eBUSINESSLOTSE
INFOBÜRO FÜR UNTERNEHMEN
RUHR

Überlegungen zur Effizienz bei der Umsetzung von *iT*-Sicherheits-Maßnahmen für KMUs

Roadshow: Cybercrime –
eine Bedrohung auch für kleine und mittlere Unternehmen

Tobias Rademann, Bochum, 19. November 2013

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:

- Infrastrukturmanagement
- Entwicklung
- strategische *iT*-Beratung

Microsoft Partner
Silver Server Platform
Silver Management and Virtualization
Silver Midmarket Solution Provider

symantec.
Symantec Silver Partner

Preferred
hp
Partner

astaro
authorized reseller

www.RiT.de

Ziel des Vortrags

➔ ***Wie*** können ***Sie***

das Thema ***iT-Sicherheit***

konkret und effizient angehen?

Agenda

EDV-Betreuung *jenseits* vom Mittelmaß!

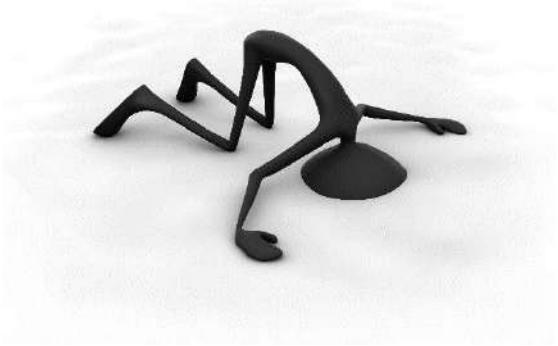
- Erfahrung: *iT*-Sicherheit und KMU
- *iT*-Sicherheitsmaßnahmen effizient umsetzen
  - eigene Rahmenbedingungen klären
  - systematisch Prioritäten setzen
- Zusatz: Appetizer
- Résumée

Ergebnis von Neukundenaufnahmen oder *iT*-Assessments:

Unternehmen machen kaum etwas

oder

unkoordinierter Aktionismus



Gründe:

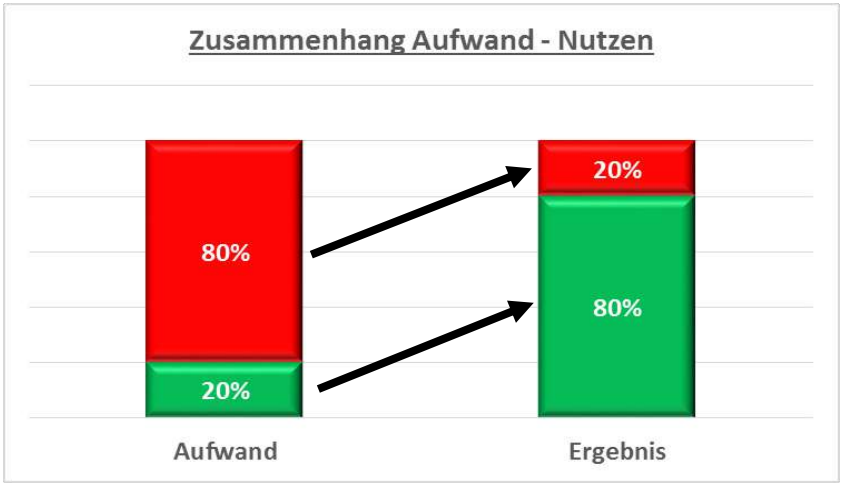
- Komplexität wirkt abschreckend
- Themen überfordern Nicht-*iT*-Sicherheitsfachleute

Sonderfall KMU:

- begrenzte Ressourcen
  - Geld
  - *iT*-Fachleute
  - Wissen / Erfahrung im Bereich *iT*-Sicherheit

➔ Herausforderung: **Wie** das Thema angehen!

