



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

## *iT*-Trends Sicherheit 2012

Tobias Rademann, M.A.

[-DRUCKVERSION!-]



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



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

# Ziel des Vortrages

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

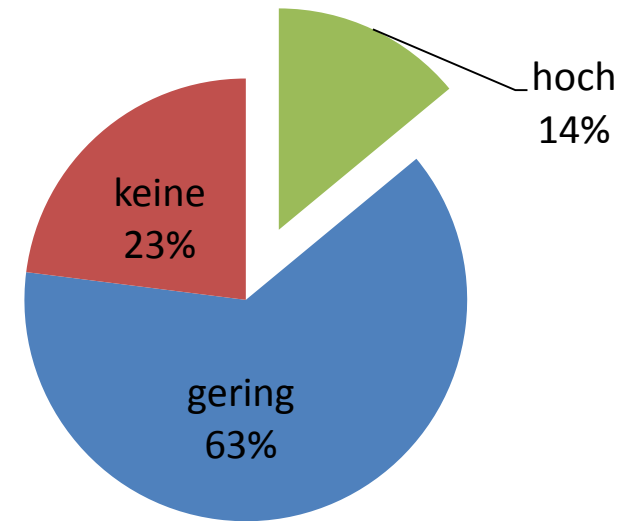
# Bedrohungen in der *iT*



# 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

- unbeabsichtigt:
  - Unachtsamkeit (Verlust USB Stick, priv. Medien, Umgang mit Passwörtern)
  - 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



# Wie erfolgen die Angriffe?

## 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-

**Abhilfe:**

Content Control

→ Zugriff beschränken!

