IT-TRENDS Sicherheit

iT-Sicherheit *im* Unternehmen: Effektive Absicherung gegen interne Bedrohungen

iT-Trends Sicherheit 2012

Tobias Rademann, M.A.

[-DRUCKVERSION!-]

R.iT® SOLUTIONS

EDV-Betreuung *jenseits* vom Mittelmaß!

Kurzprofil

R.iT SOLUTIONS
EDV-Betreuung *jenseits* vom Mittelmaß!

- Name: Tobias Rademann, M.A.
  (MBSS, MCPS, MCNPS, STS, SSE, ASE)
- Funktion: Geschäftsführer R.*iT*-Solutions GmbH
- Firma: mehrfach zertifizierter EDV-Dienstleister
  Schwerpunkte:
  - *iT*-Beratung und Konzeption
  - Infrastrukturmanagement
  - interne / externe Kommunikation

Microsoft Partner
Silver Midmarket Solution Provider

astaro
authorized reseller

2012
Preferred
Partner

symantec.
Symantec Silver Partner

www.RiT.de

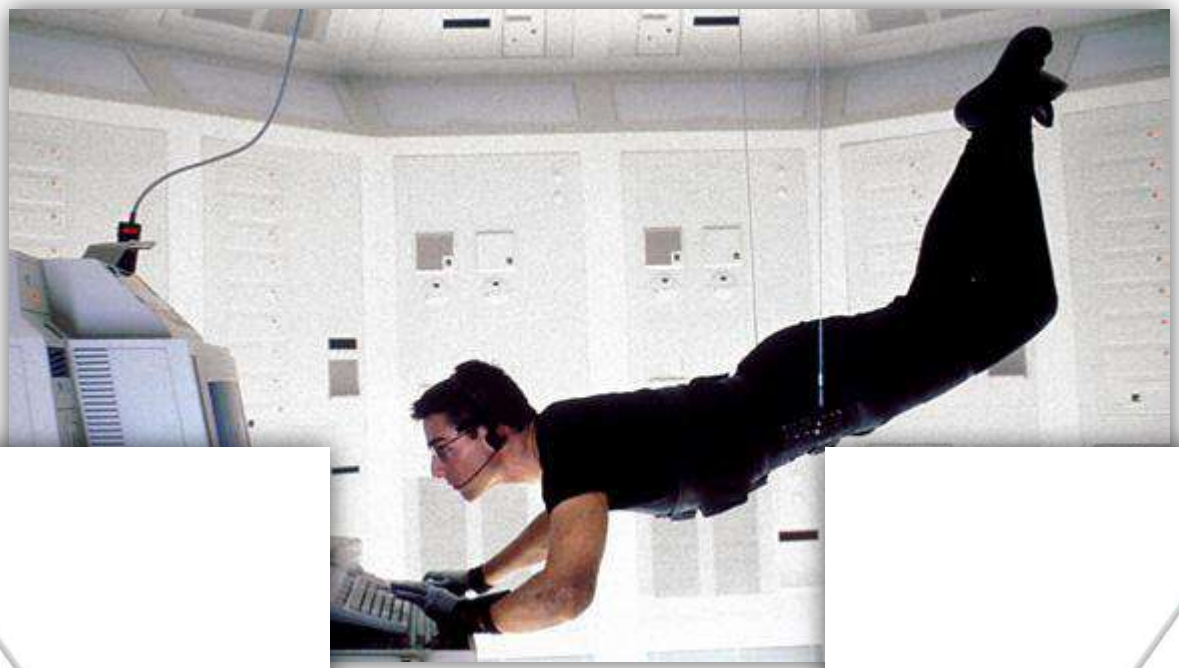
Agenda

- Ziel des Vortrags
- Wer steckt hinter internen Bedrohungen?
- Bedrohungsarten und -ziele
- (Potentielle) Schwachstellen
- Maßnahmen
- Résumée

Ziel des Vortrages

- Sensibilisierung
  - Risiken
  - Lösungen
- Denkanstöße
  - Wie geht man das Thema an?
  - Was verbirgt sich dahinter?
- Tipps für
  - Prävention
  - Erkennung
  - Ahndung

