität verantwortlich beteiligt:

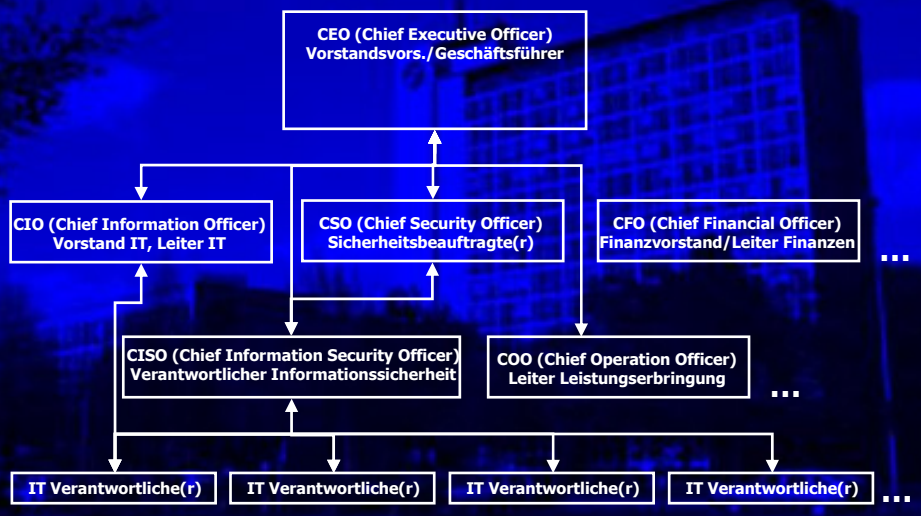
(1) Der/die zentrale IT-Sicherheitsbeauftragte (s. § 4)
(2) Dezentrale IT-Sicherheitsbeauftragte (s. § 4)
(3) Der Sicherheitsstab (s. § 5)
(4) Das RRZN
(5) Einrichtungen der Universität gemäß § 2

§ 4
Einsetzung der IT-Sicherheitsbeauftragten

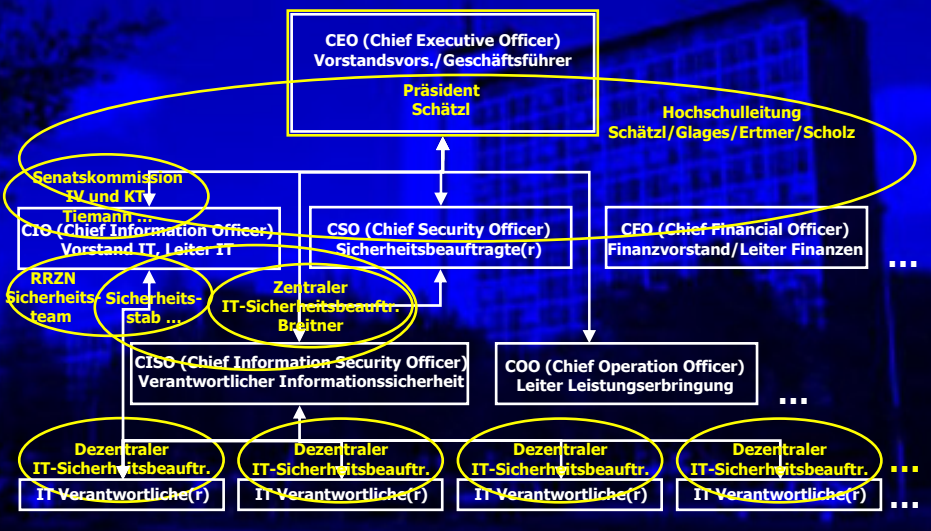
(1) Der Präsident bestellt eine/n zentrale/n IT-Sicherheitsbeauftragte/n und eine/n Stellvertreter/in[5].

[5] Diese Rolle kann auch dem "Generalverantwortlichen für Information und Kommunikation" (CIO, Chief Information Officer) zugeordnet werden, wie er in den derzeit aktuellen Empfehlungen der Kommission für Rechenanlagen der DFG zur Informationsverarbeitung an Hochschulen vorgeschlagen wird.

