KEYLDO
... Businessprocess- and IT-Consulting

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Praxistipps – Informationssicherheit und Datenschutz für kleine Kommunen

Nürnberg, den 19.10.2017

Ulla Ohaus
Keyldo GmbH
Talblickstraße 63
75305 Neuenbürg

Tim Hermann
Büro Mayer GmbH & Co KG
Emil-Kemmer-Straße 11
96103 Hallstadt

Begrüßung und Einführung

- Hintergründe
  - Was bedeutet Informationssicherheit ?
  - Was ist ein Informationssicherheitskonzept ?
  - Was unterscheidet ein Informationssicherheitskonzept von einem ISMS ?
  - Warum benötigen Kommunen ein Informationssicherheitskonzept ?
  - Bis wann ist das Informationssicherheitskonzept einzuführen?
  - Was ist konkret zu tun?
- Umfang
  - Überblick über die Standards
  - Was ist sinnvoll für wen ?
  - Was ist konkret zu tun ?
  - Wie sieht die zeitliche Kalkulation aus ?

Was bedeutet Informationssicherheit ?

Informationssicherheit ist *der Schutz von*

- wichtigen
- durch Rechtsvorschriften

zu schützenden Informationen vor →

- Änderung
- Missbrauch
- Verlust
- Zerstörung

Dabei wird KEIN Unterschied zwischen

- analogen oder digitalen
- personenbezogenen oder nicht personenbezogenen

Daten gemacht.

Aspekte der Informationssicherheit

- Personell
  - Umgang mit Mitarbeitern
    - vor
    - während
    - nach

    der Anstellung

→
- Wissenssicherung
- Verantwortlichkeiten
- Schulungen
- Anweisungen
- etc.

- Rechtlich
  - Auflagen
  - Datenschutz
  - Sozialgesetzbüchern
  - Spezialgesetzen wie
    - EGovernment Gesetze
    - Verwaltungsverfahrensgesetze
    - EU-DSGVO zum Mai 2018

4 Aspekte der Informationssicherheit

- Personell
- Rechtlich
- Technisch
- Organisatorisch

Aspekte der Informationssicherheit

- Technisch
  - Beschaffung
  - Betrieb
  - Veränderung

  } der EDV Technologie
- Organisatorisch
  - Änderung von Raumnutzungen
  - neue zusätzliche Gebäude/ Räume
  - neue Mitarbeiter / Stellenwechsel
  - neue Zulieferer
  - neue / veränderte Gesetze
  - Richtlinien
  - Prozesse
  - etc.

Was unterscheidet ein Informationssicherheitskonzept von einem ISMS

Informationssicherheitsmanagementsysteme (ISMS) bieten:

- ISO 27001
- BSI IT-Grundschutz
- ISIS12
- ISA+ (Informationssicherheits-Analyse)
- VdS3473

→ eine bewährte Systematik zur
- Einführung
- Aufrechterhaltung

von Informationssicherheit in Organisationen an.

→ Maßnahmen
- zur Risikoidentifikation
- Maßnahmenplanung

→ Verfahrensweisen, die einen kontinuierlichen Betrieb der Systematik sicherstellen.

→ Prüf- bzw. Zertifizierbarkeit und können von unabhängiger Stelle geprüft werden.

Bei erfolgreicher Prüfung erfolgt ein Nachweis darüber und regelmäßige Nachprüfungen erfolgen.

Was ist ein Informationssicherheitskonzept?

Konzeptlösungen

- Innovationsstiftung Bayerische Kommune

- Vorgehensweisen
  - zur Identifikation von Risiken
  - zum Umgang mit diesen Risiken
  - zur Entwicklung einer „Sicherheitskultur“

- Verantwortliche Personen mit
  - ausreichend Zeit
  - Mitteln

  } zum Betrieb des Sicherheitskonzepts

- Regeln, Richtlinien und Anweisungen → für die Organisation und die Mitarbeiter zur Umsetzung und dem Betrieb des Konzepts

- Maßnahmen zur kontinuierlichen Schulung und Sensibilisierung für Informationssicherheit.

Was unterscheidet ein Informationssicherheitskonzept von einem ISMS ?

