IBM Global Services

Besondere Sicherheitsaspekte beim externen Betrieb von IT-Lösungen im Zusammenhang mit sensiblen Daten

Peer Klimmek
IBM Deutschland GmbH - Applikation Management Services
11. Dezember 2006

Betrachtet man die Gesamtheit von operationellen Risiken eines Unternehmens näher, zeigen sich viele Berührungspunkte mit der Sicherheit von Informationstechnologie.

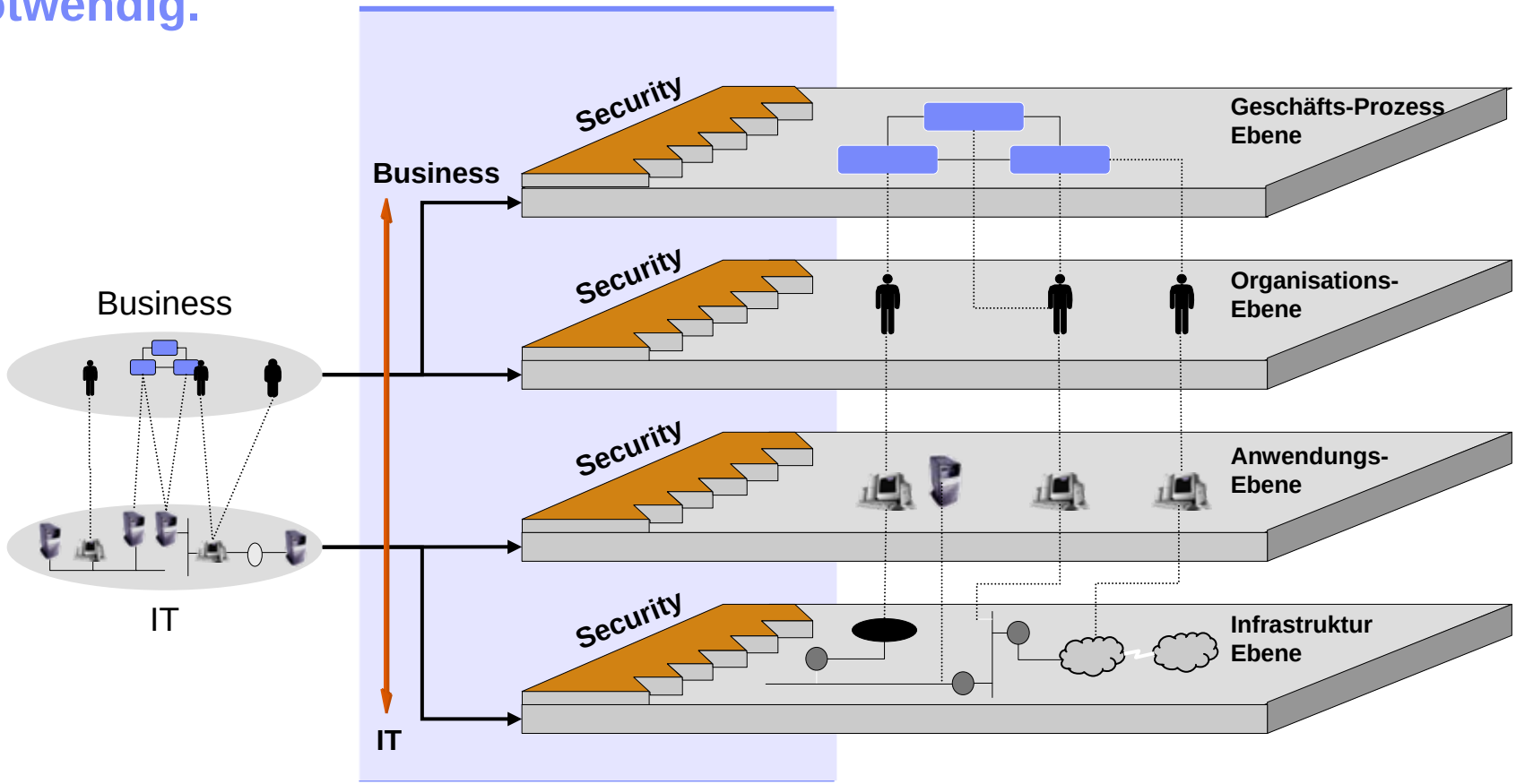
Interne Verfahren	Systeme	Menschen	Externe Ereignisse		
		Mitarbeiter	Externe	Direktes Umfeld	Katastrophen
▪ Falsche Strategie ▪ Fehlende Zielausrichtung ▪ Unklare Verantwortlichkeiten ▪ Schlechte Prozessdefinition und -umsetzung ▪ Mangelnde Anpassungsfähigkeit an neue Anforderungen	▪ Hardwaredefekte ▪ Softwarefehler ▪ Schlechte Administration ▪ Mangelhafte Benutzerfreundlichkeit ▪ Anfälligkeit gegen Würmer und Viren ▪ Inadäquate Architekturen ▪ Stromausfall	▪ Missbrauch ▪ Diebstahl ▪ Unachtsamkeit, Unwissenheit ▪ Menschliches Versagen ▪ Bestechung ▪ Fluktuation	▪ Computerviren und Würmer ▪ Hacking ▪ Einbruch ▪ Betrug ▪ Vandalismus ▪ Raub, Diebstahl ▪ Sabotage ▪ Spionage ▪ Terrorismus	▪ Ausfall der Kommunikationsverbindungen (Telefon, Mail, Web) ▪ Änderung der regulatorischen Anforderungen ▪ Verlust der Verkehrsverbindungen ▪ Extreme Nachfrageschwankungen	▪ Erdbeben ▪ Hochwasser ▪ Sturm ▪ Frost ▪ Feuer ▪ Explosion ▪ Chemieunfälle ▪ Flugzeugabsturz, Verkehrsunfälle ▪ Krieg

