



DIGITIZE YOUR BUSINESS

Mehr Effektivität bei der operativen iT-Sicherheit: **Wie komme ich bei all den Sicherheitsrisiken noch hinterher?**

Vortrag im Rahmen der 14. iT Trends Sicherheit

Tobias Rademann, M.A.



Effektivität = die **richtigen Dinge** tun

im iT-Sicherheitsumfeld:

richtige Dinge = solche, die **zentrale iT-Sicherheitsrisiken** minimieren

Agenda

1. effektives **Vorgehen**
2. Auswahlkriterien für effektive **Werkzeuge**
3. Résumé

Kurzprofil: Tobias Rademann

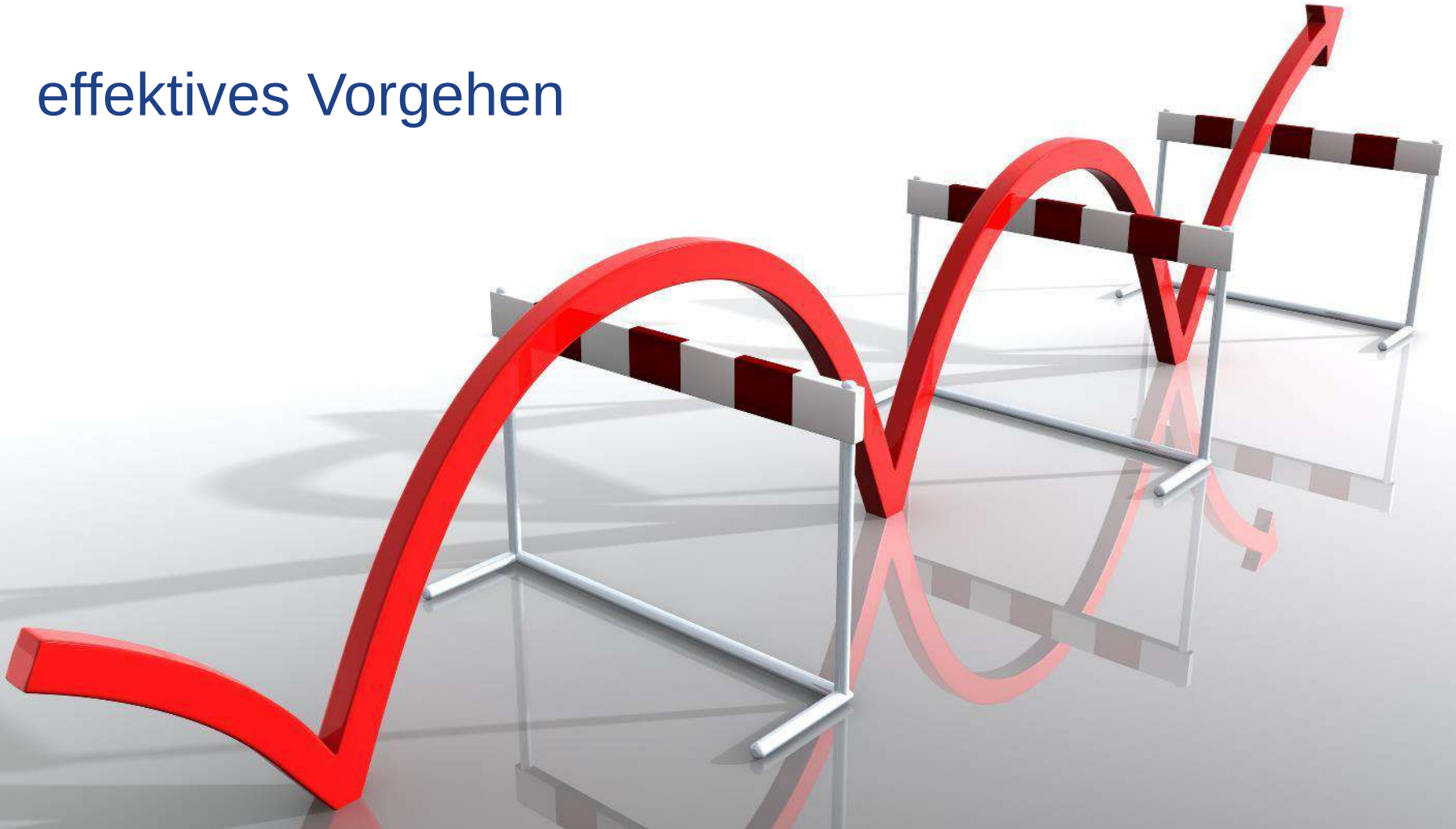
- **Funktion:** Geschäftsführer R.iT GmbH
- **Fokus:** iT-Unternehmensberatung für den digitalen Wandel
- **gegründet:** 2001, Spin-Off der Ruhr-Universität
- **Standorte:** Zentrale: Bochum
Region Nord: Bad Schwartau
- **Zertifizierung:** BMWi-autorisiert für iT-Sicherheit und digitale Geschäftsprozesse
- **Engagement:**
 -  networker NRW
Der IT Verband
 -  Microsoft Partner
Silver Midmarket Solution Provider
Silver Dalacenter
 -  nrw-units
Netzwerkpartner
 -  eco
VERBAND DER
INTERNETZWERKE
MITGLIED
 -  BMW
Bundesverband
mittelständische Wirtschaft

