HST SYSTEMTECHNIK

IT-Sicherheit in der kommunalen Wasserwirtschaft am

Agenda

1. Einführung
2. Ist Situation
3. Reales Beispiel aus der Praxis
4. Definition der Schutzziele
5. IT-Sicherheit - Standards
6. Vorgehensweise zur Einführung

Einführung

Die Informationssicherheit in Kommunen ist eng mit deren Aufgabenerfüllung verbunden. Sie ist mittlerweile zum kritischen Schlüssel für verlässliches und nachvollziehbares Verwaltungshandeln geworden. Über die letzten Jahrzehnte hat dabei die Sicherheit der Informationstechnik (IT) einen größeren Stellenwert eingenommen. Die Komplexität der IT, der hohe Grad der Vernetzung und die Abhängigkeit der Verwaltung von IT-gestützten Verfahren verlangen nach einer Systematisierung und Organisation der Informationssicherheit – nach einem Informationssicherheits-Managementsystem (ISMS). **Die Grundlage für ein solches ISMS ist ein Bekenntnis der Behördenleitung zur Informationssicherheit.** Dieses Bekenntnis wird durch eine Informationssicherheitsleitlinie (ISLL) verbrieft.

Quelle: Deutscher Städtetag: Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen (11/2014)

Einführung – Ist-Situation

- **Stetige Steigerung der Komplexität der IT-Landschaft**
  - Steigender Vernetzungsgrad (M2M, GIS, ERP, PLS….)
  - IT-Verbreitung und Durchdringung (Internet der Dinge, Mobile Geräte)
  - Verschwinden von Netzgrenzen (wo läuft denn meine Anwendung? / Cloud-Anwendungen…)
  - Kürzere Angriffszyklen
  - Höhere Interaktivität von Anwendungen. (Paypal nutzt Facebook Account)

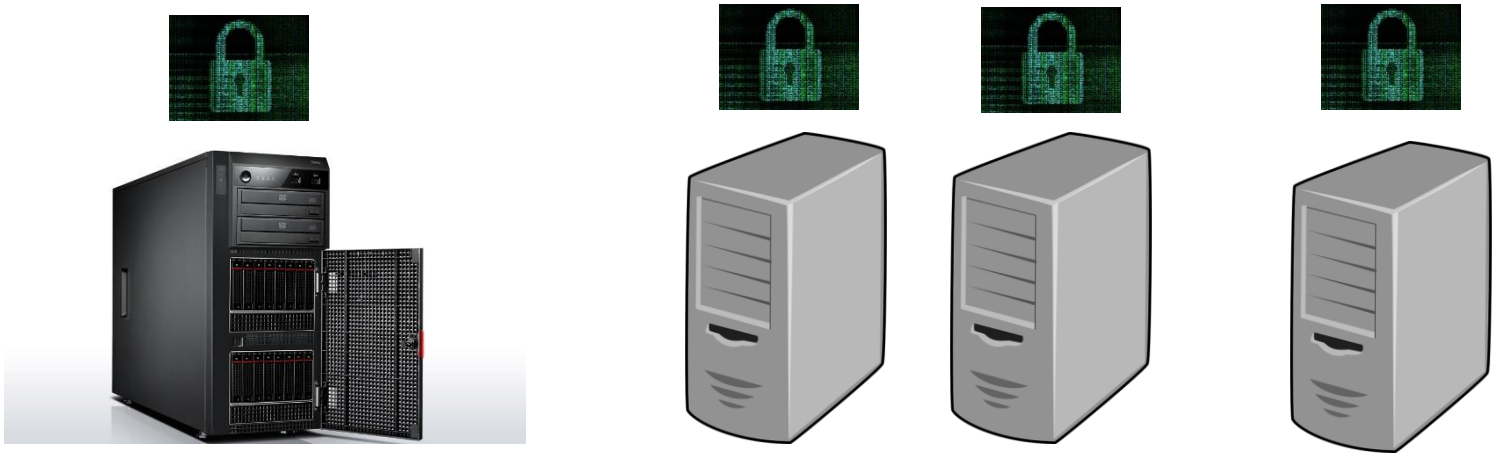
- **Fehlendes Know How der Betreiber**
  - Kerngeschäft ist das Betreiben wasserwirtschaftlicher Anlagen und nicht die Administration der IT-Infrastruktur

- **Anforderungen des Gesetzgebers**
  - Der Gesetzgeber fordert die Sicherung der IT-Infrastruktur IT-Sicherheitsgesetz (KRITIS)

Einführung – Ist-Situation – Beispiel aus der Praxis

Während der Nachtschicht surft eine Mitarbeiter eines Wasserwerkes über den Leitsystemarbeitsplatz im Internet. Dabei fällt der Mitarbeiter einer Ransomware - Attacke zum Opfer.

