Sicherheitstage RRZN
Leibniz Universität Hannover
WS 2006/07

20. November 2006

Michael H. Breitner

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Darüber werden wir reden:

- Ein paar Worte zu mir **persönlich**;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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

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

Datei Bearbeiten Ansicht Favoriten Extras ?

Adresse http://www.iwi.uni-hannover.de/wir_index.html?/mitarbeiter/mb.html Wechseln zu Links

Institut für
Wirtschaftsinformatik
der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

- Home
- Wir
  - Mitarbeiter
  - Adresse/ Anfahrt
- Lehre aktuell
- Lehre
- Forschung
- Publikationen
- Tagungen
- Service
- IT-Sicherheits-beauftragter
- CIP-Pool
- 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

Fertig Internet

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- **IT-Sicherheit** – aus meiner Sicht besser: **Informations-sicherheit** – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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 LUH bereitzustellen
- **Informationsverarbeitungs-** und **Kommunikations-systeme wachsen zusammen**, vgl. z. B. globale IP-Telefonie neben Chats und Email, Videokonferenzen, MS Messenger oder Datenübertragung mit GPRS, UMTS, usw.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Trends & Technologiefolgenabschätzung:

Mobile IP-Telefonie durch weitverbreitete WLANs

COMPUTER ZEITUNG

Die Website für die Informationsgesellschaft

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.

CZ
H
D
Fa
Li
CZ
Stel
Bus
Terr

Quelle: Computerzeitung 12, 2004, Seite 18

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Aktuelle Smartphones & PDAs: handit.de

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Trends & Technologiefolgen:
„Der PC in zehn Jahren“

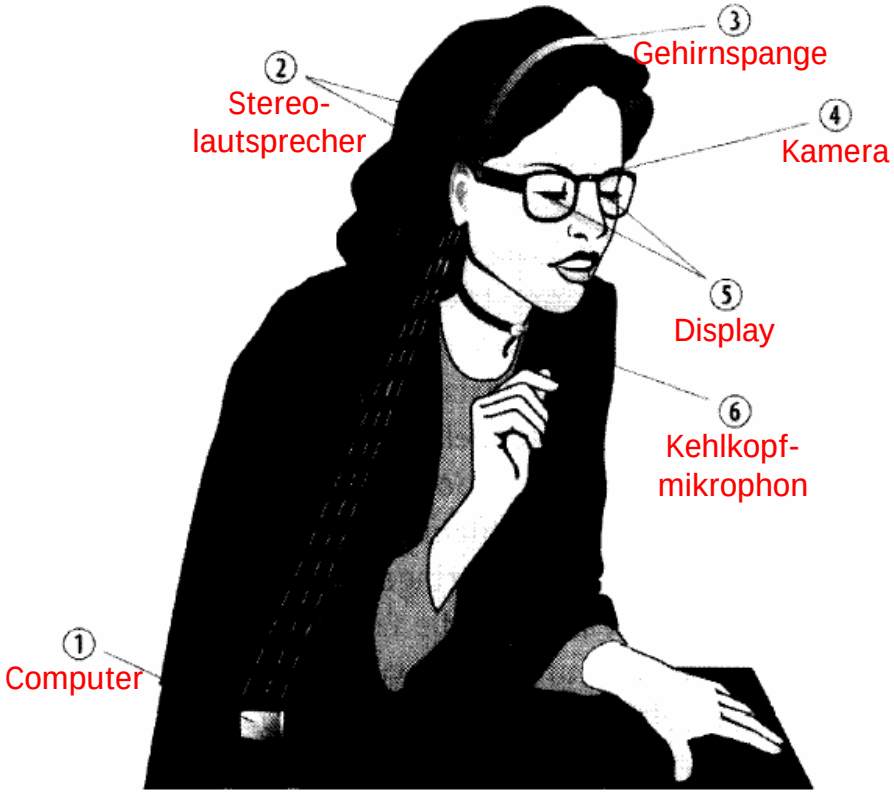


Abb. 1

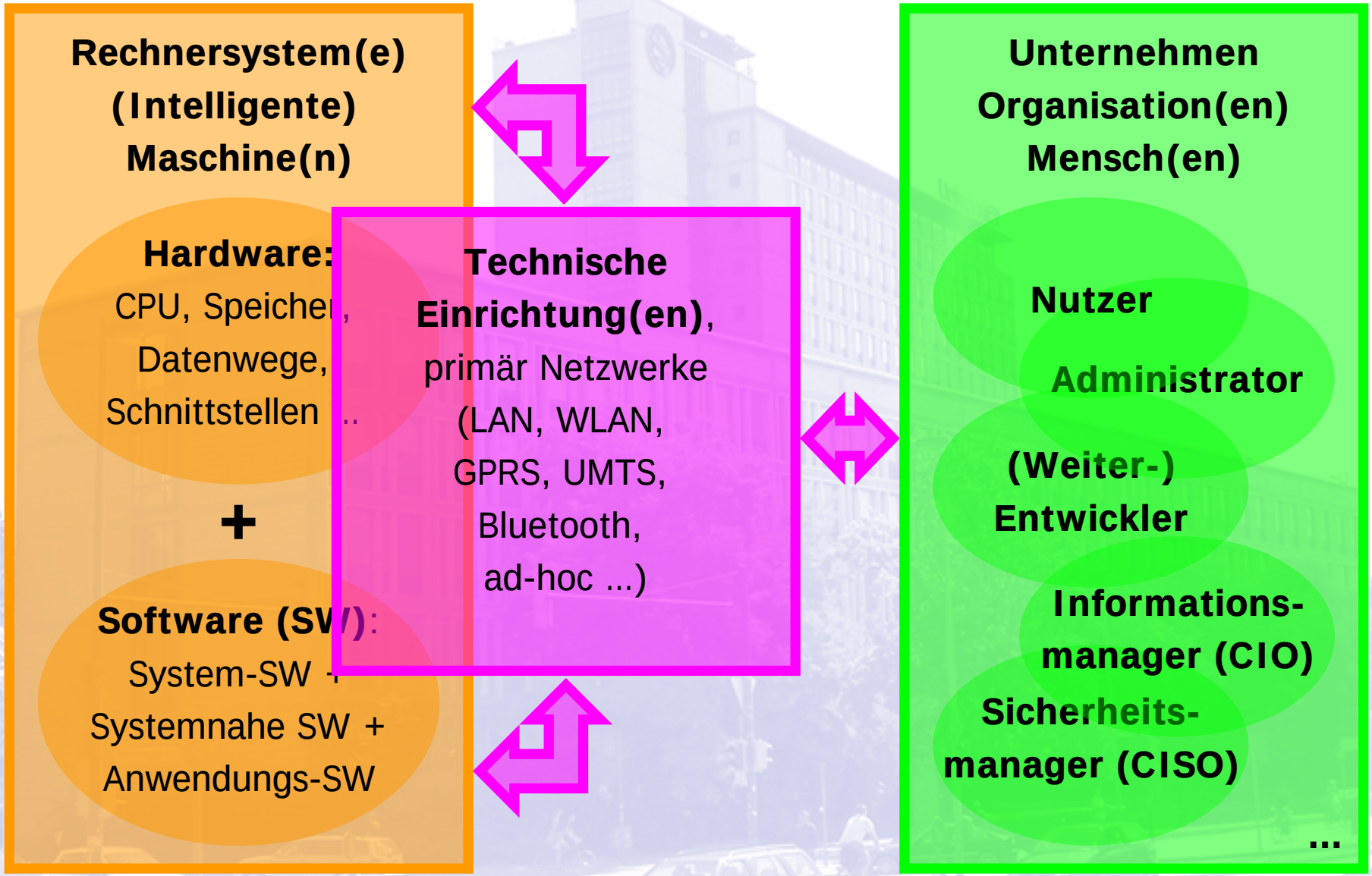
hohen Tönen, manche – wie Delete-, Enter- oder

