E-ComHamburg

Hamburger Initiative für electronic commerce im Mittelstand

IT-Sicherheitskonzepte für den Mittelstand

Bernd Ewert
Geschäftsführer der

consequa

continuity · security · quality

Wer referiert?

consequa GmbH

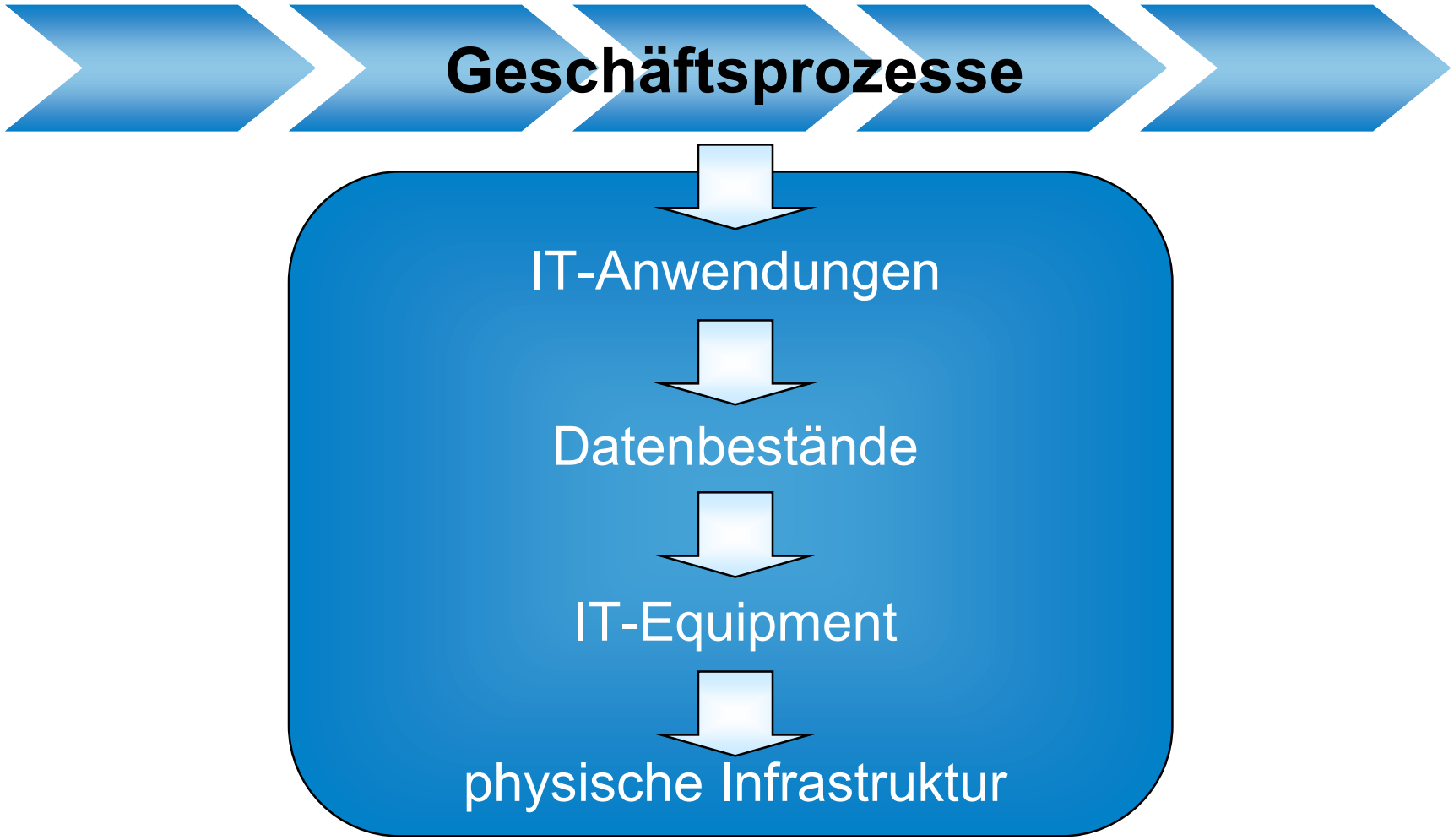
- Unternehmensstandort Hamburg
- gegründet 1.4. 2005
- langjährige Beratungserfahrungen
  - Business Continuity / IT-Recovery
  - IT-Sicherheit
  - Service Level Agreements
- bei Großunternehmen und Mittelstand
  - Banken und Versicherungen
  - Industrie und Handel
  - Logistik- und Medienunternehmen
  - Behörden
- Wir helfen unseren Kunden,
  - ihre Geschäftsfähigkeit gegen operationelle Risiken abzusichern
  - und so ihre Wettbewerbsfähigkeit zu verbessern.