Einführung – Ist-Situation – Beispiel aus der Praxis



Ergebnis:

- Auf allen über den infizierten Arbeitsplatz erreichbaren Server und Arbeitsplatzrechner werden sämtliche Festplatten verschlüsselt und das gesamte IT-System kann nicht mehr genutzt werden.
- Keine Überwachung und Steuerung des Wasserwerks über das Leitsystem möglich
- Hohe Geldforderung des „Hackers“ an den Betreiber
- Hohe Wiederherstellungskosten des IT-Systems
- Hohes Gefahrenpotential, da ohne das Leitsystem die Anlage nahezu blind gefahren wird

Einführung

Top 10 Bedrohungen (BSI 01.08.2016)

1. Social Engineering und Pishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet/Intranet
4. Einbruch über Fernwartungszugänge
5. Menschliches Fehlverhalten und Sabotage
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet- und Cloud-Komponenten
9. (D)DoS Angriffe
10. Kompromittierung von Smartphones im Produktionsumfeld

Einführung

Bedrohungen resultieren aus Angriffen oder Ereignissen die aufgrund existierender Schwachstellen Schäden verursachen

USB - Geräte

Emails - Anhänge

Definition der Schutzziele

Verfügbarkeit

Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein

Authentizität

Die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft ist gewährleistet

Vertraulichkeit

Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. geändert werden. Das gilt sowohl für den Zugriff auf gespeicherte Daten als auch während der Datenübertragung

Integrität

Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.

Einführung - ISMS

- Unkoordinierte Einzelmaßnahmen können keinen ausreichend sicheren IT-Betrieb gewährleisten und sind nicht geeignet, die eigenen Bemühungen um einen sicheren IT-Betrieb gegenüber Kunden oder dem Gesetzgeber nachzuweisen.

- Ein strukturiertes Vorgehen mit definierten Prozessen und die Dokumentation dieses Vorgehens ist daher erforderlich.

- Standardisierte Verfahren erleichtern eine solche Herangehensweise und ermöglichen die Bemühungen unterschiedlicher Organisationen zu vergleichen und zu bewerten.

- Im deutschsprachigen Raum sind mit der Norm ISO/IEC 27001 und dem BSI-Grundschutz zwei Standards weit verbreitet, die den Aufbau eines Managementsystems für Informationssicherheit (ISMS) in Organisationen beschreiben.

Welche Standards gibt es für ein ISMS

ISO27000-Reihe: Internationaler Standard

ISO27001: Informationssicherheits-Managementsysteme
114 zu behandelnde Maßnahmen (Controls)

ISO27002: Risikoanalyse und Handlungsanweisungen
123 Kontrollpunkte (Kochrezept zur Umsetzung)

ISO27004: Bewertung der Umsetzung und Wirksamkeit anhand verschiedener Kenngrößen

ISO27005: Rahmenempfehlungen zur Risikoanalyse

- Aktueller Stand in deutscher Sprache ist die ISO27001:2013
- Zertifizierung möglich

Welche Standards gibt es für ein ISMS

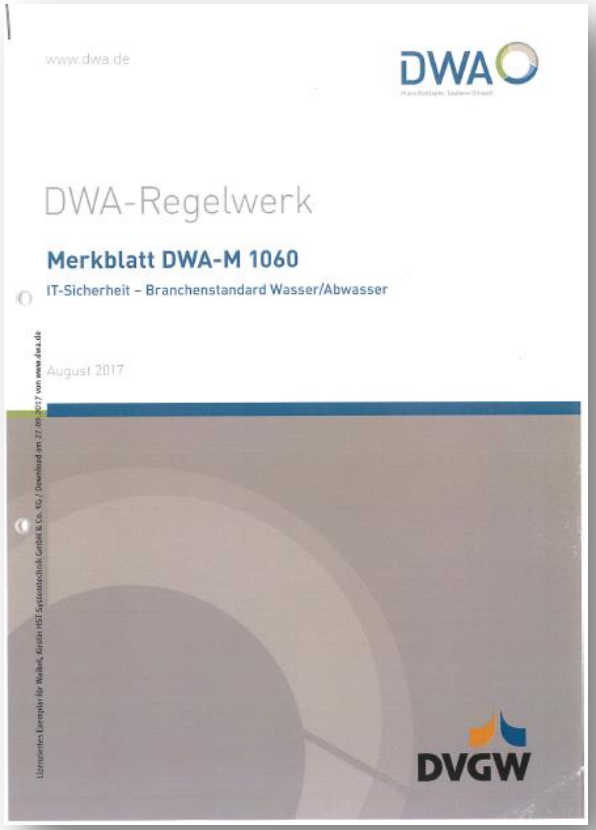
BSI Grundschutz: Nationaler Standard, IT-Grundschutzkompendium (wird jährlich nach dem Stand der Technik aktualisiert)

BSI 200-1	Management für IT-Sicherheit (10/2017)
BSI 200-2	IT-Grundschutz Methodik (Kochrezept)
BSI 200-3	Risikoanalyse auf Basis IT-Grundschutz
BSI 200-4	Notfallmanagement

Zertifizierung möglich

Welche Standards gibt es für ein ISMS

Branchenstandard DWA-M 1060 (08 2017)



Branchenspezifischer IT-Sicherheits-standard (B3S) für den Sektor Wasser – Trinkwasserversorgung und Abwasserbeseitigung.