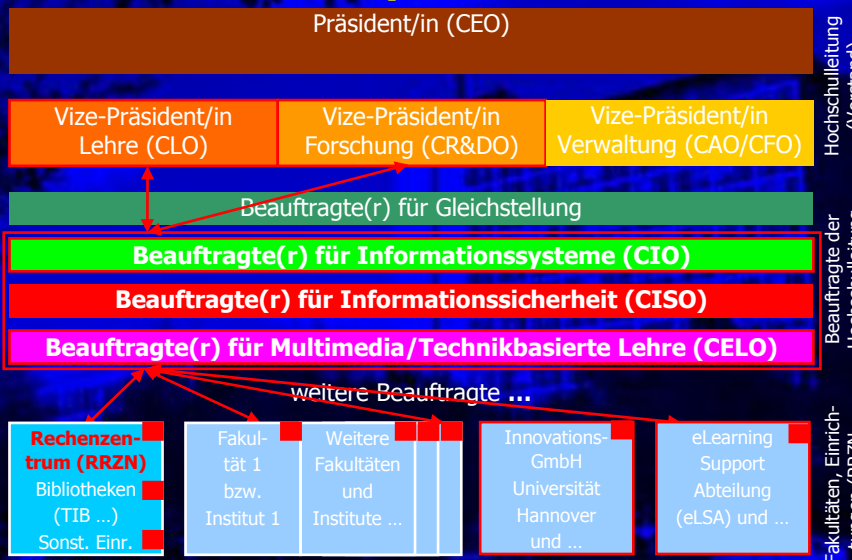
IT-Sicherheitstruktur Uni H im Vergleich zu privatwirtschaftlichen Unternehmen



IT-Sicherheitstruktur Uni H im Vergleich zu privatwirtschaftlichen Unternehmen



Struktur*plan* der Uni H



= Operative/taktische/dezentrale Verantwortliche für Informationssicherheit

CIO an der Uni H

Liebe Kolleginnen und Kollegen,

wie heute morgen bei unserem Initiativtreffen zur Einrichtung eines Chief Information Officers (CIO) an der Universität Hannover (UH) besprochen, senden wir Ihnen einen Fragenkatalog zur Bestandsaufnahme des Ist-Zustandes sowie der möglichen Probleme und Problemfelder im IuK-Bereich der UH.

Dieser Fragenkatalog wendet sich an verschiedene Adressaten: Verwaltung (1), Bibliothek (2), Lehre (3) und Forschung (4) allgemein, Studentische Verwaltung (5) sowie an Fakultäts (6) - und Instituts (7) - Ebenen. Wir wollen vermeiden, dass Fragen „unsinnige" bzw. irrelevante Informationen triggern. Sie sollten daher bitte nur die Ihrer Meinung nach für Ihren Bereich zutreffenden Informationen sammeln und liefern[1]. Außerdem geht es bei quantitativen Fragen nur um Größenordnungen bzw. einen Überblick und nicht um absolute Detailtreue.

1. Welche Software-Plattformen befinden sich in Ihrem Bereich:
   - Betriebssysteme,
   - Webdienste,
   - Fachspezifische Software,
   - Archivierung,
   - Email,
   - .....
2. Wer ist für Beschaffung, Wartung/Pflege, Sicherheit und Service zuständig?
   - RRZN
   - Besonders ausgewiesene Mitarbeiter (Positionen), (zentral, dezentral?)
   - „jeder für sich"
3. Wer entscheidet über Art und Umfang von Beschaffungen im IT-Bereich (1, 2, 6, 7)?
   - Finanzierungsquelle ?
4. Welche Hardware ist im Einsatz (1-4)?
   - Pools, Laptops, PC, ...
5. Welche Netz-Infrastruktur ist vorhanden (1, 2, 6, 7)?
   - Uni-Netz usw.
6. Welche IT-Services bietet Ihr Bereich an (1, 2, 6 ,7)?
   - Intern
   - Uni-intern
   - Extern
7. Welche IuK-Kompetenz ist in Ihren Bereich vorhanden (1, 2, 3, 7)?
   - Zentral ?
   - Dezentral ?
8. Welche IuK-Services werden in Anspruch genommen (3, 4, 5)?
   - Uni-intern ?
   - Extern ?
9. Wer wird gefragt, wenn Probleme auftreten (3, 4, 5, 6)?
10. Wie viel Aufwand wird in den verschiedenen Bereichen in den IuK-Betrieb investiert?
    - Hardware (finanziell/Jahr) (Auskunft über die Verwaltung)
    - Software (finanziell/Jahr) (Auskunft über die Verwaltung)
    - Betreuung/Wartung (Betrifft RRZN, Verwaltung und Bibliothek)
    - Schulung (Betrifft RRZN, Verwaltung und Bibliothek)
11. Wer/Welche Bereiche sind auf IuK angewiesen?

