+CLOUDS

IT als Fremdleistung: Risikomanagement und Strategien für Anwender.

Dr. Eberhard von Faber

T Systems

Dienstleister übernehmen IT-Services und IT (nahezu vollständig)

Treiber

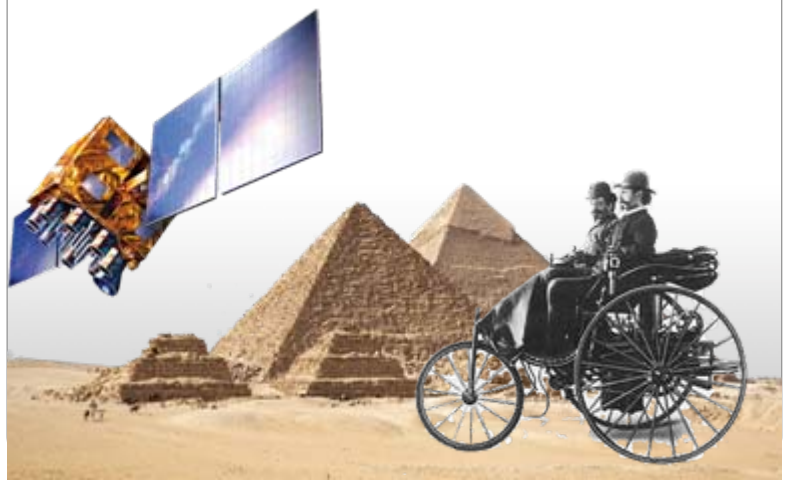
- Skaleneffekte realisieren;
  Kosten senken
- Wertschöpfungstiefe reduzieren;
  Kerngeschäft beherrschen,
  Flexibilität erhöhen
- Qualität erhöhen;
  Know-how und Ressourcen gewinnen
- Industrialisieren, Standardisieren;
  Kosten senken, Qualität erhöhen

Hemmnisse

- alles nur vorübergehende Angelegenheiten,
  für die sich schon 10 Jahre danach keiner mehr interessiert.

Indikatoren

- von 6000 v. Chr. bis 2009 (heute)
  Zunahme der Arbeitsteilung
- Unternehmen werden bald
  keine produzierende
  IT-Abteilung mehr haben.



T · · Systems

Geschäftsrisiken lassen sich nicht einfach „outsourcen“ (wie auch das Business)

Geschäftsinteresse, Gesetze, Regularien:

...Die Unternehmensführung ist verpflichtet, ein Risikomanagementsystem einzuführen und zu betreiben, sowie Aussagen zu Risiken und zur Risikostruktur des Unternehmens im Lagebericht der Gesellschaft zu veröffentlichen...

...Der Vorstand haftet gegenüber den Anlegern im Falle mangelnden Risikomanagements oder Verstoßens gegen das Risikohandbuch des Unternehmens. [KonTraG]

IT-Risiken sind Geschäftsrisiken!

Unternehmen können Risiken:

- akzeptieren,
- vermeiden,
- abwälzen oder
- verringern.

Security
Services and Solutions

T · · Systems

Das Grundproblem (warum ich hier bin):

Sicherheit

Sicherheit erfordert Steuerungsmöglichkeit / Kontrolle.

Risikomanagement

Risikomanagement erfordert Transparenz und Wissen.

oder?

IT als Fremdleistung („Outsourcing“)

Arbeitsteilung

- verringert direkte Steuerung / Kontrolle
- verringert Transparenz und apriori Wissen

1. Anbieterbewertung. Sicher oder unsicher?
2. Service-Modelle und Bedrohungen.
3. Anforderungen der Anwender und Maßnahmen.
4. Vorgehensmodell für Anwender.
5. Integration ins Risikomanagement des Anwenderunternehmens.

