ITSiG: Ziel, Inhalt und Herausforderung

16. März 2017

Ralph Belfiore
Karl Jaeger

Pro4bizz GmbH
https://www.pro4bizz.de
ralph.belfiore@pro4bizz.de
karl.jaeger@pro4bizz.de
0721-909 81 720

Unsere moderne Gesellschaft

Heute sind wir in hohem Maße von einer funktionierenden IT-Infrastruktur abhängig.

Bundesnetzagentur

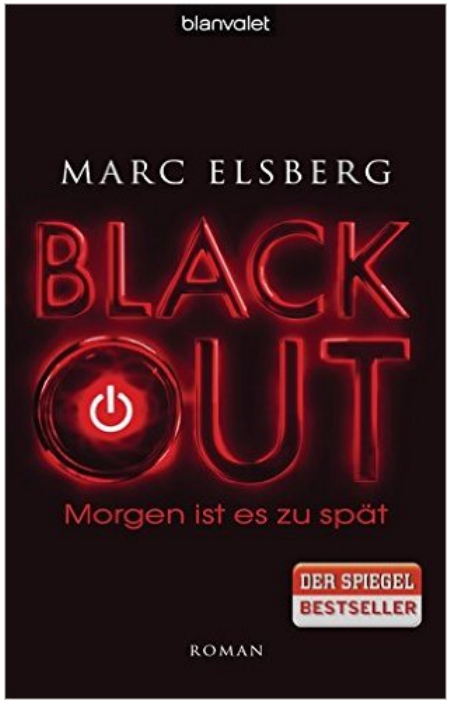
A. Einleitung

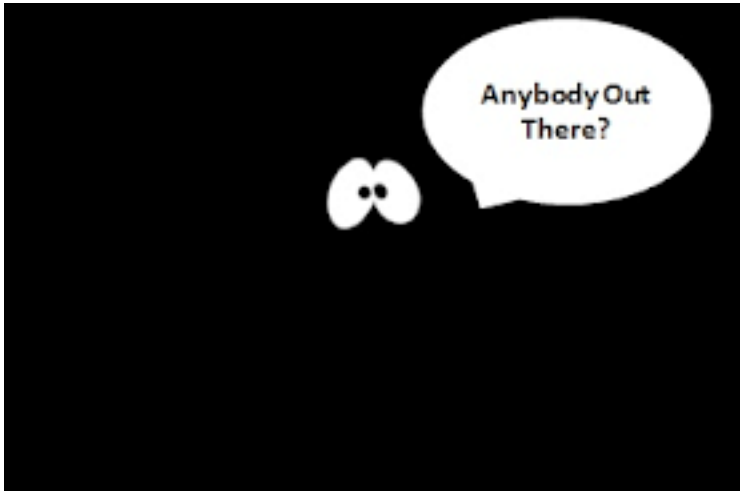
Unsere moderne Gesellschaft ist in hohem Maße von einer funktionierenden Energieversorgung abhängig. Fehlen Strom und Gas, kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden. Gleichzeitig ist die Funktionsfähigkeit der Energieversorgung von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig. Dies gilt im Besonderen für einen sicheren Netzbetrieb.

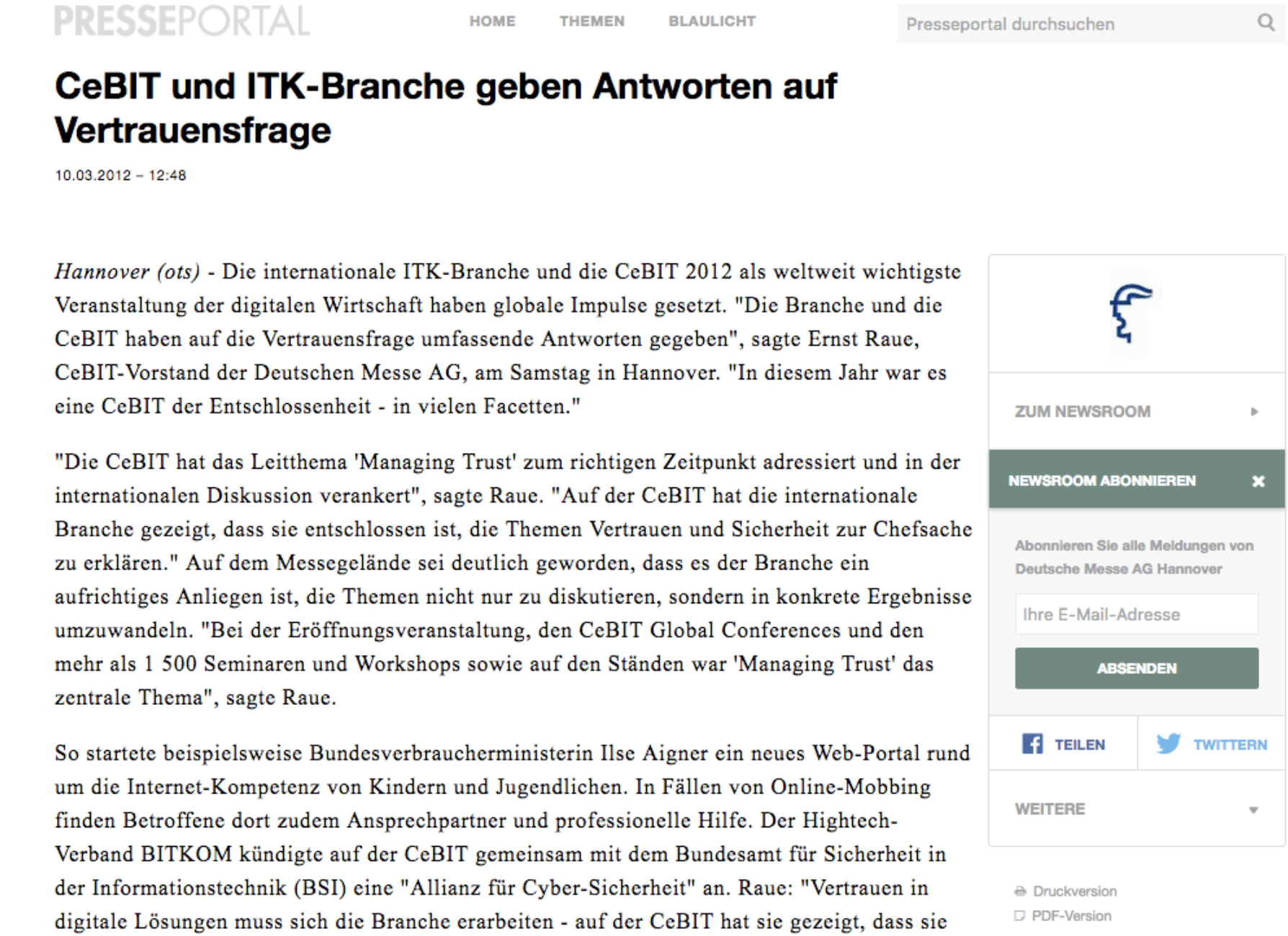
IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz

Unsere moderne Gesellschaft

Fehlen Elektrizität, Gas, Geld, Lebensmittel, Treibstoff, Wasser oder auch jede Form von Telekommunikation kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden.







PRESSEPORTAL HOME THEMEN BLAULICHT Presseportal durchsuchen

CeBIT und ITK-Branche geben Antworten auf Vertrauensfrage

10.03.2012 – 12:48

Hannover (ots) - Die internationale ITK-Branche und die CeBIT 2012 als weltweit wichtigste Veranstaltung der digitalen Wirtschaft haben globale Impulse gesetzt. "Die Branche und die CeBIT haben auf die Vertrauensfrage umfassende Antworten gegeben", sagte Ernst Raue, CeBIT-Vorstand der Deutschen Messe AG, am Samstag in Hannover. "In diesem Jahr war es eine CeBIT der Entschlossenheit - in vielen Facetten."

"Die CeBIT hat das Leitthema 'Managing Trust' zum richtigen Zeitpunkt adressiert und in der internationalen Diskussion verankert", sagte Raue. "Auf der CeBIT hat die internationale Branche gezeigt, dass sie entschlossen ist, die Themen Vertrauen und Sicherheit zur Chefsache zu erklären." Auf dem Messegelände sei deutlich geworden, dass es der Branche ein aufrichtiges Anliegen ist, die Themen nicht nur zu diskutieren, sondern in konkrete Ergebnisse umzuwandeln. "Bei der Eröffnungsveranstaltung, den CeBIT Global Conferences und den mehr als 1 500 Seminaren und Workshops sowie auf den Ständen war 'Managing Trust' das zentrale Thema", sagte Raue.

So startete beispielsweise Bundesverbraucherministerin Ilse Aigner ein neues Web-Portal rund um die Internet-Kompetenz von Kindern und Jugendlichen. In Fällen von Online-Mobbing finden Betroffene dort zudem Ansprechpartner und professionelle Hilfe. Der Hightech-Verband BITKOM kündigte auf der CeBIT gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine "Allianz für Cyber-Sicherheit" an. Raue: "Vertrauen in digitale Lösungen muss sich die Branche erarbeiten - auf der CeBIT hat sie gezeigt, dass sie entschlossen ist, dies zu tun."

ZUM NEWSROOM

NEWSROOM ABONNIEREN

Abonnieren Sie alle Meldungen von Deutsche Messe AG Hannover

Ihre E-Mail-Adresse

ABSENDEN

TEILEN TWITTERN

WEITERE

Druckversion

PDF-Version

Quelle

IT SiG/IT SiKat

25. Juli 2015: IT-Sicherheitsgesetz – Inkrafttreten des IT-SIG

Ziel: Deutschland will die sichersten IT-Systeme & digitalen Infrastrukturen weltweit

worum geht es?

- *Änderung BSI-G, AtG, EnWG, TMG, TKG, ...*

Für wen gilt das Gesetz?

- *Betreiber von Webangeboten*
- *Telekommunikationsunternehmen*
- *Betreiber Kritischer Infrastrukturen*

Quelle BSI

IT SiG/IT SiKat

12.August 2015: Veröffentlichung des IT-SiKat
Gemäß §11 Absatz 1a Energiewirtschaftsgesetz (EnWG)