Application Control

GPOs

VLANs

AppLocker

Kennwortrichtlinien

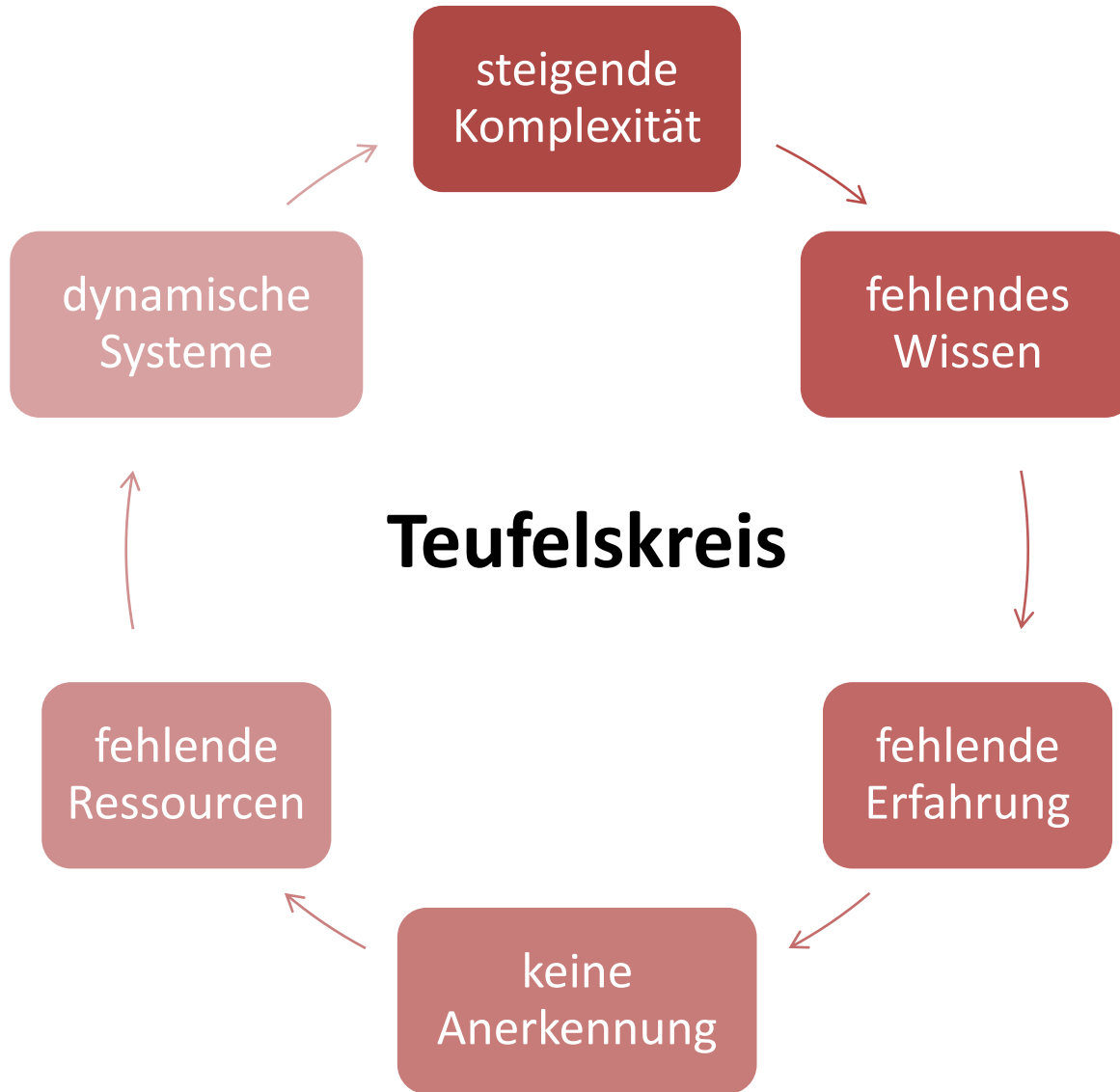
PROXY



NAP

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!



## Drei Ebenen:

1. Prävention
2. Detektion
3. Reaktion

## 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, ...



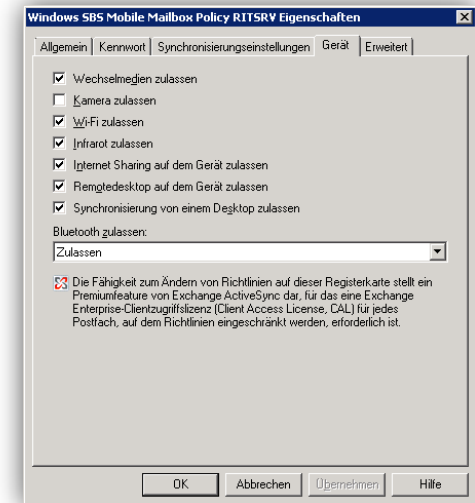
## 1. Prävention

- 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

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



# Abhilfe / Maßnahmen

## 1. Prävention

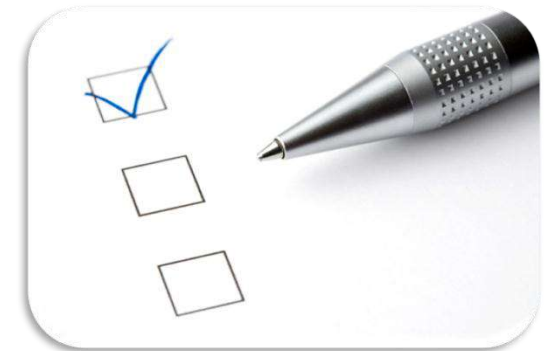
- Nachvollziehbarkeit schaffen ✓
- Zugriff einschränken ✓
- **Redundanzen schaffen**



## 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)



**Astaro Security Gateway V8**

Remote Access

Activity Session

Completed sessions

Connections: Last 30 days

number of rows

Results: 1-6 of 6

Top	User	Service	Source IP	Login	Duration	Virtual IP	Down	Up
1	Tobias_RAdemann	SSL VPN	79.253.135.26	2012-03-25 15:40:25	02:53:35	10.242.2.6	0	0
2	Tobias_RAdemann	SSL VPN	79.253.178.200	2012-03-25 10:35:30	01:13:02	10.242.2.6	0	0
3	Tobias_Rademann	SSL VPN	79.253.157.125	2012-03-23 11:55:39	00:19:58	10.242.2.6	0	0
4	Tobias_RAdemann	SSL VPN	87.155.235.10	2012-03-22 10:48:39	00:33:21	10.242.2.6	0	0
5	Tobias_RAdemann	SSL VPN	79.253.137.64	2012-03-19 10:19:19	00:42:08	10.242.2.6	0	0
6	Tobias_RAdemann	SSL VPN	79.253.137.64	2012-03-19 10:19:19	00:07:17	10.242.2.6	0	0