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.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Informationssystem: Prinzipieller Aufbau



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das **BSI** zu IT-Sicherheit: **Grundschutz** kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Leitfaden IT-Sicherheit des BSI

Bundesamt
für Sicherheit in der
Informationstechnik

Leitfaden
IT-Sicherheit

IT-Grundschutz kompakt

Download als PDF Datei: http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Leitfaden IT-Sicherheit des BSI

Dr. Udo Helmbrecht
Präsident des Bundesamtes für Sicherheit
in der Informationstechnik (BSI)

Arbeits- und Geschäftsprozesse basieren immer stärker auf IT-Lösungen. Umso wichtiger wird deshalb die Sicherheit und Zuverlässigkeit von Informations- und Kommunikationstechnik. Mit dem richtigen IT-Sicherheitskonzept können Sie ein solides Fundament für ein vertrauenswürdiges IT-Sicherheitsniveau legen. Dieser Leitfaden hilft Ihnen dabei: In kompakter Form finden Sie einen Überblick über die wichtigsten Sicherheitsmaßnahmen. Praxisbeispiele machen auf Gefahren aufmerksam und veranschaulichen die notwendigen organisatorischen, infrastrukturellen und technischen Maßnahmen. Checklisten unterstützen Sie bei der Analyse der eigenen Situation. Damit steht fest:

Der Weg zu mehr Sicherheit ist auch ohne große IT-Budgets möglich.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Leitfaden IT-Sicherheit des BSI

Inhaltsverzeichnis

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

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

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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

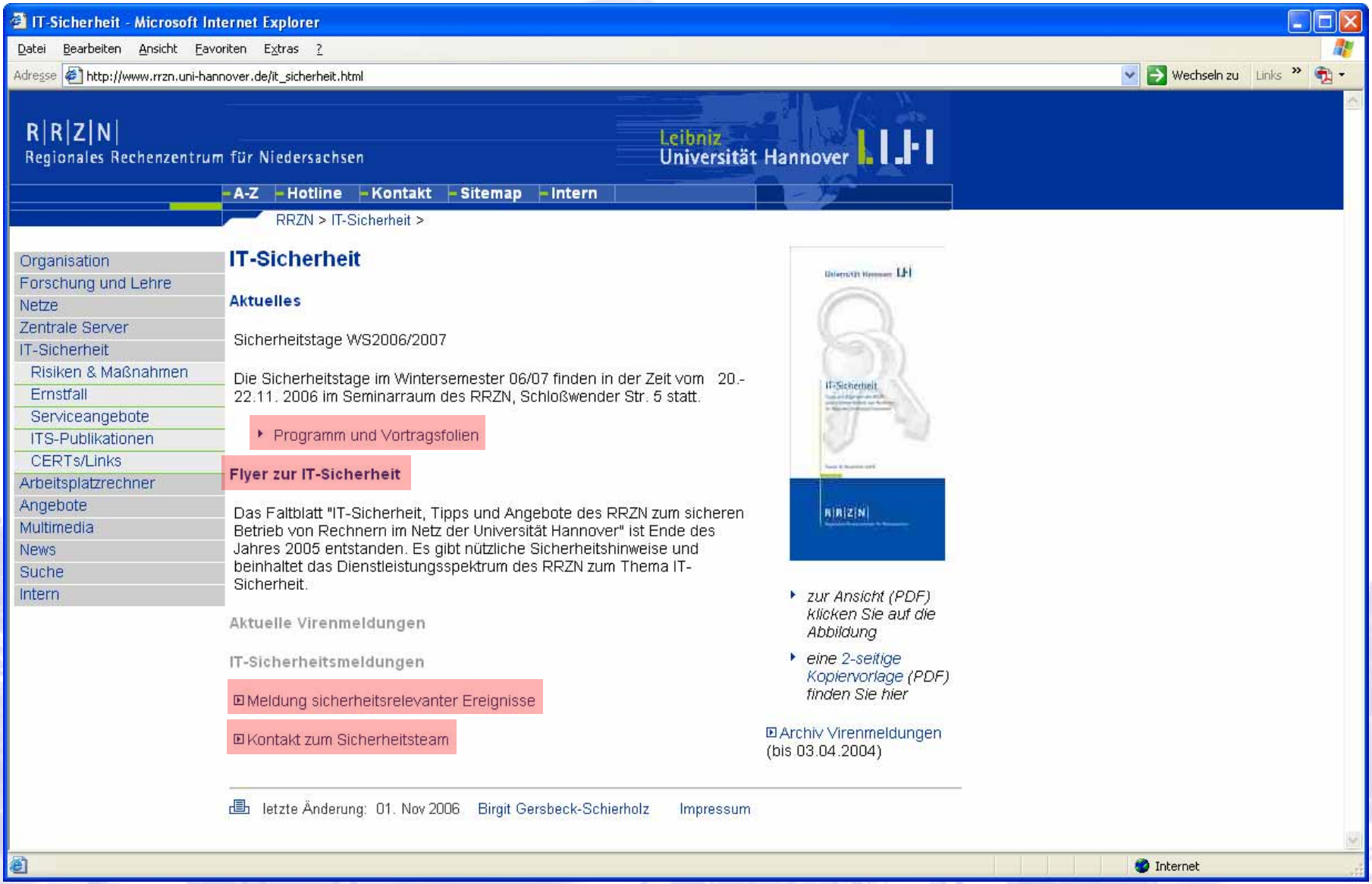
- **Planung**, die
- **Realisierung** und die
- **Kontrolle** der **Informations-** und **Datensicherheit**,

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**.

