www.dvgw-cert.com

Informationssicherheit kritischer Infrastrukturen: Wie schützen wir unsere moderne Gesellschaft?

Kolloquium EUROLAB-D, Berlin 24.4.2018

Gabriele Schmidt / Geschäftsführerin der DVGW CERT GmbH

Themen

- Gesetzliche Rahmenbedingungen
- Was sind kritische Infrastrukturen?
- Anforderungen an die kritische Infrastruktur?
- Was bedeutet Informationssicherheit für kritische Infrastrukturen?
- Was ist Informationssicherheitsmanagement?

Verletzlichkeitsparadoxon

Der Umstand, dass sich mit zunehmender Robustheit und geringerer Störanfälligkeit ein durchaus trügerisches Gefühl von Sicherheit entwickelt und die Auswirkungen eines „Dennoch-Störfalls" überproportional hoch sind, wird als „Verletzlichkeitsparadoxon" bezeichnet.
(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)

Informationssicherheit kritischer Infrastrukturen

Gesetzliche Rahmenbedingungen

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Gesetzliche Rahmenbedingungen

„Evolution“ des Bewusstseins

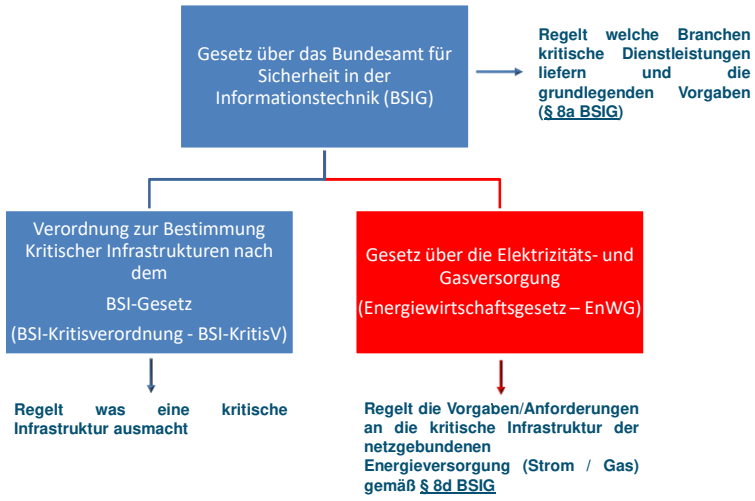
- USA: Bereits 1996 „Critical Infrastructure Protection Program”
- EU: 2004 „European Programme for Critical Infrastructure Protection (EPCIP)”
- EU: Direktive EU COM (2006) 786
- D: 2009 Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) vom Bundesministerium des Inneren
- D: 2009 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
- D: 2011 Cybersicherheitsstrategie für Deutschland
- D: 2015 IT-Sicherheitsgesetz (IT-SiG)
- EU: 2016 NIS-Richtlinie
- D: 2016: Cybersicherheitsstrategie 2016
- D: 2016/2017 BSI-Kritisverordnung (BSI-KritisV)

Informationssicherheit kritischer Infrastrukturen
Gesetzliche Rahmenbedingungen

Das IT-SiG umfasst Änderungen an:

- BSI-Gesetz (BSIG)
- Atomgesetz (AtG)
- Energiewirtschaftsgesetz (EnWG)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Bundesbesoldungsgesetz (BBG)
- Bundeskriminalamtgesetz (BKAG)

Informationssicherheit kritischer Infrastrukturen
Gesetzliche Rahmenbedingungen



Informationssicherheit kritischer Infrastrukturen

Was sind kritische Infrastrukturen?

Informationssicherheit kritischer Infrastrukturen
Was sind kritische Infrastrukturen

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) definiert …

… wer Betreiber Kritischer Infrastruktur im Sinne des BSIG ist.