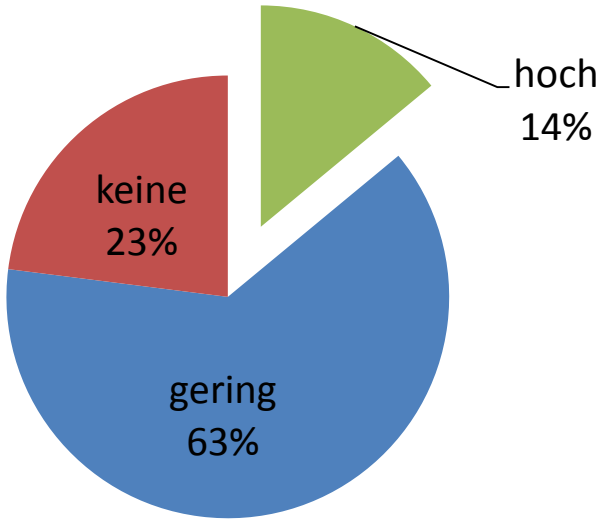
Bedrohungen in der *iT*



Was bedeutet *intern*?

- Mitarbeiter
  - Ex-Mitarbeiter
  - Mitarbeiter
  - Leiharbeiter
  - Management
- Geschäftspartner & Dienstleister
- Besucher

emotionale Bindung der Mitarbeiter zum Unternehmen (2011)



Quelle: Gallup.de, 2012

intern vs. extern

- hohes Schadenspotential vs. niedrige Barrieren:
  - Zugriff auf System ist gewollt
  - intime Kenntnisse über Prozesse vorhanden
  - *iT*-Abteilung: höchstes Risiko

- intern wichtiger als extern?
  - beides Bedrohungen
  - viele Überschneidungen

➔ es gibt hier kein wichtiger / unwichtiger
➔ beides muss berücksichtigt werden

Gründe für die Betroffenen

R.iT SOLUTIONS
EDV-Betreuung *jenseits* vom Mittelmaß!

- unbeabsichtigt:
  - Unachtsamkeit (Verlust USB Stick, priv. Medien, Umgang mit Passworten)
  - Unwissenheit / inhaltliche Überforderung (privates Surfen auf zweifelhaften Seiten, Social Engineering, Konfigurationsfehler)
  - organisatorische Überforderung (fehlende Zeit, falsche Prioritäten)

- beabsichtigt:
  - persönliche Motive (Rache)
  - finanzielle Motive (Habgier, Bereicherung, finanzieller Druck)
  - tätigkeitsbezogene Motive (Interessenkonflikte, Gelegenheit)

Bedrohungsarten und -ziele

- (Daten-)Diebstahl / Spionage
  - Kunden- und Arbeitnehmerdaten
  - Kreditkarteninformationen
  - Pläne, Prozess- oder Verfahrensdokumentationen, Quellcode, …
  - Geräte / Medien
- Missbrauch von Ressourcen
  - eMail / Internet
  - Netzwerk
  - Raubkopien
- Verlust von Daten und Geräten
- Sabotage / Schädigung
  - Zugriff auf Daten & Maschinen
  - Finanzen
  - Image
- Werkzeug für externe Angreifer

Ansatzpunkte

- fehlende / bekannte Kennworte
- ungenügender Zugriffsschutz
  - intern: Ordnerfreigaben, Sicherheitsgruppen, …
  - extern: OWA, RWW, …
- fehlende Kontrolle der Anwender-Aktivitäten
  (Surfen, etc.)
- fehlende Inhaltskontrolle beim Kopieren von Daten
  (Dateisystem / Datenbanken -> USB-Sticks, Notebooks, eMail, Web, etc.)

➔ Angreifer brauchen Zugriff auf Daten & Systeme!

BitLocker

eMail-Content Control

Application Control

Abhilfe:

➔ Zugriff beschränken!