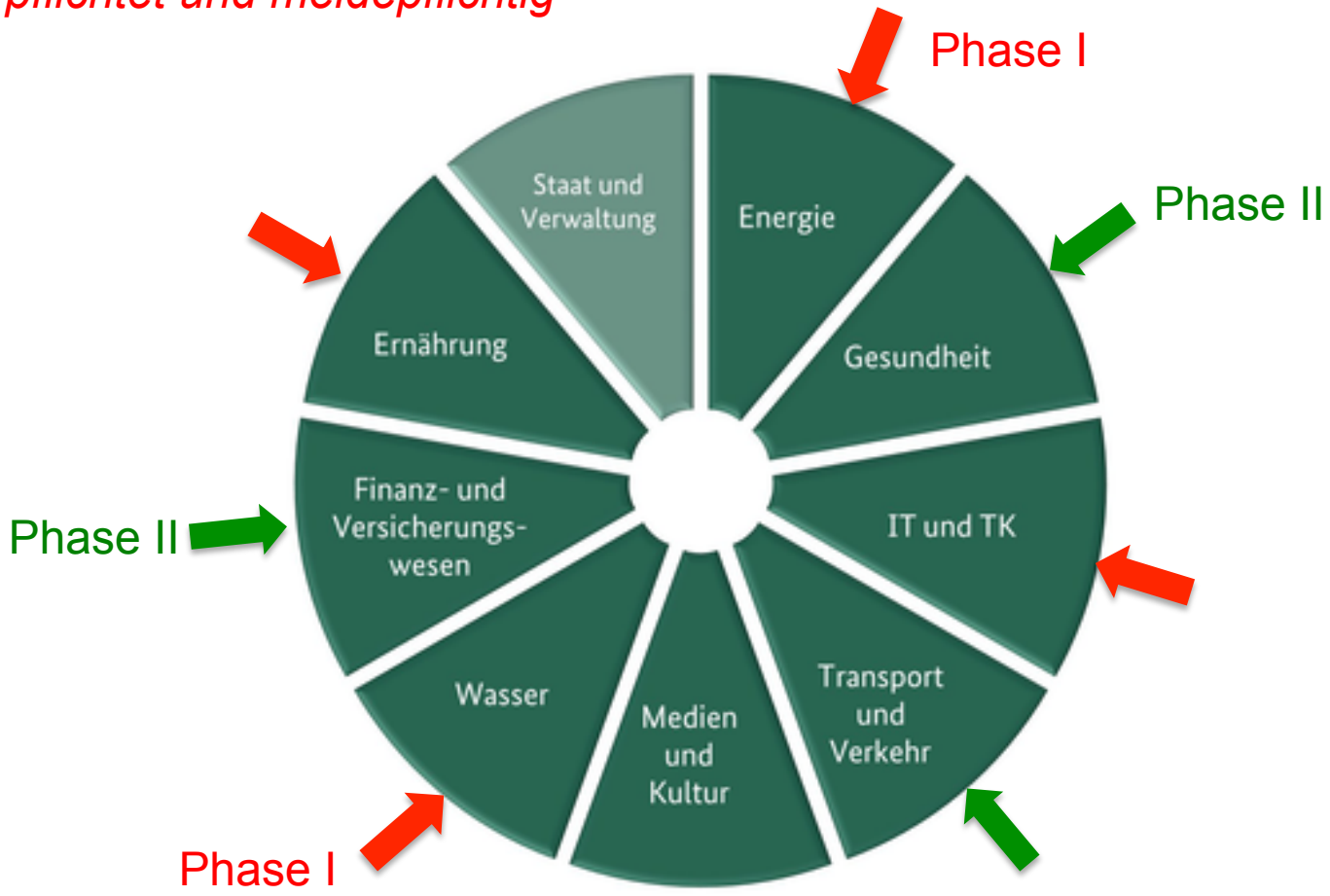
Geltungsbereich:
Alle zentralen und dezentralen Anwendungen, Systeme und Komponenten die der Netzsteuerung und –überwachung dienen und zur Gewährleistung des stabilen und sicheren Netzbetriebs benötigt werden.

Quelle BNA

KRITIS-Verordnung (BSI-KritisV) am 3. Mai 2016

Ziel

Betreiber Kritischer Infrastrukturen, sind zur Umsetzung von Mindest-sicherheitsstandards verpflichtet und meldepflichtig



Quelle BSI

IT SiKat

Kernanforderung:

Einführung eines **ISMS** gemäß **ISO27001**, Umsetzungsfrist bis 31.1.2018, Zertifizierung durch unabhängige Stelle und Benennung eines Ansprechpartners IT-Sicherheit für die Bundesnetzagentur (bis 30.11.2015)

worum geht es?

Prozess zum Informationssicherheitsmanagement planen, durchführen, überprüfen und anpassen (PDCA)

was bedeutet das genau?

Anwendungsbereich, Awareness, Audit, Bestandsaufnahme, Dokumentation, Leitlinie, Maßnahmen, Risikoanalyse, Zertifizierung

IT SiKat

Kernanforderung:

Implementierung des **ISMS** gemäß **ISO 27002 und ISO 27019**, Umsetzungsfrist bis 31.1.2018, Zertifizierung durch unabhängige Stelle und Benennung eines Ansprechpartners IT-Sicherheit für die Bundesnetzagentur (bis 30.11.2015)

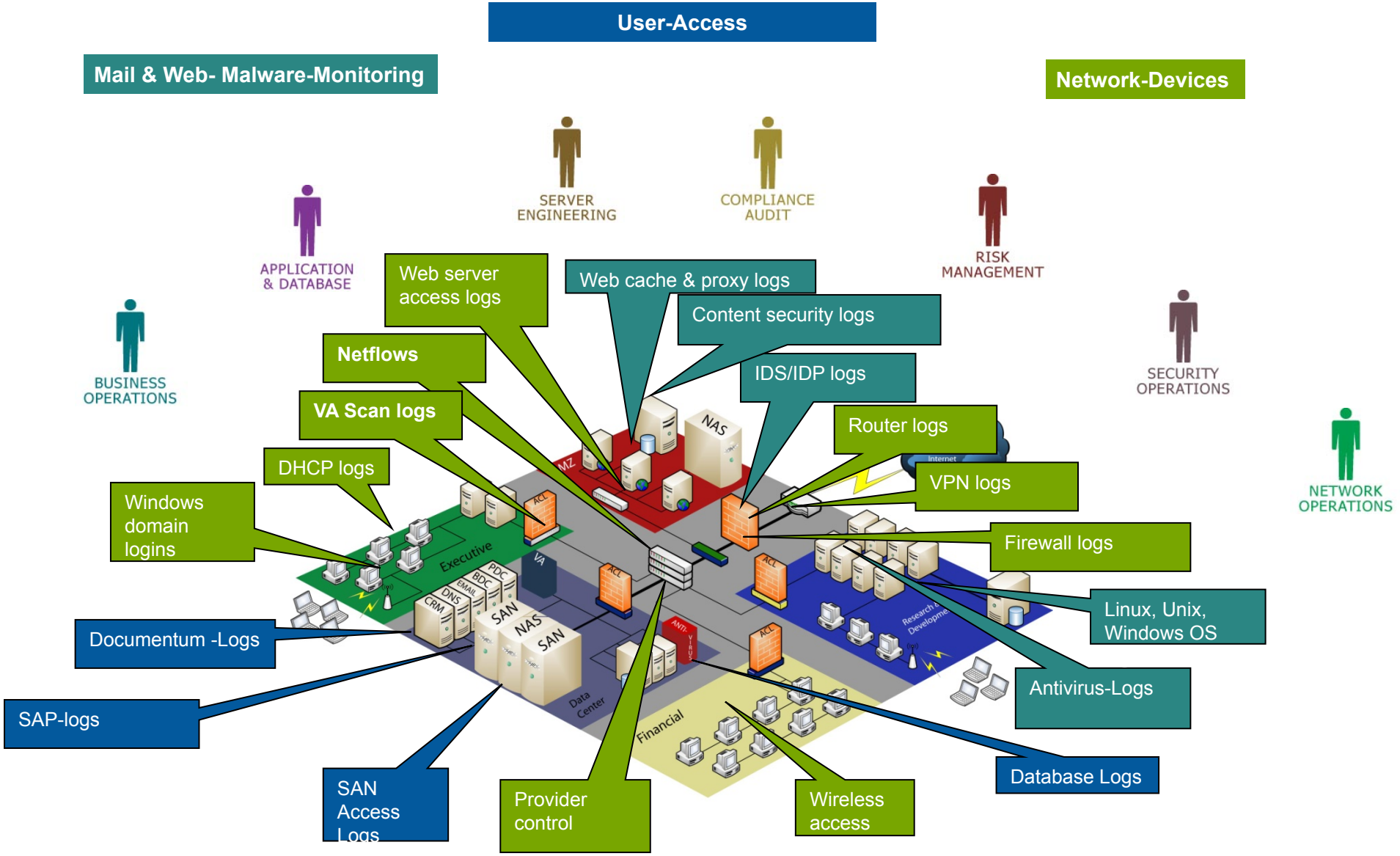
worum geht es?