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages

effektives Vorgehen



effektives Vorgehen

Phase 1: Prävention

Phase 2: Detektion & Reaktion

Phase 1: Prävention

- **richtige Dinge:** Orientierung am Durchschnitt:

- Datenverlust
- Ausnutzen von Sicherheitslücken
- Fehler von Anwendern

- **Werkzeuge:**



1.) Datensicherung



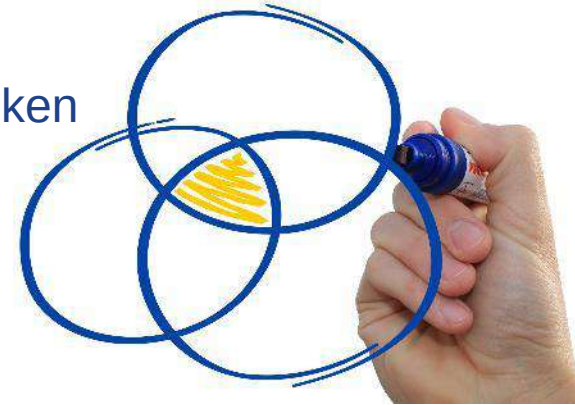
2.) Patchmanagement



3.) Mitarbeiter-Sensibilisierung



4.) Perimetersicherheit (Firewalls, Endgerätesicherheit)