	Konzeptlösung	ISMS
Verantwortliche Personen		
Regeln		
Richtlinien		
Anweisungen		
Verfahren die einen kontinuierlichen Betrieb der Systematik gewährleisten		
Maßnahmen zur kontinuierlichen Schulung der Mitarbeiter		
Maßnahmen zur Sensibilisierung der Mitarbeiter		
bewährte Systematik		
Möglichkeit zur Zertifizierung		
Risiko Prüfkataloge		

Wer die Wahl hat,.....

Alle Managementsysteme (ISMS) wie auch Konzepte haben Gemeinsamkeiten

- sie erledigen sich nicht von selbst
- sie erfordern einen erheblichen internen Zeit-, Personal- und Budgetaufwand

→ Je weniger interne Ressourcen zur Verfügung stehen,
umso mehr muss auf externe Unterstützung zurückgegriffen werden

- das Thema Informationssicherheit ist keineswegs komplett auslagerbar

Der Implementierungsaufwand von Informationssicherheit unterscheidet sich lediglich in der Ausprägung der Maßnahmen.
Der Einführungsaufwand ist nahezu identisch ob ein ISMS oder eine Konzeptlösung gewählt wird.

Gesetzliche Situation in der BRD

	Eigenes Gesetz	Änderung des Verwaltungsverfahrensgesetzes	Anpassung des Landesverwaltungsrecht
Baden-Württemberg			
Bayern			
Berlin			
Brandenburg			
Bremen			
Hamburg			
Hessen			
Mecklenburg-Vorpommern			
Niedersachsen			
Nordrhein-Westfalen			
Rheinland-Pfalz			
Saarland			
Sachsen			
Sachsen-Anhalt			
Schleswig-Holstein			
Thüringen			

Warum benötigen Kommunen ein Informationssicherheits-konzept?

Am Beispiel Bayern !!!

Artikel 8 Absatz 1;2 BayEGovG:

- *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.*

Mindestanforderung
Die Einführung eines Informationssicherheitskonzeptes
z.B.: Innovationsstiftung Bayerische Kommune

Artikel 10 Absatz 2 BayEGovG:

- *1 Dieses Gesetz tritt am 30. Dezember 2015 in Kraft.*
- *2 Abweichend von Satz 1 treten in Kraft:*
  [...] 3. Art. 8 Abs. 1 Satz 2 am 1. Januar 2018.

ab dem 1. Januar 2018
ist es ERFORDERLICH
den Nachweis führen zu können

Überblick über die Standards und Vorgehensweisen

- BSI
- ISO27001
- ISIS12
- ISA+
- VDS3473

} Informationssicherheitsmanagement Systeme (ISMS)

- Innovationsstiftung Bayrische Kommune

→ Informationssicherheitskonzept

Was ist konkret zu tun?

- Grundlagen zur Einführung und zur Aufrechterhaltung von Informationssicherheit
- Grundlegende Umsetzungen im Datenschutz (auf Basis des gültigen Datenschutz Gesetzes) als elementarer Bestandteil der Informationssicherheit
- Gebäudesicherheit
- Zugang zu IT-Systemen
- Berechtigungskonzepte und Protokollierung
- Notfallmanagement (Vorsorge und Notfallplan)
- Richtlinien und Dienstanweisungen
- Schulungen und Sensibilisierung – Mitarbeiter als elementarer Bestandteil der Informationssicherheit
- Externe Dienstleister – Anforderungen an externe Dienstleister, nicht nur im Rahmen einer Auftragsdatenverarbeitung

Was kostet das ganze ???

Was ist konkret zu tun?