GPOs

VLANs

AppLocker

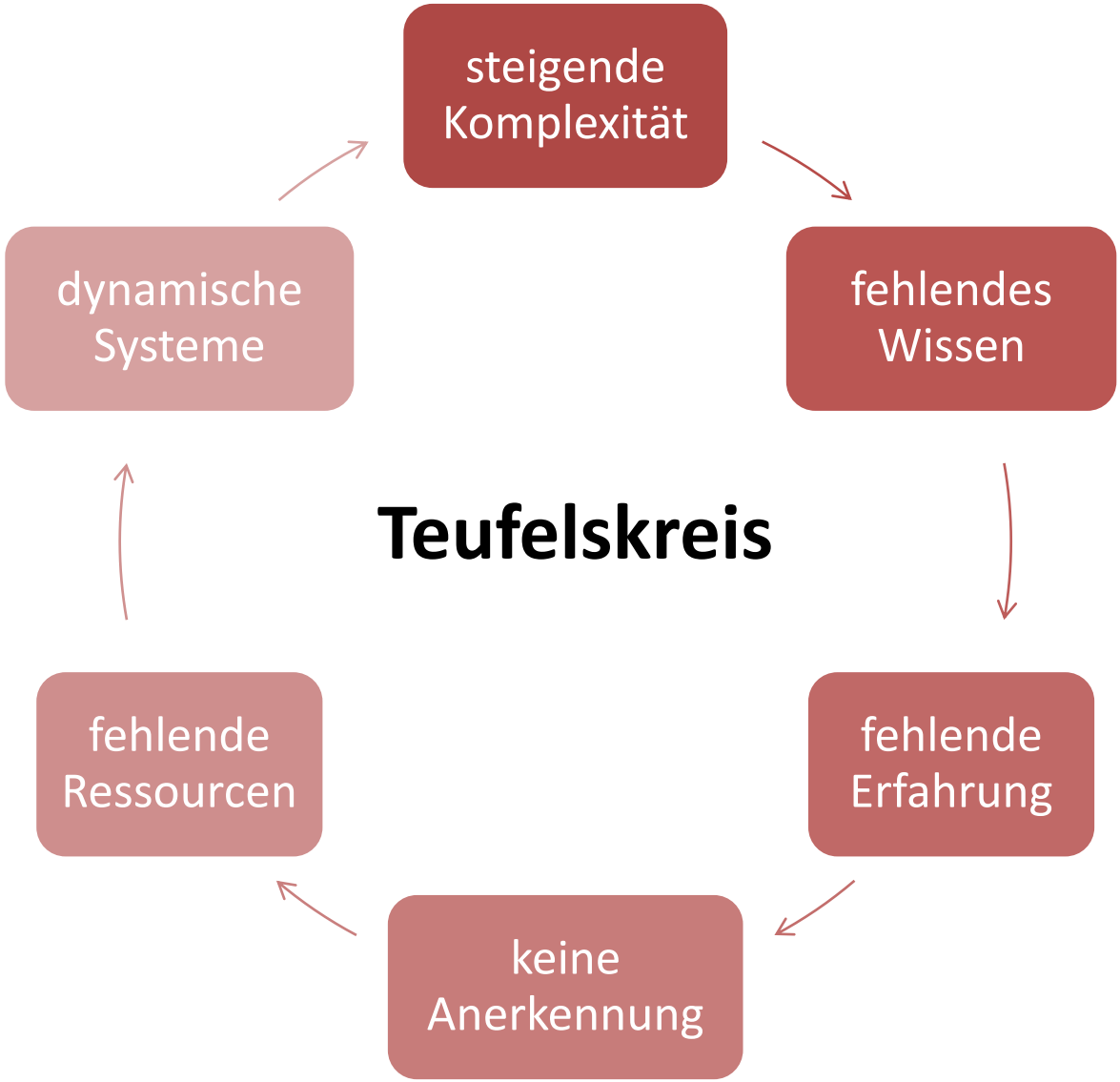
Kennwortrichtlinien

NAP

Proxy

Data Loss Prevention

Warum bislang so wenig unternommen?



Hinderungsgründe: Ergebnis

Ergebnis:

- hilflos, ratlos
- Angst, etwas falsch zu machen
- Unabwägbarkeit der Konsequenzen

➔ Nur Technik: viel zu kurz gegriffen!

Abhilfe / Maßnahmen

Drei Ebenen:

1. Prävention
2. Detektion
3. Reaktion

Abhilfe / Maßnahmen

1. Prävention
   - **Nachvollziehbarkeit schaffen**
   - Zugriff einschränken

Prävention: Nachvollziehbarkeit

Mittel:

- Awareness Workshop

Ziel:

- alle ins Boot holen
- Komplexität des Themas verringern
- geplant vorgehen

Prävention: Nachvollziehbarkeit / II

Inhalte:

- schützenswerte Daten identifizieren
- Bedrohungen konkretisieren
- Vorgehensweisen & Auswertungslisten erstellen
  - Datensicherungskontrolle
  - Kennwortänderungen, v.a. Admin-Kennwort
  - Sicherheitsgruppen
  - (kritische) Freigaben
  - Ausscheiden von Mitarbeitern / Abteilungswechsel
  - …