Bewertung erfolgt aufgrund einer Methodik:

1. Welche Dienstleistung ist wegen ihrer Bedeutung kritisch?
2. Welche Anlagen werden für die Erbringung kritischer Dienstleistungen benötigt?
3. Ab welchem Versorgungsgrad ist die Anlage für die Erbringung kritischer Dienstleistung von Bedeutung (kritische Infrastruktur)?
   - Schwellenwerte (Einwohnereinheiten) nicht die Größe des Versorgungsgebiets

Informationssicherheit kritischer Infrastrukturen
Was sind kritische Infrastrukturen

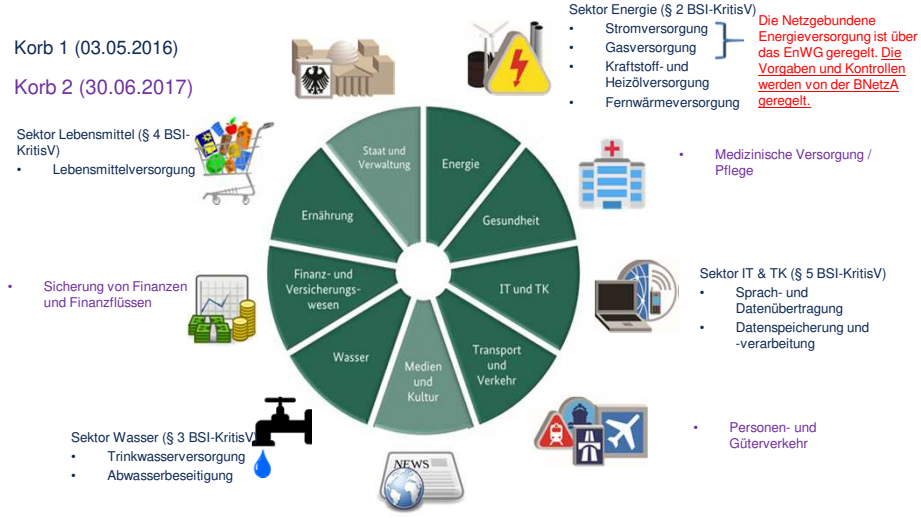
Korb 1 (03.05.2016)

Korb 2 (30.06.2017)

Sektor Energie (§ 2 BSI-KritisV)
- Stromversorgung
- Gasversorgung
- Kraftstoff- und Heizölversorgung
- Fernwärmeversorgung

Die Netzgebundene Energieversorgung ist über das EnWG geregelt. Die Vorgaben und Kontrollen werden von der BNetzA geregelt.

Sektor Lebensmittel (§ 4 BSI-KritisV)
- Lebensmittelversorgung



- Medizinische Versorgung / Pflege

- Sicherung von Finanzen und Finanzflüssen

Sektor IT & TK (§ 5 BSI-KritisV)
- Sprach- und Datenübertragung
- Datenspeicherung und -verarbeitung

Sektor Wasser (§ 3 BSI-KritisV)
- Trinkwasserversorgung
- Abwasserbeseitigung

- Personen- und Güterverkehr

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Was sind kritische Infrastrukturen

Wie hoch sind die Schwellenwerte der kritischen Infrastrukturen in den Sektoren Energie und Wasser?

Festlegung Regelschwellwerte:
500.000 versorgte Personen / Jahr

- Strom:
  - Erzeugung: 420 MW
  - Netz: 3.700 GWh/Jahr
- Gas:
  - Erzeugung / Förderung: 5190 GWh/Jahr
  - Netz: 5190 GWh/Jahr

Hinfällig!!! Es gelten das EnWG bzw. die Vorgaben der BNetzA

- Wasser:
  - Gewinnung / Aufbereitung: 22 Mio m^3/Jahr
  - Verteilung: 22 Mio m^3/Jahr
- Abwasser:
  - 500.000 Einwohner
  - 500.000 Einwohnergleichwerte

Informationssicherheit kritischer Infrastrukturen

Anforderungen an die kritische Infrastruktur?

Informationssicherheit kritischer Infrastrukturen Anforderungen die kritischen Infrastrukturen?