Agenda

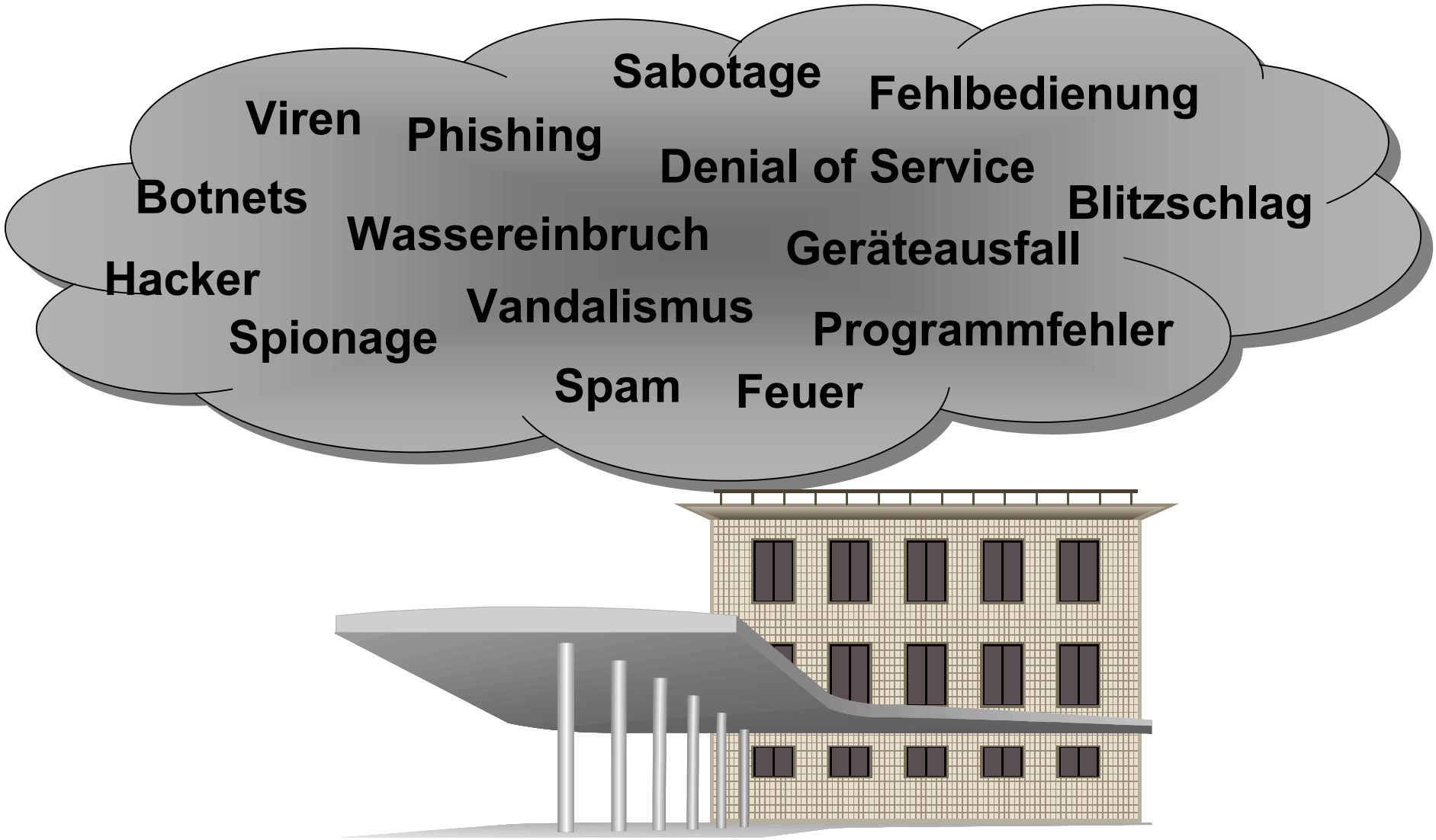
- Warum denn IT-Sicherheit?
- Orientierungshilfen
- Was ist zu tun?
- Hilfe!

Warum denn IT-Sicherheit?

Informationstechnik als „Ermöglicher“ ...



