Bundesministerium
für Wirtschaft
und Technologie

„Informationssicherheit in der Bundesverwaltung und das ITSM im Bundeswirtschaftsministerium“

Andreas Schmidt
IT-Sicherheitsbeauftragter im
Bundesministerium für Wirtschaft und
Technologie

www.bmwi.de

Bundesministerium
für Wirtschaft
und Technologie

Andreas Schmidt

bis 2001	Unabhängiges Landeszentrum für Datenschutz S-H *Projekt: Java Anon Proxy (anon.inf.tu-dresden.de)*
01 bis 05	Bundesamt für Sicherheit in der Informationstechnik *Projekte: Bund Online 2005; Virtuelle Poststelle*
05 bis 07	Bundesministerium des Innern *Fachaufsicht über das Bundesamt für Sicherheit in der IT*
07 bis 10	Bundesanstalt für den Digitalfunk der BOS *Leiter der Arbeitsgruppe „Sicherheit und Geheimschutz“*
seit 2011	Bundesministerium für Wirtschaft und Technologie *IT-Sicherheitsbeauftragter, ISO 27001 Auditor*

Bundesministerium
für Wirtschaft
und Technologie

Agenda

- Ausgangssituation in den Bundesbehörden
- Umsetzungsplan Bund und seine Folgen
- Informationssicherheitsmanagement (ISMS) im BMWi
- Praxiserfahrungen

Bundesministerium
für Wirtschaft
und Technologie

Das Beauftragtenwesen der Bundesbehörden

- IT-Sicherheitsbeauftragte
- Geheimschutzbeauftragte
- Datenschutzbeauftragte
- Brandschutzbeauftragte
- Fachkraft für Arbeitssicherheit
- …
- Notfallbeauftragte
- Korruptionsschutzbeauftragte
- Beauftragte für den Haushalt
- …

Bundesministerium
für Wirtschaft
und Technologie

Der IT-Sicherheitsbeauftragte im Bund (1/2)

- Behördentätigkeit im gesetzlichen Auftrag
- Einrichtung behördlicher IT-Sicherheitsbeauftragter
  - vereinzelt
  - organisatorisch stark unterschiedlich
  - Aufgaben- und Kompetenzzuschnitt stark unterschiedlich

- BSI-Gesetz 1991(neu seit 2009)
- „Legaldefinition“ in IT-GS-Katalogen
- IT-GS-Standards 100-1 und 100-2 (analog den ISO-Standards 2700x)

Bundesministerium
für Wirtschaft
und Technologie

Der IT-Sicherheitsbeauftragte im Bund (2/2)

- Verschärfte IT-Sicherheitslage
  - → 2005: Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)
  - → 2007: Umsetzungsplan für die Bundesbehörden

- 2007: Konzept der IT-Steuerung im Bund (CIO-Konzept)

Rat der IT-Beauftragten

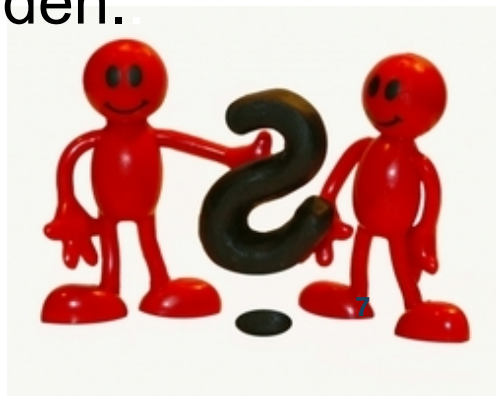
- Somit seit 2007:
  - Klare Zuständigkeiten und Verantwortlichkeiten
  - Aufgabenbeschreibung für den IT-SiBe
  - aber Fokus auf IT und TK statt Informationen

Bundesministerium
für Wirtschaft
und Technologie

Kernprobleme der ersten Stunde des UP Bund

Die **Verantwortung** für die personelle und finanzielle Bereitstellung der Ressourcen liegt bei den **Ressorts** (bzw. Behörden / Beauftragten für IT).

Sehr **ehrgeizige Fristen** waren zu hinterfragen, aber das Ziel einer sicheren Infrastruktur der Bundesverwaltung darf nicht gefährdet werden.



Bundesministerium
für Wirtschaft
und Technologie

Was bringt der UP Bund Neues?

vor UP Bund:	**durch** UP Bund:
IT-Sicherheit war Betriebsaufgabe	IT-Sicherheit wurde Managementaufgabe
Verantwortung bei IT-Leitern und Administratoren	Verantwortung bei Behördenleitung
jede Behörde hat Art und Tiefe selbst verantwortet	Verantwortung bei Ressort-IT-SiBe und CIO

Allgemeine Konsequenzen

Neue **Steuerungsmechanismen** mussten geschaffen werden.

