guten Morgen

Alfons Rissberger

www.**rissberger**.de

- Geschäftsführer
  DVZ M-V GmbH
- Geschäftsführender Gesellschafter
  DVZ Consulting GmbH
- Ideengeber und Mitglied des
  Vorstands der INITI@TIVE D21

- ohne IT keine Zukunft im Wettbewerb: Weiterentwicklung noch schneller, konzentrierter, prozessorientierter, kostenbewusster ...
- „IT vernichtet Arbeitsplätze“: 1979 DGB-Kongress Mainz, 1996 CeBIT-Ausgabe der FAZ, Sept. 2002 Bundespressekonferenz: Okt. 2002, Gartner USA „IT vernichtet massenhaft Arbeitsplätze“

IT im Zeitalter des Sparens

was können und müssen wir uns erlauben?

Problem 1: nie da gewesener Kostendruck auch im Bereich IT

- stark gekürzte IT-Budgets fließen in Betrieb; Zeit und Geld für Innovation als Teil notwendiger IT-Strategie fehlen
- 20 Jahre IT: ständig neue Aufgaben und Forderung nach mehr Mitarbeitern; zweistellige Wachstumsraten der IT-Budgets waren Alltag
- IT muss sich auf Wesentliches fokussieren und scharf fragen, was sich eine Institution leisten kann
- durch Effizienzsteigerungen mit IT lässt sich mehr sparen als man investieren muss
- Ausgaben für Betrieb der IT-Systeme < 60% des Budgets
- keine Nützlichkeitsversprechen, sondern nachgewiesene Vorteile zählen
  - selbst kein Neuland betreten; Erfahrungen anderer nutzen
  - qualitatives und quantitatives Benchmarking
  - optimales Projektcontrolling

IT im Zeitalter des Sparens

was können und müssen wir uns erlauben?

Problem 2: weiter zunehmende Innovationsgeschwindigkeit

- papierloses Büro
- Spracherkennung
- Handschrifterkennung
- Wissensmanagement: Lotus Discovery Server
  erstmals: wirksame Nutzung von Wissensdatenbanken
  > Lernen just in time statt Lernen auf Vorrat
- Wireless LANs, Hotspots, UMTS: Sicherheit
- BLACKBERRY
- Sprachübersetzung

- **Gefahr: Innovationsmüdigkeit,**
  da früher Nutzwertversprechen nicht eingelöst wurden

IT im Zeitalter des Sparens

was können und müssen wir uns erlauben?

Problem 3: wer verantwortet die IT-Strategie, wer hat das entsprechende Know-how und was gehört dazu

- Know-how des CIOs: primär geschäftsorientiertes Denken und Handeln und bereichsübergreifende Zuständigkeit:
  mehr Generalist als Spezialist !
  - Management
  - Organisation, Prozesse
  - IT-Aufwand und –Nutzwert
- aber: die Verantwortung für prozessbezogene IT-Projekte liegt bei Fachabteilungen
- Projektleiter: 80% Psychologie, 10% Fachexperte, 10% Betriebswirt
- auch die negativen Seiten der Medaille aktiv kommunizieren: Auswirkungen auf Arbeitsplätze
  (neuer Fürsprecher: Thomas Ganswindt,
  Siemens-Konzern-Vorstand, neuer VV der INITI@TIVE D21)

IT im Zeitalter des Sparens

was können und müssen wir uns erlauben?

Problem 4: Paradigmenwechsel

- nicht IT-Unterstützung bestehender Prozesse, sondern bessere/neue Prozesse durch IT
- IT betrifft alle Bereiche: „nichts geht ohne IT“

Problem 5: Pflicht vor Kür

- IT-Sicherheit , insbesondere der Netzwerke
- Datenschutz
- Serverkonsolidierung

- Beispiel für Kür kann sein: CRM-Software
  (leitet sich aus Ihren Geschäftsanforderungen inkl. Ihrer Geschäftsprozesse ab)

IT im Zeitalter des Sparens

was können und müssen wir uns erlauben?

