

# Delegieren von IT-Sicherheitsaufgaben:

Benutzer-Risiken

Nicht zu weit links, nicht zu weit rechts,  
mittendurch geht der Weg

- Was Sie für Ihr Unternehmen über Sicherheit wissen müssen
- These 1: „Sicherheitsaufgaben können nicht delegiert werden“
- These 2: „Alle Sicherheitsaufgaben können (vollständig) delegiert werden“
- „Denn Sie wissen, was Sie tun!“

- Delegieren kann nur, wer sein Problem kennt
- Nicht das Problem, „nur“ die Lösung ist delegierbar
- Delegieren führt zu neuen Problemen, weil zusätzliches Wissen aufgebaut und gepflegt werden muss
- **Wenn Sie delegieren wollen, müssen Sie jederzeit Aussagen über die aktuelle und die geplante Sicherheit in Ihrem Unternehmen machen können**

# ...was Sie über Ihre Sicherheit wissen müssen

- Benennen Sie die grössten Schadenpotentiale...
  - ...konzentrieren Sie sich auf die zumutbaren Massnahmen gegen voraussehbare Ereignisse
- Messen Sie Ihren IT-Sicherheitszustand und vergleichen Sie...
  - ...mit früheren Messungen
  - ...mit anderen ähnlich gelagerten Firmen
  - ...mit Ihrem Schutzbedarf
- Streben Sie eine Zertifizierung an

## ...und was Sie nicht übersehen dürfen

- Machen Sie, was „alle“ machen...
  - ...besonders wenn die Kosten offensichtlich kleiner sind als der unmittelbar zu befürchtende Schaden
- Bauen Sie Sicherheit in die Projekte ein.
  - Sicherheitsmassnahmen werden teurer, je später sie eingeplant werden.
  - Die Projekte verlangen IT-Sicherheit, deshalb gehören die IT-Sicherheitskosten in die Projekt-Investitionsrechnung

# These 1: Sicherheitsaufgaben können nicht delegiert werden

- IT ist grundsätzlich nicht strategisch, aber die IT muss die Geschäftsprozesse optimal unterstützen
- ...das gleiche gilt für die IT Sicherheit
- Supportprozesse eignen sich für Delegation, da in der Regel ein Markt entsteht
  - Betrieb / Unterhalt / Betreuung von Komponenten
  - Projektierung / Einführung
  - Architektur / Engineering / Methodik / Beratung
  - Operative Führung

# Markt für Sicherheitsdienstleistungen

- Angebot von standardisierten Produkten
  - Verträge mit „echten“ SLA, die auf das konkrete Bedürfnis, insbesondere den konkreten Schutzbedarf ausgerichtet sind
  - Standardisierte Dienstleistungen, bestehend aus kombinierbaren Teilleistungen (Massenware für Viele anstelle von Massware für Einzelkunden)
  - Vergleichsmöglichkeiten (Quantität, Qualität, Preis)

- Fehlendes Wissen oder keine Übersicht über den bereits bestehenden oder noch entstehenden Markt...wann einsteigen?...wann aus- bzw. umsteigen?
- Geeignete Auswahl aus einem (derzeit) fragmentierten Markt mit isolierten Einzelangeboten und geringer Standardisierung
- Aufwand für Koordination, Steuerung und Reporting wird unterschätzt

## These 2: Alle Sicherheitsaufgaben können delegiert werden

- Sicherheitsprobleme gibt es...
  - an den Grenzen des eigenen Territoriums
  - unterwegs auf fremdem Territorium
  - innerhalb des eigenen Territoriums
- Keine systematischen Unterschiede zwischen „klassischer“ und „elektronischer“ Welt:  
Im zugewiesenen Perimeter hat der Wachdienst...
  - ...Einblick in alles
  - ...überall Zugang
  - ...kann alles mitnehmen bzw. kopieren
- EIN grosser Unterschied:  
Verstösse sind in der E-Welt schwer nachweisbar

- Unterschätzung der objektiven Risiken betr. Systemverfügbarkeit, Datenexistenz, Integrität und Vertraulichkeit
- Vernachlässigung der eigenen, nicht delegierbaren strategischen und leitenden Aufgaben in der IT und in den Kernprozessen
  - z.B. Katastrophen-Vorsorge
- Vernachlässigung von einseitigen, nicht umkehrbaren Abhängigkeiten
  - verpasster KnowHow Aufbau
  - unüberlegter Verlust an Handlungsfähigkeit

# Denn Sie wissen, was Sie tun

- **Risikodialog** kann nicht delegiert werden; Ergebnis (**Schutzbedarf**) ist Basis für das Design der Sicherheit bzw. des Sicherheitsniveaus
  - „Dienstleister kennt Auftrag“
  - „Dienstleister und Auftraggeber haben kompatibles Verständnis betr. Sicherheit und Dienstleistungen“
  - Einbezug der Linie (Geschäftsprozesse) in die Definition und Produktion des benötigten Sicherheitsniveaus

## Denn Sie wissen, was Sie tun

- Aussagen zu Sicherheits-**Audits** auch für Sicherheits-Dienstleister („Zertifikat“)
  - „Dienstleister macht es richtig“
  - Aufbau eines Kontroll- und Vertrauensverhältnisses
  - Nachweis des verantwortungsvollen Umgangs mit Sicherheit

# Denn Sie wissen, was Sie tun

- Periodische Marktvergleiche / **Benchmarks** auf Quantität, Qualität und Preise
  - „Dienstleister hat konkurrenzfähiges und marktgängiges Angebot“
  - Entwicklungen werden nicht verpasst: Wahrnehmen von Chancen, Vermeiden von unnötigen Risiken

## Zusammenfassend:

- Delegieren bietet viele Chancen, aber auch grosse Risiken
- Delegieren eignet sich nicht, um Schwächen in Stärken zu verwandeln
- Zum Beginn: Beurteilen Sie auf Grund Ihrer Informationen zur Unternehmenssicherheit und auf Grund der Marktinformationen Ihre Delegations-Fähigkeit!
  
- *Quidquid agis prudenter agas et respice finem*