... ist gefährdet



Kriterien der IT-Sicherheit

Verfügbarkeit

Ein System gewährleistet Verfügbarkeit, wenn seine ***Leistungen in ausreichender Form und Qualität*** **beziehbar** sind

Vertraulichkeit

Ein System gewährleistet Vertraulichkeit, wenn die in ihm enthaltenen ***Informationen nur Berechtigten zur Kenntnis*** gelangen

Integrität

Ein System gewährleistet Integrität, wenn ***nur zulässige Veränderungen der*** in ihm enthaltenen ***Informationen*** stattfinden
(darin beim BSI (*) auch Verbindlichkeit)

(*) BSI: Bundesamt für Sicherheit in der Informationstechnik

Orientierungshilfen

Standards zur IT-Sicherheit: ISO

- ISO/IEC 27001
  - Best-Practice-Ansatz für Aufbau und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS) *(analog z.B. ISO 9001)*
- ISO/IEC 17799 (in Zukunft 27002)
  - Best-Practice-Ansatz zum Umgang mit den Bereichen der Informations-Sicherheit
- für beide gilt:
  - High Level
  - für Auditierung im Prinzip gut geeignet, aber in englischer Sprache
  - Zertifizierung möglich
- weitere Normen vorgesehen, z.B. zu den Themen
  - Maßstäbe für IT-Sicherheit
  - Risikomanagement
  - Business Continuity
  - IT-Service-Management (bisher ITIL)

Standards zur IT-Sicherheit: BSI

- BSI-Standards
  - Beschreibung von Anforderungen und Vorgehensweisen
  - 100-1 Anforderungen an ein ISMS
  - 100-2 IT-Grundschutz-Vorgehensweise
  - 100-3 Risikoanalyse auf der Basis von IT-Grundschutz
- IT-Grundschutz-Katalog
  - organisatorische und technische Standard-Schutzmaßnahmen
  - gegliedert nach Bausteinen, Gefährdungen und Maßnahmen
  - Nachschlagewerk, für Soll/Ist-Vergleich weniger gut geeignet
- für Gesamtwerk gilt:
  - Unterstützung durch Tool vorhanden
  - Zertifizierung möglich
  - kostenlos zugänglich unter www.bsi.bund.de

Standards zur IT-Sicherheit: IDW

- FAIT1: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie
  - Verarbeitung von Geschäftsvorfällen oder betrieblichen Aktivitäten, die in die Rechnungslegung einfließen
  - Buchführung, Jahresabschluss, Lagebericht

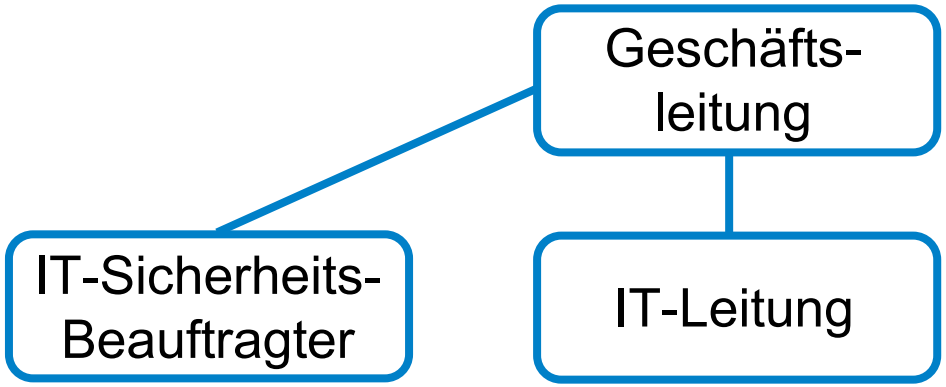
- FAIT2: Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Electronic Commerce
  - Anbahnung und Abwicklung von Geschäftsvorfällen in elektronischer Form über öffentliche Netze, z.B. Electronic Banking

- FAIT3: Grundsätze ordnungsgemäßer Buchführung beim Einsatz elektronischer Archivierungsverfahren
  - Aufbewahrung rechtlich relevanter elektronischer Unterlagen

- IT-Sicherheit ist ein wesentlicher Aspekt der Ordnungsmäßigkeit
  - FAIT ist Grundlage für Wirtschaftsprüfer

Was ist zu tun?

Einrichtung des IT-Sicherheits-Managements



verantwortlich für Unternehmen
und Gesetzeseinhaltung

verantwortlich für Funktion der IT
einschließlich deren Sicherheit

verantwortlich für:

- Kommunikation mit Risikomanagement und Datenschutz
- Information über Gefährdungen
- Erhebung der Anforderungen
- fachliche Beratung der IT-Leitung
- Überprüfung der IT-Sicherheit

- und besser nicht Umsetzung der IT-Sicherheit

Ermittlung des Schutzbedarfs

1. Feststellung der Beziehungen von
   - Anwendungen untereinander
   - Anwendungen und IT-Komponenten

2. Ermittlung des Schadenspotentials bei Beeinträchtigung für alle Anwendungen bezüglich
   - Verfügbarkeit
   - Vertraulichkeit
   - Integrität