„Stand der Technik“ umsetzen

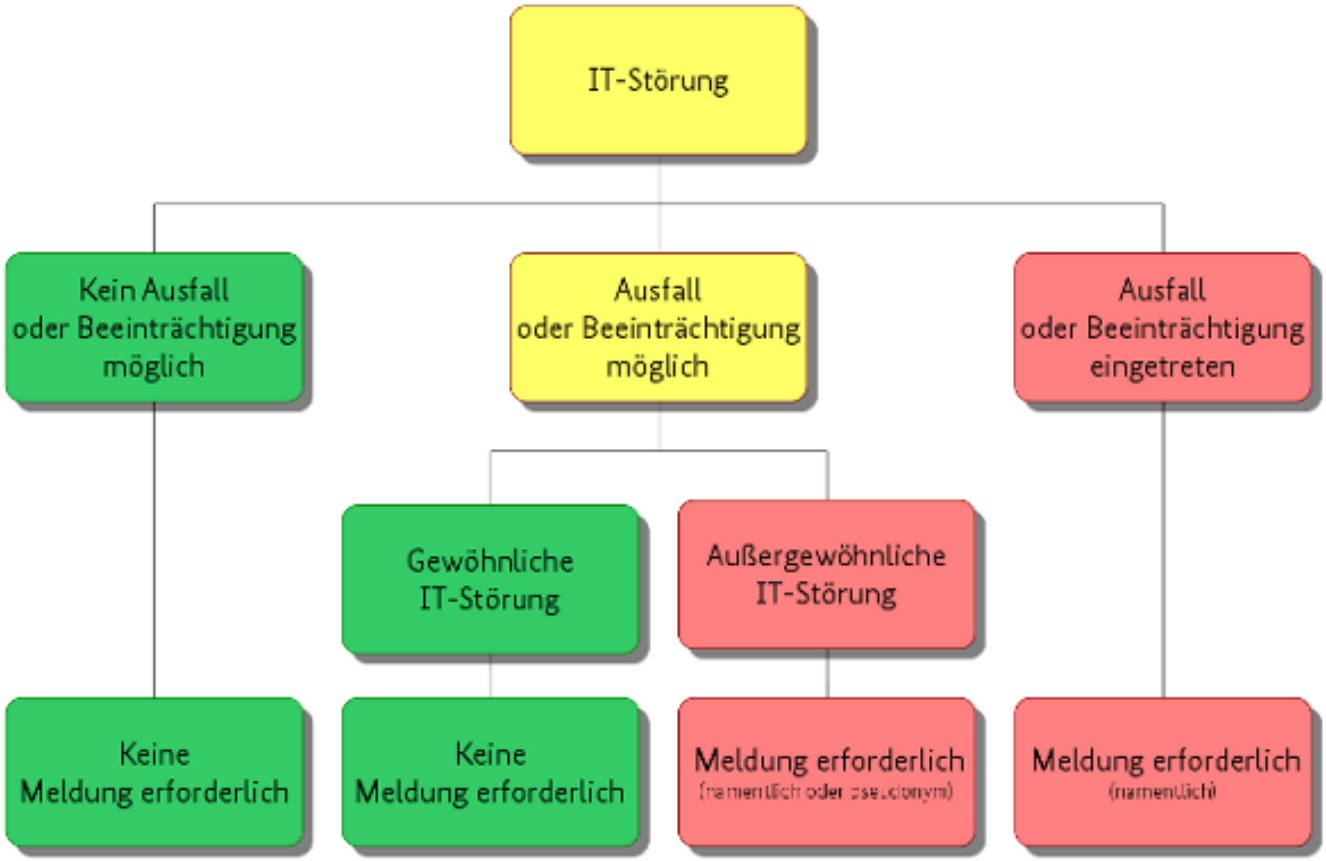
was bedeutet das genau?

18 Kapitel:
Scope ..., security policies, organization of security ..., asset management, access control ..., operations security ..., incident management, BCM, Compliance.

Scope festlegen



*Meldekriterien für IT-Störungen *)*



*) Quelle BSI

Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime *)

- Sicherung aller relevanten, bereits bestehenden Protokolle bzw. Logdaten.
- Zeitpunkte, d. h. Daten und Uhrzeiten (ein- schließlich Zeitzone), an denen relevante Ereignisse entdeckt wurden bzw. stattfanden.
- Angaben (Namen, Daten, Uhrzeiten) zu relevanten Telefonanrufen, E-Mails und anderen Verbindungen.
- Identität der Personen, die Aufgaben im Zusammenhang mit dem Schadensfall bearbeiten, eine Beschreibung dieser Aufgaben und der Zeitaufwand.
- Kennung der von dem Angriff betroffenen Systeme, Konten, Dienste, Daten und Netze sowie die Art der Beeinträchtigung.
- Angaben zu Umfang und Art des entstandenen Schadens.