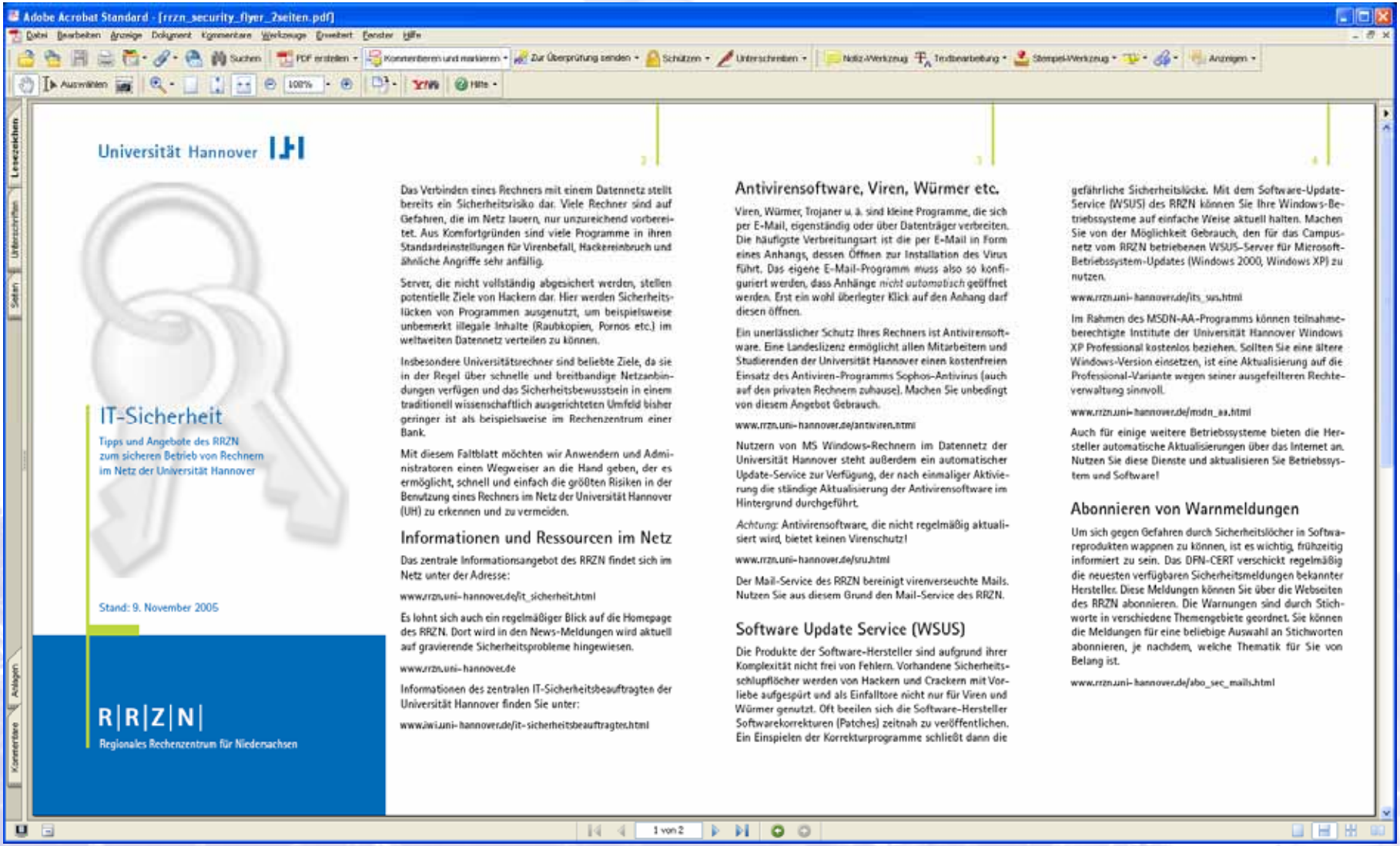
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

RRZN Flyer zur IT-Sicherheit



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

RRZN Flyer zur IT-Sicherheit



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die **Ordnung zur IT-Sicherheit an der LUH**;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

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

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Ordnung zur IT-Sicherheit

ITS-Ordnung - Entwurf Revision 2005

Ordnung zur IT-Sicherheit in der Universität Hannover
(vom Senat beschlossen am tt.mm.2005)

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.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Ordnung zur IT-Sicherheit

§ 4
Einsetzung der IT-Sicherheitsbeauftragten

(1) Das Präsidium bestellt eine/n zentrale/n IT-Sicherheitsbeauftragte/n und eine/n Stellvertreter/in[4].

(2) Jede Einrichtung im Sinne von §2 hat eine/n dezentrale/n IT-Sicherheitsbeauftragte/n und mindestens eine/n Stellvertreter/in[5] zu benennen. Hierbei können mehrere zentrale Einrichtungen in Abstimmung mit dem zentralen IT-Sicherheitsbeauftragten eine/n gemeinsame/n dezentrale/n IT-Sicherheitsbeauftragte/n benennen.

(3) Die Einrichtungen im Sinne von §2 benennen Personen, die im Auftrag der Leitung der jeweiligen Einrichtung die operativen Aufgaben der IT-Sicherheit vor Ort wahrnehmen, als lokale IT-Sicherheitsbeauftragte.[6]

(4) Durch die Benennungen nach (2) müssen **alle** Netzzugänge und IT-Systeme im Geltungsbereich sowie alle lokalen IT-Sicherheitsbeauftragten einer/m dezentralen IT-Sicherheitsbeauftragten zugeordnet sein. Erforderlichenfalls entscheidet der/die zentrale IT-Sicherheitsbeauftragte in Abstimmung mit den Betroffenen über geeignete Zuordnungen.