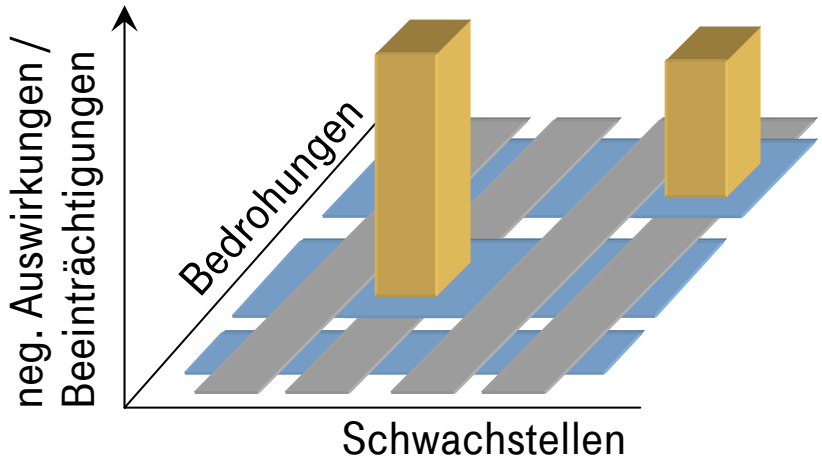
1. Sicher oder unsicher:
   Reale Risiken oder nur unklare Situation?
2. Service-Modelle und Bedrohungen.
3. Anforderungen der Anwender und Maßnahmen.
4. Vorgehensmodell für Anwender.
5. Integration ins Risikomanagement des Anwenderunternehmens.

Sicherheit und Unsicherheit.
Was ein Anwender wissen muss.

Dienstleister

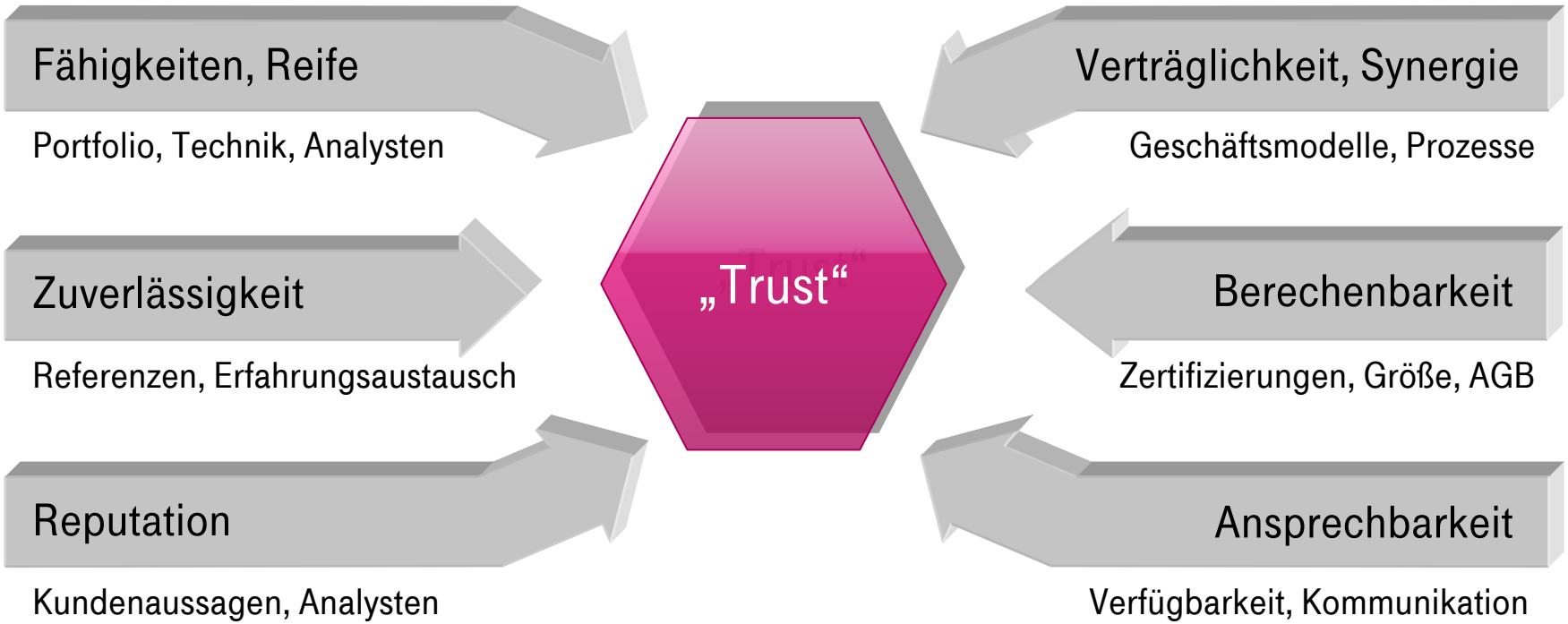
Anwender

- Unsicherheit 1: Vorhandensein nicht akzeptabler Risiken
  - Bedrohung / threat (Szenario)
  - Schwachstelle / vulnerability (keine oder unzureichende Sicherheitsmaßnahmen)
  - Schaden / business impact (Wert der Aktivposten, Wahrscheinlichkeit)
- Unsicherheit 2: Das Wissen darüber.
  - Grund für Vertrauen, Zutrauen u.ä. (assurance, reputation...)



