ITSECURITY

Bavarian IT Security & Safety Cluster

IT-SICHERHEITSMANAGEMENT MIT ISIS12

ANDREAS REISSER, BAYERISCHER IT-SICHERHEITSCLUSTER E.V.,
SYSGRADE GMBH
KOMMUNALE 2015, NÜRNBERG


AGENDA

- **Vorstellung des Bayerischen IT-Sicherheitsclusters e.V.**
- Rahmenbedingungen und Förderprogramm für Kommunen
- ISIS12 – Informationssicherheit in 12 Schritten
- ISIS12-Blaupause für Kommunen


DAS BAYERISCHE IT-SICHERHEITSCLUSTER

ECKDATEN

Gründung:

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

Mitglieder:

- Im Bayerischen IT-Sicherheitscluster haben sich Unternehmen der IT-Wirtschaft und Unternehmen, die Sicherheitstechnologien nutzen sowie Hochschulen, Weiterbildungseinrichtungen und Juristen zusammengeschlossen

SILVER Cluster Management Excellence
DEDICATED TO CLUSTER EXCELLENCE


DAS BAYERISCHE IT-SICHERHEITSCLUSTER

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

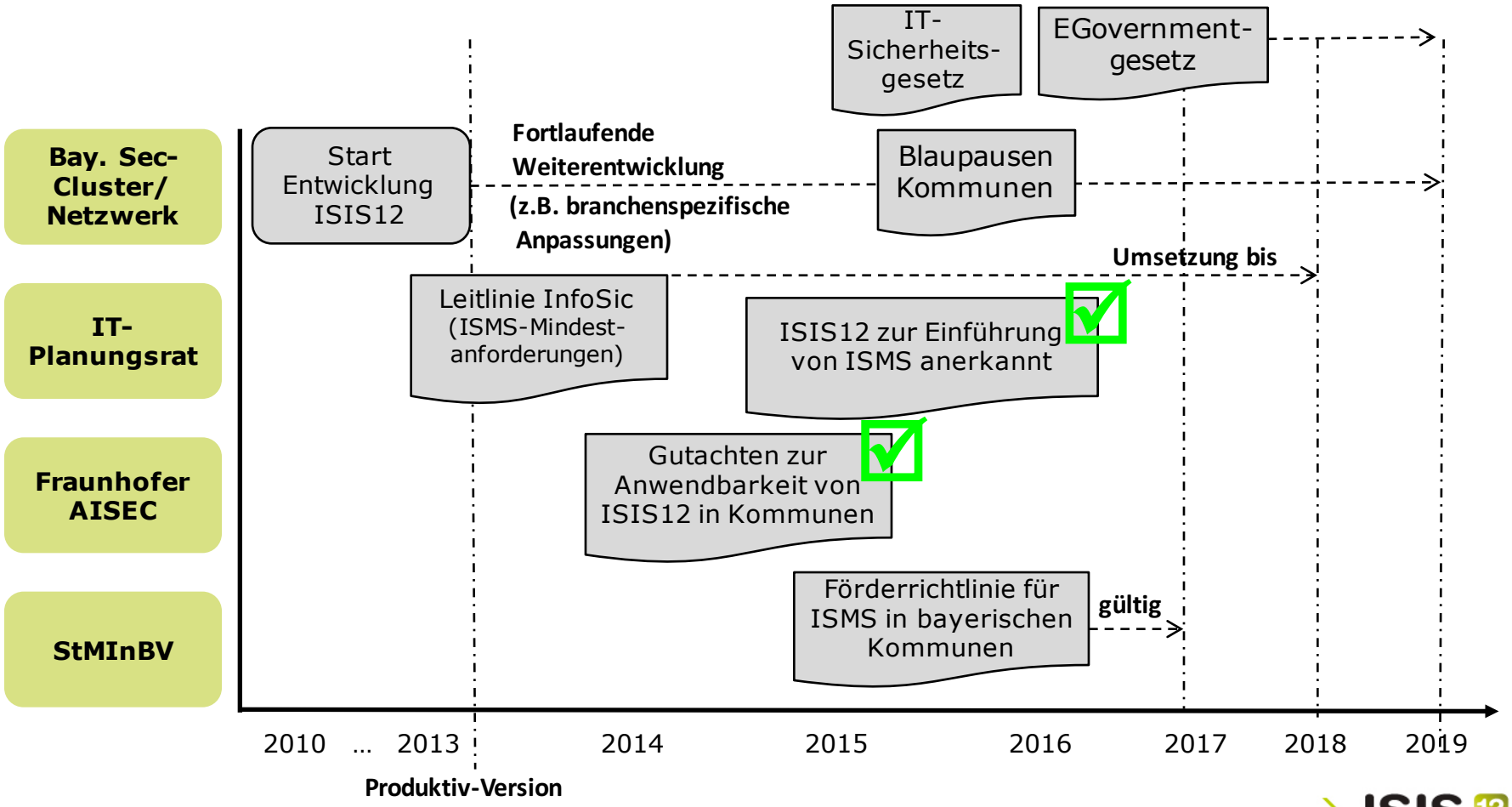
102
Unternehmen

ITSECURITY
Bavarian IT Security & Safety Cluster


AGENDA

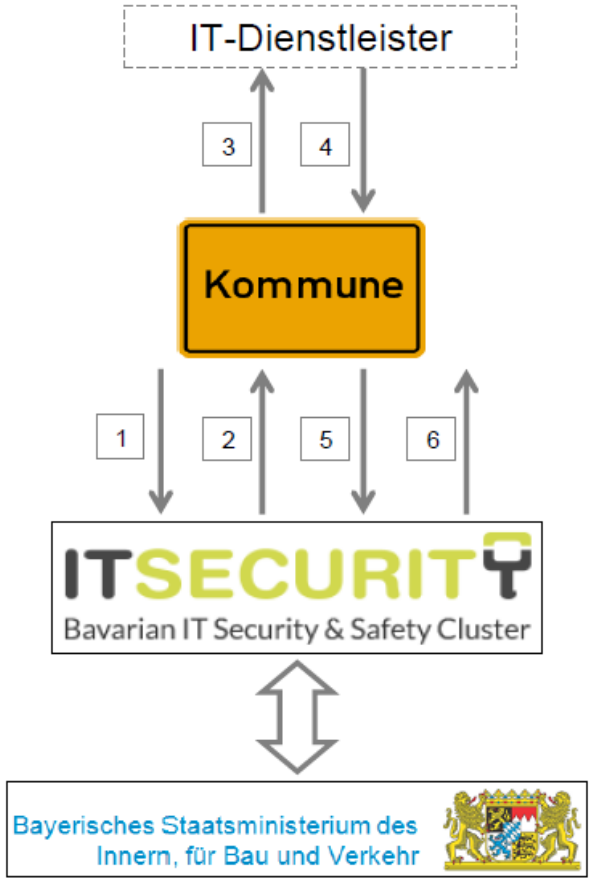
- Vorstellung des Bayerischen IT-Sicherheitsclusters e.V.