3. Einordnung aller Anwendungen in Schutzbedarfsklassen nach dem Schadenspotential

4. Ableitung der Schutzbedarfsklassen der IT-Komponenten durch Berücksichtigung der Abhängigkeiten

5. bei besonderen Bedrohungen oder Gefährdungen zusätzliche Risikoanalyse

Klassifizierung des Schadenspotentials

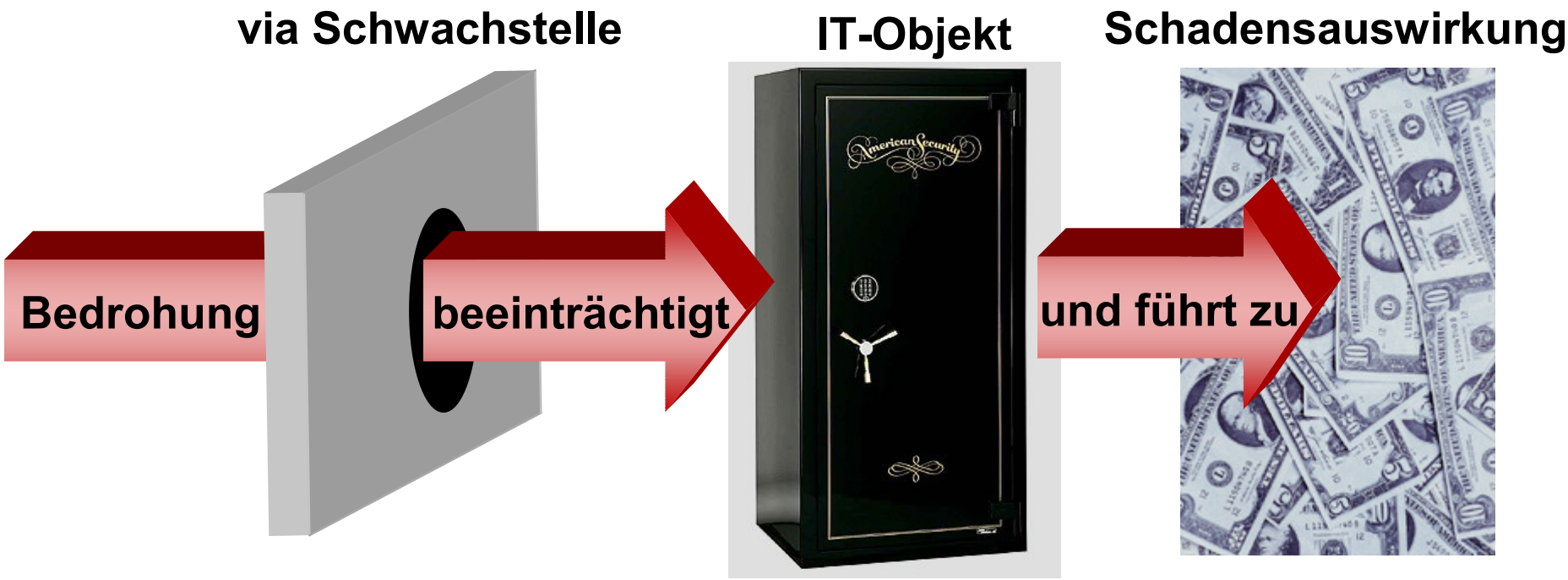
Schadenspotential / Schadensart	mittel	hoch	sehr hoch
Beeinträchtigung des Geschäftsablaufs	Betriebsbehinderung	deutliche Einschränkung	existenzbedrohende Handlungsunfähigkeit
negative Außenwirkung/ Wettbewerbsnachteile	Beschwerden	Verluste einzelner Kunden	deutliche Marktverluste
direkte finanzielle Auswirkungen	gering	deutliche Bilanzauswirkung	existenzbedrohend / Konkurs
Verstoß gegen Gesetze / Vorschriften / Verträge	geringe Vertragsstrafen u. Haftungsschäden	hohe Vertragsstrafen u. Haftungsschäden	existenzbedrohende Vertragsstrafen und Haftungsschäden
Materialverluste	Verlust einzelner Komponenten	Verlust erheblicher Materialmengen	Materialverlust in existenzbedrohendem Ausmaß

Klassifizierung für einzelne Anwendungen jeweils
bei Beeinträchtigung von Verfügbarkeit, Vertraulichkeit und Integrität