(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 regelmäßig besonders geschult werden.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Ordnung zur IT-Sicherheit

§ 6
Aufgaben der am IT-Sicherheitsprozess Beteiligten

(1) Der/Die zentrale IT-Sicherheitsbeauftragte ist für Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich und berät das Präsidium in Angelegenheiten der IT-Sicherheit.

(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.[8]

(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 und die lokalen 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 und die lokalen IT-Sicherheitsbeauftragten sind verpflichtet, ihre Kenntnisse bezüglich der für ihren Zuständigkeitsbereich relevanten Aspekte der IT-Sicherheit auf aktuellem Stand zu halten.[9] Zu diesem Zweck sollen auch dezentrale IT-Sicherheitsbeauftragte ihre Kenntnisse an die lokalen IT-Sicherheitsbeauftragten ihres Zuständigkeitsbereiches weitergeben.

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

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Ordnung zur IT-Sicherheit

ITS-Ordnung - Entwurf Revision 2005

§ 9
Strafrechtliche und zivilrechtliche Verantwortlichkeit

Für den Fall rechtlich relevanter Sicherheitsvorfälle behält sich die Universität eine strafrechtliche und/oder zivilrechtliche Verfolgung vor.

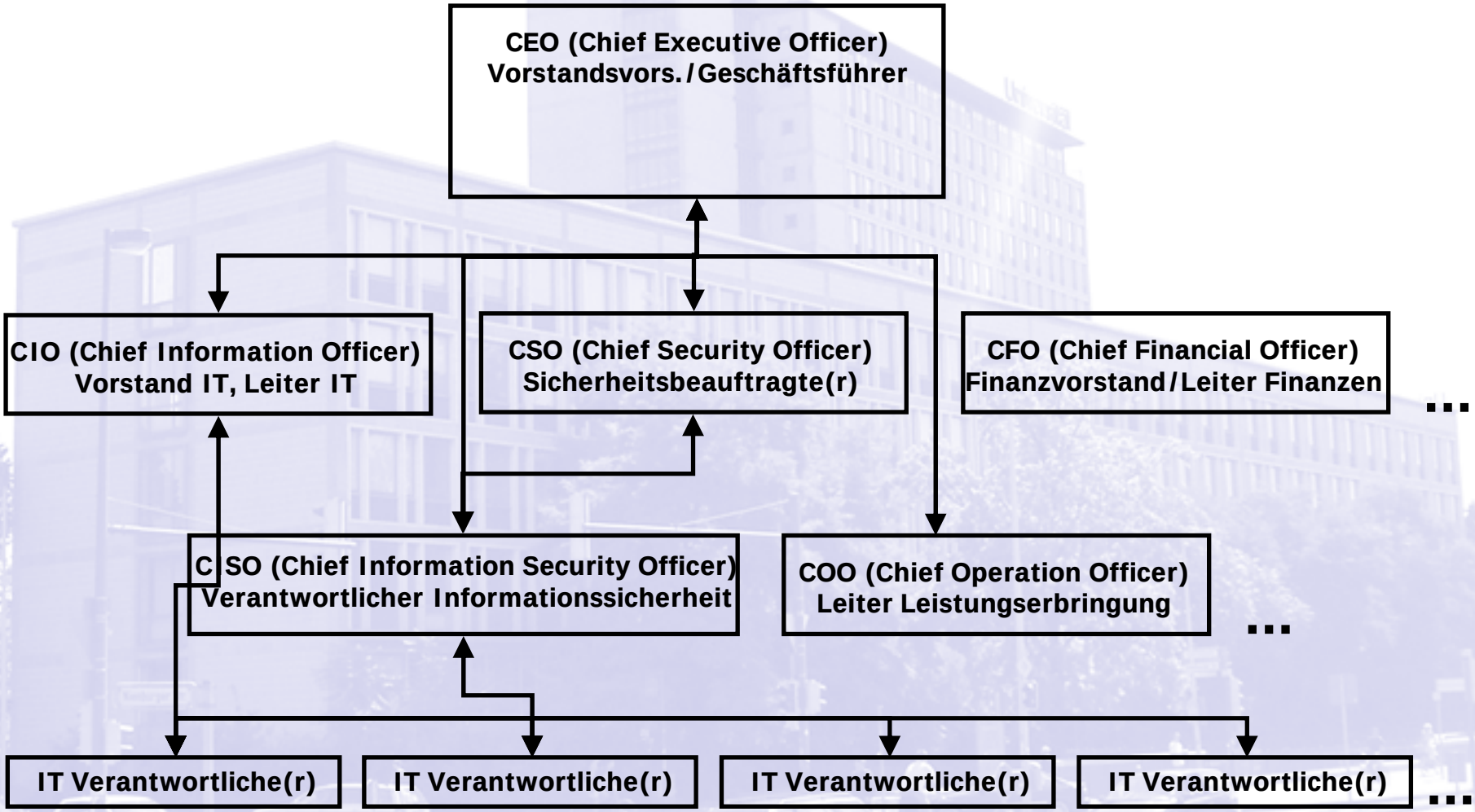
§ 10
Finanzierung

(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, begründet der/die zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Sicherheitsstab die Dringlichkeit und schlägt dem Präsidium - ggfs. auf Basis einer Prioritätenliste - die Finanzierung vor.