- **Rahmenbedingungen und Förderprogramm für Kommunen**
- ISIS12-Vorgehensmodell
- ISIS12-Blaupause für Kommunen


RAHMENBEDINGUNGEN - ÜBERBLICK UND KONTEXT



ISIS 12
Informationssicherheit für den Mittelstand

FÖRDERPROGRAMM FÜR KOMMUNEN



1: Elektronischer formgebundener Antrag

2: Bestätigung der Förderfähigkeit und Abschluss des Fördervertrags

3: Beauftragung eines lizensierten IT-Dienstleisters

4: Rechnungstellung an die Kommune

5: Auszahlungsantrag mit Verwendungsnachweis

6: Auszahlung der Förderung

Bewilligung und Auszahlung gemäß Zuwendungsvereinbarung

ITSECURITY
Bavarian IT Security & Safety Cluster


AGENDA

- Vorstellung des Bayerischen IT-Sicherheitsclusters e.V.
- Rahmenbedingungen und Förderprogramm für Kommunen
- **ISIS12 – Informationssicherheit in 12 Schritten**
- ISIS12-Blaupause für Kommunen


ISIS12

INFORMATIONS-SICHERHEITSMANAGEMENTSYSTEM (ISMS) IN 12 SCHRITTEN

- Verständlich beschriebener 12-stufiger Prozess, der den Einstieg ins ISMS erleichtert (ISIS12 Handbuch)
- Öffentliches ISIS12-Handbuch & Maßnahmenkatalog
- Speziell entwickelte ISIS12-Software (vgl. GSTOOL)

