SWISS INFOSEC

I S M S
PRAXIS FORUM

Sicherheitsaspekte an der Schnittstelle Business – IT

9.12.2009

Kurt Schädler

KSS Partners Establishment
Schaan, Liechtenstein

Agenda

- **Vorstellung**
- **Sicherheitsaspekte**
  - Unterschiedliche Sichtweisen
  - aus der Sicht IT
  - aus der Sicht Business
- **Risikobetrachtung**
  - Fokus
  - Konfliktpotential
- **Entscheidungen**
- **Massnahmen**
- **Fazit**
- **Vorschläge**
- **Diskussion**

Kurt Schädler

Alter: 50 Jahre

Nationalität: Liechtenstein

Wohnort: Buchs SG, Schweiz

Zivilstand: verheiratet, 3 Kinder, 1 Enkel, Hund, 2 Pferde

Ausbildung: Studium in Informatik und Betriebswirtschaft an der Universität Zürich – Abschluss lic.oec.publ.

Studium in Master of Business Administration an der Universität of Chicago – Abschluss MBA

Ausbildung in Marketing zum eidg.dipl. Marketingleiter

Beruf: Geschäftsführender Partner
KSS Partners Est., Schaan

KSS Partners Establishment (Anstalt)

Zweck: Interim Management
Projekt Management
Management Consulting

Spezialgebiet: Organisation, Organisationsentwicklung, Aufbau, Abbau, Umbau von Unternehmen, Bereichen oder Abteilungen, Re-Strukturierungen

Einsatzorte: Liechtenstein – Schweiz – Deutschland - Österreich

Netzwerk: Eingegliedert in ein professionelles Netzwerk

Weitere Infos: www.kss.li, www.ksspartners.com

Eine Anstalt (Establishment) ist wie eine kleine AG nach Liechtensteinischem Recht

Sicherheitsaspekte

Diskrepanz:

- **Unterschiedliche Sichtweisen** über Sicherheit von IT und Business
- **Unterschiedliche Auffassung** über die Wichtigkeit von Sicherheit und Sicherheitsaspekten
- **Wenig Verständnis** über IT und IT-Sicherheit durch das Business
  - Viele technische Begriffe
  - Schlechte Kommunikationsfähigkeit der IT und IT-Mitarbeiter (Stichwort: technische Begriffe, eigene IT Sprache)
  - Begriffe werden erst bekannt, wenn sie in den Medien sind (Stichwort: Virus „I love you“ (2000))
- **Unterschiedlicher Fokus**
  - Business: Umsatz – Gewinn
  - IT: Betrieb, Zuverlässigkeit, Sicherheit

Sicherheitsaspekte – aus der Sicht IT (1)

Informationssicherheit

- **Globale Informationssicherheit**
- **Technische Informationssicherheit**
- **Applikatorische Informationssicherheit**
- **Datenorientierte Informationssicherheit**

Sicherheitsaspekte – aus der Sicht IT (1)
…und Business

Informationssicherheit

- **Globale Informationssicherheit**

  Business versteht darunter: global verfügbare IT
  (das Wort Sicherheit wird unterdrückt

- **Technische Informationssicherheit**

  IT Systeme müssen einfach laufen, wie ist egal

- **Applikatorische Informationssicherheit**

  Die Software muss machen, was der Benutzer will
  Sicherheitsaspekte werden ausgeblendet

- **Datenorientierte Informationssicherheit**

  Zugriff auf alle Daten von allen Standorten zu jeder Zeit
  muss möglich sein, sonst ist das „Business“ gefährdet

Sicherheitsaspekte – aus der Sicht IT (2)

Datenschutz vs. Datensicherheit

Vertraulichkeit

Verfügbarkeit

Systemintegrität, Datenintegrität

Firewall

Viren, Würmer, Trojaner

Sicherheitsaspekte – aus der Sicht IT (2)
…und Business

Datenschutz vs. Datensicherheit

Unterschied ist im Business unbekannt (kritisch!!!)

Vertraulichkeit

Eigene Daten sind vertraulich, auf alle anderen will man Zugriff

Verfügbarkeit

Zugriff auf alle Daten von allen Standorten zu jeder Zeit muss möglich sein

Systemintegrität, Datenintegrität

Integrität wird mit Personen verbunden, nicht Systemen oder Daten

Firewall

Solange keine Störung bei der eigenen Arbeit auftritt, geduldet

Viren, Würmer, Trojaner

Werden unterschätzt, bis es passiert

Risikobetrachtung – aus der Sicht IT

- **Benutzer ist ein potentieller Risikofaktor**
  → die Benutzer müssen kontrolliert werden

- **Jedes System ist a priori fehleranfällig**
  → Systeme müssen überwacht werden

- **Jede Software ist a priori fehlerhaft**
  → Ständige Suche nach besserer Software

- **Netzwerke sind potentiell unsicher, Angriffspotential intern-extern**
  → Firewalls, Router, VLANs etc. etc.