Beispiel für Schutzbedarf

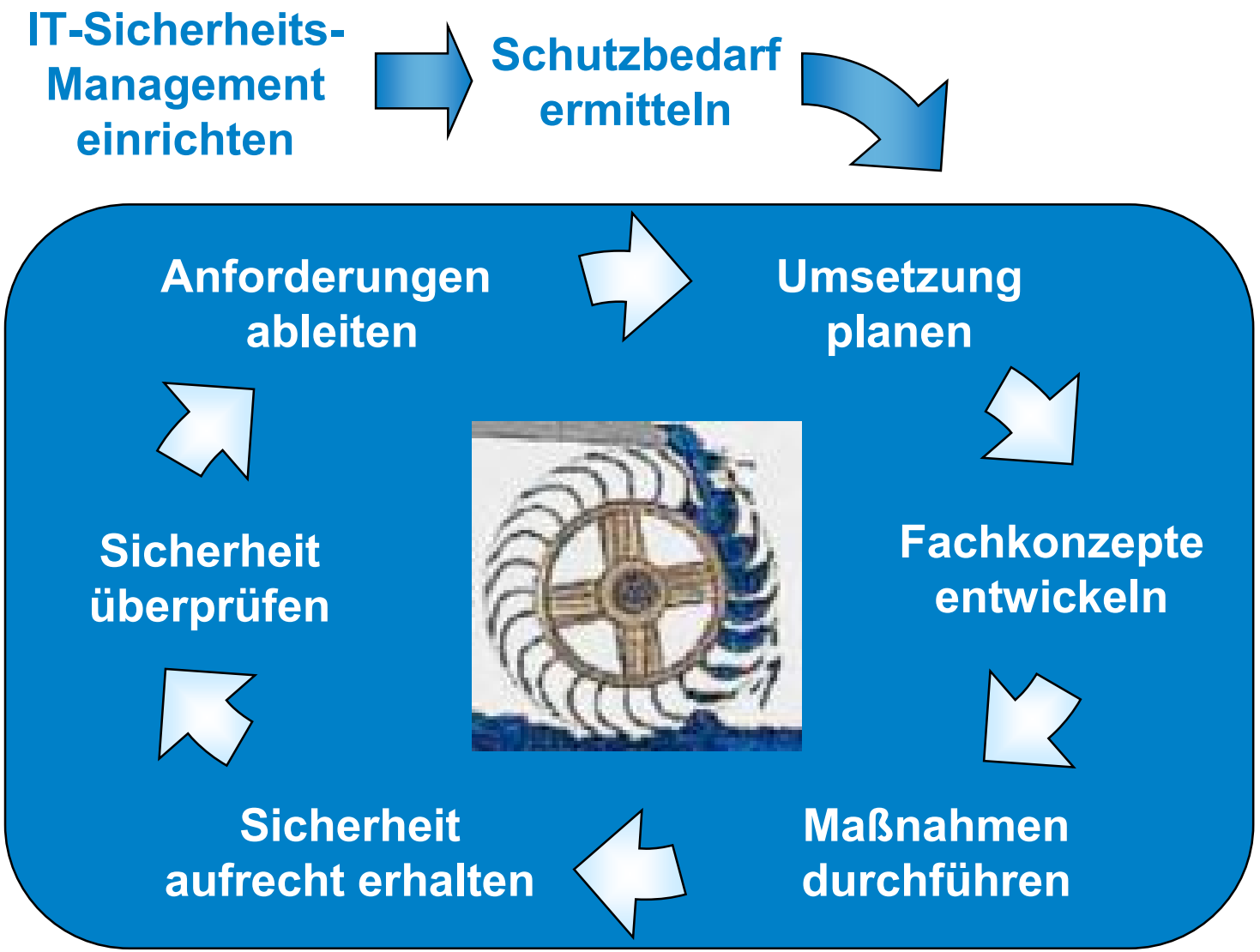
Anwendung / Datenbestand	Schutzbedarfsklasse	Verfüg-barkeit	Integrität	Vertrau-lichkeit	der Anwendung zugeordnete IT-Komponente(n) (System-IDs mit Semikolon getrennt)
Personalverwaltung		mittel	mittel	hoch	Act. Direct. Server; Netzdienste-Server; ERP-Server; SAN-Plattensystem; SAN-Netz; LAN Verwaltung; Büro-PCs
Rechnungswesen		mittel	hoch	mittel	Act. Direct. Server; Netzdienste-Server; ERP-Server; SAN-Plattensystem; SAN-Netz; LAN Verwaltung; Büro-PCs
Materialverwaltung		hoch	hoch	mittel	Act. Direct. Server; Netzdienste-Server; Lager-Server; LAN Lager; Lager-PCs
Produktionssteuerung		hoch	hoch	mittel	Act. Direct. Server; Netzdienste-Server; PPS-Server; SAN-Plattensystem; SAN-Netz; LAN Werk; Werks-PCs; Werks-Roboter
Vertriebssystem		hoch	mittel	hoch	Act. Direct. Server; Netzdienste-Server; ERP-Server; SAN-Plattensystem; SAN-Netz; Anbindung Filialen; LAN Filialen; Büro-PCs
Web-Auftritt mit Online-Shop		mittel	sehr hoch	hoch	Web-Server; Firewall / DMZ; Anbindung Internet
EDI		hoch	hoch	mittel	Act. Direct. Server; Netzdienste-Server; ERP-Server; SAN-Plattensystem; SAN-Netz; Firewall / DMZ; Anbindung Internet
Archivierung		mittel	hoch	hoch	Act. Direct. Server; Netzdienste-Server; ERP-Server; SAN-Plattensystem; SAN-Netz; Mail-Server; File-Server; Datenarchiv
E-Mail		hoch	mittel	mittel	Act. Direct. Server; Netzdienste-Server; Mail-Server; LAN Verwaltung; Anbindung Filialen; LAN Filialen; Büro-PCs; LAN Werk; Werks-PCs; LAN Lager; Lager-PCs
Textverarbeitung		hoch	mittel	mittel	Act. Direct. Server; Netzdienste-Server; File-Server; LAN Verwaltung; Anbindung Filialen; LAN Filialen; Büro-PCs; LAN Werk; Werks-PCs; LAN Lager; Lager-PCs
E-Banking		mittel	hoch	hoch	Act. Direct. Server; Netzdienste-Server; ERP-Server; Firewall / DMZ; Anbindung Internet; LAN Verwaltung; Büro-PCs
Telefonie		sehr hoch	mittel	mittel	Telefonanlage; Telefone