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

Initiative Cybersicherheit Bayern

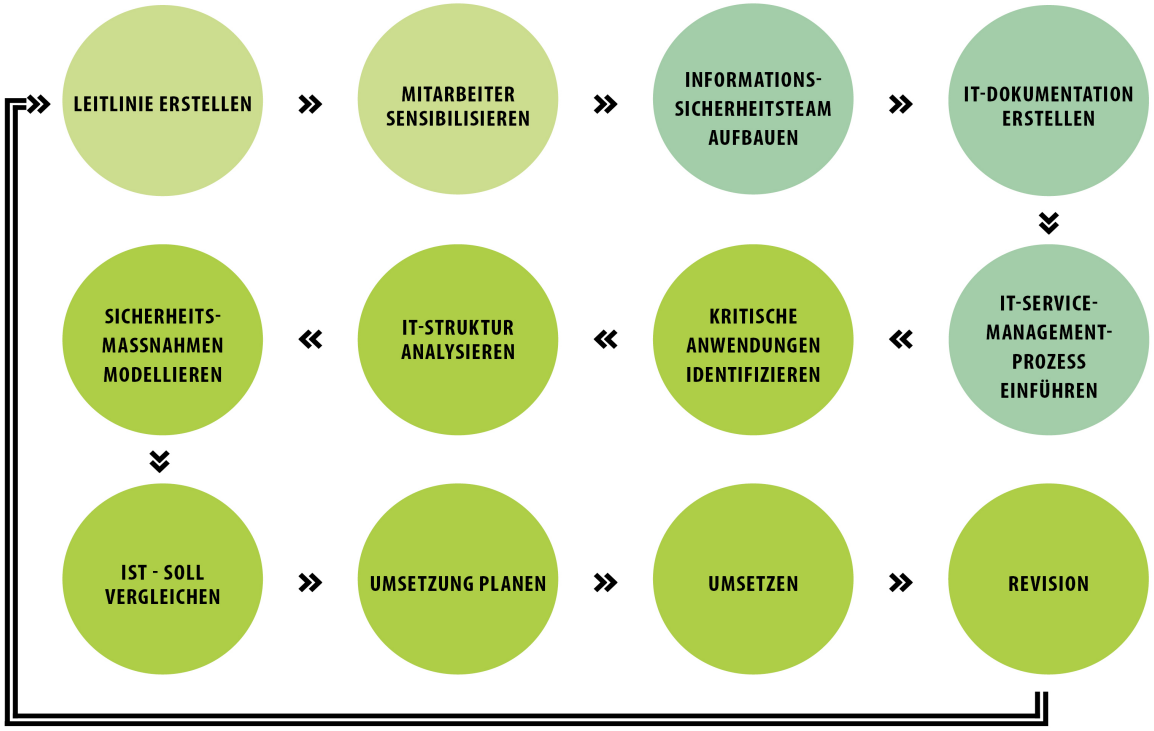
ISMS-VERGLEICH


DAS ISIS12-VORGEHENSMODELL

Initialisierungsphase
Schritte 1-2

Aufbau- und
Ablauforganisation
Schritte 3-5

Entwicklung und
Umsetzung ISIS12
Konzept
Schritte 6-12



ISIS 12
Informationssicherheit für den Mittelstand


ISIS12

ZERTIFIKAT

- Möglichkeit zur Zertifizierung durch die DQS GmbH
- Zertifikatsgültigkeit von 3 Jahren
- 2 Überwachungsaudits
- Auditierung durch zertifizierte ISIS12-Auditoren
- Unterstützung durch ISIS12-Dienstleister

ISIS 12
Informationssicherheit für den Mittelstand


AGENDA

- Vorstellung des Bayerischen IT-Sicherheitsclusters e.V.
- Rahmenbedingungen und Förderprogramm für Kommunen
- ISIS12 – Informationssicherheit in 12 Schritten
- **ISIS12-Blaupause für Kommunen**