Problem 6: IT Chefsache?

Beispiel GF Deutscher Landkreistag

davon verstehe ich nichts
dafür habe ich meine Leute
aber vor Einführung Betrachtung von Aufwand und Nutzwert

notwendig: schriftliche Darstellung von Aufwand und Nutzwert, Management-summary für Geschäftsleitung nachvollziehbar, d.h. verständlich !

- sind Ihnen Ihre IT-(Rest-)Risiken bekannt?
- notwendig: Verschriftlichung aller Risiken und der Maßnahmen zur Risikominimierung
- insbesondere der Gründe, warum Sie bestimmte Risiken hinnehmen
- es ist grob fahrlässig, wenn die Dokumentation angemessener Maßnahmen fehlt!

IT-Revision zwingend?

Verantwortung der Organschaft

- strategische IT-Entscheidungen sind Chefsache, Grundsatzentscheidungen nicht delegierbar
- notwendig: schriftliche Darstellung von Aufwand und Nutzwert, Summary für Geschäftsleitung nachvollziehbar
- für Datensicherheit und Datenschutz haftet Organschaft und verlässt sich auch auf Wirtschaftsprüfer (Risikomanagement)
- sind uns die alltäglichen Risiken eigentlich ausreichend bewusst?
  - Beispiel Vertraulichkeitserklärung per Fax > unverschlüsselte Mail mit Firmengeheimnissen
- wird man fahrlässig, wenn lange Zeit kein Unfall passiert ist?

Externe IT-Revision

nachgewiesener Kundenutzen

- Risikobewusstsein, Risikominimierung (KonTraG)
  = „Gewissen“ der Unternehmens-IT
- Transparenz der IT-Komplexität und neutrale Beurteilung
- Gewissheit über tatsächliches Sicherheitsniveau, Restrisiken, Nutzwert von Vorhaben und Projekten, Zweckmäßigkeit ...
- Schwachstellen > Empfehlung machbarer, wirkungsvoller Maßnahmen
- kein dauerhafter eigener Aufwand für kurzfristige jährliche Notwendigkeit
- gleichzeitig Know-how-Transfer durch zertifizierten Prüfer, Prüfer muss CISA sein
  (Certified Information System Auditor)