Ergänzende Analyse in besonderen Fällen



➔ **Risiko**

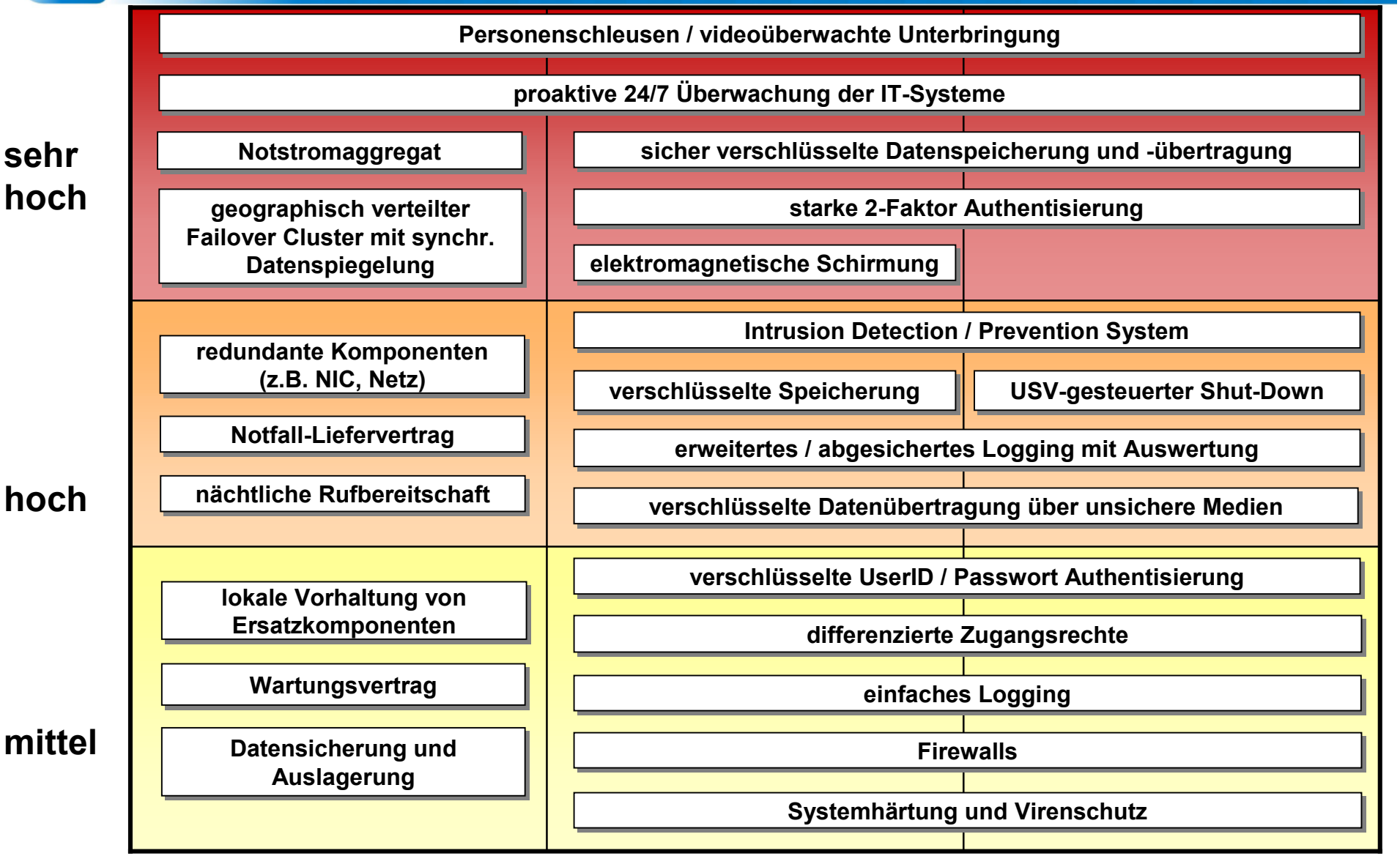
Regelkreis der IT-Sicherheit



Typische organisatorische Maßnahmen

- Personalführung
  - Leitfaden, Auswahl, Einweisung, Verpflichtung, Schulung
- IT-Planung und -Entwicklung
  - frühe Schutzbedarfsfeststellung, Trennung Produktion und Entwicklung
- Steuerung von IT-Dienstleistern
  - Auswahl, Verträge mit SLAs, Kontrollen
- Bereitstellung und Aussonderung von IT-Ressourcen
  - Auswahl nach Standards, zertifizierte Vernichtung