Web Usage

Total time: 11:25:23

TOP10 Clients by time

Client	Duration	%
1 Robi	03:16:41	29.70 %
2 Star	02:11:32	19.19 %
3 Alex	01:33:46	13.68 %
4 Mor	01:06:05	9.64 %
5 192	00:55:22	9.08 %
6 War	00:47:05	6.87 %
7 192	00:28:46	4.20 %
8 192	00:18:56	2.76 %
9 Bar	00:10:24	1.52 %
10 Dirk	00:09:50	1.43 %

TOP10 Clients by traffic

Total traffic: 223.6 MB

Client	Traffic	%
1 Alex	100.4 MB	44.92 %
2 192	28.9 MB	12.94 %
3 Mor	27.8 MB	12.41 %
4 192	23.3 MB	10.40 %
5 Star	15.9 MB	7.13 %
6 192	8.5 MB	3.82 %
7 War	5.9 MB	2.65 %
8 192	3.6 MB	1.62 %
9 192	3.6 MB	1.62 %
10 Dirk	3.3 MB	1.48 %

TOP10 Domains by time

Total time: 27:27:02

Domain	Duration	%
1 adobe.com	01:59:36	7.26 %
2 reyhende	01:43:12	6.27 %
3 google-analytics.com	01:22:33	5.01 %
4 78.129.148.121	01:21:08	4.93 %
5 eyewonder.com	01:21:00	4.92 %
6 176.223.198.118	01:20:51	4.91 %
7 doubleclick.net	01:05:59	4.01 %
8 google.de	00:54:52	3.95 %
9 gemius.pl	00:37:03	2.25 %
10 google.com	00:35:26	2.15 %

TOP10 Domains by traffic

Total traffic: 223.7 MB

Domain	Traffic	%
1 omka.com	57.2 MB	25.58 %
2 reyhende	26.3 MB	11.76 %
3 ejot.de	23.2 MB	10.36 %
4 bild.de	17.4 MB	7.76 %
5 macromedia.com	10.9 MB	4.88 %
6 eyewonder.com	7.1 MB	3.19 %
7 fbodn.net	6.1 MB	2.72 %
8 steeline.biz	6.1 MB	2.71 %
9 heidelberg.com	5.8 MB	2.57 %
10 amazonaws.com	5.7 MB	2.57 %

Web Filtering

TOP10 Blocked Categories

Total requests blocked by url filter: 143

Category	Attempts	%
1 Games	43	30.07 %
2 Sports	40	27.97 %
3 Streaming Media	21	14.68 %
4 Travel	13	9.09 %
5 Personal Pages	11	7.69 %
6 Fashion/Beauty	9	6.29 %
7 Entertainment	4	2.80 %
8 Gambling	2	1.40 %



# 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 Nahliegendes konzentrieren

## Vielen Dank für Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:



Tobias Rademann  
**R.iT-Solutions GmbH**  
[www.RiT.de](http://www.RiT.de)

Kortumstraße 76, 44787 Bochum

Tel.: (0234) 438800-0, Fax: (0234) 438800-29

eMail: [Tobias.Rademann@RiT.de](mailto:Tobias.Rademann@RiT.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](http://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf)
- Nink, Marco (2012): Engagement Index Deutschland 2011. Pressegespräch. Gallup, Inc.  
URL: <http://eu.gallup.com/file/Berlin/153302/Pressemitteilung%20zum%20Gallup%20Engagement%20Index%202011.pdf.pdf>
- Bilder: Fotolia.de  
<http://tomcruiseinhollywood.blogspot.de/>