Realität

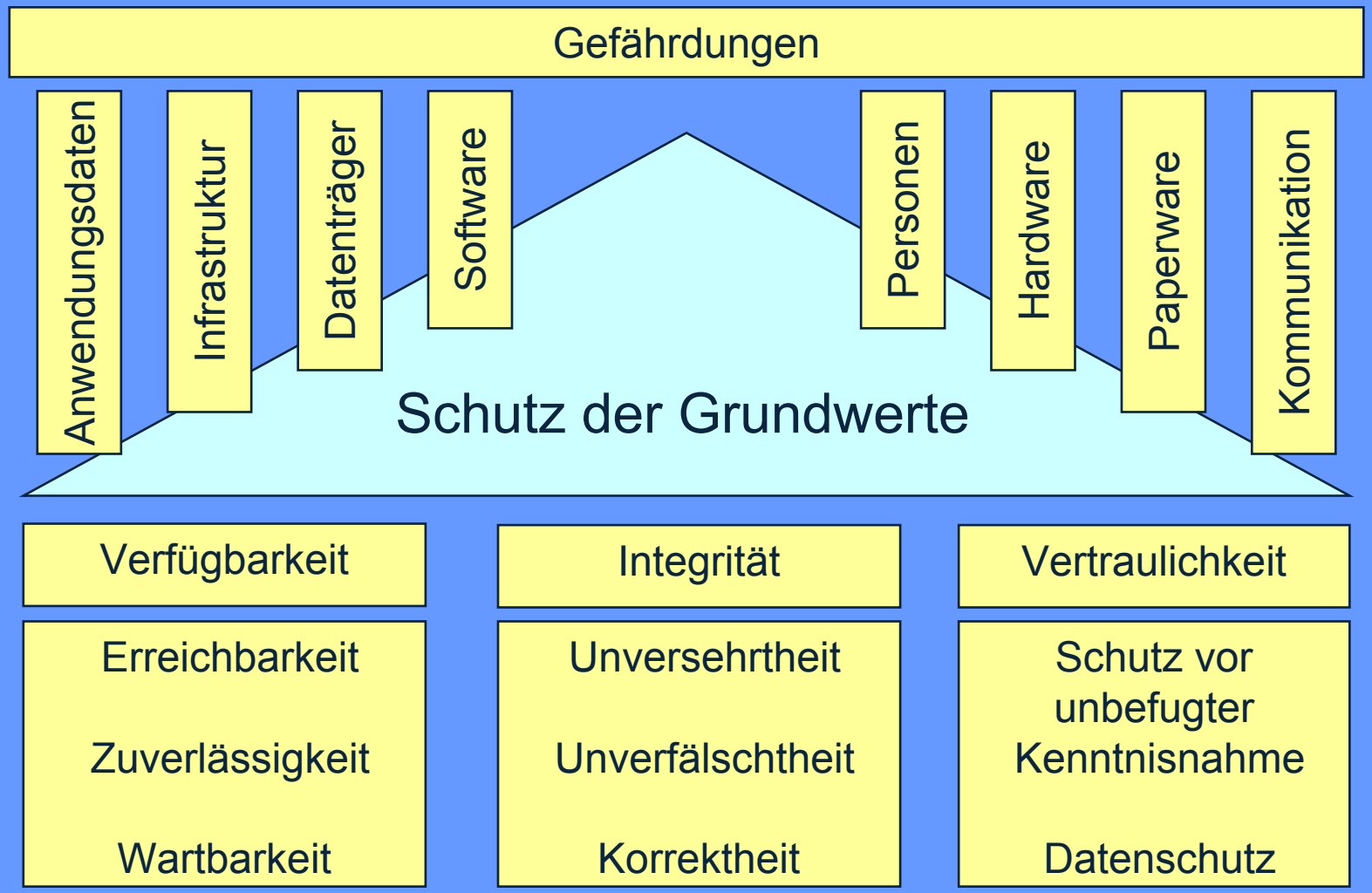
oder: ein Vorstand ist schockiert...

- völlig unzureichende Zugangsregelungen zu aktiven Netzkomponenten und Servern
- unkontrollierte Anwesenheit von Fremden in sensiblen Bereichen
- Vielzahl potentieller Angriffspunkte für Datenklau und Sabotage
- ungenügender Zugriffsschutz auf Router und Server
- bislang unbemerkt gebliebene, unberechtigte Zugriffsversuche auf Systemressourcen
- eklatante Mängel bei der Datensicherung und Notfallvorsorge

- wollen Sie mit einem Bein vor dem Richter stehen?

