ITSECURITY

Bavarian IT Security & Safety Cluster

ISIS12 - INFORMATIONSSICHERHEIT FÜR DEN MITTELSTAND UND DIE DS-GVO

22.07.2016 WORKSHOP


AGENDA

1 Bayerischer IT-Sicherheitscluster e.V.

2 ISIS12 – Status Quo

3 ISIS12 und die DS-GVO

4 Revision und Zertifizierung

5 Neuer Baustein: DS-GVO

6 Fazit


MICHAEL GRUBER

BSP-SECURITY

Fachbeirat Datenschutz (Bayerischer IT-Sicherheitscluster e.V.)
Gründungsmitglied NIM – ISIS12 Initiator und Architekt

Seit 30 Jahren im IT Bereich tätig (UNIX, LAN/WAN, IT-Security)
Seit 16 Jahren Berater im Bereich IT-Compliance (IS und Datenschutz)

Mitgliedschaften:

- Bayerischer IT- Sicherheitscluster e.V.
- Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
- Gesellschaft für Datenschutz und Datensicherheit e.V.
- Mitglied BSI Cyber-Allianz
- …

www.bsp-security.de

ISIS 12
Informationssicherheit für den Mittelstand


1 BAYERISCHER IT-SICHERHEITSCLUSTER E.V.

Gründung:

- 2006 als Netzwerk (Cluster) in Regensburg
- 2012 Eröffnung der Geschäftsstelle Augsburg
- 2013 Überführung in einen Verein
- Geschäfte des Vereins führt die R-Tech GmbH über einen Geschäftsbesorgungsvertrag

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

ITSECURITY
Bavarian IT Security & Safety Cluster


1 BAYERISCHER IT-SICHERHEITSCLUSTER E.V.

ÖFFENTLICHKEITSARBEIT / KOOPERATIONSPROJEKTE

SECURITY

- Datenschutz
- Cloud Security
- Industrial IT Security
- Sicheres Smart Grid
- Cybersicherheit
- Informationssicherheitsmanagement

SAFETY

- Automotive Safety
- Safety Standards
- Methoden der funktionalen Sicherheit
- Eingebettete Systeme

14
Hochschulen, Forschungs- und Weiterbildungsinstitute

102
Unternehmen


2 ISIS12 - STATUS QUO

- ISIS12 = **I**nformations-**SI**cherheitsmanagement**S**ystem in **12** Schritten
- Grundwerte **Vertraulichkeit**, **Integrität**, **Verfügbarkeit**
- Verfahrensmodell für die Zielgruppe KMU (zunächst)
- ISMS wird mit IT-Service Management verknüpft
- ISIS12-Handbuch, -Katalog und -Software
- Skalierbarkeit: Mögliche Vorstufe zur ISO/IEC 27001
- Beinhaltet Baustein Datenschutz (BDSG)
- Zertifizierung durch die DQS GmbH

www.isis12.de


ZERTIFIKAT

pascom Netzwerktechnik GmbH & Co. KG

ISIS

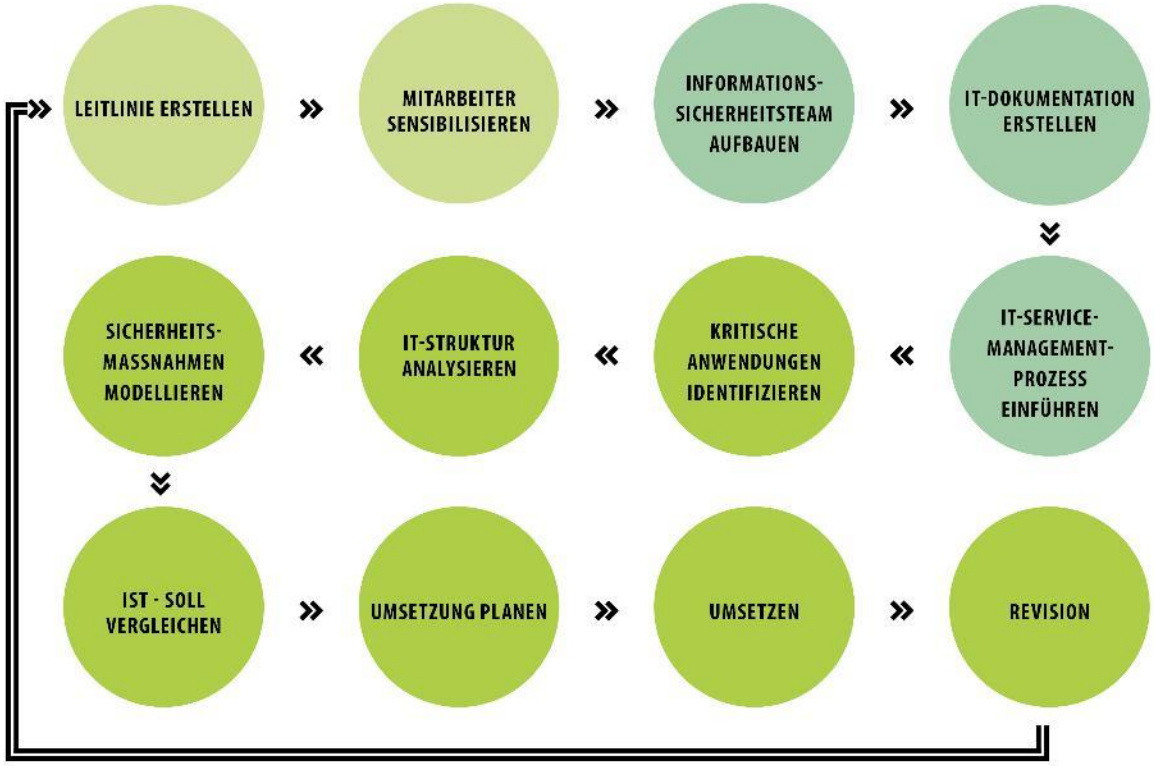
ITSECURITY
Bavarian IT Security & Safety Cluster