Ressourcenfragen musste bedacht und geklärt werden.

Bundesministerium
für Wirtschaft
und Technologie

Konsequenzen für jedes Ressort

im Ressort:
Aufsetzen eines **IT-Sicherheitsmanagementsystems** (ISMS)

im Ministerium:
Umsetzen von **Maßnahmen** zur IT-Sicherheit und Schaffen einer **IT-Sicherheitsorganisation**

Ziele des ISMS Ressort

Die Ziele des ISMS wurden von zwei Interessengruppen erarbeitet.

- Ziele der IT-SiBe

- Ziele des CIO

Ziele des CIO:

- Gute und angemessene Absicherung aller Ressortbehörden
- Effektive Steuerung & Kontrolle
- Aktuelle Informationen

Ziele der IT-SiBe:

- Einheitliche Strukturen in der Dokumentation
- Förderung der Zusammenarbeit der IT-SiBe im Ressort
- Gemeinsame Ausrichtung der IT-Sicherheit im Ressort (Vorgaben der Mutterbehörde)
- Sichere Kommunikation unter den IT-SiBe
- Kontinuierliche Weiterentwicklung des ISMS
- Klare geregelte Verantwortungen

Zusammenarbeit

Kommunikation

Abstimmung zum Umgang mit Dokumenten im Ressort:

• Leitlinien	Sicherheitsleitlinien
• Konzepte	Sicherheits-, Notfall-, Krisen-Konzepte,
• Regelungen	Richtlinien, Hausmitteilungen, Verfahrensanweisungen
• Berichte	Statusberichte, Meldungen
• Sonstiges	Definitionen, Schulungsunterlagen, Adresslisten

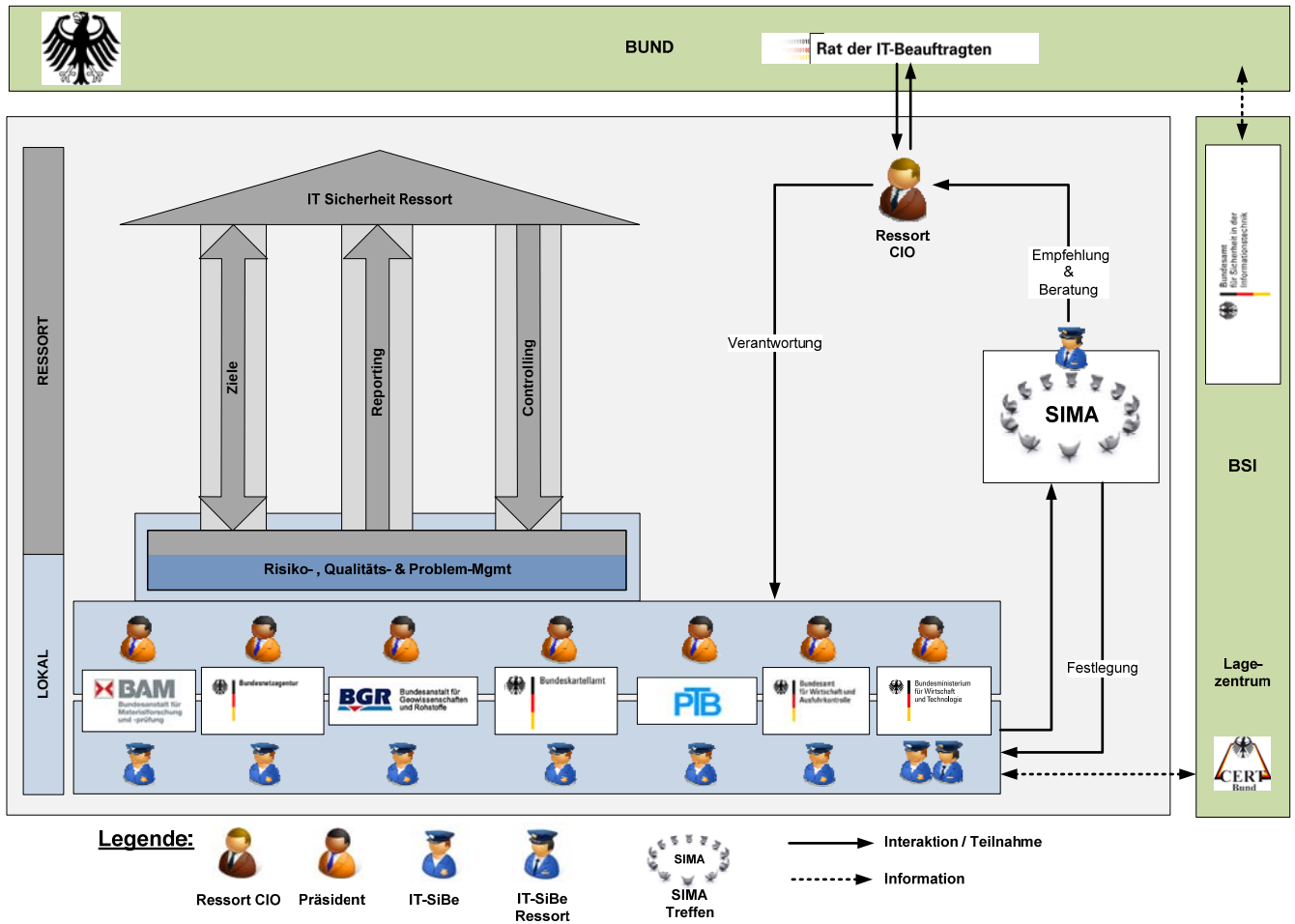
SIMA Treffen der IT-SiBe im Ressort:

Inhalt:	- Förderung des Austauschs - Gemeinsame Weiterentwicklung des ISMS - Abstimmung v. Maßnahmen und Empfehlungen - Einrichtung v. Projektgruppen
Regelmäßig:	1x im Quartal
Dauer:	1,5 Tage
Ort:	Abwechselnd bei den Behörden im Ressort
Form:	offene Diskussion
Ergebnisse:	In Form von Festlegungen und Empfehlungen

Bundesministerium
für Wirtschaft
und Technologie

Organisationsstruktur ISMS Ressort

ISMS Ressort BMWi



Bundesministerium
für Wirtschaft
und Technologie

Beispiel: Prozess Qualitätsmanagement (KPI)

#	Ziel	KPI - Beschreibung	KPI Messpunkt	Einheit	grün	gelb	rot
1	1. Absicherung Ressort	Maßnahmen zur Awareness der eigenen Mitarbeiter	Anzahl der Maßnahmen	Anzahl	x ≥ 2	2 > x ≥ 1	1 > x
2	1. Absicherung Ressort	Berücksichtigung der BSI Warnungen & CERT	Zeit bis zur Berücksichtigung	Arbeitstage	x < 1	1 ≤ x ≤ 2	2 < x
4	2. Steuerung IS	Umsetzung UP Bund im Ressort	Summe der Ampeln, linear	Prozent	x ≥ 85	85 > x ≥ 75	75 > x
5	2. Steuerung IS	Termintreue	Quote der zeitgerechten Berichte	Anzahl von sieben	x = 7	x = 6	5 ≥ x
6	2. Steuerung IS	Durchschnittliche Lösungsdauer im Problem-Mgmt im Ressort	Durchschnittliche Dauer	Arbeitstage		Noch offen	
8	3. aktuelle Informationen	Sofortmeldungen an das BSI	Zeit vom Vorfall bis zur Meldung	Arbeits-stunden	x < 3	3 ≤ x ≤ 8	8 < x
11	5. Zusammenarbeit	Regelmäßige Treffen der IT-SiBe -> SIMA Treffen	Anzahl der Treffen im Jahr	Anzahl	x ≥ 4	x = 3	3 > x
13	7. Kommunikation	Funktionstüchtigkeit VSnfD Telefone	Teilnehmer wurde erreicht, nach Ankündigung	Anzahl von sieben	x = 7	x = 6	5 ≥ x

Tabelle: Auswahl aktueller KPI, Stand 2012

Bundesministerium
für Wirtschaft
und Technologie

ISMS - Organisation

Teams

Verantwortliche

Kernteam des IT-Sicherheits Mgmt. Teams	**Besteht aus**	**IT-Sicherheitsbeauftragte/r, Ressort CIO, IT-Leiter/in**
IT-Sicherheits Mgmt. Team (ITSiMT)	**Besteht aus**	**IT-Sicherheitskernteam Personalvertreter/in, Datenschutzbeauftragte/r Geheimschutzbeauftragte/r Fachlicher Vertreter/in CERT Mitglied Ressort-IT-SiBe**
Computer Emergency Response Team (CERT)	**Besteht aus**	**IT-Sicherheitsexperten**

Bundesministerium
für Wirtschaft
und Technologie

Praxiserfahrungen

- IT-Sibe ist **Koordinator und Kommunikator**.
  Er braucht Kompetenzen sollte aber auch nah genug an der Technik sein. **Verantwortung trägt die Leitung**!

- Es gibt oft mehr Sicherheit in der Institution als man denkt. Alle Sicherheitsthemen sollten **gleich wichtig** behandelt werden. Es gibt keine „weichen“ Themen!

- **Auslagerung ist** heute **Standard**, wird bei den Sicherheitsbetrachtungen aber oft vergessen. Dies gilt auch für **selbstbestimmte Nutzer** (BYOD)!

Ausblick und Resümee