Externe Risikoquellen

Interne Risikoquellen

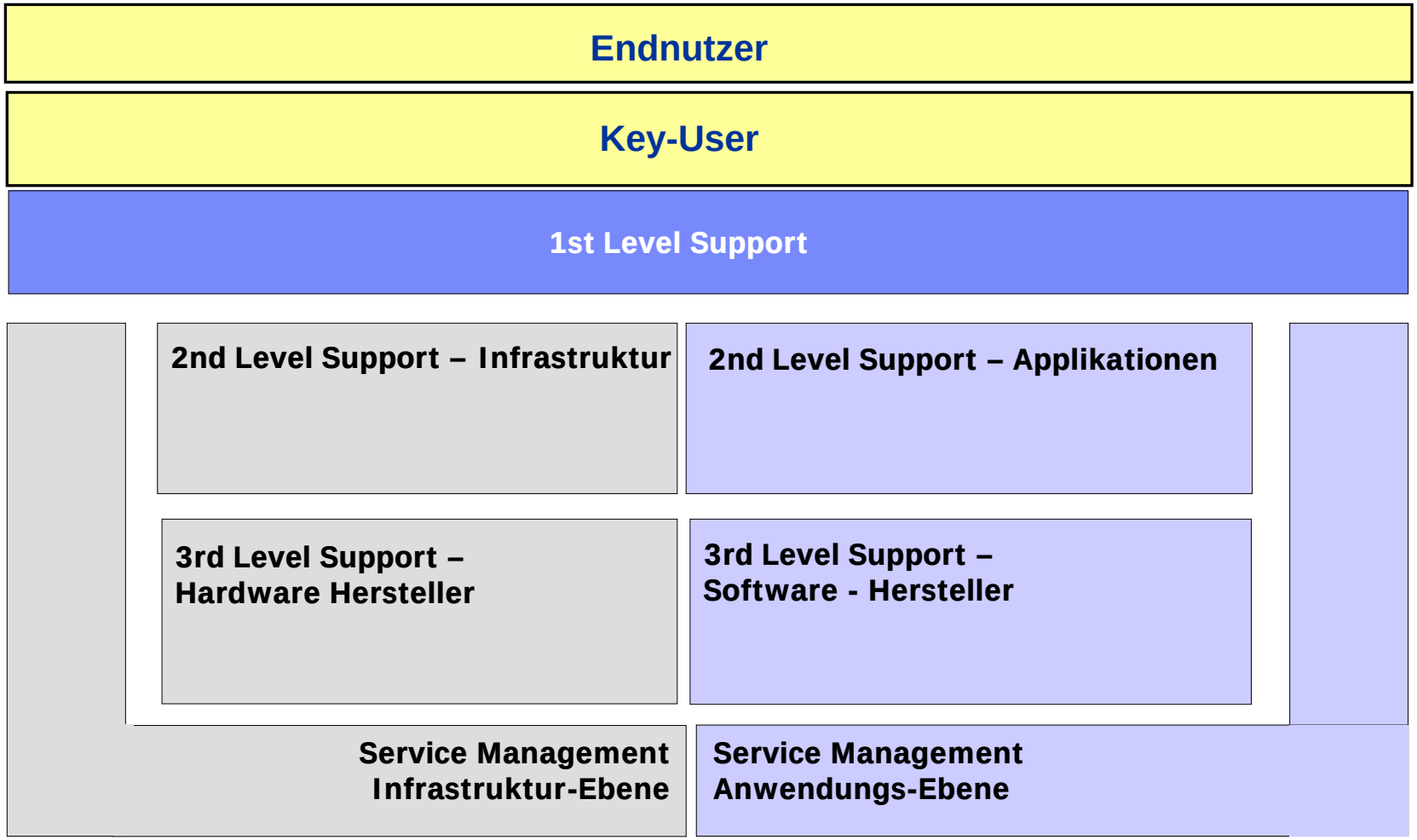
Orange: Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, d.h. IT-Sicherheit

Um Sicherheitsschwächen zu erkennen und zu bewerten und entsprechende Sicherheitsmechanismen ableiten zu können, ist eine ganzheitliche Betrachtung des Unternehmens auf allen Ebenen notwendig.