2 ISIS12 - STATUS QUO

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12



ITSECURITY
Bavarian IT Security & Safety Cluster


2 ISIS12 - STATUS QUO

- **IT-Planungsrat:** ISIS12 erfüllt die Mindestanforderungen zur Umsetzung der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung – InfoSic (2013) und wird für den Einsatz in Kommunalverwaltungen empfohlen (Entscheidung 2015/05).
- **Grundlage war ein Gutachten der Fraunhofer AISEC:** ISIS12 ist eine geeignete Vorgehensweise (bis 500 Mitarbeiter)
- **In Bayern:**
- Förderprogramm ISIS12 für Kommunen seit 2015
- Förderprogramm ISIS12 für KMU noch in 2016

- **Deutschland, Europa …**

ITSECURITY
Bavarian IT Security & Safety Cluster


3 ISIS12 UND DIE DS-GVO

ISIS12
Informations
sicherheit

DS-GVO
Datenschutz

ISIS 12
Informationssicherheit
für den Mittelstand


3 ISIS12 UND DIE DS-GVO

- „Die TOMs des BDSG werden erwachsen“
- Informationssicherheit und Datenschutz werden durch die DS-GVO eng verbunden (Art. 32 DS-GVO)
- Grundwerte:
  - Vertraulichkeit, Integrität und Verfügbarkeit (ISMS) + Belastbarkeit (DS-GVO)


3 ISIS12 UND DIE DS-GVO

Matching ISIS12 DS-GVO (Auszug)

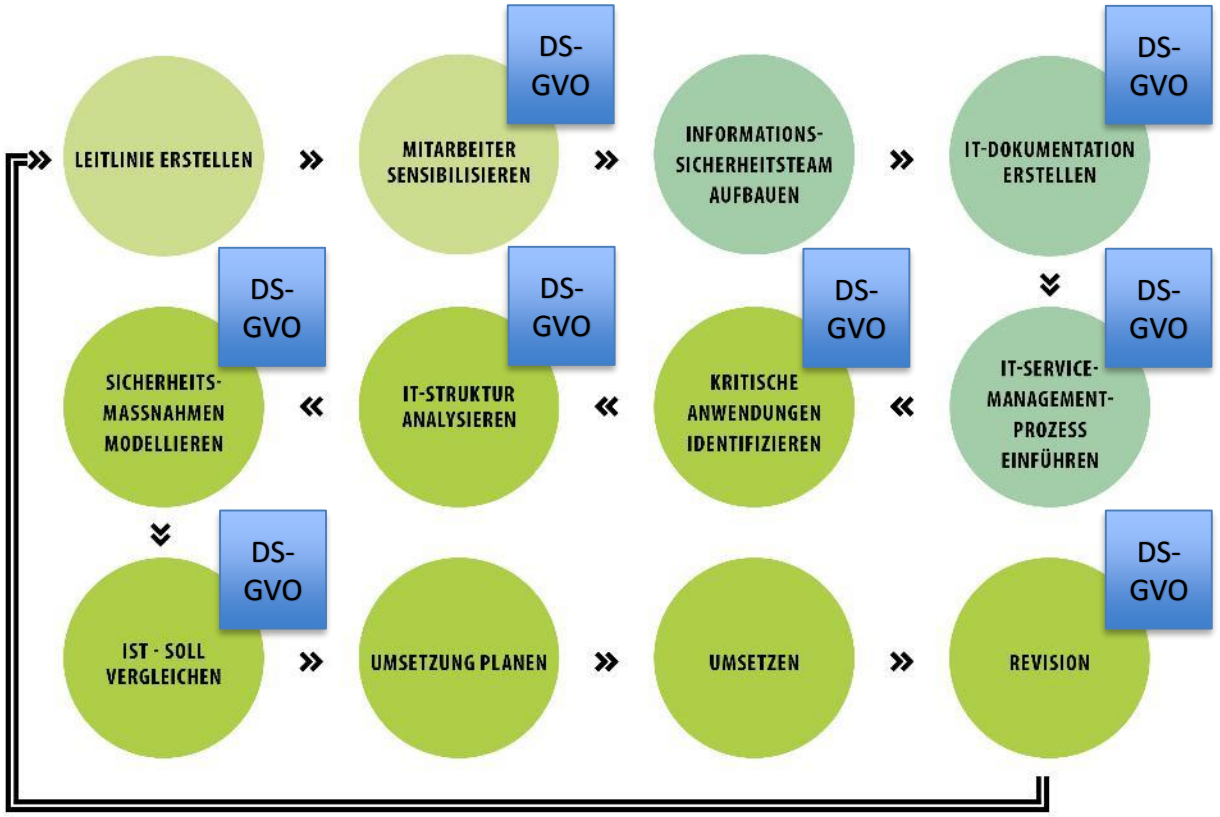
ISIS12	DS-GVO
Schritt 4: IT-Dokumentation	Voraussetzung für Risikobewertung (Basis)
Schritt 5: IT-SM Prozesse (Change)	Änderungsdienst Voraussetzung für Risikobewertung
Schritt 6: Schutzbedarf	Risikobewertung (vgl. BSI 100-3)
Schritt 9:	Geeignete technische und organisatorische Maßnahmen
Schritt 12:	Revision Zertifizierung