Die Basis ist Vertrauen bzw. Vertrauenswürdigkeit.
Security-Kriterien für die Bewertung von Dienstleistern.

- Vermeidung von anbieterabhängigen “Risiken”
- Prognose hinsichtlich der Verlässlichkeit des Anbieters und der Qualität der Leistung

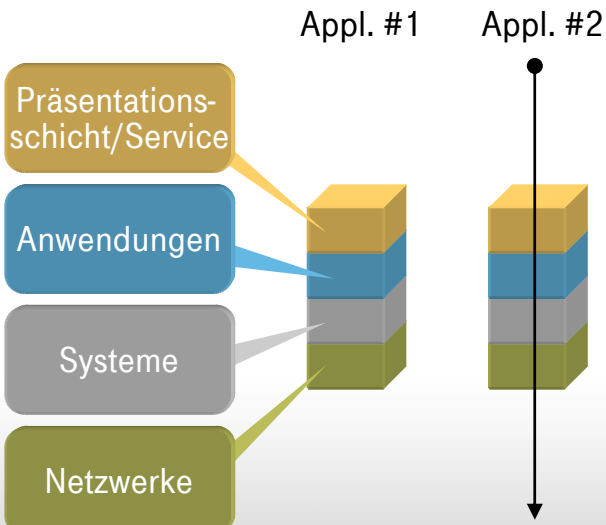


1. ✓ Anbieterbewertung. Sicher oder unsicher?
2. Mögliche Bedrohungen: Charakteristika und Unterschiede der einzelnen Service-Modelle.
3. Anforderungen der Anwender und Maßnahmen.
4. Vorgehensmodell für Anwender.
5. Integration ins Risikomanagement des Anwenderunternehmens.

Wirtschaftliche Anforderungen, Wandel der Technik:
Neue Modelle erfordern neue Sicherheitsmaßnahmen.

“früher”

Monolithisch, Silos absichern



IT as Service:
- “Cloud-Computing”

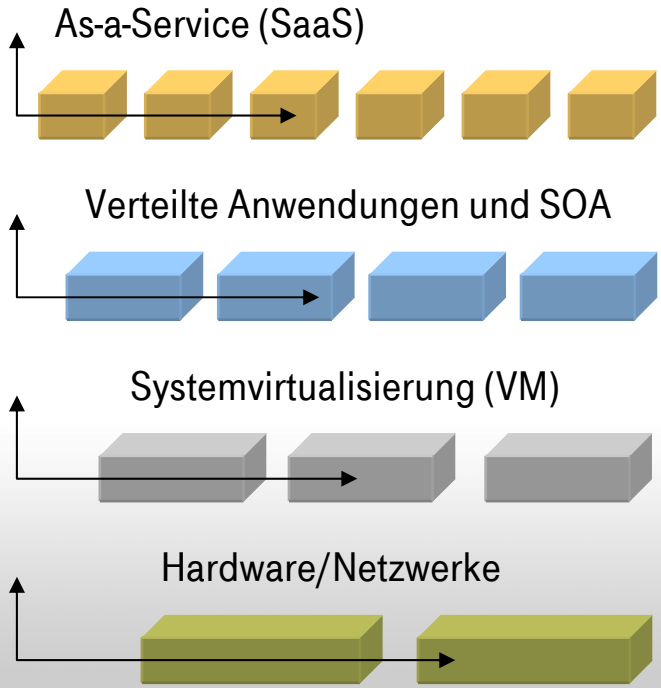
Common Application:
- “e-Collaboration”

Common Systems:
- “Outsourcing”

Common Networks:
- “Internet”