[1] Mit *Ihrem Bereich* ist die heute morgen verabredete Zuständigkeit gemeint: Forschung (Tiemann, Johmann, Ertmer), Lehre (Vogt), Bibliothek u. Zentrale Einrichtungen (May), Verwaltung und Studentische Verwaltung (Bergmann) und RRZN mit Zentralen Diensten (von Voigt)

Ordnung zur IT-Sicherheit der Uni H

§ 4
Einsetzung der IT-Sicherheitsbeauftragten

(1) Der Präsident bestellt eine/n zentrale/n IT-Sicherheitsbeauftragte/n und eine/n Stellvertreter/in[5].

(2) Jeder Fachbereich sowie jede zentrale Einrichtung hat eine/n dezentrale/n IT-Sicherheitsbeauftragte/n und Stellvertreter/in[6,7] zu benennen.

(3) Die Fachbereiche können zusätzliche dezentrale IT-Sicherheitsbeauftragte und Stellvertreter[6] benennen, die je für ein oder mehrere Einrichtungen im Fachbereich zuständig sind.

[6] Vor dem Hintergrund des Einsatzes möglichst qualifizierten Personals bestehen keine Bedenken, Administratoren als Sicherheitsbeauftragte zu benennen, obwohl prinzipiell eine Rollentrennung anzustreben wäre.
[7] Mehrere Fachbereiche können mangels geeigneter Alternativen auch eine/n **gemeinsame/n** Sicherheitsbeauftragte/n benennen.

Ordnung zur IT-Sicherheit der Uni H

§ 4
Einsetzung der IT-Sicherheitsbeauftragten

(1) Der Präsident bestellt eine/n zentrale/n IT-Sicherheitsbeauftragte/n und eine/n Stellvertreter/in[5].

(2) Jeder Fachbereich sowie jede zentrale Einrichtung hat eine/n dezentrale/n IT-Sicherheits-beauftragte/n und Stellvertreter/in[6,7] zu benennen.

(3) Die Fachbereiche können zusätzliche dezentrale IT-Sicherheitsbeauftragte und Stellvertreter[6] benennen, die je für ein oder mehrere Einrichtungen im Fachbereich zuständig sind.

(4) Durch die Benennungen nach (2) und (3) müssen **alle** IT-Systeme im Geltungsbereich sowie die vor Ort für deren Betrieb verantwortlichen Personen einer/m IT-Sicherheits-beauftragten auf Fachbereichs- oder Einrichtungsebene zugeordnet sein.

(5) Bei der Bestellung/Benennung der IT-Sicherheitsbeauftragten sollen der strategische Aspekt und die dafür erforderliche personelle Kontinuität berücksichtigt werden. Die IT-Sicherheitsbeauftragten sollen deshalb möglichst zum hauptamtlichen Personal der Universität gehören. Sie sollen in IT-Sicherheitsfragen besonders geschult werden.

Ordnung zur IT-Sicherheit der Uni H

§ 5
Einsetzung des Sicherheitsstabs

(1) Ständige Mitglieder des Sicherheitsstabs sind:

- der/die zentrale IT-Sicherheitsbeauftragte (Vorsitz) — Prof. Dr. M. H. Breitner
- ein/eine Vertreter/in des RRZN (stellvertretender Vorsitz) — Dipl.-Math. H.-J. Hille
- ein/eine Vertreter/in des Rechtsdezernats — Dr. N. Neuvians
- der/die Datenschutzbeauftragte der Universität, der/die sich vertreten lassen kann — Prof. Dipl.-Ing. H.-G. Genenger

