IT - Security Forum #4

Sicherheitsrelevante Projekte
Die ‚Todsünden'

Markus Trinkner
Managing Consultant
Skybow AG
markus.trinkner@skybow.com

IT - Security Forum #4

Schlagzeilen der letzten Monate

- Schweizer Unternehmen haben massive Probleme mit Datensicherheit
- Weiterhin steigende Investitionen in IT-Sicherheit
- Schweizer CIOs geben mehr Geld für Sicherheit aus
- Security ist für Schweizer CIOs von Grossunternehmen zum mit Abstand wichtigsten IT-Thema geworden (bei eher sinkenden Ausgaben für ERP und IT-Infrastruktur)

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inSinova

interway net intelligence

SKYBOW

IT - Security Forum #4

Informationssicherheit

- IT-Sicherheitskonzept
  - Was genau muss ich schützen?
  - Wogegen muss ich es schützen?
  - Wie kann ich einen wirksamen Schutz erreichen?
  - Kann ich mir diesen Schutz leisten, verglichen mit dem möglichen Schaden?
- Notwendige Fragen
  - Schutzbedarf: Was will ich schützen?
  - Risikoanalyse: Wogegen muss ich mich schützen?
  - Massnahmenauswahl: Wie kann ich einen wirksamen Schutz erreichen?
  - Wirtschaftlichkeit: Kann ich mir diesen Schutz leisten, verglichen mit dem möglichen Schaden?

3

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

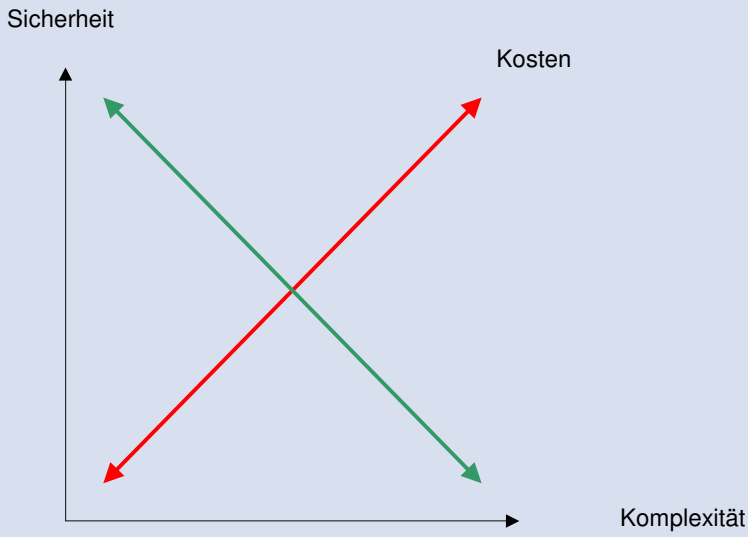
inSinova

interway net intelligence

SKYBOW

IT - Security Forum #4

Sicherheit und Komplexität vs. Kosten



4

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

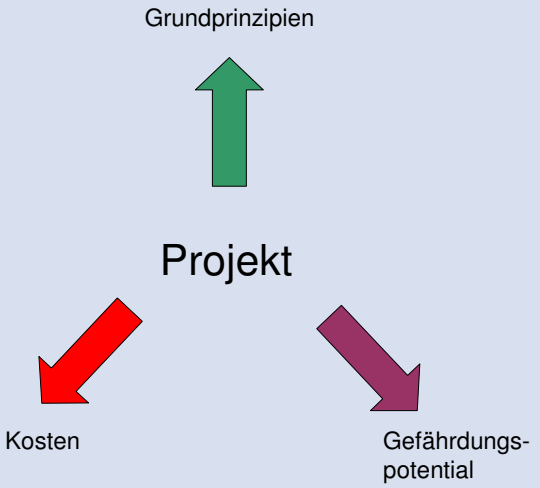
instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

Drei Dimensionen



5

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

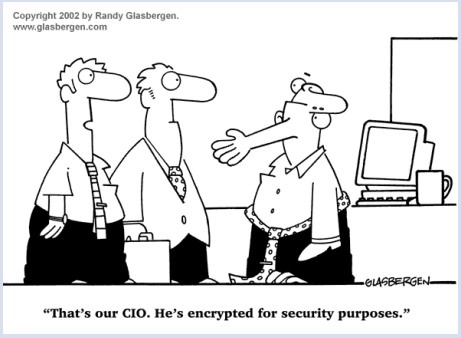
instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

Kennen wir alles schon!
Und jetzt?



"That's our CIO. He's encrypted for security purposes."

IT - Security Forum #4

Die Realität
Szenario 1

- KMU, 120 Mitarbeiter, internationale Niederlassungen, voll vernetzt, sehr grosse Mailboxen, viel Spam
- Auftrag der GL
  - Unser Messagingsystem muss revidierbar sein
- Fragen
  - Was heisst revidierbar?
  - Wieviele Jahre zurück?
  - Mit oder ohne Spam?
  - Falls ohne Spam: Was aber, falls Spam kein Spam ist?

7

IT - Security Forum #4

Die Realität
Szenario 2

- Eine Schweizer Privatbank
- Kleines IT-Team
- Die Geschäftsleitung stellt fest, dass sich vermehrt Kunden nach den Sicherheitsrichtlinien und Policies erkundet, neue gesetzliche Vorschriften sind zu erfüllen
- Projektaktiviäten:
  - Erstellen einer Analyse
  - Erstellen von Policies, Richtlinien, Prozessdefinitionen aus Erkenntnissen der Analyse
  - Durchführung von Schulungen (alle Mitarbeiter)
  - Projektübergabe
- Nach 4 Jahren?

8

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

Die Realität
Szenario 3

- International tätige Grossfirma (Produktion)
- IT-Abeilung mit mehreren 100 Mitarbeitern (!)
- IBM-Grossrechnerumgebung (RACF)
- Risikoabschätzung
  - Grosse, sensitive Datenbestände
  - IT-Fachpersonal
- Vorkehrungen
  - State of the art security
- Totzdem: Timebombed Code (Datenzerstörung nach Austritt des Mitarbeiters)

9

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

Die Erfahrungen

- Investitionen in IT-Sicherheit
  - vielfach planlos, ad hoc
  - ohne rationale Begründung
  - nicht nachhaltig
  - Mittel- und Ressourceneinsatz unzweckmässig
- Mitarbeiterselektion und -auswahl
  - Fachliche Selektion alleine ist ungenügend
  - Weiche Faktoren sehr wichtig bei …
    - Zusammensetzung der Projektgruppen
    - Aufgabenzuteilung

10

Kritische Erfolgsfaktoren

- Management Attention und vor allem Engagement
- Transparenz
- Selektion der Mitarbeiter (Softfaktoren)
- Zusammensetzung der Projektgruppen
- Ausbildung aller Beteiligten
- Einbettung in die Geschäftsziele
- Dauernde und regelmässige Überprüfung

IT-Sicherheit ist kein Selbstzweck, der Nutzen muss im Vordergrund stehen