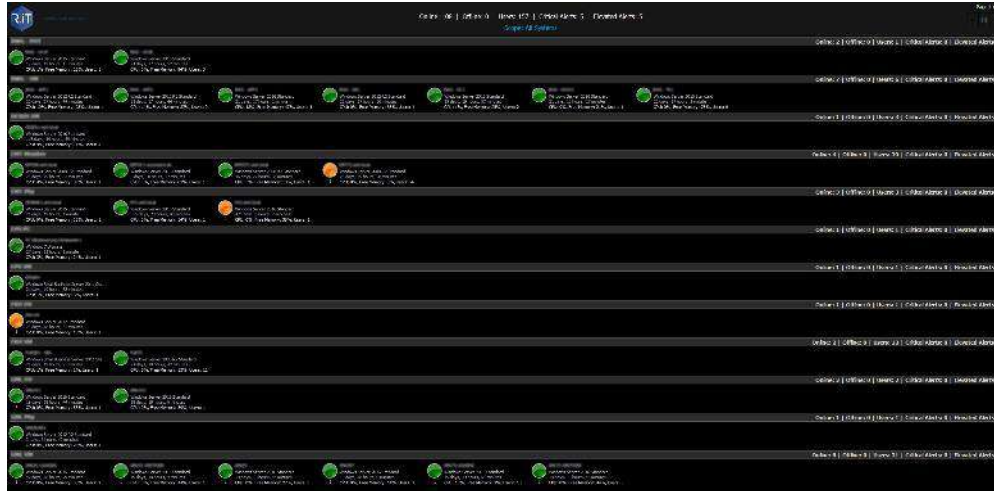
Phase 2: Detektion & Reaktion

- **richtige Dinge:** Orientierung am individuellen Status Quo:
 - Überblick behalten
 - bei Problemen: zielgerichtet handeln
 - bei Ruhe: Sicherheitsinfrastruktur ausbauen
- **Werkzeuge:**
 - proaktive Warnungen:** Momentaufn., **push**, anwendungsbez.
 - Monitoring:** s.o., **aggregiert**
 - Berichte:** s.o., Historie
 - Dashboards:** s.o., **Grafiken**, **pull**

- iT-Risk Assessments:** s.o., **ganzheitlich**



gezeigte Screenshots



Backup job: Vollsystem (Full)
Created by HV Adminstrator at 04.08.2017 13:45

Monday, 26. Februar 2018 22:00:19

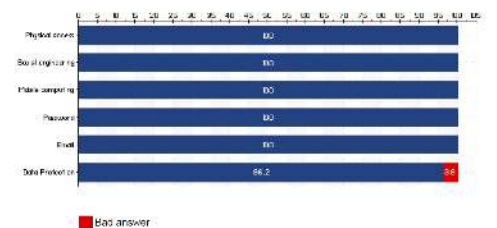
Success	0	Start time	22:00:19	Total size	0,0 B	Backup size	0,0 B
Warning	0	End time	22:01:57	Data read	0,0 B	Deduce	1,0 B
Error	0	Duration	0:01:38	Info/failure	0,0 B	Compression	1,0 B

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
AVL	Error	22:00:25	22:01:45	0,0 B	0,0 B	0,0 B	0:01:20	Unable to allocate processing resources. Error: Unable to find upper V hosts where VM 'back670' and '220 302' is registered
DCI	Error	22:00:25	22:01:47	0,0 B	0,0 B	0,0 B	0:01:21	Unable to allocate processing resources. Error: Unable to find upper V hosts where VM 'back670' and '220 302' is registered
BOCH	Error	22:00:25	22:01:47	0,0 B	0,0 B	0,0 B	0:01:21	Unable to allocate processing resources. Error: Unable to find upper V hosts where VM 'back670' and '220 302' is registered
AVL	Error	22:00:25	22:01:47	0,0 B	0,0 B	0,0 B	0:01:21	Unable to allocate processing resources. Error: Unable to find upper V hosts where VM 'back670' and '220 302' is registered
TSL	Error	22:00:25	22:01:47	0,0 B	0,0 B	0,0 B	0:01:21	Unable to allocate processing resources. Error: Unable to find upper V hosts where VM 'back670' and '220 302' is registered

RAPID
Awareness

Categories



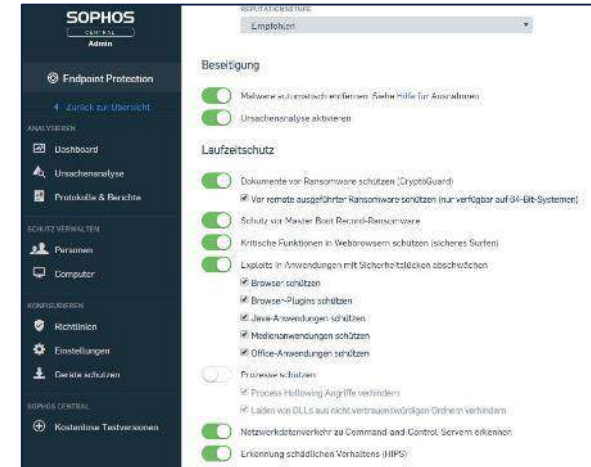
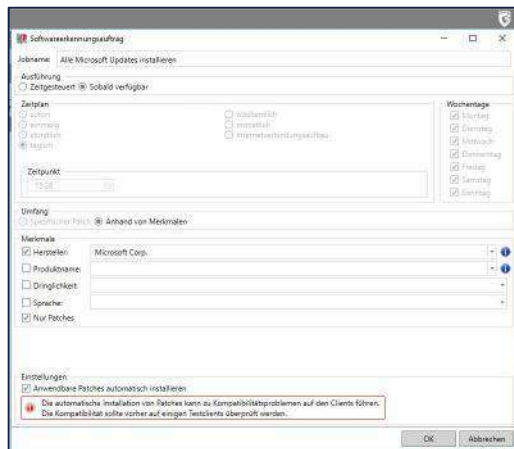
Auswahlkriterien für effektive Werkzeuge