- Verwaltung von IT-Nutzern und ihren Berechtigungen
  - Rollenmodelle, Antrags-Workflow, Überprüfung
- Datensicherung und Archivierung
  - Kontrolle, Test der Wiederherstellung, Auslagerung
- Steuerung von Änderungen der IT
  - Test und Freigabe, Aktualisierung, Rückfallabsicherung, Dokumentation
- Behandlung von Vor- und Notfällen
  - Eskalationsstufen, CERT-Services, Zweitstandort für IT, Notfallpläne

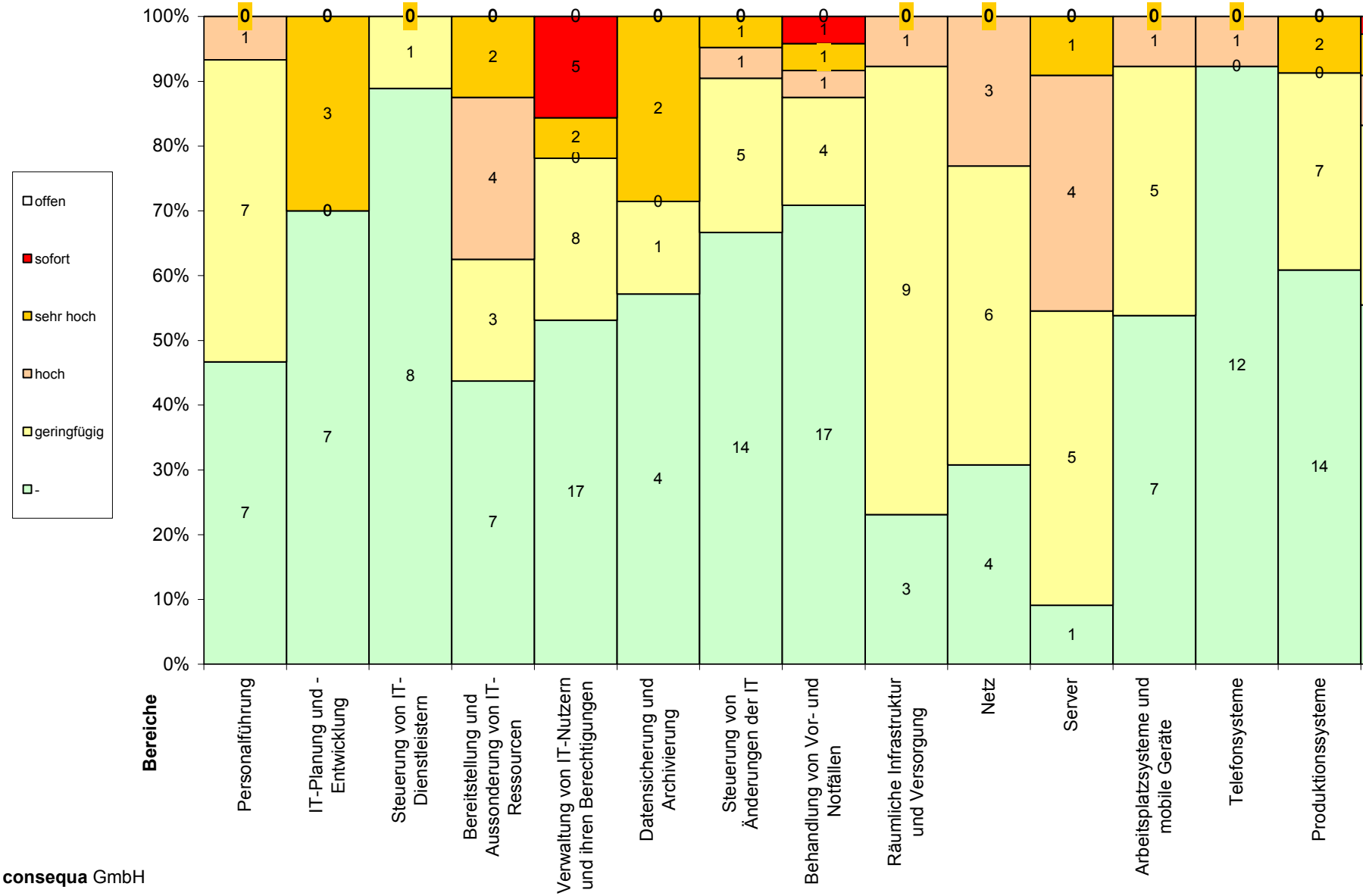
Infrastrukturmaßnahmen nach Schutzbedarf



