Gemeinde Adelsdorf
ZUSAMMENWACHSEN

ISIS 12

Einführung eines Informationssicherheits-managementsystems in der Gemeinde Adelsdorf

Gemeinde Adelsdorf, 16.10.2017

Die Gemeinde

Gründe und Entscheidungsfindung

Grundlagen Informationssicherheit

Informationssicherheitskonzept wird im BayEGovG zum 01.01.2018 gefordert
„Nachweisbares, dauerhaft geplantes Vorgehen zur Informationssicherheit“

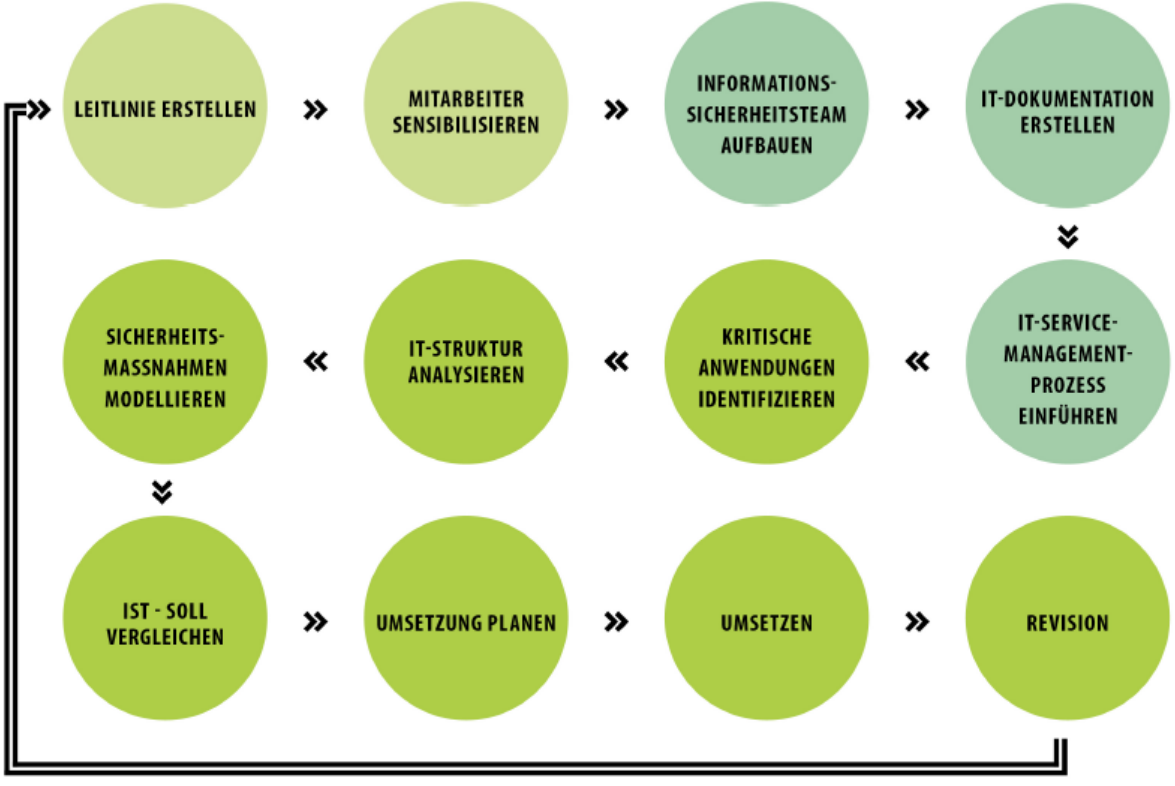
Varianten:

BSI-Grundschutz,
ISO27001,
ISIS12,
VdS 3473,
Arbeitshilfe Innovationsstiftung Bayerische Kommune (AKDB/BayGT)
... und wahrscheinlich noch viele „Eigenkreationen“

ISIS12 ist das kleinste zertifizierfähige ISMS

Basis für alle *deutschen* Vorgehensweisen ist der Grundschutzkatalog des BSI

ISIS12 – Ein ISMS in 12 Schritten



Erstgespräch, Erstsichtung + Dokumentation

- Willenserklärung der Geschäftsleitung und des Bürgermeisters
- Bildung des ISIS12 Teams bestehend aus ISB, DSB und IT Admin
- Rundgang im Haus mit dem Datenschutzberater Herrn Turban
- Zu Beginn Erstsichtung und Erstellung der Dokumentation

- Alle Gebäude, Büros, Dokumentationen, etc.