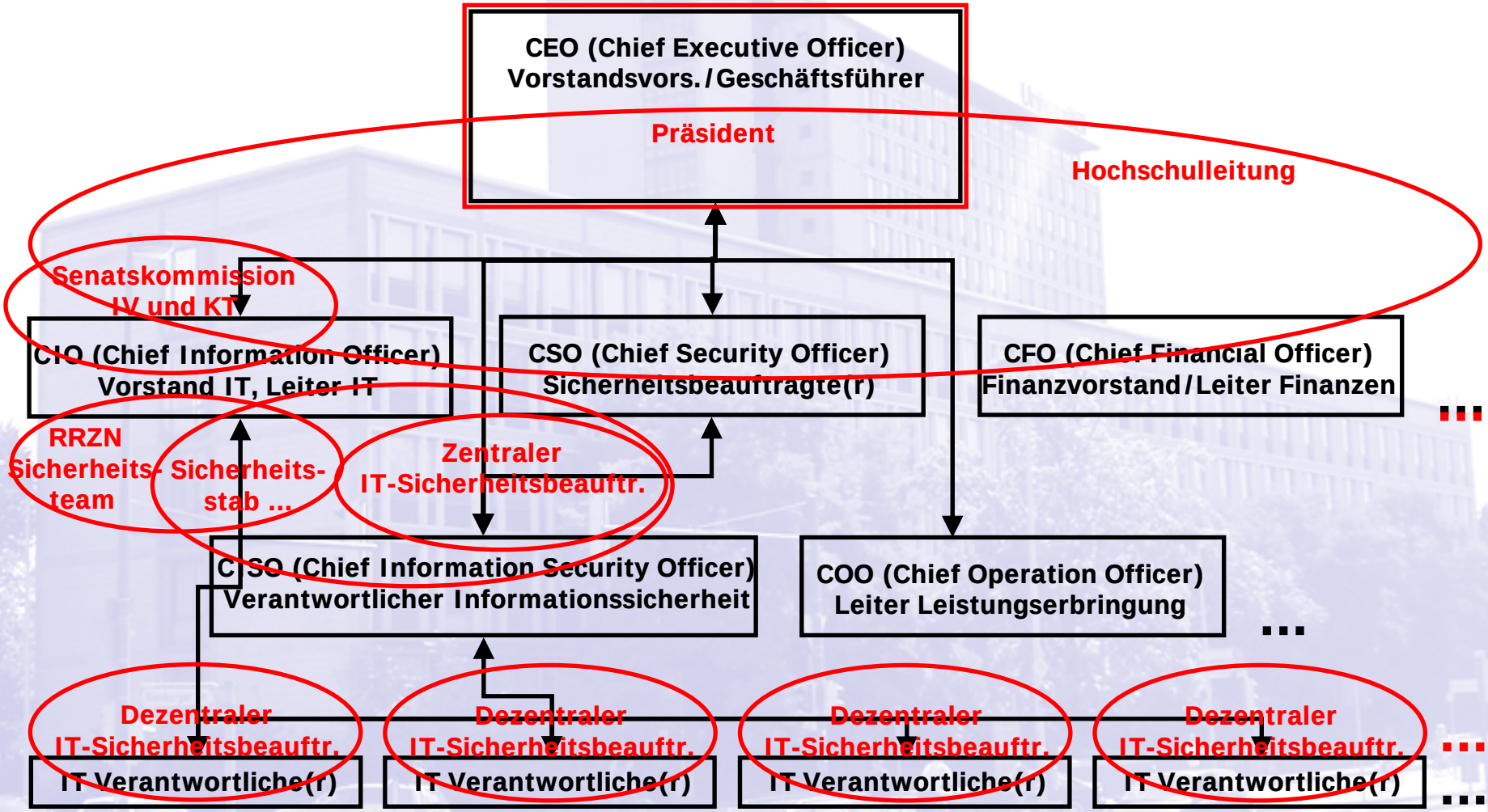
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

IT-Sicherheitstruktur LUH im Vergleich zu privatwirtschaftlichen Unternehmen



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

IT-Sicherheitstruktur LUH im Vergleich zu privatwirtschaftlichen Unternehmen



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Rundschreiben zur IT-Sicherheit

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Rundschreiben zur IT-Sicherheit

IT-Sicherheit	1.4.1

Universität Hannover

Universität Hannover, Postfach 60 09, 30060 Hannover

Das Präsidium
Der zentrale IT-Sicherheitsbeauftragte

bearbeitet von:
Herrn Harnisch
Tel + 49(0)511.7 62-79 46 63
Fax + 49(0)511.7 62-30 03
e-mail: **harnisch**
@rrzn.uni-hannover.de

Rundschreiben A Nr. 35/2005

Universitätseinrichtungen
gem. Verteiler 1 2 3 4 5

h i e r

27.10.2005

Mein Zeichen:
02031-1-2
(bitte bei Antwort angeben)

Ihre Nachricht vom:

Ihr Zeichen:

Vermeidung von Schadsoftware auf Rechnern im Netz der Universität Hannover

Durch den Befall von Rechnern mit Schadsoftware (d. h. Virus, Wurm oder Trojaner) drohen u. a. der Verlust, die Manipulation und der Dieb-

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Probleme und Maßnahmen an der LUH

- Problem: Strukturen, d. h. u. a. die **Aufteilung** von **Lasten** und **Pflichten** versus **Ressourcen** und **Befugnissen**, an der LUH sind (noch?) **nicht mit einem privatwirtschaftlichen Unternehmen vergleichbar**
- **Notfallblatt** (inkl. Mobilfunknummern der Anwesenheitsliste)
- **Rundschreiben** für das **Vademecum** (4.1.4 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, ...)

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Probleme und Maßnahmen an der LUH

- **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 **Betriebs-systemen** und **Software** allgemein
- **Spam** und **unerlaubte Attacken** Dritter, **urheberrecht-liche Fragen** und **verbotene Inhalte** (Filme, Musik, politische und pornographische Inhalte, ...)
- **Belangung** von **Straftätern** (Studierende, Mitarbeiter, ...)

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Probleme und Maßnahmen an der LUH

- **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**

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Probleme und Maßnahmen an der LUH

- **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)