Pareto-Prinzip:



➔ i.d.R. führen 20% Aufwand zu 80% des Ergebnisses

Ziel:

- Maßnahmen identifizieren,
  mit denen ***Sie* für *Ihr Unternehmen*** 80% Wirkung erzielen

Agenda

- *Erfahrung: iT-Sicherheit und KMU* ✓
- ***iT*-Sicherheitsmaßnahmen effizient umsetzen**
  1. eigene Rahmenbedingungen klären
  2. systematisch Prioritäten setzen

Rahmenbedingungen I: Was

1. eigene Rahmenbedingungen:
   - Was ist ***im eigenen Unternehmen*** wichtig?
     - Welche **Daten** sind kritisch?
     - Welche **Systeme** sind kritisch?

2 Ansätze:

- analytisch: viel Zeit, Fragebögen
- pragmatisch: Was sind die häufigsten Bedrohungen?

Rahmenbedingungen I: Was

häufigste Bedrohungen:

- Datenverlust (und kein Backup)
- Befall durch Viren
- Ausfall des Administrators
- Hackerangriff aus dem Internet
- Innentäter

Bundesamt für Sicherheit in der Informationstechnik

Quelle: Bundesamt für Sicherheit in der Informationstechnik (2012): Leitfaden Informationssicherheit. IT-Grundschutz kompakt.

Was: zentrale Schutzmaßnahmen

EDV-Betreuung *jenseits* vom Mittelmaß!

Primärziel:	Maßnahme
I. Sicherung der Datenverfügbarkeit	Datensicherung
	Datenwiederherstellung
	Schutz mobiler Geräte
II. Schutz vor externen Angriffen	Firewall
	Viren- und Endgeräteschutz
	eMail-Schutz
	Sicherheitsupdates
	Wartung (kritischer) Systeme / regelmäßige Kontrollen
III. Schutz vor internen Angriffen	Aufklärung & Sensibilisierung
	Richtlinien (bspw. Kennwortrichtl.)
	Checklisten (Ein- / Austritt von Mitarbeitern)
	physikalischer Zugriff
	Sicherheitsgruppen
	Segmentierung von Daten (Zugriffsschutz)
IV. Sicherung der Reaktionsfähigkeit	klare Zuständigkeiten (Pflege, im Schadensfall)
	Zusammenarbeit mit Dritten / Vertreterregelungen
	aktuelle Dokumentation inkl. Datenträgern

Rahmenbedingungen II: Budget

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

1. eigene Rahmenbedingungen:
   - Was ist wichtig? ✓
   - Wie hoch ist das **eigene Budget?**

   Festlegen:

   - **Kosten**budget (€) *(i.d.R. extern)*
     - Hardware und Lizenzen
     - Dienstleistungen
   - **Zeit**budget (h) *(i.d.R. intern)*
     - Administrator
     - andere Mitarbeiter

Vorgehen

1. eigene Rahmenbedingungen klären:
   - Was ist **im eigenen Unternehmen** wichtig? ✓
   - Wie hoch ist das **eigene Budget**? ✓
2. **Prioritäten setzen:**
   - Aufwand je Maßnahme
   - konkrete Planung (Was wann wie)

Aufwand (€/h) je Maßnahme festhalten:

- dabei: Kategorisierung der o.g. Maßnahmen in 2 Blöcke:
  - primär Kosten -> extern vergeben
  - primär Zeit -> intern vergeben
- berücksichtigen: einmalig vs. laufend

Übersicht: Aufwand (in €) je *iT*-Sicherheitsmaßnahme

Maßnahmen	Kosten	
	initial	laufend
Firewall	1.500,00 €	600,00 €
Viren- und Endgeräteschu		
eMail-Schutz		
physikalischer Zugriff		