(2) Weitere sachverständige Mitglieder werden vom Senat in Abstimmung mit dem Präsidenten benannt. Thomas Bergmann, Dr.-Ing. habil. Jürgen Brehm, Christian Knopf

(3) Der Gesamtpersonalrat kann ein beratendes Mitglied benennen. Martin Pracht

(4) Die Zusammensetzung des Sicherheitsstabs sollte - unter Beschränkung der Anzahl der Mitglieder auf das notwendige Maß - sowohl die unterschiedlichen Aufgabenbereiche der Universität widerspiegeln als auch den unterschiedlichen, für die Universität relevanten Aspekten der IT-Sicherheit Rechnung tragen.[8]

[8] Dies kann beispielsweise eine Vertretung - durchaus auch in Personalunion - der wiss. Einrichtungen, der Verwaltung und der IT-Anwender beinhalten.

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(1) Der/Die zentrale IT-Sicherheitsbeauftragte ist für Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.

- Der zentrale IT-Sicherheitsbeauftragte Prof. Dr. Michael H. Breitner ist für die Konzeption, Umsetzung und Überwachung der Informations- und Datensicherheit verantwortlich (**primär strategisches Management**). Er
  - **initiiert**,
  - **steuert** und
  - **kontrolliert**

  unter **Beteiligung** des **Sicherheitsstabs** den **Informationssicherheits-prozeß**, der nach **festzulegenden Prioritäten**
  - **Maßnahmen** sowohl **präventiver** als auch
  - **Maßnahmen reaktiver Art**, insbes. zu schneller **Krisenintervention**

  umfassen muß.

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(1) Der/Die zentrale IT-Sicherheitsbeauftragte ist für Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.

- Der zentrale IT-Sicherheitsbeauftragte **berichtet** dem
  - **Präsidenten** und dem
  - **Senat**

  aus **gegebenem Anlaß** und macht **Vorschläge** für die
  - **Erhaltung** und
  - **Verbesserung** der **Informations-** und **Datensicherheit**

  unter Berücksichtigung der
  - **Ausgewogenheit**,
  - **Durchgängigkeit** und
  - **Angemessenheit** der **Maßnahmen**.

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(2) Das RRZN ist verantwortlich für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit und gibt in diesem Rahmen technische Standards zur IT-Sicherheit für die Universität vor.[9]

[9] Im Rahmen dieser Vorgaben können Einrichtungen der Universität die Zuständigkeit für Systeme zur IT-Sicherheit in ihrem Bereich in Absprache mit dem RRZN teilweise oder vollständig übernehmen.

- Verantwortlich ist das

  IT-Sicherheitsteam der Universität Hannover

  (www.rrzn.uni-hannover.de/kontakt.html, security@rrzn.uni-hannover.de)

  im **Regionalen Rechenzentrum für Niedersachsen** (**RRZN**). Das RRZN ist verantwortlich für die
  - **system-** und **netztechnischen Aspekte** und
  - **betriebstechnischen Aspekte**

  der IT-Sicherheit und gibt in diesem Rahmen **technische Standards zur IT-Sicherheit** für die Universität vor (drahtgebundene und drahtlose Netzwerke, Switches und Router, Hard- und Software-Firewalls, Betriebssysteme, usw.).

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(2) Das RRZN ist verantwortlich für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit und gibt in diesem Rahmen technische Standards zur IT-Sicherheit für die Universität vor.[9]

[9] Im Rahmen dieser Vorgaben können Einrichtungen der Universität die Zuständigkeit für Systeme zur IT-Sicherheit in ihrem Bereich in Absprache mit dem RRZN teilweise oder vollständig übernehmen.

- Soweit das RRZN eine **akute Gefährdung** feststellt, kann es z. B. **Netzanschlüsse**, ggf. auch ohne vorherige Benachrichtigung der Betroffenen, **vorübergehend sperren**, wenn zu befürchten ist, daß ein voraussichtlich **gravierender Schaden** für die **IT-Infrastruktur der Universität**
  - **in Teilen** oder
  - **insgesamt**

  nicht anders abzuwenden ist. Das IT-Sicherheitsteam des RRZN ist Ansprechpartner für alle **Fragen zur IT-Sicherheit**, vgl. auch die WWW-Seiten des RRZN zur IT-Sicherheit, die z. B. umfassend über
  - **Antivirensoftware** und
  - **Firewalls** Auskunft geben.