ISIS12 „BLAUPAUSE“ FÜR KOMMUNEN

Ziele

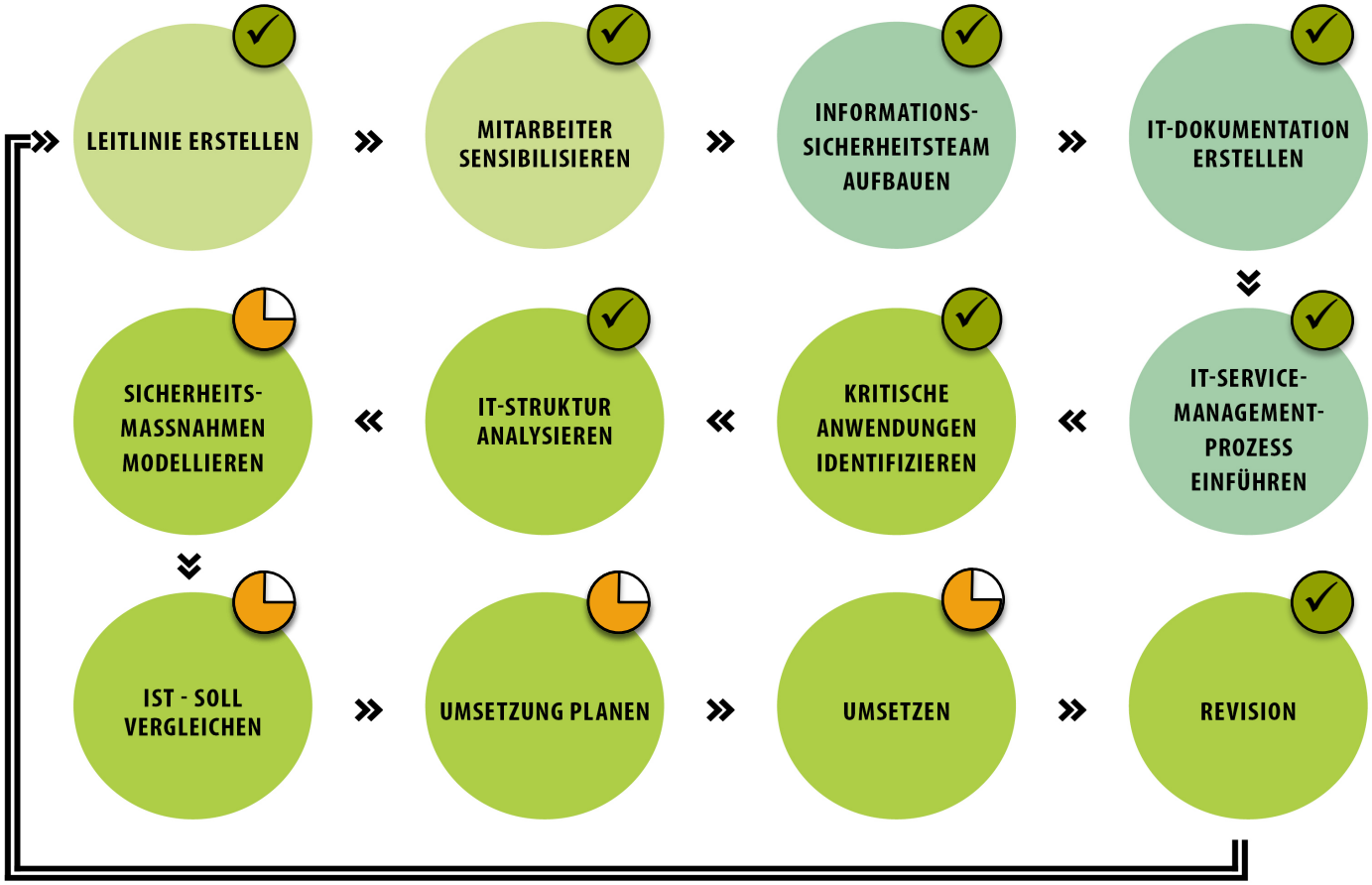
- Kommunen und ISIS12-Dienstleistern die Arbeit zur erleichtern
- Die Qualität des ISMS soll intersubjektiv vergleichbar werden (Standardisierung)
- Ständige Aktualisierung der Arbeitshilfe
- Kein neues ISIS12-Handbuch sondern konkrete Ergänzungen für jeden der 12 Schritte

Vorgehensweise

- Erfahrungen aus BSI IT-Grundschutz-Projekten
- Erfahrungen aus den ersten ISIS12-Projekten mit Kommunen
- Workshops mit Kommunen

ISIS 12
Informationssicherheit für den Mittelstand

ISIS12 BLAUPAUSE – AKTUELLER STAND



ISIS 12
Informationssicherheit für den Mittelstand


SCHRITT 1: LEITLINIE ERSTELLEN

- Im ISIS12 Vorgehensmodell spielt die Sicherheitsleitlinie eine zentrale Rolle.
- Für Kommunen wurde eine Muster-Sicherheitsleitlinie erstellt (Dienstanweisung)
- Diese kann mit **wenig Aufwand** an die jeweilige Kommune angepasst werden.