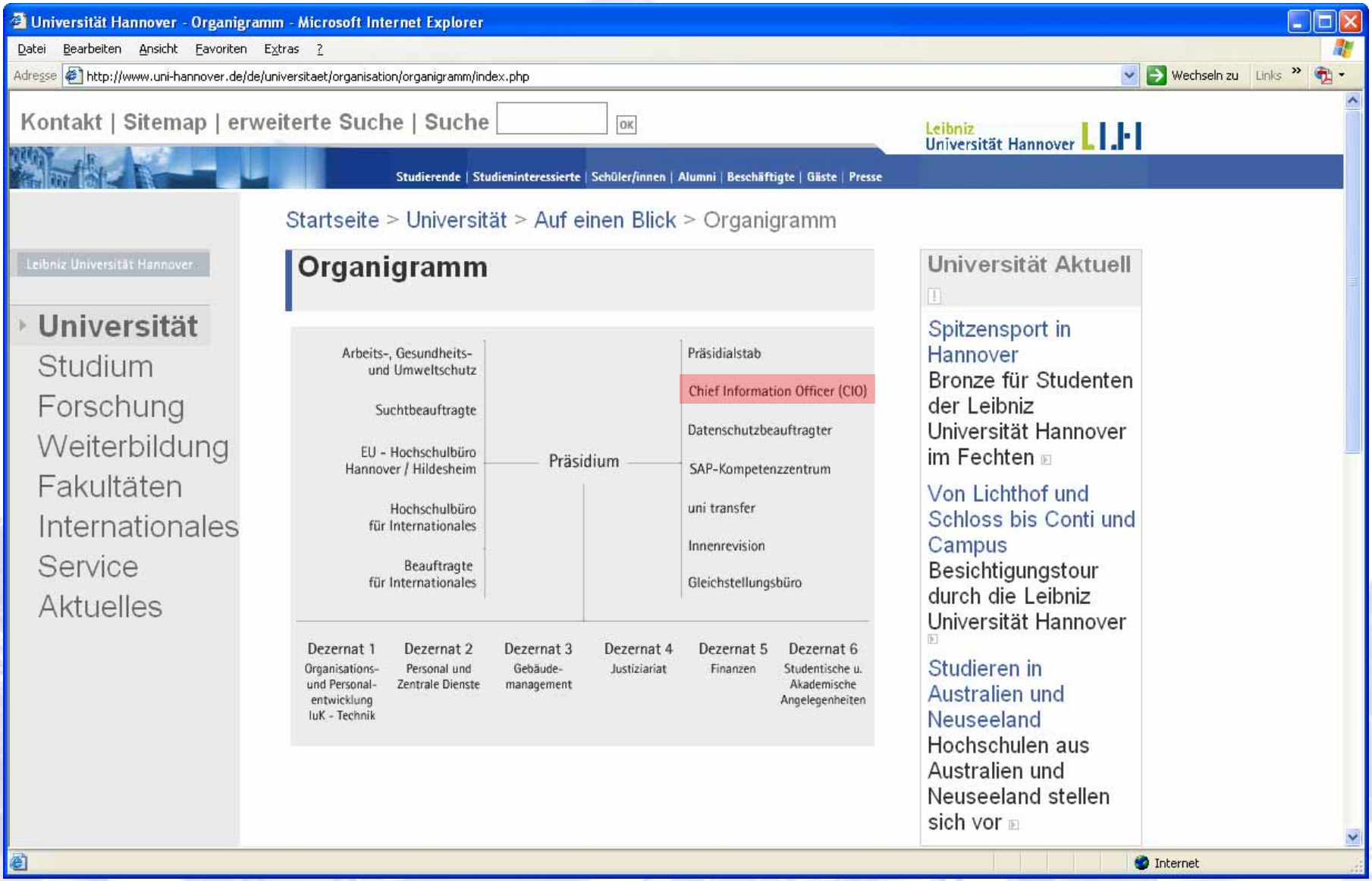
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen **„Chief Information Officer“ (CIO)**;
- IT-Kunden-, IT-Service- und IT-Qualitätsorientierung an der LUH: Ausblick auf ITIL & Co.

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Verwaltungsstruktur der LUH



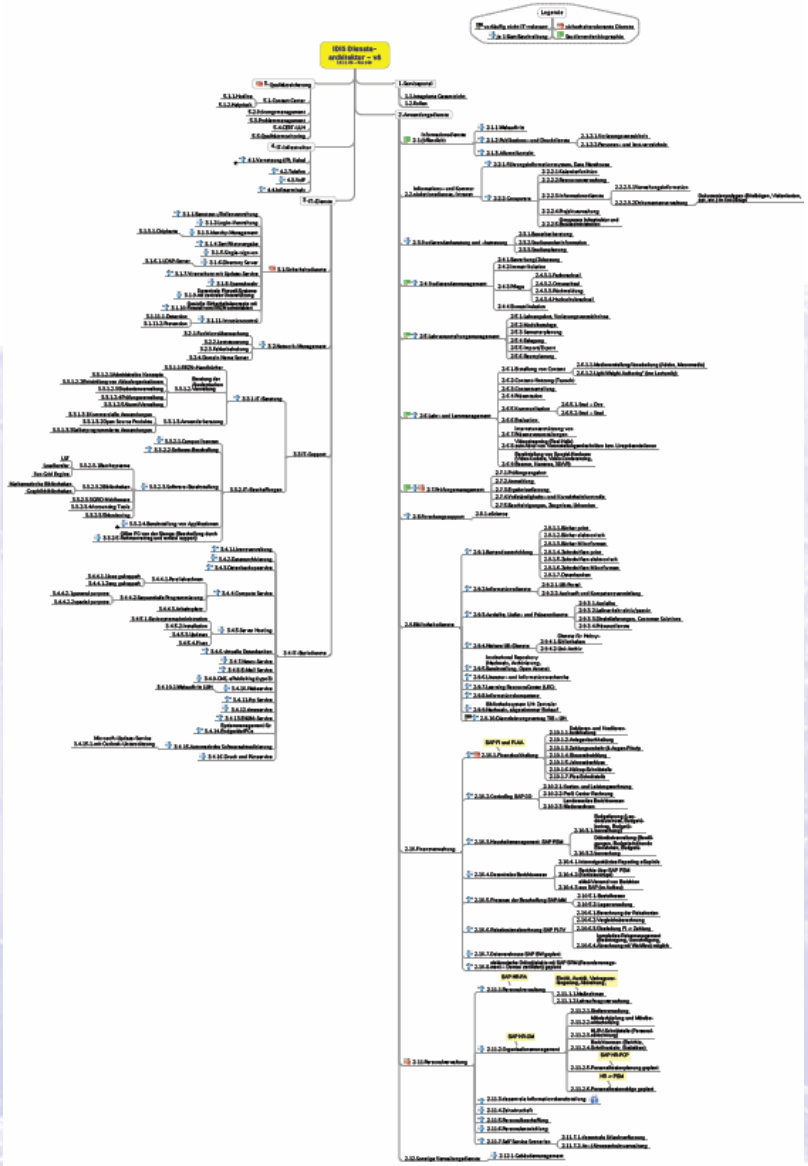
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

Darüber werden wir reden:

- Ein paar Worte zu mir persönlich;
- IT-Sicherheit – aus meiner Sicht besser: Informations-sicherheit – aus der Sicht eines Wirtschaftsinformatikers;
- Das BSI zu IT-Sicherheit: Grundschutz kompakt;
- IT-Sicherheit an der Leibniz Universität Hannover (LUH): Die Ordnung zur IT-Sicherheit an der LUH;
- Und jetzt hat die LUH auch noch einen „Chief Information Officer“ (CIO);
- **IT-Kunden-**, **IT-Service-** und **IT-Qualitätsorientierung** an der LUH: Ausblick auf ITIL & Co.