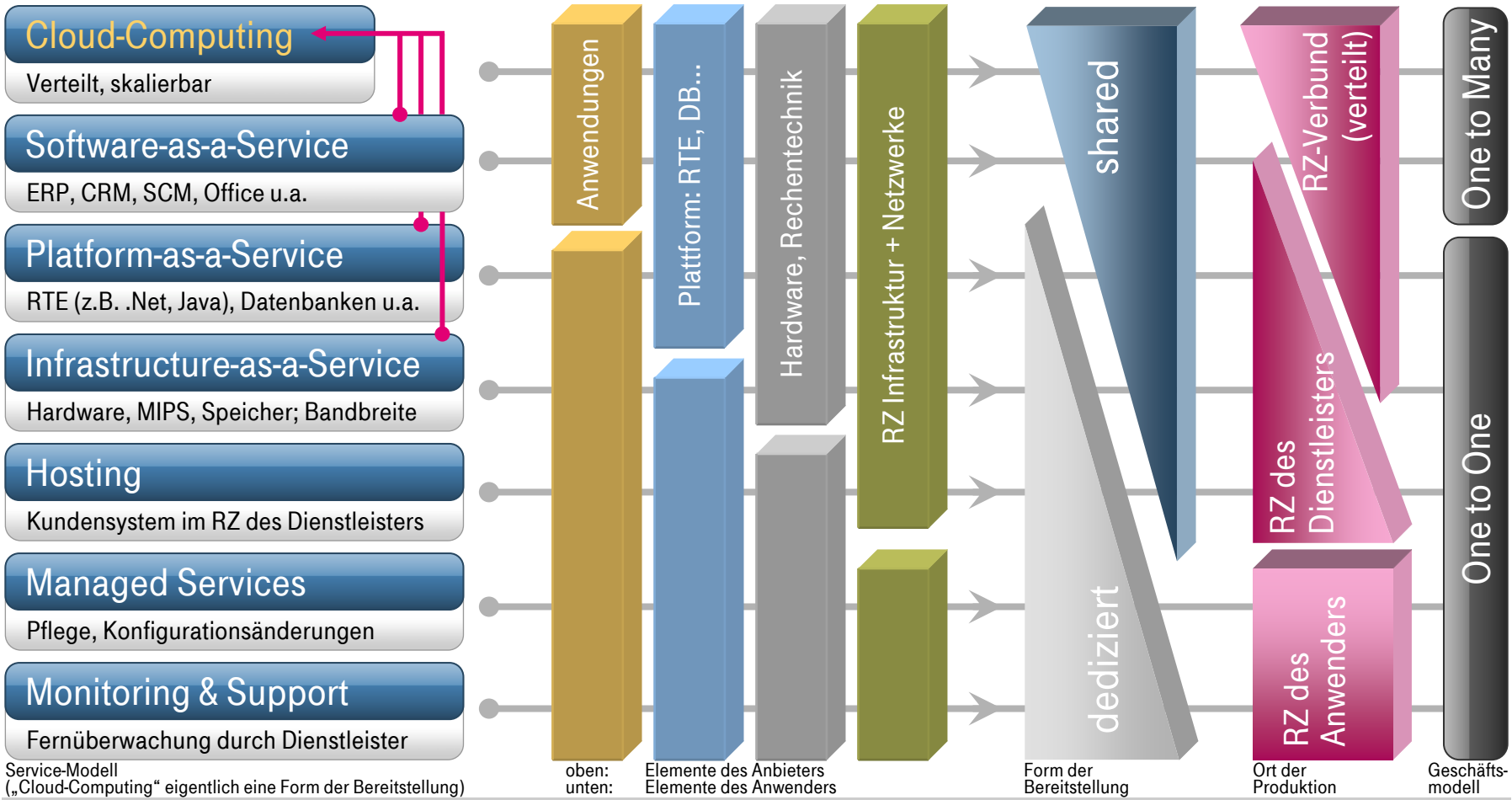
“heute”

Entkoppelt, virtualisiert + modularisiert



T Systems

Charakteristika der einzelnen Service-Modelle.
Arbeitsteilung und IT-Stack.



Charakteristika der einzelnen Service-Modelle.

Kontrolle und Angriffsvektoren.

Cloud-Computing
Verteilt, skalierbar

Software-as-a-Service
ERP, CRM, SCM, Office u.a.