➔ Erfahrungen systematisch sammeln und verschriftlichen
➔ Wissen im Unternehmen behalten

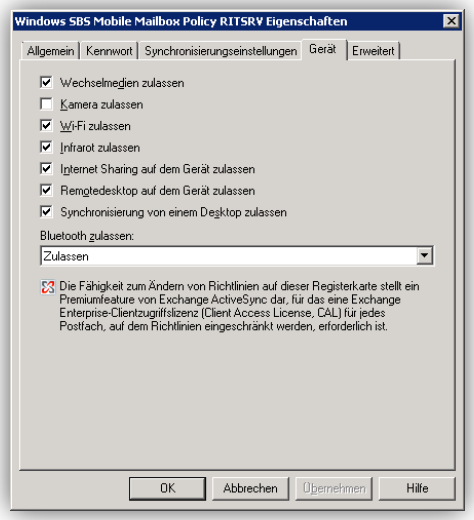
- **Zuständigkeiten regeln**
  - Umsetzen von Prozessen
  - Kontrollen (s.u.)
- **Klare Regeln und Richtlinien formulieren**
  (ggf. auch zunächst *nur* als Ziele)
  - Surfen
  - eMail-Nutzung
  - BYOD
  - Nutzung von Wechselmedien, …

Abhilfe / Maßnahmen

1. Prävention
   - Nachvollziehbarkeit schaffen ✓
   - **Zugriff einschränken**

Prävention: Zugriff einschränken

- Umgang mit Kennworten:
  - Kennwortrichtlinien
  - unterschiedliche Kennworte
- Sicherheitsgruppen wirklich nutzen
- Lösch- und Exportverbot in LOB Applikationen
- Nutzung von mobilen Geräten:
  - Synchronisierung:
    offline Dateien; Datenbanken / LOB-Applikationen
  - Verschlüsselung externer Medien und Geräte
  - Zugriffsbeschränkung
  - Smartphones: Kameranutzung, Wechselmedien, etc.
- Webzugriff: Proxy und Application Control
- Netzwerksegmentierung (W-/V-LANs)
- eMail-Nutzung: Inhaltscheck



Microsoft Exchange Server 2007 / Verwaltungskonsole

Prävention: Zugriff einschränken / II

- ***fortgeschrittene Projekte:***
  - NAC / NAP
  - 2-Faktor-Authentifizierung
  - DMS- / Archivierungslösungen
  - Data Loss Prevention Systeme

Abhilfe / Maßnahmen

1. Prävention
   - Nachvollziehbarkeit schaffen ✓
   - Zugriff einschränken ✓
   - **Redundanzen schaffen**

1. Prävention

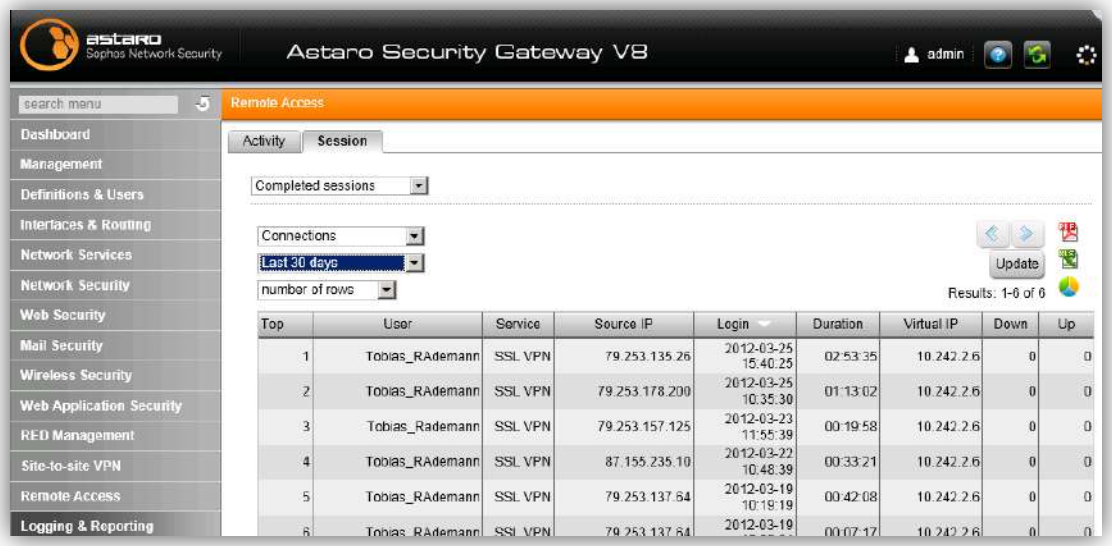
2. **Detektion**
   - regelmäßige Kontrolle der Systeme und Prozesse