Fazit: IT ist „pessimistisch“ eingestellt

Risikobetrachtung – aus der Sicht IT
…und Business

- **Einschränkungen stören den Arbeitsablauf**

  → Benutzer möchte keine Einschränkungen

- **Einschränkungen verhindern höheren Umsatz und Gewinn**

  → Business wünscht die Möglichkeit von „schnellen“ Entscheidungen

- **IT Sicherheit ist übertrieben**

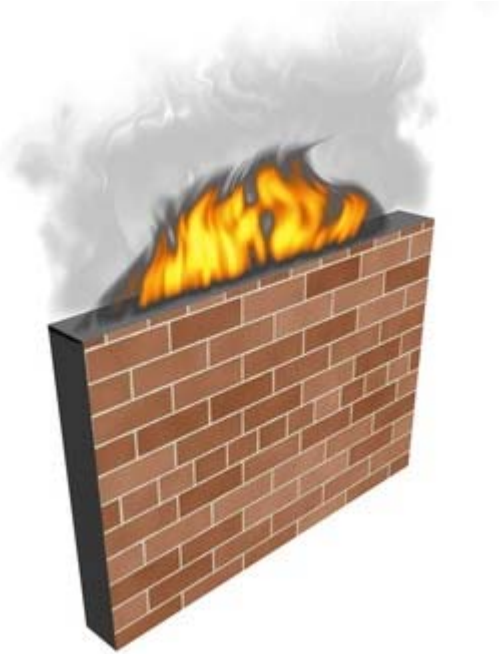
  → Aussage Business: warum braucht es all die Sicherheitsmassnahmen, es funktioniert ja alles“

Fazit: Business ist „leichtgläubig“ eingestellt

Konfliktpotential

Business

Zugriff von überall möglich
IT muss einfach laufen
IT übertreibt
IT ist zu teuer



IT

Risiken werden immer grösser
Sicherheit muss laufend verbessert werden

Am Ende gewinnt der Stärkere, häufig das Business

Entscheidungen

Am Ende gewinnt der Stärkere, häufig das Business**, warum…**

- **Menschlich:**
  - IT ist vielfach introvertiert, auch der IT Leiter
  - (human) Kommunikation ist nicht die Stärke der IT
- **Organisatorisch:**
  - IT Leiter ist nicht überall Mitglied der Geschäftsleitung (kein CIO)
- **Business-Orientierung:**
  - Aussage Business „wir brauchen das jetzt, sonst gefährden wir den Erfolg“
  - Erfolg steht über Sicherheit (solange nichts passiert)

Massnahmen aus der Sicht IT-Sicherheit

Business-Entscheidungen sind häufig wichtiger als Sicherheitsaspekte, die einen Entscheid verzögern

- → IT und IT-security müssen klein bei geben

Vielfach müssen Business-Entscheide akzeptiert werden. Auf eine mögliche Nachbehandlung wird verzichet, bis der Supergau eintritt, woran wiederum die IT Schuld ist.

Aber…

- IT darf die Sicherheitslücken nicht ohne weiteres akzeptieren
- IT muss darauf drängen, dass die Sicherheitslücken geschlossen werden
  - Gröbste Lücken sofort schliessen
  - Lücken „nachbehandeln“ (Empfehlung: Projekt aufsetzen mit klarer Verantwortlichkeit in der IT (z.B. IT Security Officer), klaren Zielvorgaben, klarem Terminplan, Priorität 1 ist nicht verhandelbar

Fazit

IT versucht Probleme zu vermeiden

- …durch permanente Verbesserung der Sicherheit

Daraus folgt: Probleme tauchen im Business nie auf

- Business merkt gar nicht, was die IT macht
- Business hat den Eindruck, die IT beschäftigt sich mit sich selbst

IT hat keine Zeit für andere Aufgaben

- Aussage Business: „IT ist zu teuer“

Wie kann man diese Meinung vermeiden?

Vorschläge

Regelmässiges Reporting

- Die IT orientiert über ihre Tätigkeiten (Intranet, „Anschlagbrett“, newsletter)
- Gegenüber GL wie auch gegenüber dem Kunden (Business)
- IT orientiert über Sicherheits-Probleme anstatt sie zu verstecken

Beispiel:

- Server wird durch DoS Attacke angegriffen
- Server ist eine bestimmte Zeit nicht verfügbar
- IT orientiert über die Massnahmen, was zu tun ist, damit dies nicht mehr passiert
- IT orientiert über die bereits vorhandenen Massnahmen, womit grösserer Schaden verhindert werden konnte

Offene Kommunikation

Kontakt

KSS Partners Establishment

Landstrasse 130

LI-9494 Schaan

Telefon: +423 233 29 29

Kurt Schädler

lic.oec.publ., MBA UofChicago

Telefon: +423 233 29 27 oder +41 76 371 54 80

Web www.kss.li , www.ksspartners.com

Mail kurt.schaedler@kss.li

Weitere Infos: Unterlagen, Flyer

In eigener Sache: Was ist Interim Management

Ausfall einer wichtigen Führungskraft

- Auf der ersten oder zweiten Führungsebene fällt plötzlich und unerwartet eine Führungskraft aus. Die Position muss überbrückt werden, bis der Nachfolger gefunden ist

Projektmanagement

- Ein wichtiges Projekt ist geplant und Sie benötigen einen erfahrenen, zielorientierten Projektmanager

Vorteile

- Der Interim Manager kann die Situation neutral analysieren und muss nicht Rücksicht auf bestehende „Gärtchen“ nehmen
- Der Interim Manager kann auch „unpopuläre“ Massnahmen ergreifen
- Der Interim Manager ist grundsätzlich nur dem Auftraggeber verpflichtet
- Der Interim Manager ist sofort verfügbar und die Kosten sind kalkulierbar

Nachteile

- Der Interim Manager kennt die inneren Strukturen nicht (Stichwort key-people)
- Nach Beendigung des Mandates geht der Interim Manager

Unser Name steht für …

K Kompetenz

S Stabilität

S Seriosität

Danke für Ihre Aufmerksamkeit

Diskussion / Fragen