*) Quelle BKA

ISO 27002 incident management

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Implementation guidance

ISO 27002 incident management

ISO/IEC 27002:2013(E)

Event logs should include, when relevant:

a) user IDs;

b) system activities;

c) dates, times and details of key events, e.g. log-on and log-off;

d) device identity or location if possible and system identifier;

e) records of successful and rejected system access attempts;

f) records of successful and rejected data and other resource access attempts;

g) changes to system configuration;

h) use of privileges;

i) use of system utilities and applications;

j) files accessed and the kind of access;

k) network addresses and protocols;

l) alarms raised by the access control system;

m) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems;

n) records of transactions executed by users in applications.

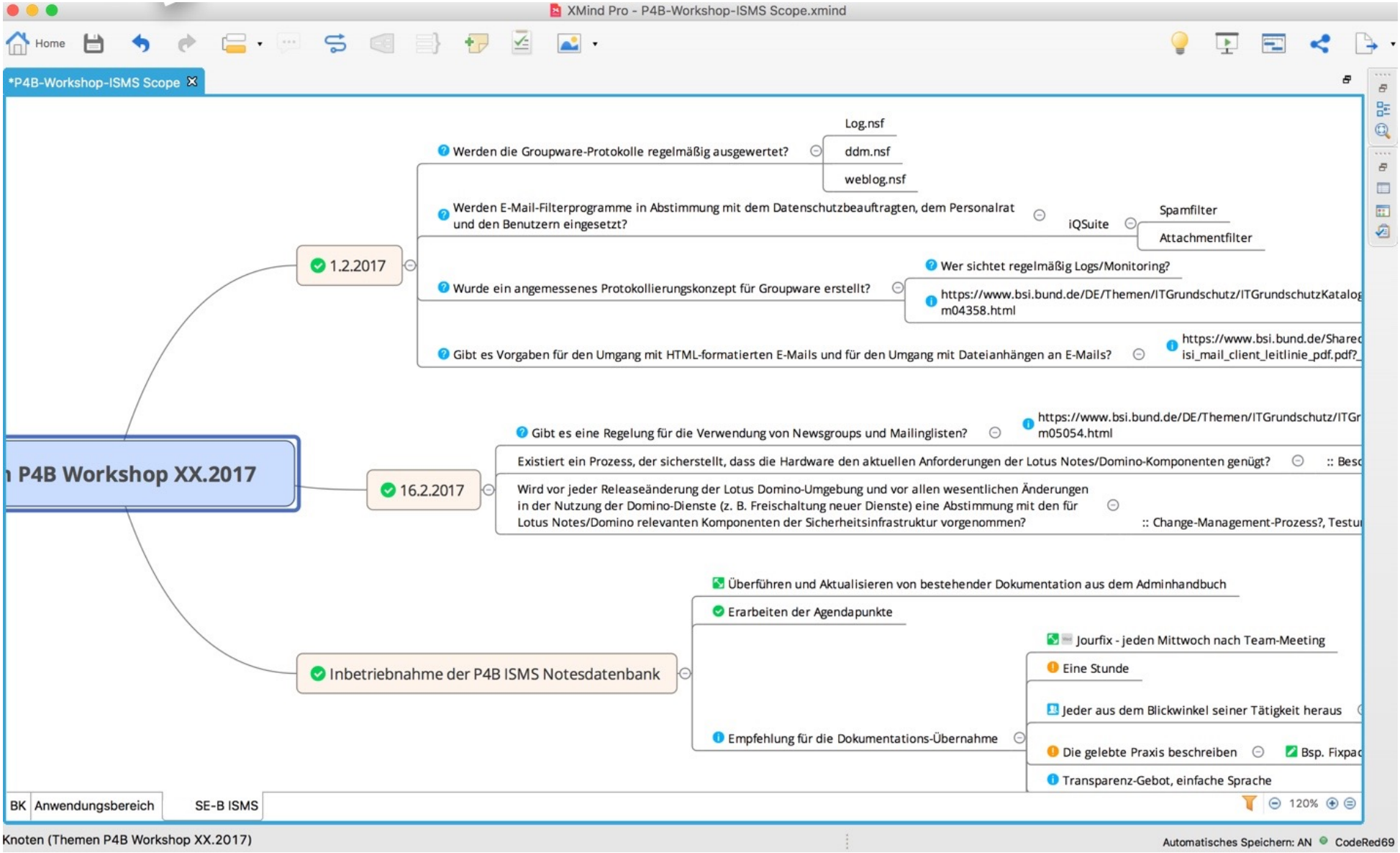
Projektbeispiel: Awareness für Anwendungsbereiche (Scope)

Verantwortung für Produkte:
>25 Produkte bei typischem EVU
Bsp.: Verschlüsselung in der Marktkommunikation (EDIFACT)

Beschreibung des Leistungsumfangs:

- Verantwortlichkeit
- DMS
- SAP Prozesse
- Webanwendungen

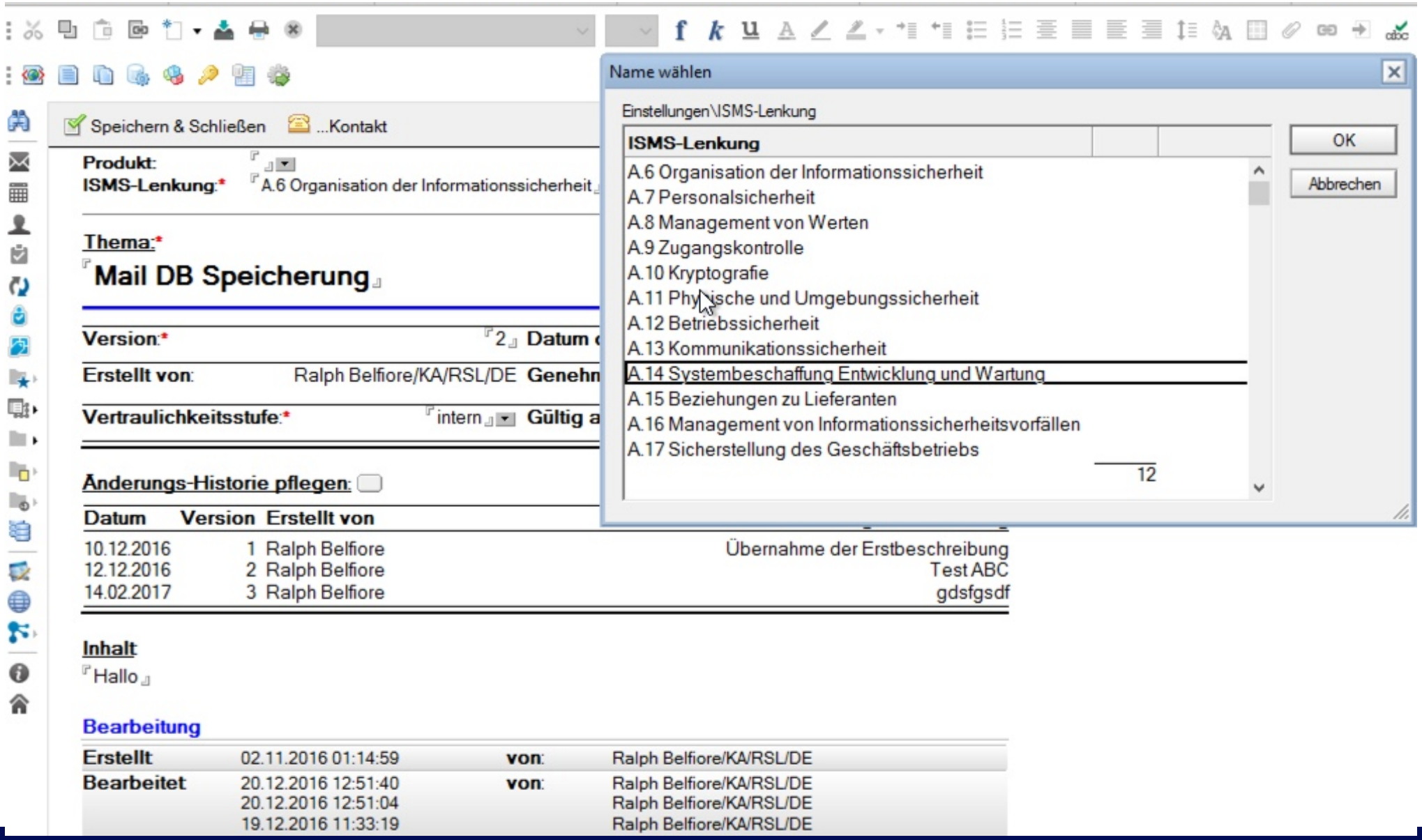
Mindmap ISO Workshop: stukturiertes Vorgehen



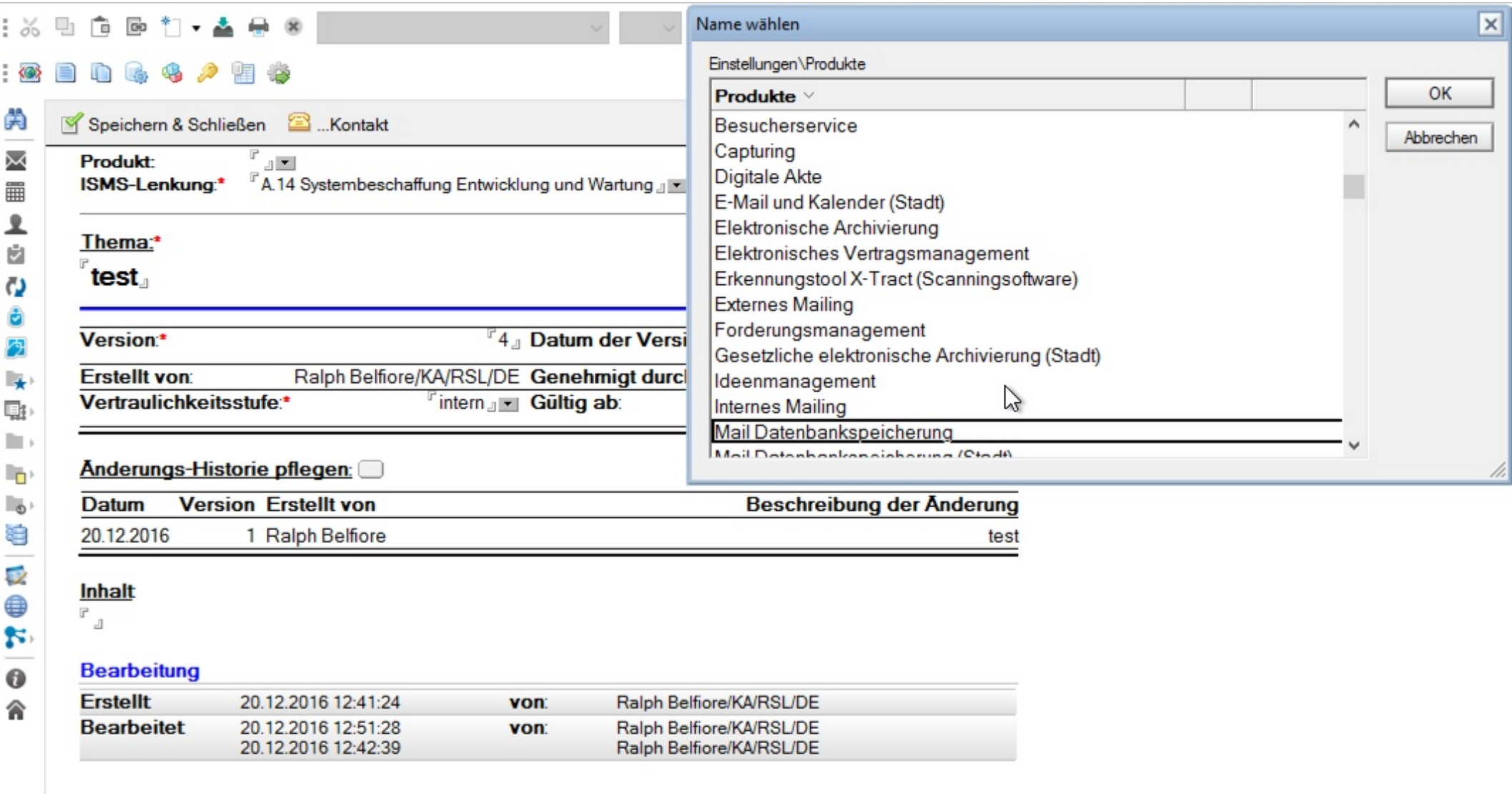
Projektbeispiel: Vorbereitung der ISMS Dokumentation

