Informationssicherheit
BSI IT-Grundschutz, ISO/IEC 27001 und ISIS12 im Praxisvergleich

BSP-SECURITY

Congress@it-sa - Der sichere Hafen für Ihre Unternehmens IT
18./19.10.2016

Michael Gruber

BSP-SECURITY

Senior Consultant für Datenschutz und Informationssicherheit

- 30 Jahre Erfahrung im Bereich UNIX/Linux, LAN/WAN, IT-Security
- 15 Jahre Erfahrung Bereich Datenschutz und Informationssicherheit
- ISIS12 Initiator und Architekt

Themen:

IT-Compliance (Datenschutz, Informationssicherheit)

Mitgliedschaften:

- Bayerischer IT- Sicherheitscluster e.V. (Fachbeirat)
- BVD e.V., GDD e.V., BSI Cyber-Allianz

BSP-SECURITY

Michael Gruber

Senior Consultant
Datenschutz und Informationssicherheit

ISIS12 Netzwerkpartner
Fachbeirat Bayerischer IT-Security Cluster e.V.

Tel: +49 (0)941 60 48 89-8 64
Fax: +49 (0)941 60 48 89-8 66
Mobil: +49 (0)152 32 01 04 95

BSP-SECURITY
Franz-Mayer-Str. 1
D-93053 Regensburg

E-Mail: michael.gruber@bsp-security.de
www.bsp-security.de

BSP-SECURITY

Gründung:

– 2006 als Netzwerk (Cluster) in Regensburg
– 2012 Eröffnung der Geschäftsstelle Augsburg
– 2013 Überführung in einen Verein

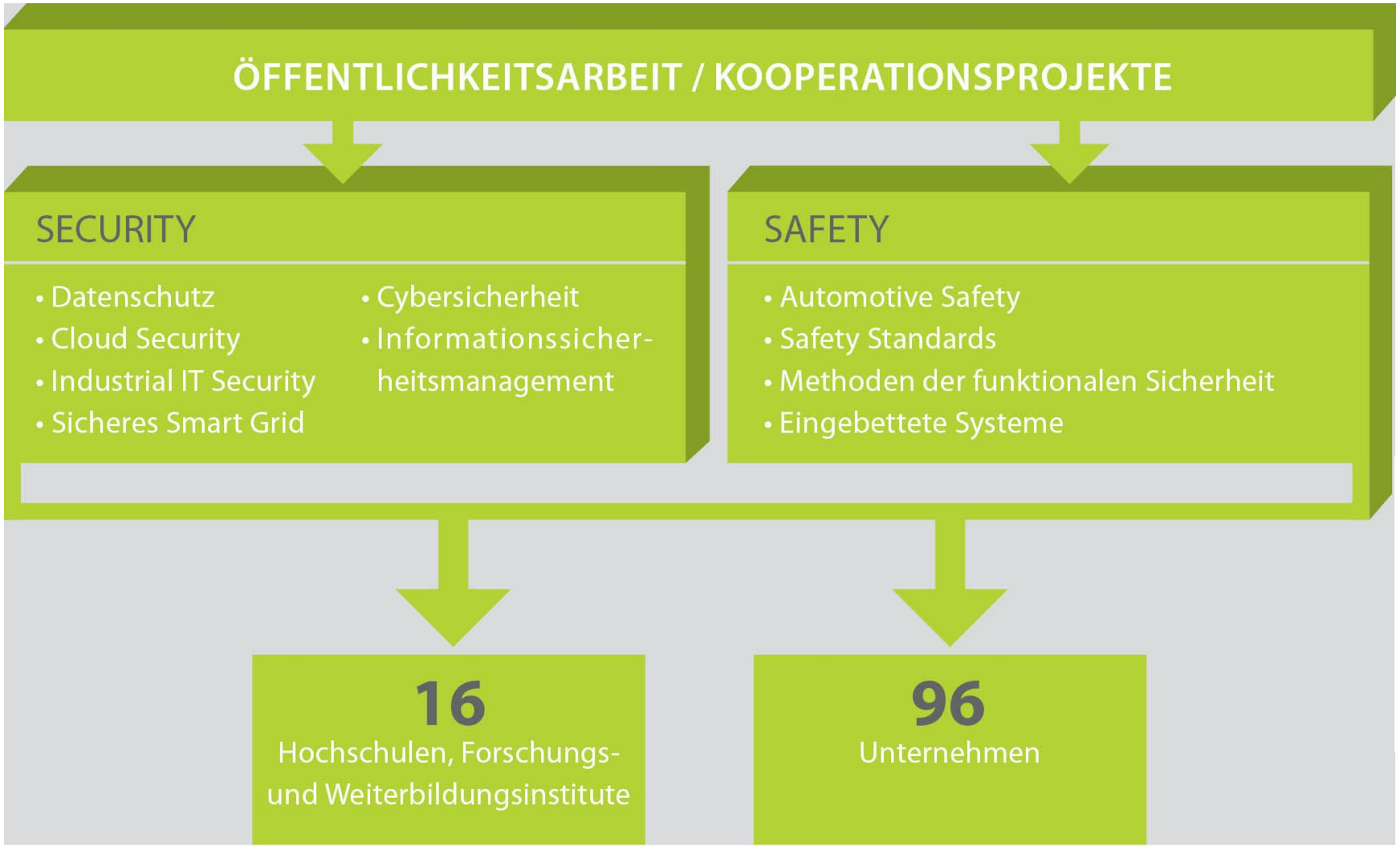
Mitglieder:

– Unternehmen der IT-Wirtschaft
– Unternehmen, die Sicherheitstechnologien nutzen
– Hochschulen und Weiterbildungseinrichtungen
– Juristen

go-cluster
EXZELLENT VERNETZT!

SILVER Cluster Management Excellence
DEDICATED TO CLUSTER EXCELLENCE

Bayerischer IT-Sicherheitscluster e.V.



BSP-SECURITY

we make security work.

Agenda

1 Informationssicherheit durch ISMS

2 ISO/IEC 27001

3 BSI IT-Grundschutz

4 ISIS12

5 Vergleich

BSP-SECURITY

"Security, like correctness, is not an add-on feature“
(Andrew S. Tanenbaum)

„Falls Sie glauben, dass Technologie Ihre Sicherheitsprobleme lösen kann,

verstehen Sie die Probleme nicht, und Sie haben von Technologie keine Ahnung.“
(Bruce Schneier)

- Informationssicherheit kann nur durch eine ganzheitliches Vorgehen garantiert werden („… is not an add-on feature”).
- Technologie + Organisation (Prozesse) sichern Informationssicherheit.
- Jeder Mitarbeiter und jede Abteilung einer Organisation erzeugen Informationssicherheit oder Informationsunsicherheit.

- ISMS (InformationsSicherheitsManagementSysteme) erfüllen diese Aufgabe:
  - Schutz der Unternehmenswerte (Verfügbarkeit, Vertraulichkeit, Integrität)
  - Systematisches ganzheitliches Vorgehen (Lifecycle)
  - Permanente Anpassung des Systems (PDCA: Plan, Do, Check, Act)

Motivation: ISMS warum?

- Gesetze (IT-Sicherheitsgesetz, KRITIS, eGovernement Gesetz, DS-GVO …)
- Verträge mit Kunden (Just in Time)
- Markteintrittserfordernis (Automotive, Marketing, Auftragsverarbeitung)
- Reaktion auf einen Sicherheitsvorfall im Unternehmen
- Unternehmerisches Handeln – Absicherung der Geschäftsziele

- ISO/IEC 2700x (27K) Normenfamilie der International Organization for Standardization (ISO) (ca. 30 Subnormen)
- ISO/IEC 27001:2013 wurde als DIN ISO/IEC 27001:2015 veröffentlicht
- Weltweit anerkannter Standard
- Unabhängig von Größe der Organisation anzuwenden
- „Fasse Dich kurz“: 9 Seiten „Normkörper“ – 12 Seiten Anhang
- Ganzheitlicher Ansatz mit PDCA-Prinzip
- Zertifizierung nach ISO/IEC 27001

www.iso.org

- 1994: IT-Grundschutzhandbuch
- 2005: Orientierung zur ISO/IEC 27001:
  - BSI 100-1: Managementsysteme für Informationssicherheit
  - BSI 100-2: IT-Grundschutz-Vorgehensweise
  - BSI 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
  - BSI IT-Grundschutzkataloge (ca. 5.082 Seiten)
- Unabhängig von Größe des Organisation anzuwenden