Bedrohungspotenzial

eine Kette ist so stark …



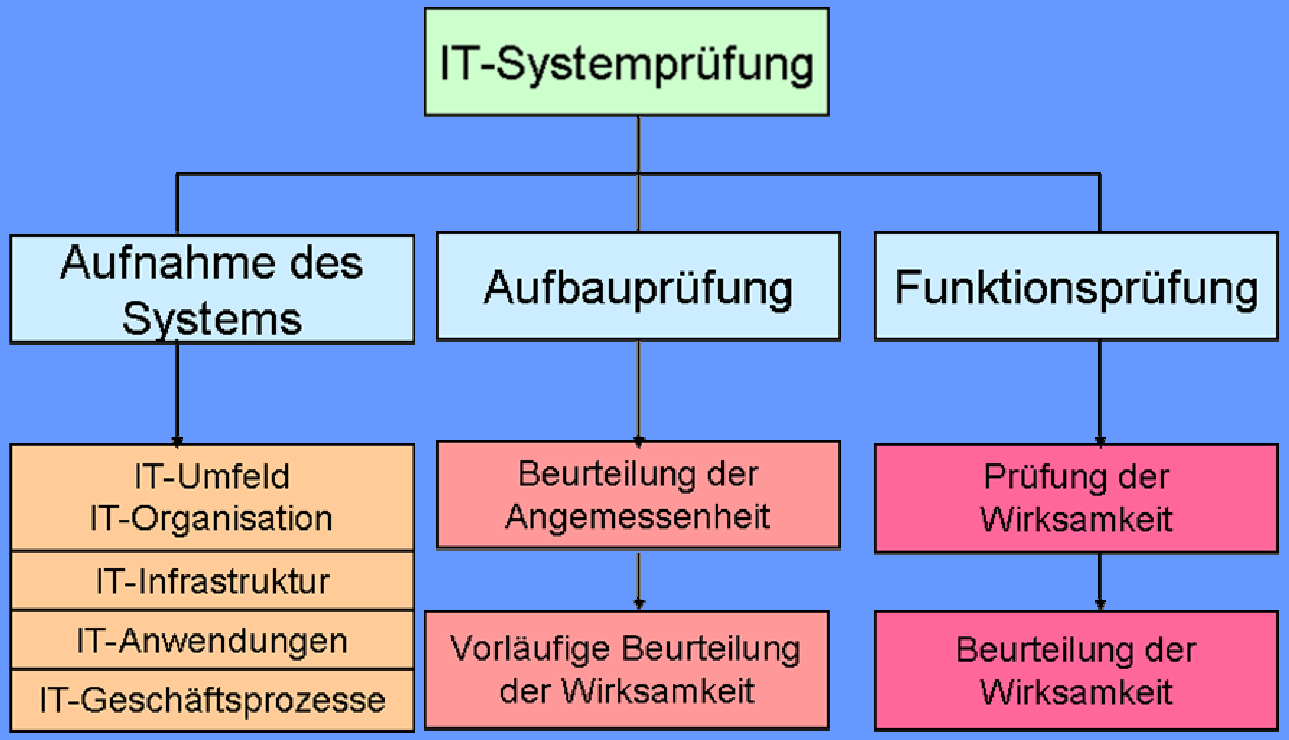
Umgang mit (Rest-) Risiken

mehr Konsequenz zwingend

- sind Ihnen Ihre IT-(Rest-)Risiken bekannt?
- notwendig: Verschriftlichung aller Risiken und der Maßnahmen zur Risikominimierung ...
- insbesondere der Gründe, warum Sie bestimmte Risiken hinnehmen
- es ist grob fahrlässig, wenn die Dokumentation angemessener Maßnahmen fehlt !

IDW Prüfungsstandard 330 [1]

„Abschlussprüfung bei Einsatz von IT“



- definitive Vorgabe für Wirtschaftsprüfer seit 2 Jahren
- macht er das - kann er das?
- sind Sie auf solche Prüfungen vorbereitet?

[1] IDW = Institut der Wirtschaftsprüfer

IDW Prüfungsstandard 330

Prüfungsumfang

- IT-Umfeld und IT-Organisation
  Strategie, Sicherheitskonzept, Aufbau- / Ablauforganisation, …
- IT-Infrastruktur
  physische Sicherung, Zugriffskontrollen, Datensicherung, Notbetrieb, Sicherung der Betriebsbereitschaft
- IT-Anwendungen
  Softwaresicherheit, GOB, Verarbeitungsregeln, Test, Freigabe
- IT-gestützte Geschäftsprozesse
  Daten-, Belegfluss, Schnittstellen, Kontrollen
- IT-Überwachungssystem
  internes Kontrollsystems, High-level-Controls des Managements
- IT-Outsourcing
  Auswirkungen / Risiken beurteilen

www.**rissberger**.de

herzlichen Dank für Ihre Aufmerksamkeit !