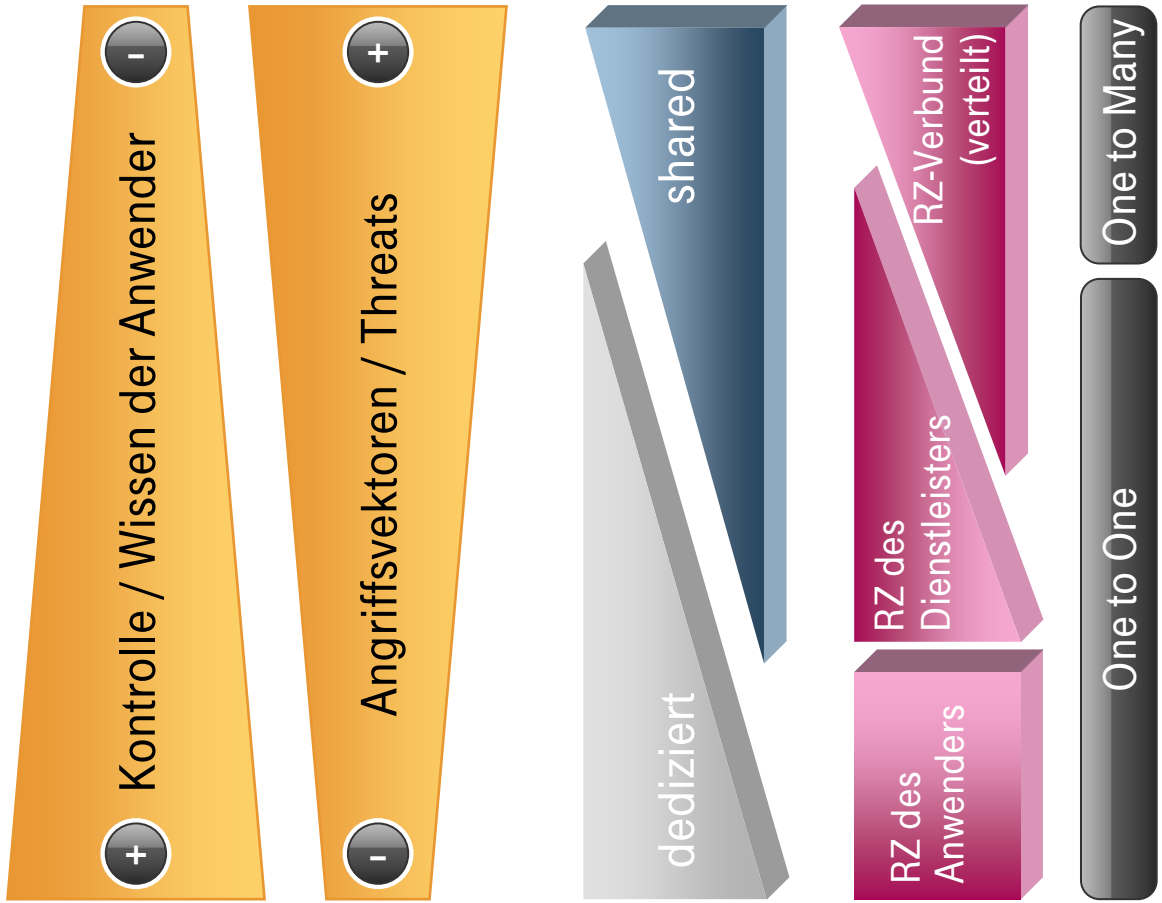
Platform-as-a-Service
RTE (z.B. .Net, Java), Datenbanken u.a.

Infrastructure-as-a-Service
Hardware, MIPS, Speicher

Housing
Kundensystem im RZ des Dienstleisters

Managed Services
Pflege, Konfigurationsänderungen

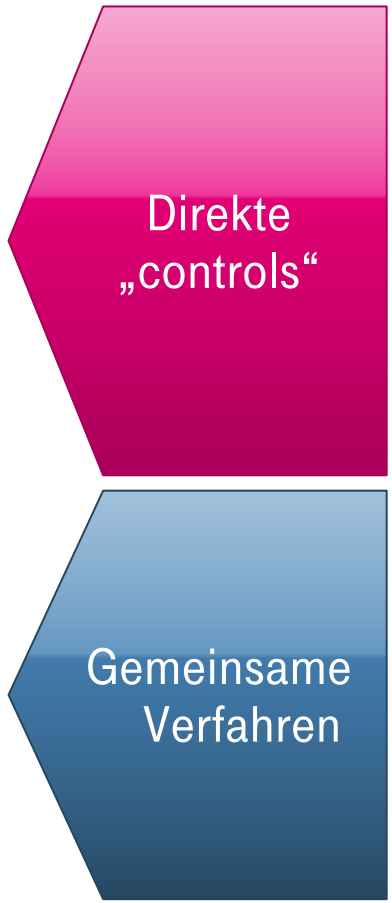
Monitoring & Support
Fernüberwachung durch Dienstleister



1. Anbieterbewertung. Sicher oder unsicher?
2. Service-Modelle und Bedrohungen.
3. Reale Probleme und Risiken: Anforderungen der Nutzer, Maßnahmen der Provider.
4. Vorgehensmodell für Anwender.
5. Integration ins Risikomanagement des Anwenderunternehmens.

Aufgaben für den Dienstleister.
Trust and Control.