§ 8a BSIG – Sicherheit in der Informationstechnik kritischer Infrastrukturen

Abs. 1 … angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse. Dabei soll der **„Stand der Technik“** eingehalten werden.

Abs. 2 … branchenspezifische Sicherheitsstandards

Abs. 3 … mindestens alle zwei Jahre die Erfüllung dieser Anforderungen auf geeignete Weise (Audits, Prüfungen oder Zertifizierungen) nachweisen und aufgedeckte Sicherheitsmängel an das BSI übermitteln

Informationssicherheit kritischer Infrastrukturen Anforderungen die kritischen Infrastrukturen?

§ 8a BSIG – Sicherheit in der Informationstechnik kritischer Infrastrukturen

Abs. 4 … das BSI kann die Einhaltung der Anforderungen nach Abs. 1 überprüfen

Abs. 5 … das BSI kann Anforderungen an Ausgestaltung des Verfahrens stellen

§ 8d BSIG – Anwendungsbereich

Abs. 2 § 8a ist nicht anzuwenden auf …

… Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Anforderungen die kritischen Infrastrukturen?

Wasserversorgung / Abwasserreinigung

Es gelten die Vorgaben gemäß § 8a BSIG

- einrichten einer 24/7 Meldestelle
- mindestens alle 2 Jahre ein Nachweis gegenüber dem BSI das die Anforderungen gemäß § 8a Abs. 1 BSIG eingehalten werden

Gilt **nur** für Betreiber kritischer Infrastrukturen gemäß BSI-KritisV

Informationssicherheit kritischer Infrastrukturen
Anforderungen die kritischen Infrastrukturen?

Wasserversorgung / Abwasserreinigung

Für das Nachweisverfahren gegenüber dem BSI gilt …

- es müssen die grundlegenden Anforderungen eines Informationssicherheitsmanagementsystems (ISMS) erfüllt sein
- es ist **keine** Zertifizierung
- ein Zertifiziertes ISMS kann als Grundlage des Nachweisverfahren verwendet werden
- **Prüfgrundlagen** für das Nachweisverfahren sind z.B.
  - die Orientierungshilfe zum Nachweisverfahren des BSI
  - Branchenspezifische Sicherheitsstandards (B3S)

Gilt **nur** für Betreiber kritischer Infrastrukturen gemäß BSI-KritisV

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Anforderungen die kritischen Infrastrukturen?

Netzgebundene Energieversorgung (Strom / Gas)

Es gelten die Vorgaben des EnWG bzw. der BNetzA

- Einrichten einer Meldestelle
- Zertifizierung nach IT-Sicherheitskatalog der BNetzA

Gilt für **alle** Betreiber von Energieversorgungsnetzen oder Energieanlagen gemäß EnWG
(Ausnahmen können bei der BNetzA beantragt werden!)

Informationssicherheit kritischer Infrastrukturen

Was bedeutet Informationssicherheit für kritische Infrastrukturen?

Informationssicherheit kritischer Infrastrukturen
Was bedeutet Informationssicherheit?

Informationssicherheit was ist das?

Informationssicherheit hat den Schutz von Informationen als Ziel. *Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.* IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird zunehmend verwendet. Da aber in der Literatur noch überwiegend der Begriff "IT-Sicherheit" zu finden ist, wird er auch in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet.
(www.bsi.de / Stand 23.11.2017)

Informationssicherheit kritischer Infrastrukturen
Was bedeutet Informationssicherheit?

Gewährleistung der Versorgungssicherheit

- Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten
- Materielle, personelle und organisatorische Maßnahmen
- Ganzheitliche Betrachtung der angestrebten Schutzziele (Sicherheitskonzept)

Sicherheitskonzept

- Orginäre IT-Sicherheit
- Physischer Zugriffsschutz
- Zutrittskonzept
- Brandschutz usw.