Status: Fertig


SCHRITT 2: MITARBEITER SENSIBILISIEREN

- Für verschiedene Zielgruppen (Leitung, Personalrat, Mitarbeiter) wurden spezielle Präsentationen entwickelt.

- Empfehlungen für die kontinuierliche Sensibilisierung von Mitarbeitern:

  - Mitarbeiter als die wichtigste Firewall

  - Mitarbeiter als Sicherheitsschwachstelle

Status: Fertig

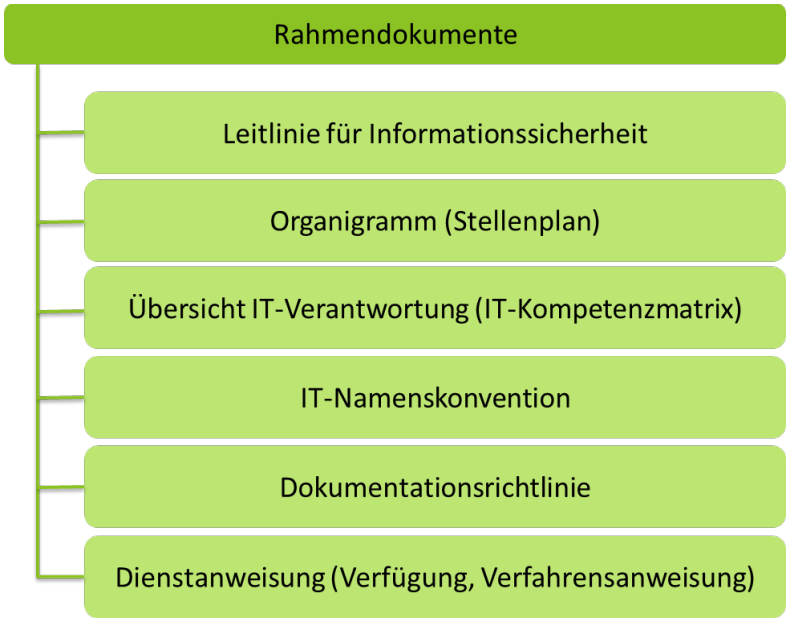

SCHRITT 3 - INFORMATIONSSICHERHEITSTEAM AUFBAUEN

- Bestellung eines Informationssicherheitsbeauftragten (ISB)
- Vorschläge für die Zusammensetzung des IS-Teams
- Spezifische Aufgaben des IS-Teams in Kommunen

Status: Fertig


SCHRITT 4: IT-DOKUMENTATION ERSTELLEN

- Vorschläge für die Struktur der IT-Dokumentation
- Musterdokumente als Arbeitsgrundlage
- Empfehlungen und Hinweise für die erforderlichen Arbeitsschritte



Status: Fertig


SCHRITT 5: IT-SERVICE MANAGEMENT PROZESSE EINFÜHREN

- Gibt es spezifische kommunale IT-SM-Prozesse?
- Externe Dienstleister sind in der Regel bei Kommunen im Vergleich zu KMU häufiger aktiv.
- Dies erfordert bei der der Prozessmodellierung eine entsprechende Berücksichtigung.
- Die externen Dienstleister müssen in die internen IT-SM-Prozesse integriert werden.
- Empfehlungen und Prozessmodellierung der IT-SM-Prozesse **Wartung**, **Änderungsmanagement** und **Störungsbeseitigung**.