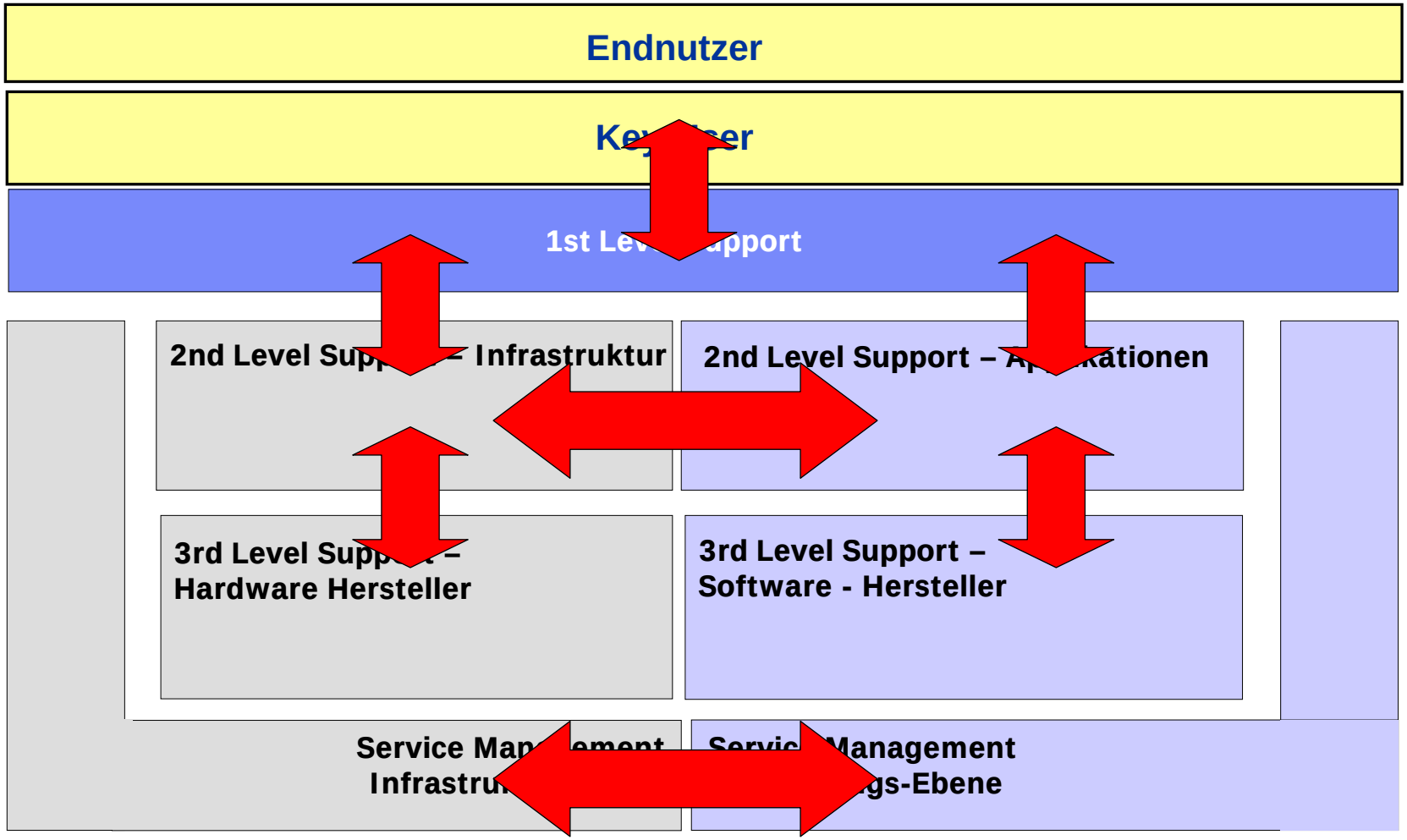


Das Schwächste Glied in der Kette bestimmt den Grad der Sicherheit für das Gesamtsystem