3 ISIS12 UND DIE DS-GVO

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12



ISIS 12
Informationssicherheit für den Mittelstand


Rechtsanwältin

Lehrbeauftragte für IT- und Wirtschaftsrecht

Tätigkeitsschwerpunkte:

Internet, Webshops, Daten, IT-Verträge, Marken

Paluka Sobola Loibl & Partner, Rechtsanwälte

Prinz-Ludwig-Strasse 11

93055 Regensburg

www.paluka.de

Sabine Sobola


4 REVISION UND ZERTIFIZIERUNG

- Revision ist wichtiger Teil bei ISIS12 (immer als letzter Punkt bei allen Schritten) und gesondert als Abschluss: Schritt 12
- Zertifizierung durch einen Auditor der DQS möglich
- Art. 42 DS-GVO: Zertifizierung ausdrücklich vorgesehen


5 ART. 42 DS-GVO: VORGABEN UND REGELN

- Möglichkeit der Zertifizierung für Alle
- Sie muss freiwillig und transparent sein
- Einhaltung aller Vorgaben aus der DS-GVO
- Europäisches Datenschutzsiegel angedacht
- Informationen an und Zugang für Zertifizierungsstelle
- Befristung der Zertifizierung auf 3 Jahre mit Verlängerungsoption (neue Prüfung?)
- Aufnahme der Zertifizierungsverfahren, Siegel und Prüfzeichen in ein Register


6 NEUER ISIS12 BAUSTEIN DS-GVO

Vorgaben Art. 6	= Verzeichnis der Rechtmäßigkeit der Verarbeitung, z.B. Einwilligung des Betroffenen
Vorgaben Art. 9	= besondere Kategorien personenbezogener Daten
Vorgaben Art. 12 ff.	= Informationspflichten, Auskunftsrecht, Recht auf Berichtigung und Löschung
Vorgaben Art. 30	= erweitertes Verzeichnis von Verarbeitungstätigkeiten
Vorgaben Art. 32	= technische und organisatorische Maßnahmen, Risikoabschätzung, bereits erfüllt, muss aber wohl als eigener Punkt geprüft werden


6 NEUER ISIS12 BAUSTEIN DS-GVO

- Zertifizierung ISIS12/DS:
  - Aktuelles Zertifizierungsschema + Baustein DS-GVO wird bei der Zertifizierung und in den Überwachungsaudits verpflichtend geprüft
- Finale Umsetzung nach Umsetzung der Öffnungsklauseln


7 FAZIT

- **ISIS12 ist ein etablierter Standard für Informations-sicherheit bei KMU**
- **ISIS12 erfüllt als Vorgehensmodell mit dem DS-GVO Baustein alle Erfordernisse der DS-GVO**
- **ISIS12-Zertifizierung durch die DQS GmbH ist möglich**
- **ISIS12 Zertifizierungsstandard ist transparent und öffentlich**
- **ISIS12 ist speziell für KMU entwickelt worden**
- **ISIS12 wird vom IT-Planungsrat empfohlen**


Kontakt:

Sandra Wiesbeck

Bayerischer IT-Sicherheitscluster e.V.

Franz-Mayer-Str. 1

93053 Regensburg

Tel.: 0941/604 88 9 18

Mail: sandra.wiesbeck@it-sec-cluster.de

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

Unterstützt durch das
Bayerische Staatsministerium des Innern, für Bau und Verkehr

Initiative Cybersicherheit Bayern