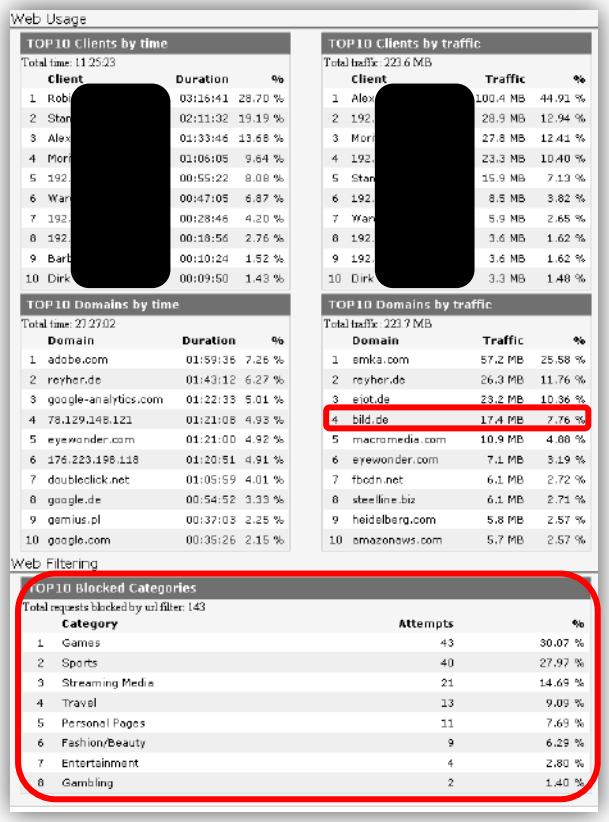
Detektion: Ziel von Kontrollen

- Ziel:
  - Sensibilisierung der Mitarbeiter
  - Verfeinerung der Wissensbasis
  - Aufdecken von Sicherheitsvorfällen
  - Abschreckung

Detektion: Ansatzpunkte

- Firewall-Berichte
  (Executive Report, Web-Proxy, Fernzugriffe)





Detektion: Ansatzpunkte

- Firewall-Berichte
  (Executive Report, Web-Proxy, Fernzugriffe)
- Ausfüllen von sicherheitsbezogenen Formularen
  - Änderung des Administrator-Kennwortes
  - Überprüfung der Sicherheitsgruppen
  - (kritische) Freigaben
  - tgl. Datensicherungscheck
- Berichte von DLP-Software

➔ Security Assessment

Reaktion:

1. Prävention

2. Detektion

3. **Reaktion**
   - Berechtigungen entziehen
   - Kennwortwechsel einleiten
   - Beweise sichern
   - Behörden einschalten (v.a. BSI)

Handlungsempfehlungen:

- Keine Hexerei sondern machbar!
- Mix aus organisatorischen und technischen Maßnahmen
- Thema ist komplex, daher:
  - anfangen
  - Erfahrungen sammeln
  - ggf. Externe hinzuziehen
- auf Naheliegendes konzentrieren

EDV-Betreuung *jenseits* vom Mittelmaß!

Vielen Dank für Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

Tobias Rademann
R.*iT*-Solutions GmbH
www.R*iT*.de

Kortumstraße 76, 44787 Bochum
Tel.: (0234) 438800-0, Fax: (0234) 438800-29
eMail: Tobias.Rademann@R*iT*.de

Quellen / Hintergrundinformationen

Geschonnek, Alexander (2010): e-Crime-Studie 2010: Computerkriminalität in der deutschen Wirtschaft. KPMG AG Wirtschaftsprüfungsgesellschaft.
URL: *www.kpmg.de/docs/20100810_kpmg_e-crime.pdf*

Nink, Marco (2012): Engagement Index Deutschland 2011. Pressegespräch. Gallup, Inc.
URL: h*ttp://eu.gallup.com/file/Berlin/153302/Pressemitteilung%20zum%20Gallup%20Engagement%20Index%202011.pdf.pdf*

Bilder: Fotolia.de
http://tomcruiseinhollywood.blogspot.de/