effektive Werkzeuge

tun das Richtige automatisch

- auf Basis eines vom Hersteller vorgegebenen Regelwerks
- eines individuell erstellten Regelwerks von Verhaltensmustern (Heuristiken)
- von künstlicher Intelligenz



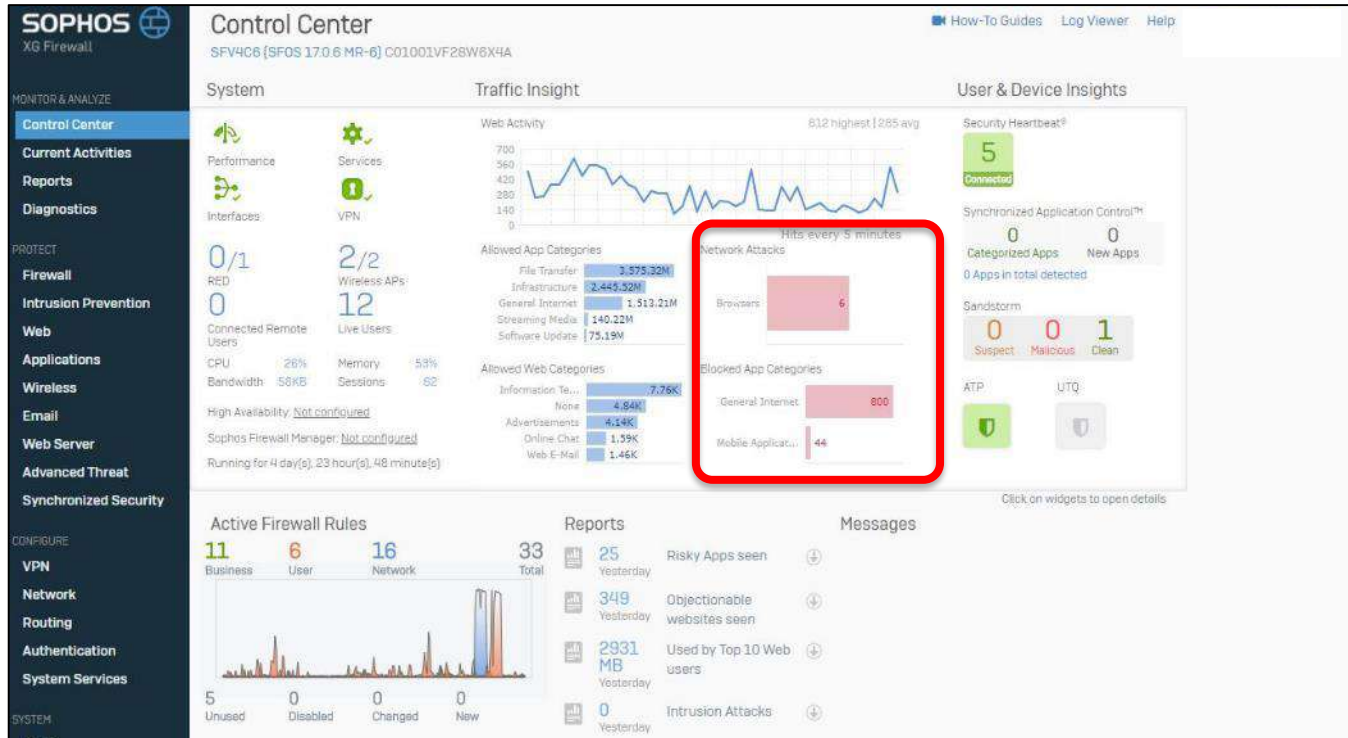
effektive Werkzeuge

befähigen den Admin, das Richtige zu tun

- **verschaffen Überblick**
 - proaktive Information: eMail, SMS
 - aggregierte Darstellung: Ampel o.ä.
 - gezielte Information: Fokus auf Bedrohungen
 - offene Schnittstellen → einbindbar in Monitoring Systeme