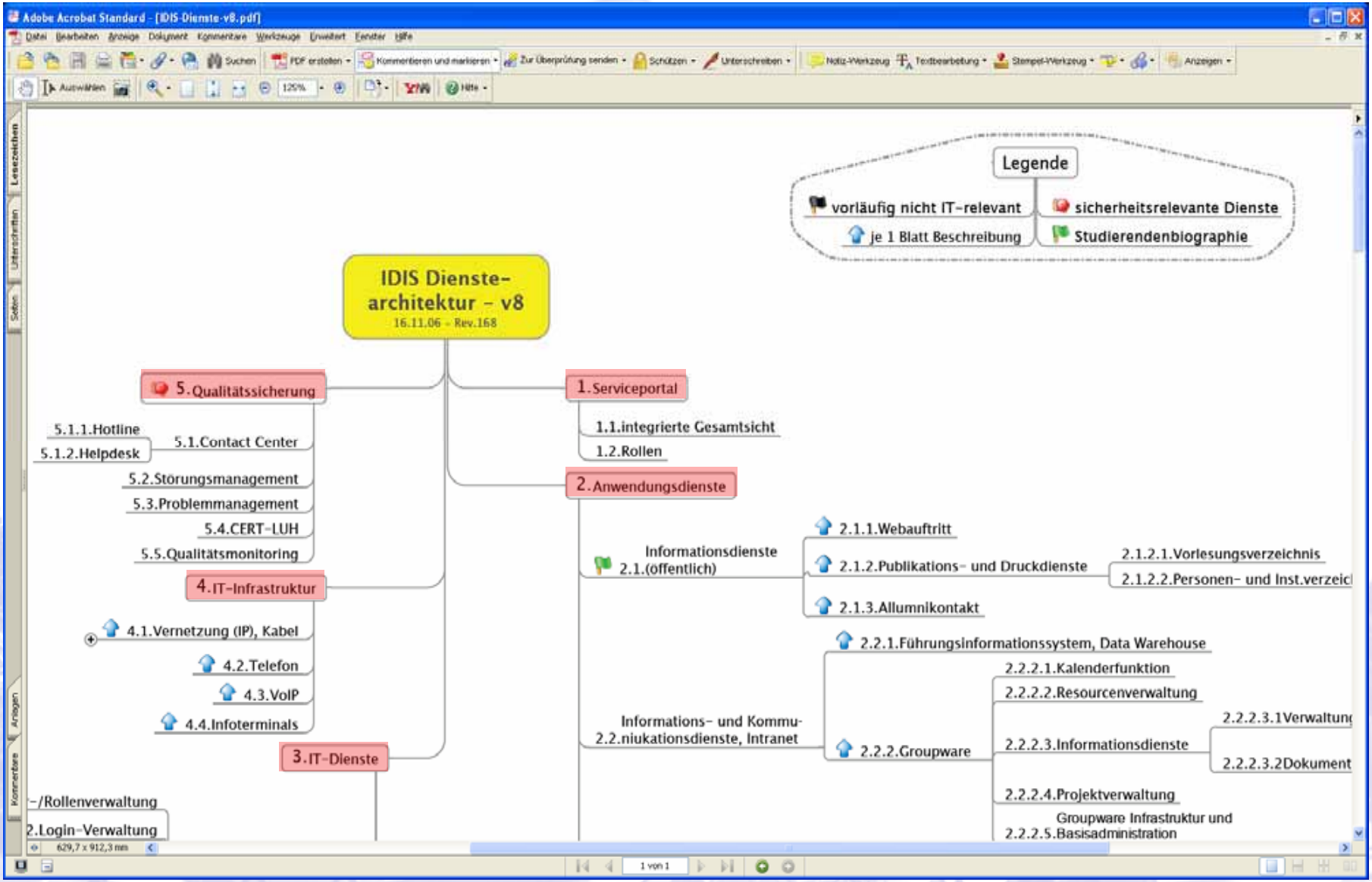
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

IT-unterstützte Dienste der LUH



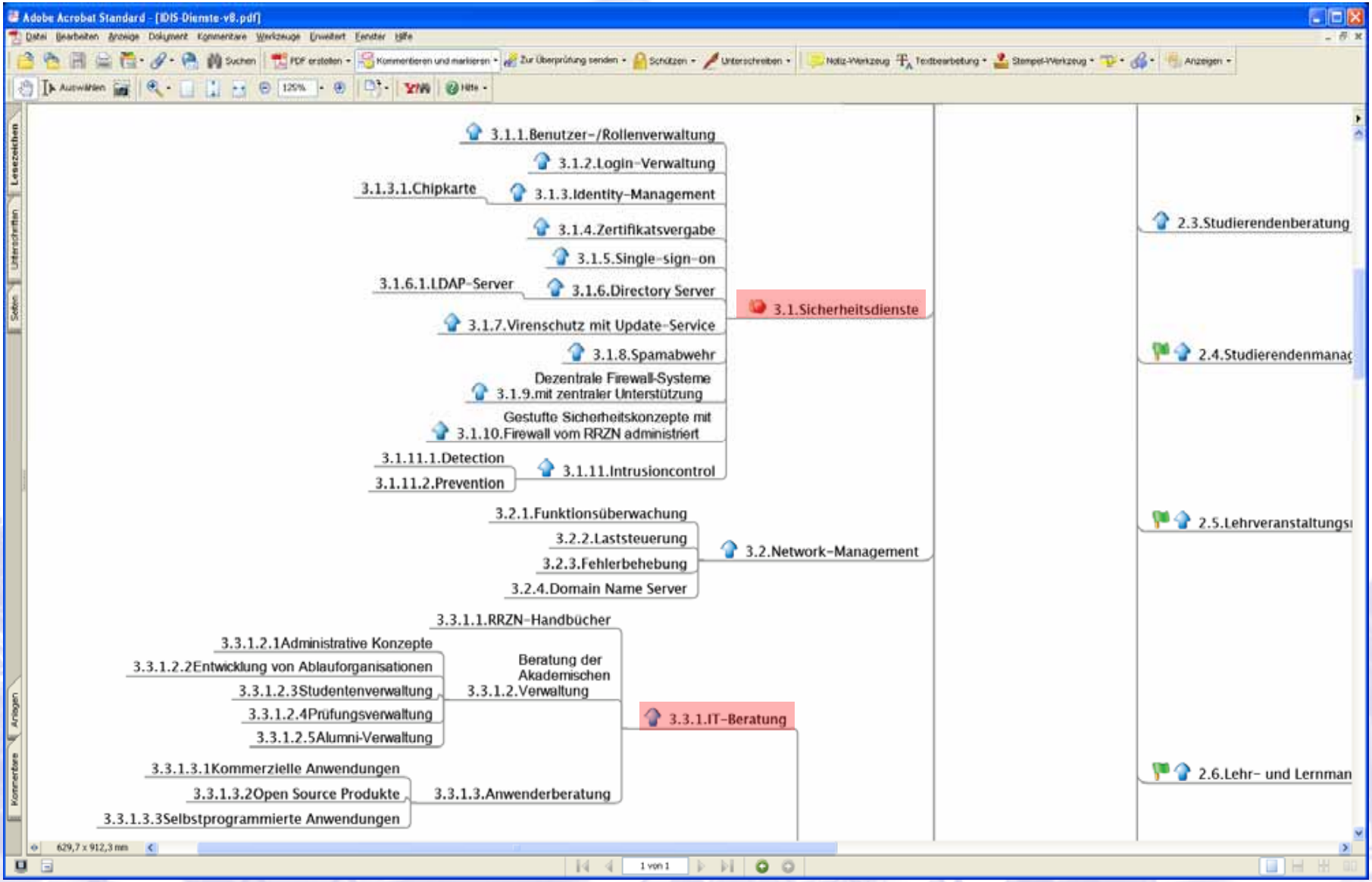
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