Der Standard sieht 18 Abschnitte vor

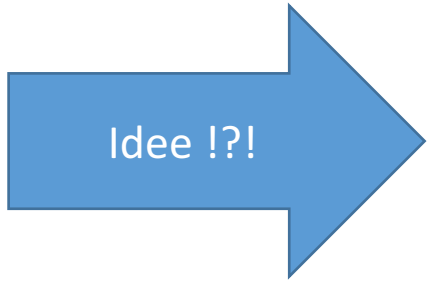
1.	Allgemeines	4 Dokumente
2.	Normative Verweise	1 Dokument
3.	Glossar	1 Dokument
4.	Organisation der Informationssicherheit	6 Dokumente
5.	Leitlinie zur Informationssicherheit	1 Dokument
6.	Richtlinien zur Informationssicherheit	2 Dokumente
7.	Personal	1 Dokument
8.	Wissen	2 Dokumente
9.	Identifikation kritischer IT-Ressourcen	3 Dokumente
10.	IT Systeme	21 Dokumente
11.	Netzwerke & Verbindungen	5 Dokumente
12.	Mobile Datenträger	In 9. enthalten
13.	Umgebung	1 Dokument
14.	IT-Outsourcing & Cloud Computing	In 9. enthalten
15.	Zugänge und Zugriffsrechte	2 Dokumente
16.	Datensicherung & Archivierung	10 Dokumente
17.	Störungen & Ausfälle	3 Dokumente
18.	Sicherheitsvorfälle	2 Dokumente

→ 65 Dokumente

16 Dokumente Schulungsrelevant

Was kann ein seriöser Anbieter leisten?

- Vom Coaching bis zur vollständigen Umsetzung!
- Die Dimensionierung und Entscheidung liegt bei Ihnen!
- Der Dienstleister hat sämtliche Vorlagen (Templates) die erforderlich sind.
- Der Dienstleister hat das Know How, das zum Befüllen der Vorlagen erforderlich ist.
- Sie haben die erforderlichen Inhalte



Mögliches Vorgehen

Bildung von Arbeitsgruppen aus mehreren Kommunen
- Erarbeitung der grundlegenden Aspekte und Dokumente im Plenum

Individuelle Aspekte jeder Kommune können im Coaching umgesetzt werden
- Der Anbieter ist bei Ihnen vor Ort und unterstützt in dem von Ihnen gewählten Maß

KEYLDO
... Businessprocess- and IT-Consulting

über 80 Jahre | Tradition & Innovation

BÜRO MAYER
IT-Systemhaus & Service

Wie sieht die zeitliche Kalkulation aus?

18 Abschnitte, 65 Dokumente und Schulung

1. Allgemeines
2. Normative Verweise
3. Glossar
4. Organisation der Informationssicherheit
5. Leitlinie zur Informationssicherheit
6. Richtlinien zur Informationssicherheit
7. Personal
8. Wissen
9. Identifikation kritischer IT-Ressourcen
10. IT Systeme
11. Netzwerke & Verbindungen
12. Mobile Datenträger
13. Umgebung
14. IT-Outsourcing & Cloud Computing
15. Zugänge und Zugriffsrechte
16. Datensicherung & Archivierung
17. Störungen & Ausfälle
18. Sicherheitsvorfälle

Planspiel
Annahme:
1) 5 Kommunen arbeiten zusammen
2) Alle Kommunen implementieren VdS 3473

Planspiel
Annahme:
1) 5 Kommunen arbeiten zusammen
2) Alle Kommunen implementieren VdS 3473

Projekt Arbeitszeit pro Kommune

Ca. 191 Stunden → Ca. 24 Tage

129 Stunden → 16 Tage

62 Stunden → 7,75 Tage Individuell & Schulung

Worauf Sie bei der Beratungswahl achten sollten!

1) Für ein ISMS benötigt man per Definition ***KEINE*** besondere Software

2) Dokument Vorlagen und Templates sind das Werkzeug des Anbieters
   – oder kaufen Sie den Schraubenschlüssel für die Autoreparatur?

3) Das Projekt wird so aufgebaut, dass Sie als Kunde ***JEDERZEIT*** den Anbieter wechseln können

4) Sie haben die Wahl, wieviel Eigenleistung Sie erbringen wollen,
   der seriöse Berater stellt Ihnen die richtigen Fragen zur Selbsteinschätzung

5) Die ***PFLICHT*** als Berater hinsichtlich potentieller Risiken und Konsequenzen wird wahr genommen
   BSP.: Bundes Netz Agentur

6) Der Anbieter versucht *EIGENSTÄNDIG* mit Ihnen den für Sie ***günstigsten Weg*** zu wählen
   ohne ein RISIKO einzugehen

Wir freuen uns nun, auf Ihre Fragen und anregende Gespräche mit Ihnen!

Ulla Ohaus
&
Tim Hermann