- bauliche und physische Sicherheitsmaßnahmen (RZ-Sicherheit)
- technische Maßnahmen der IT-Sicherheit
- Business Continuity and Desaster Recovery
- Personal und Prozesse
- Architekturen und Lokationen
- Datenaustausch, Zusammenarbeit- und Zugriffsmodelle
- Überwachung und Management von Sicherheitsvorfällen
- Prozesse und Verfahren der Übergabe (und Beendigung der Zusammenarbeit)
- Know-how-Transfer
- Change-Management
- Metriken und KPI, Kommunikation



Risiken im „offshoring“.
Beispiel: länderspezifische Risiken.

- Wissen, wo die Daten sind? Oder: Unzeitgemäß im Zeitalter der Globalisierung?
- Unterschiedliche staatliche Regelungen hinsichtlich:
  - Datenschutz und Datenschutzgesetzgebung (Vertraulichkeit persönlicher Daten),
  - Schutz von geistigem Eigentum und Gesetzgebung dazu,
  - Rechtspflichten (z.B. Auskunftspflichten, Datenherausgabe: e-discovery),
  - Risiken durch staatliche Eingriffe (unbemerkter Zugriff, Abhören) sowie Verbot oder Einschränkungen hinsichtlich der Nutzung von Sicherheitstechnologien wie z. B. Verschlüsselung,
  - Sicherheitskultur (Verständnis der Menschen, Geschichte und Erfahrungen mit IT-Sicherheit, rechtliche Tradition),
  - internationale Zusammenarbeit bei der Rechtspflege, Rechtslage und Praxis zum Schutz von Angestellten, allgemeiner Rechtsschutz von Verträgen usw.
- Sicherheit ist Vertrauenssache. Welcher „Cloud“ vertrauen Sie?

T · · Systems

1. Anbieterbewertung. Sicher oder unsicher?
2. Service-Modelle und Bedrohungen.
3. ✓ Anforderungen der Anwender und Maßnahmen.
4. Vorgehen: Strategien und Best-Practices im ”global sourcing”.
5. Integration ins Risikomanagement des Anwenderunternehmens.

„Sourcing-Strategie“.
Vorgehensmodell aus Security-Sicht.

	Aufgaben (Beispiele)
Strategiebildung	▪ Optimierungspotenzial identifizieren ▪ Risiken: globale, länderspezifische, anbieterspez., technische ▪ Szenarien “Make-or-Buy” und Bewertung
Anforderungsdefinition	▪ Bestimmung von Schutzbedarf u. Compliance-Anforderungen ▪ Anforderungen an den Dienstleister festlegen ▪ Anforderungen an die Leistung festlegen
Marktanalyse	▪ Erstellung Anbieterprofil (Soll); Definition der Leistung ▪ Analyse der Leistungen und Geschäftsmodelle; Bewertung
Verhandlungen und Abschluss	▪ Wichtung von Security, Bewertungsverfahren definieren ▪ Sicherheitsverfahren für die Angebots- und Abschlussphase ▪ Absicherung der Transition
Betrieb	▪ Business-Interface; Ressourcen und Kommunikation; Services und Vertragsmanagement; Qualitätskontrolle und SLA; Training und Weiterentwicklung; Incident-Management

T · · Systems

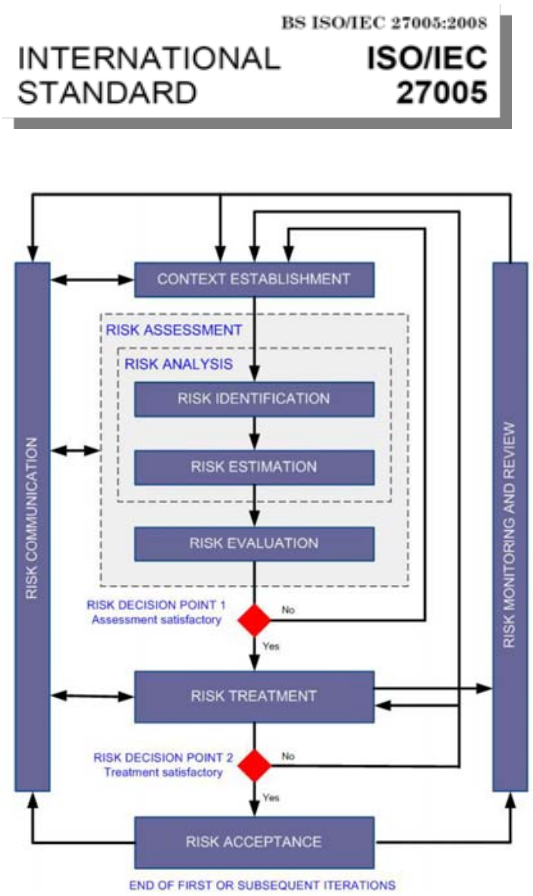
Konkrete Fragen an Ihren Dienstleister.
Beispiele.