Ordnung zur IT-Sicherheit der Uni H

www.rrzn.uni-hannover.de/kontakt.html

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(3) Der Sicherheitsstab unterstützt den/die zentrale/n IT-Sicherheitsbeauftragte/n, indem er Pläne, Leitlinien und Vorgaben für sämtliche übergreifenden Belange der IT-Sicherheit erarbeitet, Maßnahmen koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

(4) Die dezentralen IT-Sicherheitsbeauftragten sind für alle Sicherheitsbelange der IT-Systeme und -Anwendungen in den Bereichen, die ihnen jeweils zugeordnet sind, verantwortlich, soweit nicht übergeordnete Belange tangiert sind, die von dem/der zentralen IT-Sicherheitsbeauftragten wahrgenommen werden.

- **Jeder Fachbereich** bzw. **jede Fakultät** sowie **jede zentrale Einrichtung** hat eine/n
  - **dezentrale/n IT-Sicherheitsbeauftragte/n** und
  - **Stellvertreter/in**

  zu benennen. Durch die Benennungen müssen
  - **alle Informationssysteme** im Geltungsbereich sowie
  - die vor Ort für deren Betrieb **verantwortlichen Personen**

  einer/m IT-Sicherheitsbeauftragten **zugeordnet sein**.

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(4) Die dezentralen IT-Sicherheitsbeauftragten sind für alle Sicherheitsbelange der IT-Systeme und -Anwendungen in den Bereichen, die ihnen jeweils zugeordnet sind, verantwortlich, soweit nicht übergeordnete Belange tangiert sind, die von dem/der zentralen IT-Sicherheitsbeauftragten wahrgenommen werden.

- Die dezentralen IT-Sicherheitsbeauftragten sind für das **kontinuierliche**, **primär operative** und **taktische Management** der **Informations-** und **Datensicherheit** in ihrem Bereich verantwortlich. Bei **akuter Gefährdung** veranlassen die dezentralen IT-Sicherheitsbeauftragten die **sofortige vorübergehende Stilllegung** betrof-fener Systeme in ihrem Bereich, wenn zu befürchten ist, daß ein Schaden – insbesondere für andere Einrichtungen oder für die IT-Infrastruktur der Universi-tät in Teilen oder insgesamt – nicht anders abzuwenden ist. Unverzüglich sind die
  - **Leitung der Einrichtung** und das
  - **RRZN**

  zu **benachrichtigen**, das seinerseits den zentralen IT-Sicherheitsbeauftragten informiert.

Ordnung zur IT-Sicherheit der Uni H

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(5) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitungen der Einrichtungen nicht von ihrer Gesamtverantwortung für die IT-Sicherheit in ihrem Bereich.

(6) Die Einrichtungen der Universität sind verpflichtet, bei allen relevanten Planungen, Verfahren und Entscheidungen mit Bezug zu IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten sowie den/die zentrale/n IT-Sicherheitsbeauftragte/n zu beteiligen.

(7) Die am IT-Sicherheitsprozess Beteiligten arbeiten in allen Belangen der IT-Sicherheit zusammen, stellen die dazu erforderlichen Informationen bereit und regeln die Kommunikations- und Entscheidungswege sowohl untereinander als auch in Beziehung zu Dritten[10]. Hierbei ist insbesondere der Aspekt der in Krisenfällen gebotenen Eile zu berücksichtigen.

[10] Gesetzliche Beteiligungstatbestände des Gesamtpersonalrats bleiben hiervon unberührt.

Ordnung zur IT-Sicherheit der Uni H

§ 7
Verwirklichung des IT-Sicherheitsprozesses

(1) Der/die zentrale IT-Sicherheitsbeauftragte initiiert, steuert und kontrolliert unter Beteiligung des Sicherheitsstabs den IT-Sicherheitsprozess, der nach festzulegenden Prioritäten Maßnahmen sowohl präventiver als auch reaktiver Art sowie insbesondere zu schneller Krisenintervention umfassen muss. Zwecks Gewährleistung einer kontinuierlichen Steuerung des IT-Sicherheitsprozesses soll der Sicherheitsstab regelmäßig tagen.