Status: Fertig


SCHRITT 6: KRITISCHE ANWENDUNGEN IDENTIFIZIEREN

- Nur diejenigen Anwendungen sind zu erfassen, die bezogen auf mindestens einer der Grundwerte „**Vertraulichkeit**“, „**Integrität**“ oder „**Verfügbarkeit**“ als kritisch einzustufen sind.
- Kommunen sind für viele Fachaufgaben zuständig und verantwortlich.
- Dies ist von Größe und Struktur der Behörde abhängig.
- Bildung sinnvollerweise Gruppen von Anwendungen zu Clustern („Reduktion von Komplexität“).
- Die gefundenen Anwendungen werden bezogen auf die drei Grundwerte hin untersucht und klassifiziert: **Schutzbedarfsfeststellung**
- Entwicklung spezifischer Schutzbedarfskategorien

Status: Fertig


SCHRITT 7: IT-STRUKTURANALYSE

- In ISIS12 Schritt 7 werden die für in Schritt 6 für den betrieb erforderlichen Zielobjekte erfasst und mit den Anwendungen verknüpft.
- Nach Abschluss der Verknüpfung wird der in Schritt 6 erfasste Schutzbedarfs an die Zielobjekte vererbt.
- Anpassung an spezifische kommunale Besonderheiten
- Muster eines bereinigten Netzwerkplans
- Die spezielle Rolle von Behördennetzen (kommunale Behördennetze: KomBN und Bayerisches Behördennetzwerk) ist zu berücksichtigen.

Status: Fertig


SCHRITT 8: MODELLIERUNG

- Im ISIS12-Katalog sind KMU typische Bausteine mit den entsprechenden Sicherheitsmaßnahmen enthalten.

- Modellierung spezifischer Bausteine für Kommunen, die (noch) nicht im ISIS12-Katalog enthalten sind.

Status: In Arbeit


SCHRITT 9: IST/SOLL-VERGLEICH (BSC)

- Die IST-SOLL-Erhebung gibt Auskunft über den Umsetzungsgrad der geforderten Sicherheits-Maßnahmen:
  (Ja, Nein, Teilweise, Nicht notwendig)

- Hier spielen externe Dienstleister/Softwareentwickler ein wichtige Rolle: Wer sonst als Hersteller kommunalen Software kann entsprechende Antworten geben (z.B.: „SQL-Injection“)?
- Gespräche mit Softwarefirmen um diesen Schritt zentral zu erledigen, um damit den Aufwand für Kommunen gering zu halten!

Status: In Arbeit


SCHRITT 10: UMSETZUNG PLANEN

- Die aus dem IST-SOLL-Vergleich (Schritt 9) erhaltenen, noch zu realisierenden Maßnahmen werden im Rahmen der Realisierungsplanung konsolidiert und priorisiert.
- Berücksichtigung der kommunalen Prozesse der Budgetierung bzw. Haushaltsplanung.
- Die Zeitachse muss für den Projektverlauf frühzeitig berücksichtigt werden (etwa das Einstellen von erforderlichen Haushaltspositionen).

Status: In Arbeit


SCHRITT 11: UMSETZUNG

- Aus Schritt 10 resultiert ein konsolidierter und genehmigter Katalog von umzusetzenden Sicherheitsmaßnahmen.
- Die Umsetzung der noch offenen Maßnahmen vervollständigt die Informationssicherheitskonzeption.
- Für jede Maßnahme werden die Rollen des Initiators, des Umsetzers und der Zeitpunkt der Realisierung festgelegt.
- Die Kompetenz den Initiator und Umsetzer zu bestimmen ist noch genauer zu klären und entsprechend zu beschreiben.

Status: In Arbeit


SCHRITT 12: REVISION

- ISIS12 Schritt 12 stellt den letzten Schritt dar und ist zugleich der immerwährende Auftrag, das ISMS auf Aktualität und Wirksamkeit hin zu überprüfen und anzupassen (PDCA).

- Grundsätzlich sind die Schritte 1 bis 11 jährlich zu durchlaufen und auf Änderungen, Anpassungen und Ergänzungen hin zu überprüfen.

Status: Fertig


ZUSAMMENFASSUNG

ISIS12 IST EIN PRAGMATISCHES UND DENNOCH EFFEKTIVES IT-GRUNDSCHUTZ-PROFIL FÜR KOMMUNEN IN 12 SCHRITTEN

- Auf das Notwendige reduzierter Maßnahmenkatalog
- Handbuch und Katalog kostenfrei für Kommunen (Bestellung über www.it-sicherheit-bayern.de)
- ISIS12 in Verbindung mit der entwickelten „Blaupause“ sorgt für eine kosteneffiziente, an die spezifischen Gegebenheiten von Kommunen angepasste Einführung und Betrieb eines ISMS
- Erhöht die Informationssicherheit in der Kommune


VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

Sandra Wiesbeck
Bayerischer IT-Sicherheitscluster e.V.