- Wer hat welchen Zugriff? Wie erfolgt die Organisation der Zugriffskontrolle?
- Wie werden Personal und Zugriffe kontrolliert?
- Welche Schutzmaßnahmen gibt es bei der Datenübertragung?
- Wie ist die Separation der Anwendungen und Daten realisiert (Mandantenfähigkeit, Virtualisierung)?
- Wie ist die sichere Speicherung, das Backup und die Wiederherstellung gelöst?
- Wie wird die Löschung von Daten sichergestellt?
- Werden die relevanten Compliance-Anforderungen erfüllt?
  Welche Bewertungen und unabhängigen Untersuchungen (Zertifizierungen, Audits) können nachgewiesen werden?
- Welche Security-Kompetenzen kann der Anbieter aufzeigen?
- Wie können Sie sicher sein, dass der Dienstleister seinen Pflichten auch noch in 5 Jahren nachkommen kann... „It‘s all about trust“

T Systems

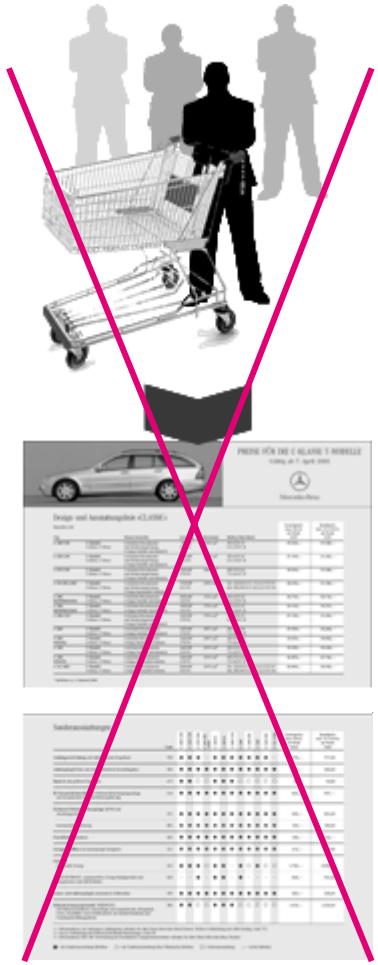
1. Anbieterbewertung. Sicher oder unsicher?
2. Service-Modelle und Bedrohungen.
3. Anforderungen der Anwender und Maßnahmen.
4. ✓ Vorgehensmodell für Anwender.
5. Integration ins Risikomanagement des Anwenderunternehmens.

IT Risikomanagement im Unternehmen. Ablauf für Outsourcing?



Ablauf Risikomanagement

1. Kontextdefinition: geschäftliche Ziele, Abhängigkeiten, Geschäftsprozesse, Rolle und Beitrag der IT
2. Identifikation von Risiken: Inventarisierung von Werten und Prozessen, Bedrohungen, existierende und geplante Maßnahmen sowie Schwachstellen
3. Risikobewertung: Konsequenzen (CIA), Wahrscheinlichkeit, Schadenspotenzial
4. Prüfung und Entscheidung
5. Risikobehandlung: Aktion und Dokumentation, Kommunikation
6. Messen und Prüfen (Metriken)
7. Schlussfolgerungen und nächste Schritte (Verbesserung)



IT Risikomanagement im Unternehmen. Ablauf für Outsourcing.

Ablauf Risikomanagement

1. Kontextdefinition: geschäftliche Ziele, Abhängigkeiten, Geschäftsprozesse, Rolle und Beitrag der IT
2. Identifikation von Risiken: Inventarisierung von Werten und Prozessen, potenzielle Bedrohungen bzw. Angriffsszenarien;

   Bewertung (antizipiert): mögliche Konsequenzen (CIA), Schadenspotenzial, Auswahl Geschäfts- und Service-Modelle
3. **Sicherheitsvorgaben: Kontext, Risikobeschreibung, Sicherheitsziele, notwendige Maßnahmen, Nachweispflichten**
4. **Evaluierung von Anbieter und Leistung:** existierende bzw. geplante Maßnahmen, Schwachstellen, Wahrscheinlichkeit von Szenarien, **Erfüllung der Vorgaben** (evtl. Optionen, Anpassung)
5. Prüfung und Entscheidung, Verhandlungen und Vertragsabschlüsse: Dokumentation, Kommunikation
6. Regelbetrieb: Mess- und Prüfberichte, SLA-Management
7. Schlussfolgerungen und nächste Schritte (Verbesserung)

Bedarf

Einkaufsliste

Einkauf

Nutzung

T Systems

Anforderungen, Prüfungen, Regelbetrieb.