Übersicht: Aufwand (in h) je *iT*-Sicherheitsmaßnahme

Maßnahmen	zeitl. Aufwand	
	initial	laufend
Sicherheitsupdates	16 h	12x 1,0h
Kennwortrichtlinien	4 h	*2 h*
Checklisten Mitarbeiter-Ein-/Austritt	6 h	0 h

iT-Sicherheitsmaßnahmen: Aufwand

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

Übersicht: Aufwand für *iT*-Sicherheitsmaßnamen im Bereich des Basisschutzes für KMUs

		externe Kosten (€)				interne Kosten (h)			
		initial		laufend		initial		laufend	
Primärziel:	Maßnahme	Lizenzen / Hardware	Dienst-leistung	Lizenzen / Hardware	Dienst-leistung	h Admin.	h je Mitarb.	h Admin.	h je Mitarb.
I. Sicherung der Datenverfügbarkeit	Datensicherung								
	Datenwiederherstellung								
	Schutz mobiler Geräte								
II. Schutz vor externen Angriffen	Firewall								
	Viren- und Endgeräteschutz								
	eMail-Schutz								
	Sicherheitsupdates								
	Wartung (kritischer) Systeme / regelmäßige Kontrollen								
III. Schutz vor internen Angriffen	Aufklärung & Sensibilisierung								
	Richtlinien (bspw. Kennwortrichtl.)								
	Checklisten (Ein- / Austritt von Mitarbeitern)								
	physikalischer Zugriff								
	Sicherheitsgruppen								
	Segmentierung von Daten (Zugriffsschutz)								
IV. Sicherung der Reaktionsfähigkeit	klare Zuständigkeiten (Pflege, im Schadensfall)								
	Zusammenarbeit mir Dritten / Vertreterregelungen								
	aktuelle Dokumentation inkl. Datenträgern								

Planung: Basis

EDV-Betreuung *jenseits* vom Mittelmaß!

iT-Sicherheitsbudget (€):	3.000,00 €						
Maßnahme	**1. Jahr**	**2. Jahr**	**3. Jahr**	**4. Jahr**	**5. Jahr**	**6. Jahr**	**7. Jahr**
Firewall							
Viren- und Endgeräteschutz							
eMail-Schutz							
physikalischer Zugriff							
verbleibendes Budget (inkl. VJ):	3.000,00 €						

Übersicht: Aufwand (in €) je *iT*-Sicherheitsmaßnahme

Maßnahmen	Kosten	
	initial	laufend
Firewall	1.500,00 €	600,00 €
Viren- und Endgeräteschutz	1.700,00 €	500,00 €
eMail-Schutz	600,00 €	600,00 €
physikalischer Zugriff	1.000,00 €	- €

Planung: 1. Jahr

EDV-Betreuung *jenseits* vom Mittelmaß!

iT-Sicherheitsbudget (€):	3.000,00 €					
Maßnahme	**1. Jahr**	**2. Jahr**	**3. Jahr**	**4. Jahr**	**5. Jahr**	**6. Jahr**
Firewall						
Viren- und Endgeräteschutz	1.700,00 €	500,00 €				
eMail-Schutz	600,00 €	600,00 €				
physikalischer Zugriff						
verbleibendes Budget (inkl. VJ):	700,00 €	2.600,00 €				

Übersicht: Aufwand (in €) je *iT*-Sicherheitsmaßnahme

Maßnahmen	Kosten	
	initial	laufend
Firewall	1.500,00 €	600,00 €
Viren- und Endgeräteschutz	1.700,00 €	500,00 €
eMail-Schutz	600,00 €	600,00 €
physikalischer Zugriff	1.000,00 €	- €

Planung: 2. Jahr

EDV-Betreuung *jenseits* vom Mittelmaß!

iT-Sicherheitsbudget (€):	3.000,00 €						
Maßnahme	**1. Jahr**	**2. Jahr**	**3. Jahr**	**4. Jahr**	**5. Jahr**	**6. Jahr**	**7. Jahr**
Firewall		1.500,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €
Viren- und Endgeräteschutz	1.700,00 €	500,00 €	500,00 €	500,00 €	500,00 €	500,00 €	500,00 €
eMail-Schutz	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €
physikalischer Zugriff		1.000,00 €	- €	- €	- €	- €	- €
verbleibendes Budget:	700,00 €	100,00 €	1.400,00 €	2.700,00 €	4.000,00 €	5.300,00 €	6.600,00 €