Bruderwöhrdstr. 15 b
93055 Regensburg

Tel.: 0941/604 88 9 18
Mail:
sandra.wiesbeck@it-sec-cluster.de

Andreas Reisser
Bayerischer IT-Sicherheitscluster e.V./
Sysgrade GmbH

Konrad-Adenauer-Allee 38
93051 Regensburg

Tel.: 0941/604 88 9 18
Mail:
andreas.reisser@sysgrade.de

ITSECURITY

Bavarian IT Security & Safety Cluster

ANHANG


IT-PLANUNGSRAT - MINDESTANFORDERUNGEN

Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (Stand 19.02.2013) Version 1.8
(10. IT-Planungsrat Beschluss 2013/01):

Die Mindestanforderungen an das ISMS umfassen:

- Erstellung von jeweiligen verbindlichen **Leitlinien für die Informationssicherheit**
- Erstellung und Umsetzung von Sicherheitskonzepten für Behörden und Einrichtungen
- Festlegung und Dokumentation der Abläufe bei **IT-Sicherheitsvorfällen**
- Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit. Hierzu gehört auch die Etablierung und Durchführung regelmäßiger Sensibilisierungsmaßnahmen für die oberste Leitungsebene


IT-PLANUNGSRAT - MINDESTANFORDERUNGEN

- Information, Weiterbildung, Sensibilisierung aller Beschäftigten der öffentlichen Verwaltung zu Themen der Informationssicherheit. Hierzu gehört auch die Etablierung und Durchführung regelmäßiger Sensibilisierungsmaßnahmen für die oberste Leitungsebene
- Etablierung von Prozessen, mit denen Umsetzung, Wirksamkeit und Beachtung der Informationssicherheitsmaßnahmen regelmäßig kontrolliert und die Einleitung ggf. erforderlicher Maßnahmen (z. B. Fortschreibung Sicherheitskonzepte) gewährleistet wird (PDCA)


IT-PLANUNGSRAT - MINDESTANFORDERUNGEN

- Anforderungsgerechte und einheitliche Fortbildung der IT-Sicherheitsbeauftragten. Eine Zertifizierung der IT-Sicherheitsbeauftragten wird angestrebt (Das Konzept für Auditorenschulung ist bereits vorhanden)
- Jahrestagungen der IT-Sicherheitsbeauftragten zum gegenseitigen Erfahrungsaustausch (Verantwortung für Organisation wechselt mit Vorsitz im IT-Planungsrat)
- Festlegung und Dokumentation von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements (z.B. Benennung **IT-Sicherheitsbeauftragte**)


IT-PLANUNGSRAT - BESCHLUSSLAGE

Leitlinie für Informationssicherheit des IT-Planungsrats:

- Zunächst nur verbindlich für Länder, aber
  - sie „ist bei Ebenen-übergreifenden IT–Verfahren .. auf die jeweiligen Verfahrensbeteiligten auszudehnen“
  - Sie fordert den Aufbau eines ISMS orientiert am IT-GS
  - D.h. ISMS orientiert an IT-Grundschutz auch für Kommunen

16. Sitzung des IT-Planungsrats, TOP 7: InfoSic in Kommunen:

- Der IT-Planungsrat „stellt fest, dass .. mit ISIS12 ein pragmatisches und skalierbares Vorgehensmodell zur Einführung eines ISMS zur Verfügung steht, das die entsprechenden Mindestanforderungen des IT-Planungsrats abdeckt
- **d.h. ISIS12 eignet sich für Kommunen zur Umsetzung der Anforderungen der Leitlinie des IT-Planungsrats**


IT-PLANUNGSRAT - BESCHLUSSLAGE

Einsatzbereich zur Umsetzung der Leitlinie:

- Kommunen mit bis zu 500 MA
- Homogene IT-Basisinfrastruktur
- Keine über öffentliche Netze ungeschützt angebundenen Außenstellen
- Überwiegend normaler Schutzbedarf

Grenzen: ISIS12 eignet sich nicht für den Einsatz bei

- Hochverfügbarkeitsanforderungen
- Kritischen Infrastrukturen
- Hohen Schutzbedarfsanforderungen