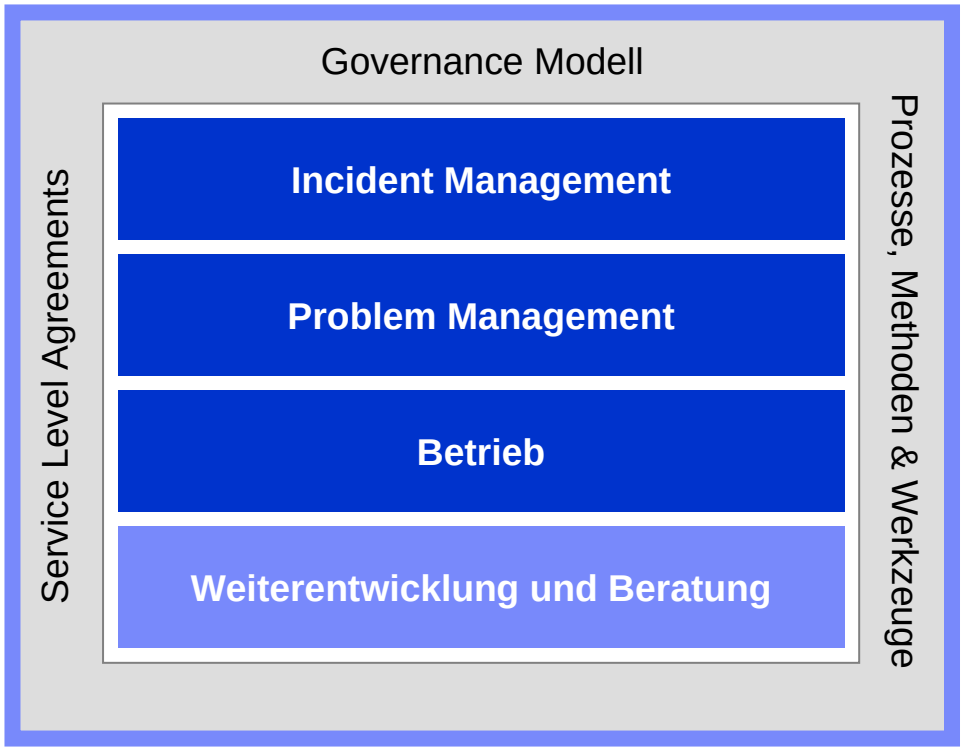
Betriebsalternativen: Für den externen Betrieb wird die Lösung in einzelne Service-Blöcke unterteilt, die einzeln optional extern oder intern betrieben werden können.



Sind verschiedene Dienstleister eingebunden, ist ein Governance Modell notwendig, um den Betrieb zu managen.



Das Governance Modell umspannt die verschiedenen Dienstleistungselemente und stellt das Funktionieren der Vertragspartnerschaft sicher.



In der Regel trägt der Auftraggeber die Verantwortung für die generelle Einhaltung gesetzlicher Bestimmungen hinsichtlich des Datenschutzes

- **unterschiedliche Optionen / Services der IT Dienstleister**
- **Weitergabe der Verantwortung an den Auftraggeber**
- **Verantwortung zur Umsetzung der IT Dienstleister**

Daraus ergeben sich vor Beauftragung und während der Laufzeit Handlungsempfehlungen

- Prüfung der angebotenen Optionen
- Prüfung der üblichen Sicherheitsrichtlinien beim Dienstleister
- Prüfung des Standortes der Infrastruktur
- Prüfung des Standortes der Mitarbeiter des Dienstleisters
- Prüfung von evtl. Unterauftragnehmern des Dienstleisters
  - HW Hersteller
  - SW Hersteller

Beispiele für Sicherheits-Richtlinien (Policies):

Risiko- Management

- Security Policy development
- Security Principles development
- Security Governance development
- Guidelines of Operation
- Measures of Compliance
- Effective Enforcement

Administrative Sicherheit

- Security Policy implementation
- Security Principles implementation
- Security Governance implementation
- Security Intelligence implementation
- Centralized Security Ops
- Threat Management
- Privacy Management
- E-mail Scanning

Anwendungs-Sicherheit

- Single Sign-on
- Digital Certificates
- Digital Signatures
- Data Encryption
- Trustworthy Security Repositories
- Meta Directories
- Authorization
- Strong Authentication
- Secure Content Mgmt

Infrastruktur-Sicherheit

- Antivirus
- Firewall, VPN
- Biometrics
- Smart Cards
- Digital Surveillance
- Security Appliances
- Recovery Services
- Security Management
- Intrusion Detection & Monitoring
- Product Solutions
- Hardware Encryption
- Assessments
- Secure Architecture

Fragen:

Peer Klimmek
IBM Deutschland GmbH
Application Management Services

Tel.: 0171-33 89 31
Email: peer.klimmek@de.ibm.com