IT-Sicherheitsleitfaden

Web Applikation zum Merkblatt DWA M1060

- Beinhaltet einen Katalog von IT-Schutzmaßnahmen
- Beinhaltet Anwendungsfälle und die dazu gehörigen Gefährdungskataloge

Einführung

ISMS: Informations-Sicherheits-Management-System

- Ableitung von Erkenntnissen aus den Befunden der Check-Phase
- Ableitung von Korrektur- und Vorbeugemaßnahmen
- Rückführung der Korrekturen in den Plan

- Festlegen der Zielsetzung
- Analyse der Problemursachen
- Abgrenzung der Rahmenbedingungen
- Erfolgskriterien abstecken zur Bemessung der Wirksamkeit
- Planung und Konzeption von Lösungen

- Überprüfung der Umsetzung mit ihren Ergebnissen
- Abgleich mit dem Plan
- Beurteilung der Wirksamkeit der bisherigen Maßnahmen

- Umsetzung und Kommunikation des Plans und Lösungskonzepts

Beispiel ISMS-Tool

- Der Aufbau und Betrieb eines solchen Managementsystems ist aufwendig und komplex, so dass hier eine Unterstützung durch spezialisierte Softwaresysteme wünschenswert ist.

  Im Sprachgebrauch wird hier der Begriff ISMS-Tool verwendet

Zusammenfassung ISMS

- **Ein ISMS Tool ist ein geeignetes Hilfsmittel zur Umsetzung eines Informationssicherheitsmanagements**

- **Strukturierte Dokumentation aller wichtigen Assets**
- **Integrierter Maßnahmenkatalog nach ISO 27001 / BSI Grundschutz / Branchenstandard**
- **Dokumentation aller Prozesse**
- **Risikoanalyse**
- **Checklisten zur Umsetzung**
- **Automatische Erinnerungsfunktion**
- **Lebenslauf für alle Assets**
- **Interne und externe Audits**

Vorgehensweise zur Umsetzung eines ISMS

Schritt 1 → Managementunterstützung für ISMS Einführung und Aufbau

Schritt 2 → Festlegung des Geltungsbereiches
Festlegung der Sicherheitsleitlinie (ISMS Policy)

Schritt 3 → Organisationsanalyse, Schutzbedarfsanalye

Schritt 4 → Risikoanalyse
Identifikation von Risiken, Erstellen von Kontrollmechanismen und Maßnahmen

Schritt 5 → (Aus-) Gestaltung des ISMS

Risikoanalyse

Das Risiko eines Assets ergibt sich aus der Eintrittswahrscheinlichkeit und der Beeinträchtigung, die bei Ausfall des Assets eintritt.

Vorgehensweise zur Einführung

- **Unterstützung der Geschäftsführung einfordern**
  - Das Management überzeugen
  - Vorteile und Risiken verdeutlichen
  - IT-Sicherheit kostet Zeit und Geld

- Projektvorbereitung
  - Den Standard ISO27001 kaufen (€ 187,60)
  - Einsatz externer Berater entscheiden
  - Projektplan aufsetzen
    - Projektmanager festlegen
    - Projektteam festlegen

Vorgehensweise zur Einführung

- **Anwendungsbereich und Absichten des Managements und Verantwortlichkeiten definieren**
  - Dokument „Anwendungsbereich“ erstellen
  - IT-Sicherheitsrichtlinie erstellen

- **Unterstützende Verfahren umsetzen**
  - Verfahren für die internen Audits definieren
  - Verfahren für Korrekturmaßnahmen definieren

- **Risikomanagement durchführen**
  - Methodik für die Risikoeinschätzung entwickeln
  - Risikoeinschätzung durchführen
  - Risikobehandlung durchführen
  - Risikoeinschätzung- und Behandlung dokumentieren

Vorgehensweise zur Einführung

- **Sicherheitsprofil und Aktionsplan zur Zielerreichung entwickeln**
  - Erklärung der Anwendbarkeit entwickeln
  - Plan zur Risikobehandlung entwickeln
  - Restrisiken akzeptieren

- **Maßnahmen umsetzen**
  - Alle Maßnahmen aus dem Plan zur Risikobehandlung umsetzen und dokumentieren

- **Interne Schulung**
  - Mitarbeiter fachlich schulen
  - Bewusstsein - Awareness

Vielen Dank für Ihre Aufmerksamkeit ☺

HST SYSTEMTECHNIK

IT-Sicherheit in der kommunalen Wasserwirtschaft am