- Ganzheitlicher Ansatz mit PDCA-Prinzip
- Vorgehensweise ist im Vergleich zur ISO/IEC 27001 exakter beschrieben
- Umzusetzende Maßnahmen sind Vergleich zur ISO/IEC 27001 wesentlich umfangreicher
- Zertifizierung „ISO/IEC 27001 auf Basis von IT-Grundschutz“ möglich
- Seit 2011 Modernisierung des BSI IT-Grundschutzes

www.bsi.de

4 ISIS12

- ISIS12 – Informations-SIcherheitsmanagementSystem in 12 Schritten
- Motivation: ISMS für KMU („Frust des Beraters“)
- Oktober 2011 auf dem BSI IT-Grundschutztag in Regensburg erstmals vorgestellt: „Auf den Schultern von Riesen“
- 12-stufiges Vorgehensmodell zur Etablierung eines ISMS (ISIS12-Handbuch): „Malen nach Zahlen“
- Entwickelt zu Beginn für KMU (ca. 100 – 2.000 Mitarbeiter)
- Integration ISMS mit IT-Service Management (ITSM) (Change-Management)
- Spezifischer ISIS12-Maßnahmensatz (ISIS12-Katalog)
- ISIS12 Software
- Zertifizierung durch die DQS GmbH (3 Jahre Gültigkeit)
- Migration zur ISO/IEC 27001 möglich

4 ISIS12 für Kommunen

ISIS 12
Informationssicherheit für den Mittelstand

BSP-SECURITY

- IT-Planungsrat:
  ISIS12 deckt die Mindestanforderungen des IT-Planungsrates ab und wird für den Einsatz in Kommunalverwaltungen empfohlen (Entscheidung 2015/05)
- Gutachten Fraunhofer AISEC:
  ISIS12 ist eine geeignete Vorgehensweise zur Umsetzung von ISMS in Kommunen und Behörden bis 500 Mitarbeiter
- Förderung ISIS12 Einführung für Kommunen in Bayern
  (2015/2016: 1.4 Millionen €)
- Entwicklung von ISIS12 Handreichungen für Kommunen und Landratsämter