- Erstellung Doku, dazu Sichtung Mitteilungsblatt, Internet und Soziale Medien

- Präsentation der Dokumentation, dazu Durchsprache und Erstellung der Informationssicherheitsleitlinie

Sensibilisierung der Beschäftigten

- Mitarbeitersensibilisierung
- Gruppengröße bis zu 25 Personen
- Dauer jeweils 2 Stunden, dazu je 0,5h Vor- und Nacharbeit)
- Individuell für Beschäftigte Rathaus, Bauhof etc.
- Individuell für Beschäftigte der Kinder- und Jugendbetreuung

Unterlagenerstellung für ISIS12 und Datenschutz

- Erstellung von Dienstanweisungen

- Erstellung von Standardprozessen

Befüllung ISIS12 Softwaretool

- Doku ISIS12 Ablauf
- Erfassung der krit. Applikationen (!)
- Eingabe der krit. Applikationen
- Eingabe IT und Raumstruktur
- IST-Soll-Vergleich
- Maßnahmenplanung

ISIS 12 Übersicht 0 1 2 3 4 5 6 7 8 9 10 11 12 — 15.03.2017 — Admin

Schritt 9: IST-SOLL vergleichen

Beschreibung

In **ISIS12 Schritt 9** wird mittels Ist-Soll-Vergleich ein Überblick über die Umsetzung der Maßnahmen aus Schritt 8 gegeben werden.Die Erhebung kann durch die vom ISB ernannten verantwortlichen Spezialisten im Unternehmen durchgeführt werden. Die hierfür vom ISIS12-Softwaretool erstellten Erhebungsbögen, können im größeren Kreis oder in Einzelinterviews abgearbeitet werden. Die möglichen Beurteilungen der Umsetzung lauten: 'Ja' (Grün), 'Teilweise' (Gelb), 'Nein' (Rot) oder 'Nicht notwendig' (Blau)

Universale Aspekte (S1) | Infrastruktur (S2) | IT-Systeme/Netze (S3) | Anwendungen (S4)

Speichern

Bausteine/Maßnahmen - Umsetzungsgrad: 27.06 % (125 von 462)			Interviewpartner	Umsetzung	Rev.-Datum	Bemerkung/Begründung
B4.2	Datenbankbasierende Anwendungen Access (Datenbanken) - Schutzbedarf A,A,A		N.N.			
	M2.132	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen		Ja	01.03.2018	
	M2.124	Geeignete Auswahl einer Datenbank-Software		Ja	01.03.2018	
	M2.125	Installation und Konfiguration einer Datenbank		Ja	01.03.2018	
	M4.7	Änderung voreingestellter Passwörter		Ja	01.03.2018	
	M2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile		Teilweise	01.03.2018	
	M2.34	Dokumentation der Veränderungen an einem bestehenden System		Nicht notwendig	01.03.2018	Begründung
	M2.128	Zugangskontrolle einer Datenbank		Nicht notwendig	01.03.2018	Begründung
	M2.129	Zugriffskontrolle einer Datenbank		Nicht notwendig	01.03.2018	Begründung
	M2.130	Gewährleistung der Datenbankintegrität		Ja	01.03.2018	
	M2.133	Kontrolle der Protokolldateien eines Datenbanksystems		Ja	01.03.2018	
	M3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung		Ja	01.03.2018	
	M4.67	Sperren und Löschen nicht benötigter Datenbank-Accounts		Nicht notwendig	01.03.2018	Begründung
	M6.49	Datensicherung einer Datenbank		Ja	01.03.2018	

			Interviewpartner	Umsetzung	Rev.-Datum	Speichern
B4.2	Datenbankbasierende Anwendungen Adebis KITA (Kindergarten Verwaltung) - Schutzbedarf A,A,A		N.N.			
	M2.132	Regelung für die Einrichtung von Datenbankbenutzern/-benutzergruppen		Ja	01.03.2018	
	M2.124	Geeignete Auswahl einer Datenbank-Software		Nicht notwendig	01.03.2018	Festgelegt durch AKDB
	M2.125	Installation und Konfiguration einer Datenbank		Ja	01.03.2018	
	M4.7	Änderung voreingestellter Passwörter		Ja	01.03.2018	
	M2.31	Dokumentation der zugelassenen Benutzer und Rechteprofile		Nein		
	M2.34	Dokumentation der Veränderungen an einem bestehenden System		Ja	01.03.2018	
	M2.128	Zugangskontrolle einer Datenbank		Ja	01.03.2018	
	M2.129	Zugriffskontrolle einer Datenbank		Ja	01.03.2018	
	M2.130	Gewährleistung der Datenbankintegrität		Nicht notwendig	01.03.2018	Festgelegt durch AKDB
	M2.133	Kontrolle der Protokolldateien eines Datenbanksystems		Nicht notwendig	01.03.2018	nicht möglich
	M3.18	Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung		Ja	01.03.2018	
	M4.67	Sperren und Löschen nicht benötigter Datenbank-Accounts		Ja	01.03.2018	
	M6.49	Datensicherung einer Datenbank		Ja	01.03.2018	