gezeigte Screenshots



effektive Werkzeuge

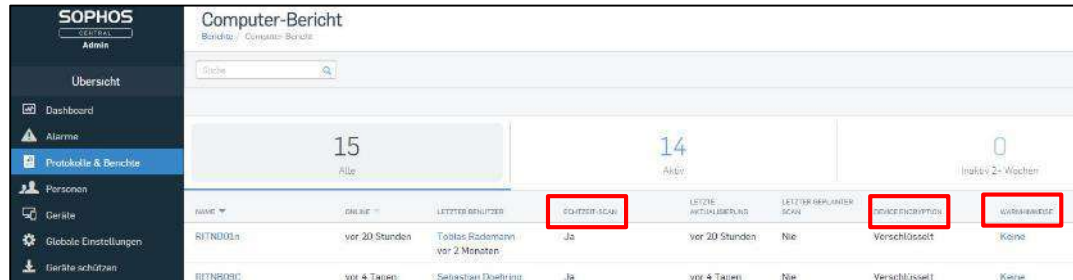
befähigen den Admin, das Richtige zu tun

- verschaffen Überblick
- **sind ressourcenschonend**
 - wenig Einarbeitungsaufwand
 - leichte Handhabbarkeit (Wartung, Umfang, Notfall)

→ **unified** oft sinnvoller als **best-of-breed**!



gezeigte Screenshots



SOPHOS Central Admin

Computer-Bericht
Berichte / Computer-Bericht

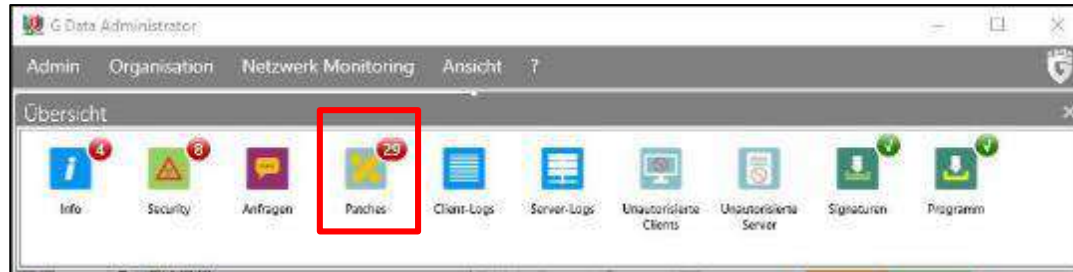
Suche

15 Alle

14 Alle

Inaktiv 2+ Wochen

NAME	DATUM	LETZTER BENUTZER	SCANNER-SCAN	LETZTE ANTI-MALWARE-SCAN	LETZTER BEPLANNTER SCAN	DEVICE ENCRYPTION	SOFTWARE UPDATE
RITN001	vor 20 Stunden	Tobias Rademacher vor 2 Minuten	Ja	vor 20 Stunden	Nie	Verschlüsselt	Kommt
RITN002	vor 4 Tagen	Sabine Schuster	Ja	vor 4 Tagen	Nie	Verschlüsselt	Kommt