IT-Sicherheits-Audit

Verteilung

Übersicht Handlungsbedarf Test XYZ



Reifegrad der Steuerung von IT-Sicherheit

Stufe		Merkmale
5	**Optimal**	Integraler Bestandteil der Unternehmenskultur (Integration in das allg. Risiko-Management, Integration in das Unternehmens-Rating)
4	**Gesteuert**	Systematisches IT-Risikomanagement (Schutzbedarfsanalyse), Fokus auf Ganzheitlichkeit (Abstimmung aller betroffenen Bereiche), Definierte Regelkreise (Audit, Reports)
3	**Definiert**	IT-Sicherheitspolitik Definierte Organisationsstruktur für IT-Sicherheit (ITSB, ...) Maßnahmen aufbauend auf IT-Strukturanalyse
2	**Wiederholbar**	Dokumentierte Konzepte und Arbeitsabläufe (Datensicherungskonzept, Ablauf Benutzerverwaltung, ...)
1	**Initial**	Technische und organisatorische Einzelmaßnahmen (Datensicherung, Virenscanner, Firewall, ...)

Hilfe!

Beratung in der Region

z.B. hier:

Hamburg
MEDIEN-IT-TELEKOMMUNIKATION
@work
Eine Initiative der Freien und Hansestadt Hamburg und Hamburger Unternehmen

Arbeitskreis Security

+

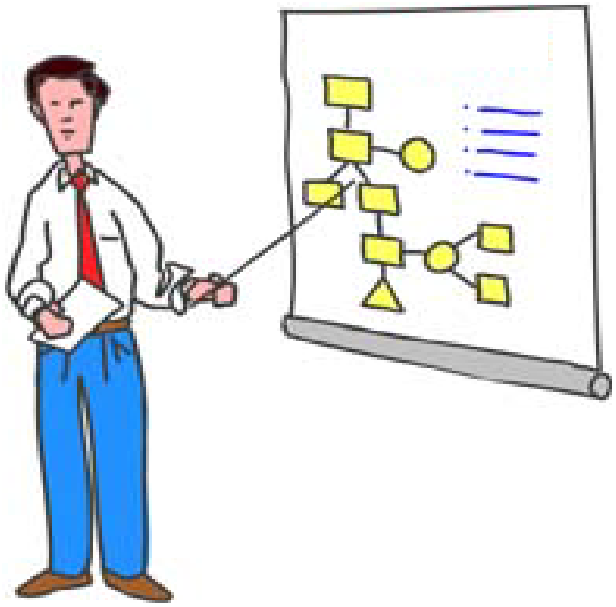
BVMW
Interessengemeinschaft mittelständischer Verbände und Unternehmer e.V.

BVMW Nord
IT:KOMMISSION
Experten für Entscheider

www.hamburg-media.net
> arbeitskreise > security

www.bvmw-nord-it.de

Vielen Dank
für Ihre Aufmerksamkeit!



consequa

Dipl.-Inform.
Bernd Ewert
Geschäftsführer

consequa GmbH
Süderstraße 73
20097 Hamburg
www.consequa.de

Tel.: 040 / 78 89 70 61
Fax: 040 / 78 89 70 66

bernd.ewert@consequa.de