DAS BAYERISCHE EGOVERNMENT-GESETZ

ZIELE

- Ausbau eines effektiven, flächendeckenden, bürger- und unternehmensfreundlichen eGovernment
- Digitale Zugangs- und Verfahrensrechte von Bürgern und Unternehmen
- Gewährleistung von IT-Sicherheit
- Modernisierung des Datenschutzes
- Kodifizierung eines allgemeinen Auskunftsanspruchs
- Infrastrukturverantwortung und IT-Kooperation, insbesondere zwischen Freistaat und Kommunen
- Erleichterter Schriftformersatz, Bürokratieabbau


DAS BAYERISCHE EGOVERNMENT-GESETZ

KONZEPTION

- Rechtsrahmen für eVerwaltung auf allen Ebenen in BY
- Subjektive Rechte auf elektronischen Zugang, elektronisches Verwaltungsverfahren, elektronische Nachweise, elektronisches Bezahlen
- Einführung der elektronischen Rechnung (2018)
- IT-Sicherheitskonzepte und Bayern-CERT
- Behördenzusammenarbeit in der IT
- Reform BayDSG: Einwilligung, Zentralisierung (Basisdienste etc.), Auskunftsanspruch
- Abbau von 40 Formvorschriften


DAS BAYERISCHE EGOVERNMENT-GESETZ

INHALT

Art. 1: Anwendungsbereich
Art. 2: Digitale Zugangs- und Verfahrensrechte
Art. 3: Elektronische Kommunikation und Identifizierung
Art. 4: Elektronische Behördendienste
Art. 5: Elektronischer Zahlungsverkehr und eRechnung
Art. 6: Elektronisches Verwaltungsverfahren
Art. 7: Elektronische Akte
Art. 8: **IT-Sicherheit und Datenschutz**
Art. 9: Behördenzusammenarbeit
Art. 9 a: Änderung anderer Rechtsvorschriften, BayVwVfG,BayDSG, Auskunftsrecht etc.
Art. 10: Übergangs und Schlussvorschriften


DAS BAYERISCHE EGOVERNMENT-GESETZ

ART. 1: ANWENDUNGSBEREICH

Art. 1
Anwendungsbereich

(1) Dieses Gesetz gilt für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Freistaates Bayern, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts, soweit nicht besondere Rechtsvorschriften des Freistaates Bayern inhaltsgleiche oder entgegenstehende Bestimmungen enthalten.
(2) [1]Dieses Gesetz gilt nicht für Schulen, Krankenhäuser, das Landesamt für Verfassungsschutz und Beliehene. [2]Dieses Gesetz ist nicht anzuwenden auf die Tätigkeit der Finanzbehörden nach der Abgabenordnung und die Verwaltungstätigkeit nach dem Zweiten Buch Sozialgesetzbuch. [3]Art. 2 Abs. 1 und 2 Nr. 2 und Abs. 3 des Bayerischen Verwaltungsverfahrensgesetzes (BayVwVfG) gelten entsprechend.
(3) Das E-Government-Gesetz des Bundes findet nur beim Vollzug von Bundesrecht im Auftrag des Bundes Anwendung.



DAS BAYERISCHE EGOVERNMENT-GESETZ

ART. 8: IT-SICHERHEIT UND DATENSCHUTZ

Art. 8
Informationssicherheit und Datenschutz

(1) [1]Die Sicherheit der informationstechnischen Systeme der Behörden ist im Rahmen der Verhältnismäßigkeit sicherzustellen. [2]Die Behörden treffen zu diesem Zweck angemessene technische und organisatorische Maßnahmen im Sinn des Art. 7 des Bayerischen Datenschutzgesetzes (BayDSG) und erstellen die hierzu erforderlichen Informationssicherheitskonzepte.

erforderlichen Daten, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise. [3]Die an das Behördennetz angeschlossenen Behörden melden dem CERT sicherheitsrelevante Vorfälle. [4]Das CERT spricht Warnungen und Empfehlungen aus und leitet Erkenntnisse an Dritte weiter, wenn dies zur Erkennung und Abwehr von Gefahren für Verwaltung, Bürger oder Wirtschaft erforderlich ist. [5]Personenbezogene Daten dürfen ausschließlich für die in Satz 2 genannten Zwecke erhoben, verarbeitet und genutzt werden.