Berücksichtigung notwendiger Schutzmaßnahmen

- Planung und Erstellung
- Beschaffung
- Beauftragung von Dienstleistungen

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Was bedeutet Informationssicherheit?

Verfügbarkeit

- Ausfälle/Ausfallzeiten der informationstechnischen Systeme, Komponenten oder Prozesse zu vermeiden und ein Zugriff auf die relevanten Daten jederzeit zu ermöglichen

Integrität

- unautorisierte Modifikation der informationstechnischen Systeme, Komponenten oder Prozesse und ihrer Daten zu verhindern

Authentizität

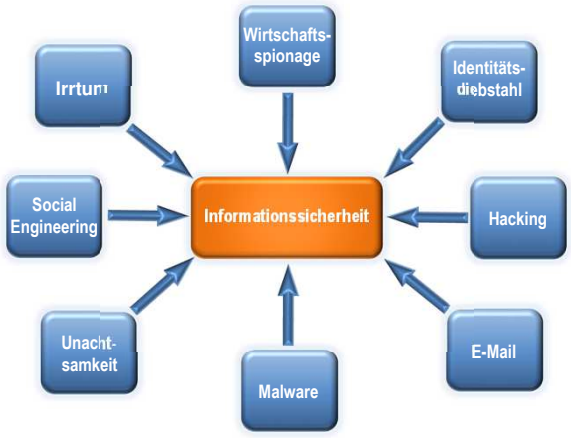
- Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft zu gewährleisten

Vertraulichkeit

- Informationen vor unbefugter Preisgabe zu schützen

Informationssicherheit kritischer Infrastrukturen
Was bedeutet Informationssicherheit?

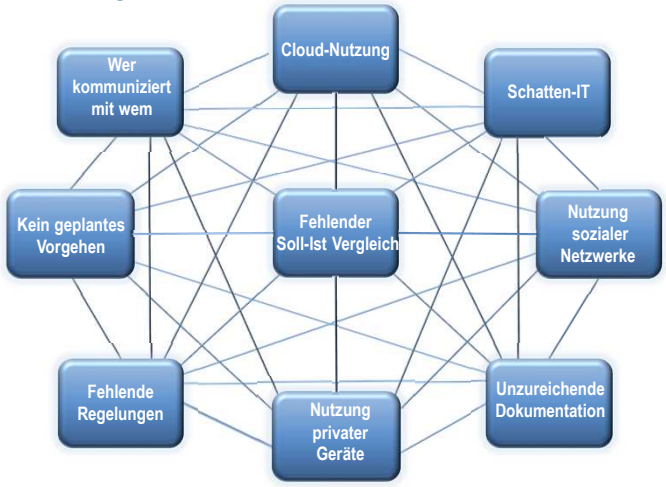
Risiken für die Informationssicherheit



Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Was bedeutet Informationssicherheit?

Problemstellungen in der Informationssicherheit



Informationssicherheit kritischer Infrastrukturen

Was ist Informationssicherheitsmanagement?

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Organisatorische Anforderungen

- Sicherstellung das Stand der Technik (für IT-Systeme) erreicht und aufrechterhalten wird
- Verantwortung für Informationssicherheit liegt bei der obersten Leitung der Organisation
- Festlegen von Verantwortlichkeiten und Befugnissen innerhalb der Organisation
- Organisation nach der Top-Down-Methode
- Überwachung der Einhaltung unterliegt der obersten Leitung
- Zwingend erforderlich sind Verfahren zur Steuerung, Kontrolle und Verbesserung der Informationssicherheit

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Dokumentation der Assets

- Festlegen des Geltungsbereichs
- IT-Komponenten, Systeme sowie Prozesse
- Beschreibung Verwendungszweck, Schnittstellen und Aufstellungsort
- Aufbau der Dokumentation muss eindeutige Identifizierung und Lokalisierung der Systeme ermöglichen
  - z.B. generischer Netzplan mit IT Systemen