(2) Die IT-Sicherheitsbeauftragten sind verpflichtet, sicherheitsrelevante Informationen jederzeit entgegenzunehmen und das jeweils Erforderliche zu veranlassen.[11] Soweit notwendig, informieren sich dezentrale IT-Sicherheitsbeauftragte zu Ursachen und Maßnahmen durch Kontaktaufnahme zur/m zentralen IT-Sicherheitsbeauftragten und/oder zum RRZN.

[11] Eine Pflicht zur **Meldung** sicherheitsrelevanter Ereignisse ergibt sich für alle Mitglieder und Angehörige der Universität aus einer separaten Ordnung zur **Nutzung** von IT-Infrastrukturen.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Bereich verantwortlich. Sie informieren sich regelmäßig über die Sicherheit der IT-Systeme in ihrem Bereich und veranlassen unverzüglich die notwendigen Maßnahmen zur Gewährleistung der erforderlichen Sicherheit. Sie informieren die Leitung ihrer Einrichtung regelmäßig über den Sicherheitsstandard und auftretende Probleme und schlagen Lösungsmöglichkeiten vor.

Ordnung zur IT-Sicherheit der Uni H

§ 7
Verwirklichung des IT-Sicherheitsprozesses

(4) Der/Die zentrale IT-Sicherheitsbeauftragte berichtet dem Präsidenten und dem Senat aus gegebenem Anlass darüber und macht Vorschläge für die Weiterentwicklung des IT-Sicherheitsprozesses unter Berücksichtigung der Ausgewogenheit, Durchgängigkeit und Angemessenheit der Maßnahmen. Dabei ist die Höhe der voraussichtlichen Kosten der einzelnen Maßnahmen anzugeben.

(5) Die dezentralen IT-Sicherheitsbeauftragten sind bezüglich ihrer Mitteilungspflichten gegenüber der/dem zentralen IT-Sicherheitsbeauftragten, dem Präsidenten und dem Senat unabhängig von Weisungen ihrer Vorgesetzten. Die IT-Sicherheitsbeauftragten geben ihre Berichte auch den Leitungen der betreffenden Einrichtungen zur Kenntnis.

Ordnung zur IT-Sicherheit der Uni H

§ 8
Gefahrenintervention

(1) Bei Gefahr in Verzug veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Bereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden - insbesondere für **andere** Einrichtungen oder für die IT-Infrastruktur der Universität in Teilen oder insgesamt - nicht anders abzuwenden ist. Unverzüglich sind die Leitung der Einrichtung und das RRZN zu benachrichtigen, das seinerseits den/die zentrale/n IT-Sicherheitsbeauftragte/n benachrichtigt.[12]

[12] Detailregelungen zu den Informations- und Entscheidungsabläufen werden nach § 6 (7) festgelegt und entsprechend bekanntgegeben.

(2) Soweit das RRZN Gefahr in Verzug feststellt, kann es Netzanschlüsse (ggfs. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Universität in Teilen oder insgesamt nicht anders abzuwenden ist. Die Benachrichtigung des/der zuständigen dezentralen sowie des/der zentralen IT-Sicherheitsbeauftragten erfolgt unverzüglich ggfs. nachträglich.

(3) Vor Wiederinbetriebnahme vorübergehend stillgelegter Systeme bzw. gesperrter Netzanschlüsse ist in der Regel die Durchführung hinreichender Sicherheitsmaßnahmen erforderlich. Im Zweifelsfall entscheidet der/die zentrale IT-Sicherheitsbeauftragte über das weitere Vorgehen.

Ordnung zur IT-Sicherheit der Uni H

§ 9
Finanzierung

(1) Die Mittel für spezielle, mit dem/r zentralen IT-Sicherheitsbeauftragten und dem RRZN abgestimmte Sicherheitsmaßnahmen in den Einrichtungen der Universität sowie insbesondere Mittel zur Schulung für die dezentralen IT-Sicherheitsbeauftragten sind von den betreffenden Einrichtungen aufzubringen, die Mittel für diese Zwecke in ihrer Finanzplanung angemessen zu berücksichtigen haben.