www.isis12.de

4 ISIS12 - Vorgehensmodell

ISIS 12
Informationssicherheit für den Mittelstand

BSP-SECURITY

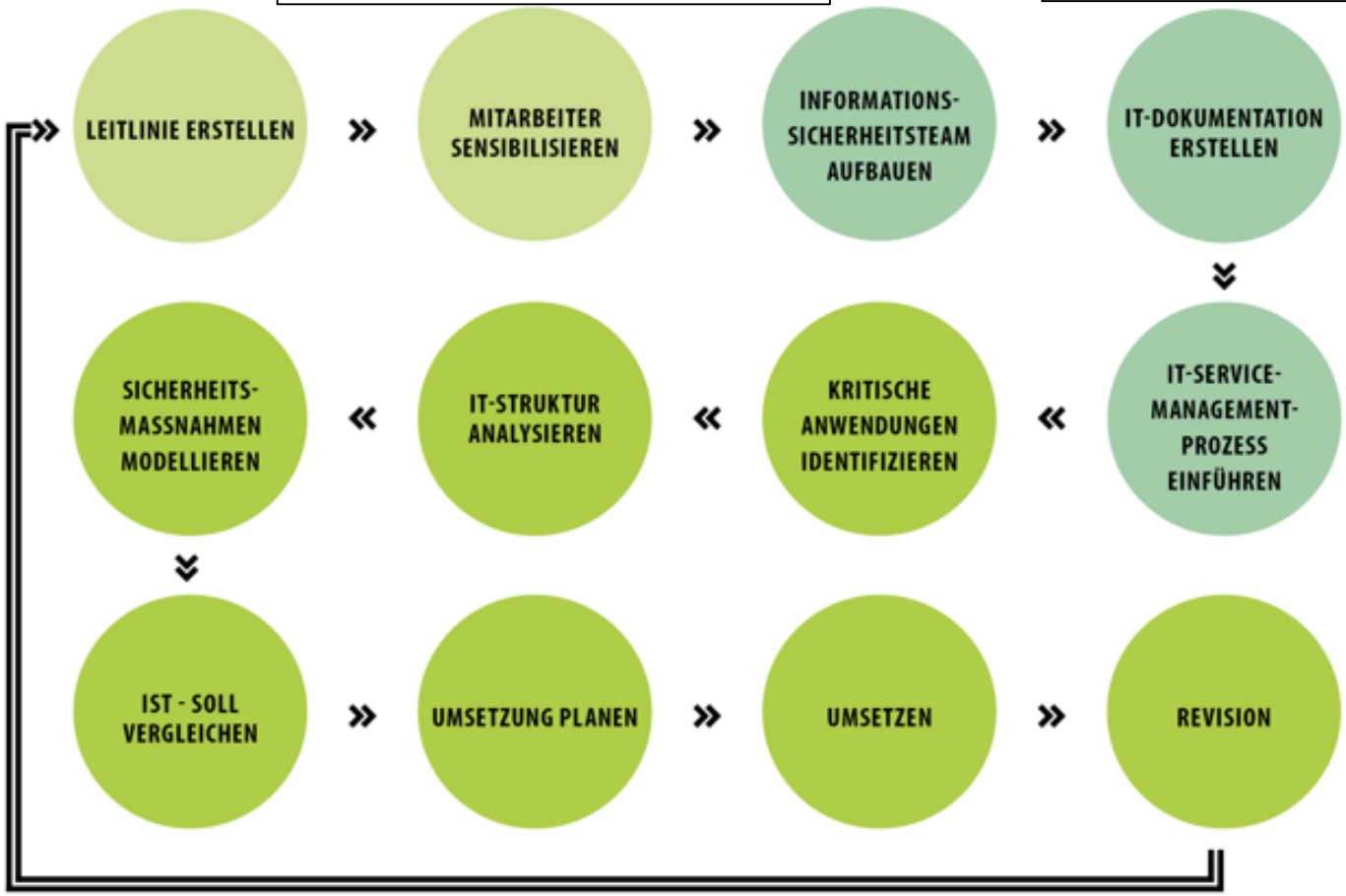
Initialisierungsphase
Schritte 1-2

Aufbau- und Ablauforganisation
Schritte 3-5

Entwicklung und Umsetzung ISIS12 Konzept
Schritte 6-12

Mitarbeiter sind die beste Firewall oder Zombies

Es gibt keine IT-Dokumentation



Ohne Change-Management kein Sicherheits-konzept

5 Vergleich

BSP-SECURITY

5 Vergleich ISMS in der Praxis

5 Vergleich

	ISO/IEC 27001:2013	BSI-Grundschutz (auf Basis ISO/IEC 27001)	ISIS12
Zielgruppe	Organisationen jeder Größe	Organisationen jeder Größe	KMU/Kommunen
Zertifizierungs-aufwand	Aufwand wird nach ISO 27006 kalkuliert beginnt bei 5 PT für das Erst-Audit	Aufwand mind. 15 PT unabhängig vom Geltungsbereich	Erst-Zertifizierungs-Audit dauert i.d.R. 2 PT und Überwachungs-Audit - 1 PT
Zertifizierungs-stellen	Zehn akkreditierte Zertifizierungsstellen	BSI	DQS GmbH
Vorgehensweise	abstrakt	abstrakt-konkret	Konkret, didaktisch geführt
Maßnahmen	Abstrakt formuliert	Umfangreicher Katalog	Katalog für KMU/Kommunen
Risikoanalyse	Basis	Ergänzend (BSI 100-3)	indirekt
Software	Verschieden Anbieter (v.de)	~~GSTOOL~~ verschiedene Anbieter (v.de)	Spezielles Tool

5 Vergleich

- Spieglein, Spieglein an der Wand – was ist das beste ISMS im Land?
- Hauptkriterium: Welches Ziel soll erreicht werden?
  Kundenanforderung, weltweite Anerkennung (z.B.: SOX), …
- DAV: „Bergsteiger übernehmen sich sehr oft – Kondition ungenügend“
  „ISMS ist kein Mittelgebirge“
  ISIS12 kann als Klettersteig verstanden werden
- Planen Sie die Einführung eines ISMS als Projekt (Anfang und Ende)
- Ohne Management-Unterstützung kein Start.
- Zertifizierung ist Katalysator für das Projekt im Unternehmen

- Viele Erfolg beim Aufbau Ihres ISMS.

BSP-SECURITY

Fragen?

- Antworten gerne jetzt

- Beratung, Erfahrungsaustausch, Anregungen gerne später am Messestand

BSP-SECURITY

Alle Inhalte dieser Präsentation unterliegen dem Urheberrecht.

BSP-SECURITY
Franz-Mayer-Str. 1
93053 Regensburg

Tel. (09 41) 60 48 89-8 64,
Fax (09 41) 60 48 89-8 66
E-Mail: info@bsp-security.de
www.bsp-security.de

^