IT-unterstützte Dienste der LUH



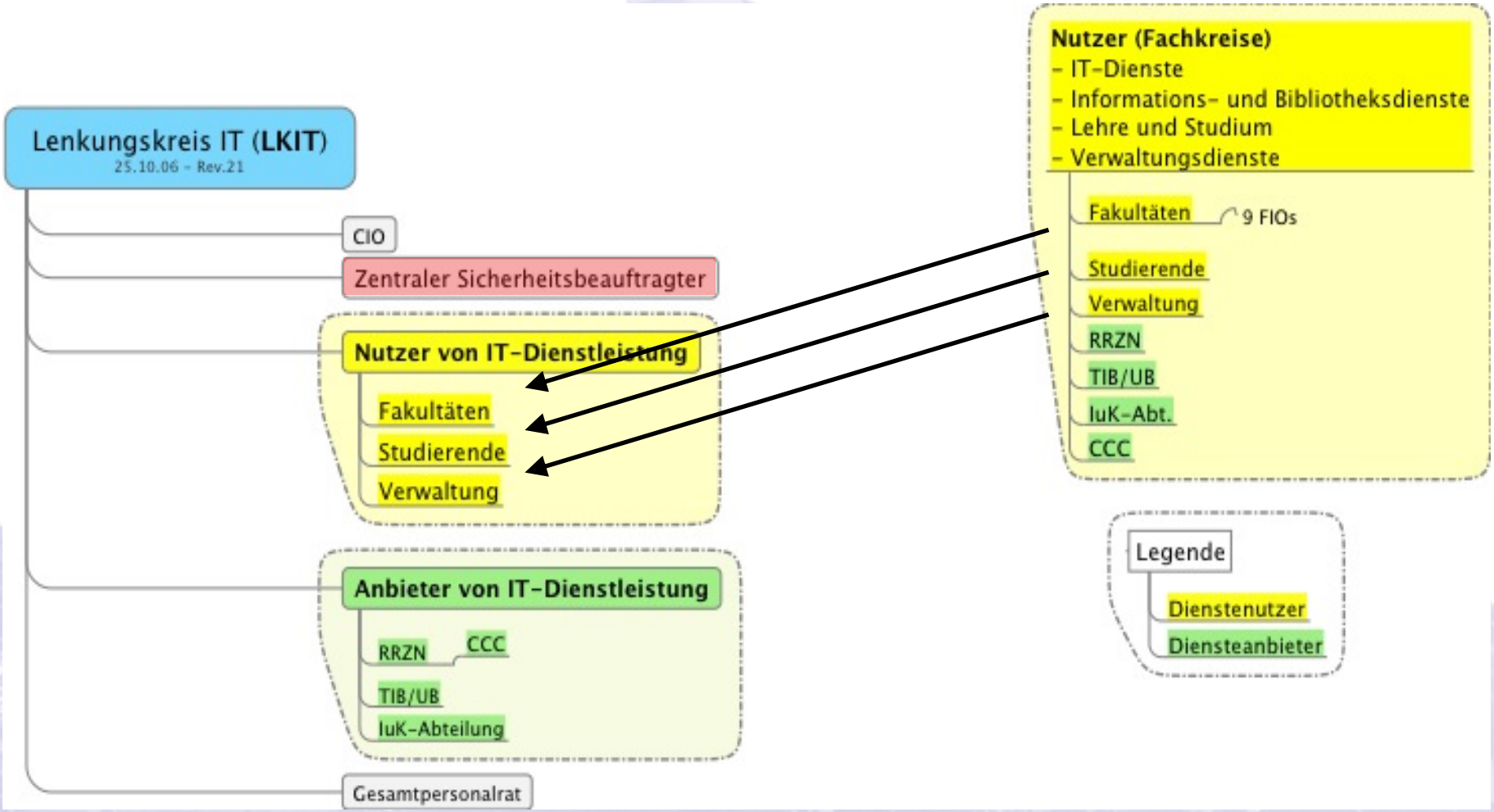
Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

IT-unterstützte Dienste der LUH



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover © 2006

IT-unterstützte Dienste der LUH



Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Auf dem Weg zu 11 ITIL-Kernprozessen

Availability Management

IT Service Continuity Management

Capacity Management

Security

Financial Management for IT Services

Release Management

Service Delivery Set

IT Infrastructure

Service Level Management

Change Management

Service Support Set

Service Desk

Configuration Management

Incident Management

Problem Management

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover

Auf dem Weg zu 11 ITIL-Kernprozessen

IT Service Continuity Management

Availability Management

Capacity Management

Service Delivery Set

Service Support

Service Desk

Configuration Management

Incident Management

Problem Management

Vielen Dank für Ihr Kommen, Ihre Aufmerksamkeit und auf gute Zusammenarbeit!

Prof. Dr. Michael H. Breitner (breitner@iwi.uni-hannover.de)
Institut für Wirtschaftsinformatik / Leibniz Universität Hannover