(2) Soweit Sicherheitsmaßnahmen aus zentralen Mitteln finanziert werden müssen, ordnet der/die zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Sicherheitsstab diese nach Dringlichkeit in einer Liste. Mit einer Begründung der Prioritäten schlägt er dem Präsidenten die Finanzierung vor.

Übersicht dieses Vortrages

- **Persönliches**
- **Informationssysteme**
- Einführung in die **Informations- und Datensicherheit** und die zugehörigen **Strukturen** an der **Universität Hannover**
- **Probleme** und **Maßnahmen** an der **Universität Hannover**

Probleme und Maßnahmen an der Uni H

- Problem: Strukturen, d. h. u. a. die **Aufteilung** von **Lasten** und **Pflichten** versus **Ressourcen** und **Befugnissen**, an der Universität Hannover sind (noch?) **nicht mit einem privatwirtschaftlichen Unternehmen vergleichbar**
- **Notfallblatt** (inkl. Mobilfunknummern der Anwesenheitsliste)
- **Rundschreiben** für das **Vademecum** (5.32 IT-Sicherheit)
- Informelle **Newsletters** (auch zum Download)
- Turnusmäßige **Schulung** (und **Prüfung**?!) der **dezentralen IT-Sicherheitsbeauftragten,** evtl. verbunden mit „Sicherheitstagen" des RRZN zweimal/Jahr)
- Evtl. **Zertifizierung** für Informations- und Datensicherheit (BSI-Grundschutz, BS 7799 bzw. ISO/IEC 17799:2002, …)

Probleme und Maßnahmen an der Uni H

- **Analyse** der **Informationssysteme** und **Klassifikation** nach **Wichtigkeit** sowie **Schutzbedarfsfeststellung**
- **Zugangskontrolle** von **Räumen**, **Rechnern** und **Netzwerkzugängen** (**drahtgebunden** und **drahtlos**) sowie sinnvolle Authentifizierung und Autorisierung
- **Firewalls** und **Virenscanner**
- **Updates** (evtl. automatisch vom RRZN) von **Betriebssystemen** und **Software** allgemein
- **Spam** und **unerlaubte Attacken** Dritter, **urheberrechtliche Fragen** und **verbotene Inhalte** (Filme, Musik, politische und pornographische Inhalte, …)
- **Belangung** von **Straftätern** (Studierende, Mitarbeiter, …)

Probleme und Maßnahmen an der Uni H

- **Vorgehen** bei **Verstößen gegen Richtlinien** für **Informations- und Datensicherheit**: Dienstweg, Zuständigkeit, Verantwortlichkeit und Befugnisse, Zugang zu Paßworten, sinnvolle Paßwörter und Verschlüsselung wichtiger Dokumente und Informationen …
- „Studentische oder Wissenschaftliche **Hilfskraft** als **Administrator**"
- **Vorkonfigurierte** und **ferngewartete Basissysteme** bereitgestellt durch das RRZN
- **Datensicherung/Backups** (evtl. automatisch vom RRZN)
- **Sicherheitsstrategien** für die **Verwaltungen** und **Datenschutz**

Probleme und Maßnahmen an der Uni H

- **Ausfallsicherheit** im **Serverbetrieb** & **Hosting** (WWW, Email, Applikationen, P2P, ...)
- **Sichere Browser** und **Netzwerkanwendungen**
- **Blacklists** von **Hard-** und **Software** mit Sicherheitslücken
- **„Externe IuK-Geräte"** von **Studierenden**, **Gästen**, ..., insb. **mobile Geräte** wie **Laptops**, **Subnotebooks**, **PDAs**, **MDAs**, **Smartphones** und auch **Mobiltelefonen** ...
- **Wichtige Informationen** nach dem **„Push-Prinzip"** (z. B. Emails des RRZN oder von anderer Seite), statt nach dem **„Pull-Prinzip"** (regelmäßiger Download)
- **Arbeitszeitkontingente für Beauftragte** für Daten- und Informationssicherheit (Anreize, statt Zusatzaufgabe, und Wertschätzung der Leitungseinrichtungen)

www.iwi.uni-hannover.de/it-sicherheitsbeauftragter.html