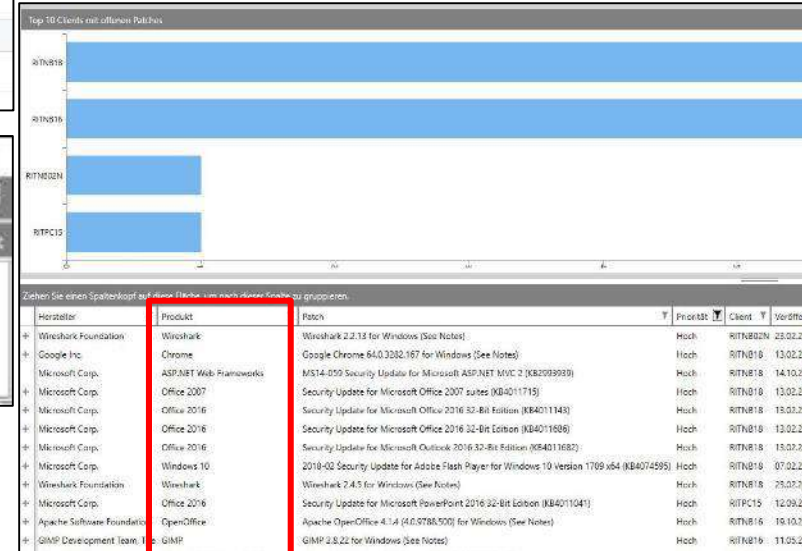


G Data Administrator

Admin Organisation Netzwerk Monitoring Ansicht ?

Übersicht

Info (4) Security (8) Anfragen Patches (29) Client-Logs Server-Logs Unautorisierte Clients Unautorisierte Server Signaturen Programm



Top 10 Clients mit offenen Patches

Client	Open Patches
RITN001	10
RITN002	8
RITN003	5
RITN004	3

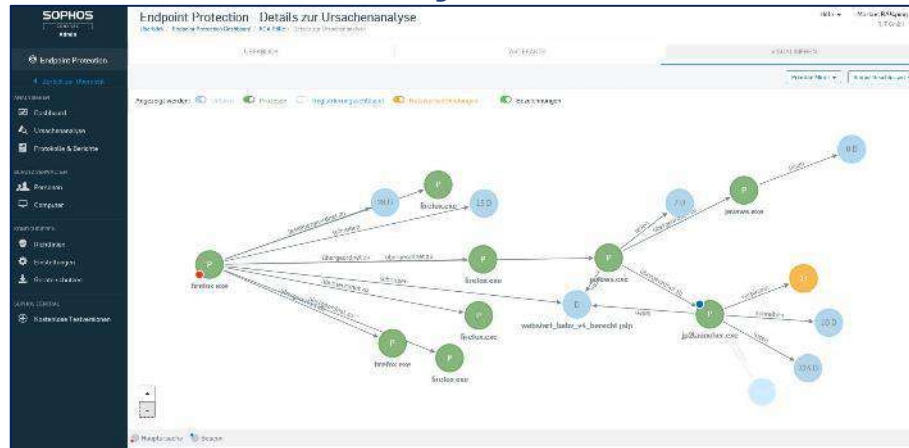
Ziehen Sie einen Spaltenkopf auf diese Ebene, um nach dieser Spalte zu gruppieren.

Hersteller	Produkt	Patch	Y	Priorität	Client	Vordr.
Wireshark Foundation	Wireshark	Wireshark 2.2.13 for Windows (See Notes)	Hoch	RITN001	23.02.20	
Google Inc.	Chrome	Google Chrome 64.0.3302.187 for Windows (See Notes)	Hoch	RITN001	13.02.20	
Microsoft Corp.	ASP.NET Web Frameworks	MS14-059 Security Update for Microsoft ASP.NET MVC 2 (KB2099999)	Hoch	RITN001	14.10.19	
Microsoft Corp.	Office 2007	Security Update for Microsoft Office 2007 suites (KB4011715)	Hoch	RITN001	13.02.20	
Microsoft Corp.	Office 2016	Security Update for Microsoft Office 2016 32-Bit Edition (KB4011143)	Hoch	RITN001	13.02.20	
Microsoft Corp.	Office 2016	Security Update for Microsoft Office 2016 32-Bit Edition (KB4011688)	Hoch	RITN001	13.02.20	
Microsoft Corp.	Office 2016	Security Update for Microsoft Outlook 2016 32-Bit Edition (KB4011682)	Hoch	RITN001	13.02.20	
Microsoft Corp.	Windows 10	2018-02 Security Update for Adobe Flash Player for Windows 10 Version 1709 x64 (KB4074595)	Hoch	RITN001	07.02.20	
Wireshark Foundation	Wireshark	Wireshark 2.4.5 for Windows (See Notes)	Hoch	RITN001	25.02.20	
Microsoft Corp.	Office 2016	Security Update for Microsoft PowerPoint 2016 32-Bit Edition (KB4011041)	Hoch	RITN001	12.09.19	
Apache Software Foundation	OpenOffice	Apache OpenOffice 4.1.4 (4.0.9760.500) for Windows (See Notes)	Hoch	RITN001	19.10.19	
GIMP Development Team	GIMP	GIMP 2.8.22 for Windows (See Notes)	Hoch	RITN001	11.05.20	