Zertifizierung

- Beauftragung durch die Verwaltung bei DQS GmbH
- Gemeinsame Terminabsprache
- Verwaltungsindividueller Ablaufplanung kommt vorab an die Verwaltung
- Versand des Zertifikates oder Übergabe etwa 4 Wochen später
- Terminabsprache für Folgeaudit (in einem Jahr)
- Abschließende Rechnungsstellung und Projektdokumentation
- Beantragung der Auszahlung der Fördermittel

Inhalt Zertifizierung: 1. Tag Vormittag 10h-13h

1. Vorstellungsrunde
2. Leitlinie Informationssicherheit erklärt:
   - Geltungsbereich der ISL, dazu Gemeindestruktur erklärt
   - Veröffentlichung auch bei betroffenen Firmen (EDV-Dienstleister)
3. Sichtung der Unterlagen:
   - Stand und Versionierung der Unterlagen ist von Interesse
   - Erklärung der Zugehörigkeiten und Netze durch ISB oder IT-Admin
   - Wer hat wohin örtlichen Zugang und unterliegt dementsprechend ISIS12
   - Zeigen der Bestellung ISB, Organigramm und Unterlagen, teilweise im Original mit Unterschriften
   - Wiederkehrend Abfrage von Zugriffsberechtigungen. Wichtig!
   - Gibt es ein Vertragsmanagement? Woher weiß man wer die ISL bekommen soll?
   - Erklärung der Entsorgung (Papier und Digital).
   - Bei der Besichtigung wird explizit auf Entsorgung geachtet und Fragen an die Beschäftigten gestellt
   - ISL durch E-Mail mit Empfangsbestätigung an alle Beschäftigten verteilt,
   - Teilnahmebestätigung an MA-Sensibilisierung. Wie wird sichergestellt, dass alle MA Bescheid wissen?
   - IT-Betriebshandbuch: Struktur und Netze, Erklärung der Zugänge, Servicelevel intern/extern

   Großer Punkt:
   - Benutzer- und Rechtekonzept. Wie werden Benutzer angelegt, wer macht dies auf wessen Veranlassung, wo ist das dokumentiert, auch in den einzelnen Fachbereichen? Wer legt an, wer gibt frei, wo steht‘s?
   - Standardfreigaben, außerordentliche Freigaben, etc.? UND wo steht das → Transparenz innerhalb der Verwaltung ist wichtig!
   - Monitoring, Fehlermeldungen, etc.?

Inhalt Zertifizierung: 1. Tag Nachmittag 14h-17.30h

3. In der Folge weiter mit den Unterlagen:

- Netzwerkstruktur (Auch Fotos dazu, Belegung von Switches, LAN Segmente)
- Notfallkonzept nach vorhandener Vorlage (nicht Docusnap) wurde angesehen und hinterfragt, Kommuniziert an Mitarbeiter? Wie die Veröffentlichung dokumentiert?
- Notfallhandbuch kommunizieren (Vorlage genau ausarbeiten und darüber nachdenken, Strom, Netzwerk, Ausstattung etc.), über Mail und Aushangtafeln oder auslegen. Eskalationswege klären, Außenvertretung gegenüber anderen klären, Informationswege klären. Nachbereitung von Vorfällen machen, dokumentieren! Dazu Notfallübungen planen! Was passiert bei Teilausfall, z.B. Stromausfall nur Rathaus, nicht Außenstellen. Wiederanlaufplanung!
- Bei der Besichtigung: Vertragsabteilung und Schlüsselverwaltung angedacht und später auch beide durchgeführt
- Plan für EDV-Erneuerung vorhanden? (z.B. USV)

4. Ab etwa 16 Uhr in ISIS12 Software-Tool:

- Erklärung der MA Sensibilisierung, dazu Unterschriftslisten
- Vorstellung des InfoSichTeam auf Personalversammlung gemacht, dazu per E-Mail
- Aufwand ISB ca. 50% während ISIS12 Einführung, dann 10% laufend OK
- Durch die ISIS12 Software geklickt, alle Felder auf Haken überprüft, Revisionsdaten drin?
- Fragen der einzelnen Schritte durchgegangen, wie wurden diese umgesetzt?
- Prozesse erklären können!
- Dokumentation der Prozesse und der Teilschritte, wie umgesetzt z.B. Änderungsprozess?
- Störungsprozess und Dokumentation? (OTRS 5 free)
- Überwachung des Netzes mittel LanGuard gezeigt

...