- Aktualisierung der bestehenden Dokumentationen:
- Ergänzen der vorhandenen Dokumentation
- Erstellen neuer Dokumente
- Verstehen der Prozesse die zu den Produkten gehören
- Kontinuierlich Dokumentation aktualisieren

ISMS Dokumentationsdatenbank: Struktur der IT-Dokumentation



ISMS Dokumentationsdatenbank: Auswahloptionen zur Unterstützung



ISMS Dokumentationsdatenbank: integrierte Hilfefunktion

Hilfe zur Auswahl:

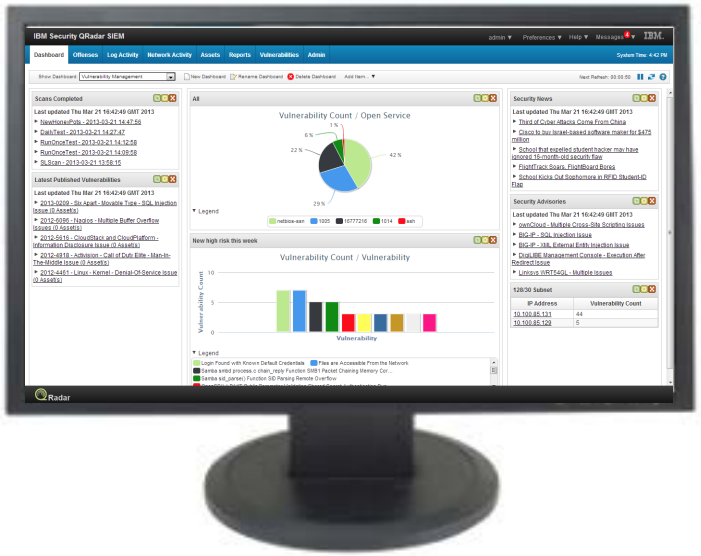
Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
▼ A5 - Sicherheitsleitlinie						
A.5	Sicherheitsleitlinie					
A.5.1	Management-Leitlinien zur Informationssicherheit					
A.5.1.1	Informationssicherheits-leitlinien				Alle Richtlinien, auf die in dieser Spalte nachstehend hingewiesen wird.	
A.5.1.2	Überprüfung der Informationssicherheitsleitlinien				Jede Richtlinie mit einem designierten Eigentümer, welcher das Dokument in vorgeplanten Intervallen zu überprüfen hat.	
▶ A.6 - Organisation der Informationssicherheit						
▶ A.7 - Personelle Sicherheit						
▶ A.8 - Verwaltung der Werte						

ISMS Workflow mit SIEM

Eine zentrale Konsole mit Blick auf die gesamte IT

Personen
schützen und beobachten von Zugriffen auf IT- Systeme, Informationen und Anwendungen



Untersuchung
ständige Beobachtung der Bedrohungslandschaft durch neue Schwachstellen

Daten
ständiges beobachten und bewerten von Datenbanken, Dateiverzeichnissen und Big-Data Umgebungen

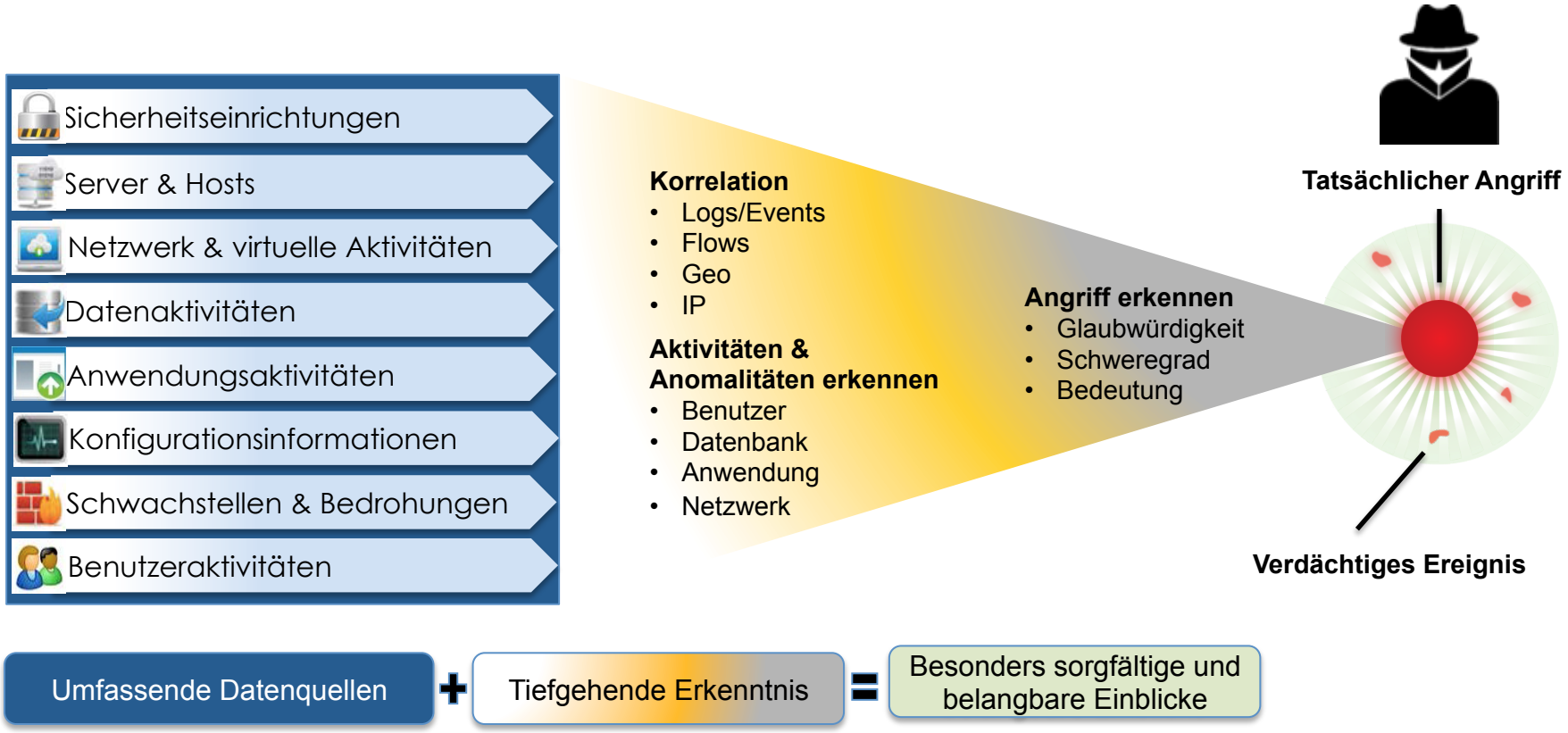
Anwendungen
erkennen und beseitigen von Schwachstellen in Webanwendungen, bevor sie betroffen sind