effektive Werkzeuge

befähigen den Admin, das Richtige zu tun

- verschaffen Überblick
- sind ressourcenschonend
- helfen bei der Analyse



Résumée



The image shows a tilted Gantt chart or PERT network diagram. It contains several colored bars (pink, yellow, green) representing tasks and their durations. The chart is titled 'PROJET - Gantt Chart' and includes a legend at the bottom. The diagram is complex, with many interconnected tasks and dependencies, typical of a project management tool.

Wie komme ich noch hinterher?
ganz einfach: Sie müssen nur die **richtigen Dinge** tun

offene Fragen / Diskussion

**Vielen Dank für
Ihre Zeit und Ihre Aufmerksamkeit!**

Stand Nr. 7

Bei Rückfragen wenden Sie sich gerne an:



DIGITIZE YOUR BUSINESS

Tobias Rademann, M.A.

R.iT GmbH

www.RiT.de

Amtmann-Ibing-Str. 10

44805 Bochum

Tel.: (0234) 43 88 00-0, Fax: -29

eMail: Tobias.Rademann@RiT.de

Quellen- und Bildverzeichnis

- Folie 2: © "Jungle green background " von [GVictoria](#), Fotolia.com
- Folie 5: "networker NRW logo" von networker NRW e.V.;
 "nrwuniTsLogo" nrwuniTS;
 "bvmwLogo" von Bundesverband für mittelständische Wirtschaft/ CC BY 3.0;
 © "eco Logo" von eco -Verband der Internetwirtschaft e.V.;
 "BMWiLogo" von Bundesministerium für Wirtschaft und Energie;
 © "Microsoft Partner Logo" von Microsoft Company
- Folie 6: © "Hürde rot Pfeil Erfolg hurdle red arrow " von [arahan](#), Fotolia.com
- Folie 8: © "5 Color Faces Feedback/Mood" von [Jan Engel](#), Fotolia.com;
 © "Schnittmenge" von [JiSign](#), Fotolia.com
- Folie 9: © "Erdmännchen" von [Andrea Seemann](#), Fotolia.com
- Folie 10: Pulseway von MMSOFT Design;
 Rapid Awareness von CONSCIO TECHNOLOGIES LTD;
 Veem 9.5 von Veeam Software AG
- Folie 11: © "Set of various equipment, instruments and tools for manual work with copy space, carpenter tool old rusty metal background." von [fusssergei](#), Fotolia.com
- Folie 12: G Data Software AG;
 Sophos SFOS von Sophos
- Folie 13: © "Erdmännchen" von [Andrea Seemann](#), Fotolia.com
- Folie 14: Sophos SFOS von Sophos
- Folie 15: © "Aufgeklapptes Schweizer Taschenmesser" von [Jörg Lantelme](#), Fotolia.com
- Folie 16: Sophos SFOS von Sophos;
 G Data Software AG
- Folie 17: Sophos SFOS von Sophos;
 © "Der Weg in Richtung "Machen!"" von [stockpics](#), Fotolia.com
- Folie 18: © "Man ready to run" von [Jan Engel](#), Fotolia.com