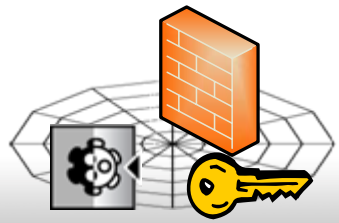
Kraftfahrzeuge – IT-Services.

KBA

1. Anforderungen (Straßenverkehrs-Zulassungs-Ordnung (StVZO), Fahrzeugteile-VO (FzTV))
2. Typgenehmigung: Bauartgenehmigung (ABG)
3. Modellbezogene Nachprüfungen
4. Produktsicherheit / Rückrufe: Geräte- und Produktsicherheitsgesetz (GPSG)
5. Fahrschule/Führerschein, Flensburg
6. Hauptuntersuchung (HU), Abgasuntersuchung (AU)
7. Feinstaubplakette

DEKRA TÜV

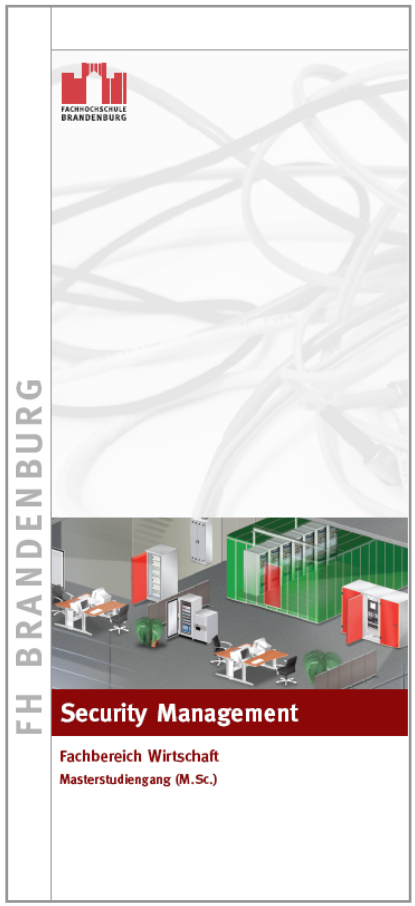
VISA MasterCard PCI



Evaluation Laboratories / Services

T Systems

Weitere Infos.
The Bulletin Security Management

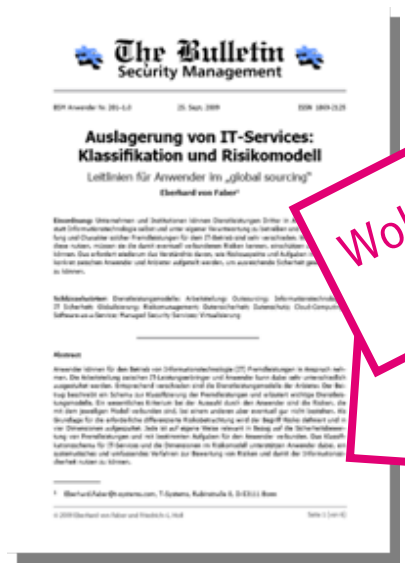


- zu einzelnen, scharf abgegrenzten Aspekten des Security Managements
- direkt anwendungsbezogenes Wissen
  in prägnanter, kurzer und strukturierter Form
- unabhängig, keine Produkt- und Anbieterbewertung;
  freies Download: **www.security-management.de**/de/publikationen/


The Bulletin
Security Management

Sicherheitsaspekte beim Cloud Computing

Leitlinien für Anwender im „global sourcing"


The Bulletin
Security Management

Auslagerung von IT-Services: Klassifikation und Risikomodell

Leitlinien für Anwender im „global sourcing"

Wollen Sie Autor des Bulletins werden?

Bitte weitersagen!

T Systems

Vielen Dank für Ihre Aufmerksamkeit.

Prof. Dr. Eberhard von Faber
Security Strategy and Executive Consulting
www.t-systems.de/ict-security

T Systems

powered by Security Management at

FACHHOCHSCHULE BRANDENBURG