Übersicht: Aufwand (in €) je *iT*-Sicherheitsmaßnahme

Maßnahmen	Kosten	
	initial	laufend
Firewall	1.500,00 €	600,00 €
Viren- und Endgeräteschutz	1.700,00 €	500,00 €
eMail-Schutz	600,00 €	600,00 €
physikalischer Zugriff	1.000,00 €	- €

Planung: Der Mix macht's

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

iT-Sicherheitsbudget (€):	3.000,00 €						

Maßnahme	1. Jahr	2. Jahr	3. Jahr	4. Jahr	5. Jahr	6. Jahr	7. Jahr
Firewall	- €	1.500,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €
Viren- und Endgeräteschutz	1.700,00 €	500,00 €	500,00 €	500,00 €	500,00 €	500,00 €	500,00 €
eMail-Schutz	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €	600,00 €
physikalischer Zugriff		1.000,00 €	- €	- €	- €	- €	- €
verbleibendes Budget:	700,00 €	100,00 €	1.400,00 €	2.700,00 €	4.000,00 €	5.300,00 €	6.600,00 €

iT-Sicherheitsbudget (h):	24 h						

Maßnahme	1. Jahr	2. Jahr	3. Jahr	4. Jahr	5. Jahr	6. Jahr	7. Jahr
Sicherheitsupdates	16 h	12 h	12 h	12 h	12 h	12 h	12 h
Kennwortrichtlinien	6 h	2 h	2 h	2 h	2 h	2 h	2 h
Checklisten MA-Ein-/Austritt		6 h	0 h	0 h	0 h	0 h	0 h
verbleibendes Budget:	2 h	6 h	16 h	26 h	36 h	46 h	56 h

Ziel: Durch bewussten Mix **einmaliger und laufender Kosten** sowie **externer und interner Kosten** viel erreichen!

Planung: Tipps & Tricks

optimales Vorgehen:

- *bewusster* Mix einmaliger und laufender sowie externer und interner Kosten
- zunächst: Etablierung Basisschutz (80/20 – nicht zu detailliert!)
- erst wenn der steht: Ausbau einzelner Maßnahmen
  (bspw. Pentests, Webfilter, Verschlüsselung, etc.)

Agenda

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

- *Erfahrung: iT-Sicherheit und KMU* ✓
- *iT-Sicherheitsmaßnahmen effizient umsetzen* ✓
  - *eigene Rahmenbedingungen klären*
  - *systematisch Prioritäten setzen*
- **Zusatz: Appetizer**

Themen, mit denen Sie i.d.R. schnell viel erreichen:

- intern:
  - Mitarbeitersensibilisierung
  - Checklisten
- extern:
  - Datensicherung
  - Viren- und Endgeräteschutz ✓
  - regelm. Sicherheitsupdates
  - Firewall
  - lokaler "Dropbox"-Ersatz

Agenda

- *Erfahrung: iT-Sicherheit und KMU* ✓
- *iT-Sicherheitsmaßnahmen effizient umsetzen* ✓
  - *eigene Rahmenbedingungen klären*
  - *systematisch Prioritäten setzen*
- *Zusatz: Appetizer* ✓
- **Résumée**

Résumée

- Hauptproblem: Umsetzung ("Wie")
- Aber:
  - Komplexität ist *ohne großen Aufwand* in den Griff zu bekommen
    -> "Standard-Bundles" gegen häufigste Bedrohungen
    -> Basiskonfiguration reicht zunächst völlig aus
  - es lohnt sich, loszulegen
- Wie?
  - strukturiert und systematisch
    - Budget festlegen
    - Maßnahmen priorisieren / geplant investieren

    ➔ dann ist auch mit vglsw. wenig Ressourcen viel erreichbar
  - KMU bedeutet immer: eigene Mitarbeiter und Dritte

EDV-Betreuung *jenseits* vom Mittelmaß!

Vielen Dank für Ihre Aufmerksamkeit!

Bei Rückfragen wenden Sie sich gerne an:

Tobias Rademann, M.A.
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