Infrastruktur
erkennen, beseitigen und blocken von Bedrohungen durch ständig wechselnde Server, Netzwerke und Endpunkte

Quelle: IBM

ISMS Workflow mit SIEM

- automatisches Erstellen der Asset Datenbank
- Umsetzung des Risikomanagement in die IT-Infrastruktur
- Sicherheitsvorfälle managen und ggfs. melden



Quelle: IBM

ITSiG: Ziel, Inhalt und Herausf

Incident Management

- aut
- We
- Res

Event Information

Event Name	Email_Executable_Extension						
Low Level Category	Mail Exploit						
Event Description	Mail attachment with a suspicious file name, see http://www.iss.net/security_center/reference/vuln/Email_Executable_Extension.htm for a detailed description						
Magnitude	(8)	**Relevance**	10	**Severity**	5	**Credibility**	10
Username	N/A						
Start Time	Feb 9, 2017, 7:31:37 PM	**Storage Time**	Feb 9, 2017, 7:31:37 PM	**Log Source Time**	Feb 9, 2017, 7:31:35 PM		

P4B Exploit: Mail Exploit Fired
QRADAR@pro4bizz.de
An: karl.jaeger@pro4bizz.de

```
   The following is an automated response sent to you by the QRadar event custom rules engine:

Feb 9, 2017 7:31:37 PM CET


Rule Name:                                  P4B Exploit: Mail Exploit
Rule Description:                           Reports a destination host attempting to be exploited using multiple types of attacks from one or more source

Source IP:                                  10.20.100.254
Source Port:                                47313
Source Username (from event):               N/A
Source Network:                             RSLNET.DMZ

Destination IP:                             10.20.100.236
Destination Port:                           25
Destination Username (from Asset Identity): N/A
Destination Network:                        RSLNET.DMZ

Protocol:                                   tcp_ip
QID:                                        5771790

Event Name:                                 Email_Executable_Extension
Event Description:                          Mail attachment with a suspicious file name, see http://www.iss.net/security_center/reference/vuln/Email_Exec
detailed description
Category:                                   Mail Exploit

Log Source ID:                              763
Log Source Name:                            IBMSecurityNetworkProtectionXGS @ 10.10.100.45

Payload:                                    <81>1 2017-02-09T19:31:37+0100 xgs LEEF:1.0|IBM|ISNP|5.3.3.2|Email_Executable_Extension|cat=Security devTimeF
devTime=Feb 09 2017 19:31:35 sev=5 proto=TCP src=10.20.100.254 dst=10.20.100.236 srcPort=47313 dstPort=25 originator=alpsd AdapterID=1.3 AdapterMode=Inline
algorithm-id=2120020 appid=smtp block=true count=1 event-type=Attack iprdstgeoname=Private Network iprdststate=categorized iprlicensed=1 iprsrcgeoname=Priva
iprsrcstate=categorized ipsid=16df2767-81b7-428b-b1d3-b86ea9d59e1a nvpdata=file=TESTNU~1.EXE,protocol=SMTP,from=Karl-Heinz Jaeger <carlomagnus@icloud.com>,t
<ralph.belfiore@pro4bizz.de>,date=Thu, 09 Feb 2017 19:31:12 +0100,adapter=2 quarantineendtime=0 ruleid=1ea359e0-36ba-012e-9a54-0017faab3ff6 ruleorder=12 ssl
```

Dashboard | Offenses | Log Activ

Offenses
- My Offenses
- All Offenses
- By Category
- By Source IP
- By Destination IP
- By Network
- Rules

Offense 65

Magnitude		**Event/Flow count**	22 events and 0 flows in 2 categories
Domain		**Start**	Feb 9, 2017, 7:31:30 PM
Description		**Duration**	4m 19s
Source IP(s)	Multiple (2)	**Assigned to**	Unassigned
Destination IP(s)	10.20.100.236 (vrslcomm1.rslnet.intra)		
Network(s)	RSLNET.DMZ		

List of Rules Contributing to Offense

Rule Name	Events/Flows	First Event/Flow	Last Event/Flow
P4B Exploit: Mail Exploit	19	6m 22s	2m 2s
Exploit: Multiple Exploit Types Against Single Destination	9	6m 13s	2m 2s

Ziel - IT-Sicherheit 2.0

Stabilität durch Wandel
Wer nichts verändern will, wird auch das verlieren, was er bewahren möchte.

Dr. Gustav Walter Heinemann

Nützliche Links

https://www.bsi.bund.de
https://www.sicher-im-netz.de
https://bitkom.org
http://www.bmwi.de
http://asw-online.de