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Grundsätzlich Aufgaben

- Identifizierung der (mit der IT verbundenen) Risiken beim Betrieb der Anlagen und den Schutz der kritischen Dienstleistung (kDl)
- Ermittlung geeigneter Maßnahmen zur Vermeidung bzw. Minderung von Risiken

© Can Stock Photo

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Risikoanalyse

- Ermittlung der Eintrittswahrscheinlichkeiten von Gefährdungen
- Es wird **nicht die Schadenshöhe** ermittelt, sondern der Einschränkungsgrad des Anlagenbetriebs bei Eintritt einer möglichen Störung

Risikobewertung

- Risikobestimmung aus Eintrittswahrscheinlichkeit und Einschränkungsgrad
- Kriterien der Risikoakzeptanz definierbar

Oberstes Ziel ist immer der Schutz der kritischen Dienstleistung und deren Bereitstellung.

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Festlegen und Umsetzen von Maßnahmen

- Identifizieren von Maßnahmen die zum Schutz der kritischen Infrastruktur / Dienstleistung beitragen (z.B. physisch / IT / Personal)
- Für jede Maßnahme sind Zuständigkeiten, Verantwortlichkeiten und Fristen für die Implementierung festzulegen
- Dokumentation der notwendigen Informationen

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

Überwachung

- Messen und bewerten von Kennzahlen
- Bewerten von Zielen und Maßnahmen sowie ableiten neuer Ziele und Maßnahmen
- Interne Überwachung (z.B. interne Audits)
- Bewertung des Informationsmanagements durch die oberste Leitung (z.B. Managementbericht / -review)

Kolloquium EUROLAB-D, Berlin 24.4.2018 Gabriele Schmidt, Geschäftsführerin der DVGW CERT GmbH

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

DVGW CERT

- Verantwortung des Top-Managements
- Politik + Ziele festlegen
- Rollen, Verantwortlichkeiten und Befugnisse
- Ressourcen zur Verfügung stellen

- Bewertung durch das Top-Management
- Management-Review
- Ableitung neuer Ziele

- Verwirklichung und Betrieb
- Maßnahmen und Verantwortlichkeiten festlegen und umsetzen
- Kommunikation innerhalb der Organisation

- Überprüfen
- Analysieren
- Korrektur- und Vorbeugemaßnahmen
- Interne Audits

Informationssicherheit kritischer Infrastrukturen
Was ist Informationssicherheitsmanagement?

DVGW CERT

Anerkannte ISMS sind aufgebaut nach …

- DIN EN ISO/IEC 27001
- IT-Sicherheitskatalog gemäß § 11 EnWG
- ISO 27001 Zertifizierung auf Basis von IT-Grundschutz gemäß BSI
- Datenschutzgrundschutzverordnung (DGSVO)

Informationssicherheit kritischer Infrastrukturen
Fazit

Informationssicherheit kritischer Infrastrukturen
Fazit

Unabhängig von der Größe der Organisationen, müssen sich diese auf die moderne Welt einrichten, d.h. nicht nur auf Soziale Medien und wie man sich dort präsentiert.

Organisationen müssen sich für die Gefahren wappnen, die mit der Digitalisierung einhergehen.

Vielen Dank für Ihre Aufmerksamkeit

Ansprechpartner

DVGW CERT GmbH
Josef-Wirmer-Straße 1-3
53123 Bonn

Jan Feldhaus
Teamleiter Managementsysteme
Tel. 0228 / 91 88-881
Email: feldhaus@dvgw-cert.cm

Raimund Alexander
Zertifizierung IT-Sicherheit
Tel. 0228 / 91 88 839
Email: alexander@dvgw-cert.com

Die DVGW CERT GmbH bietet…

- Zertifizierungsverfahren nach DIN EN ISO/IEC 27001
- Zertifizierungsverfahren nach IT-Sicherheitskatalog gemäß § 11 EnWG
- Prüfungsverfahren gemäß § 8a BSI-KritisV (Allgemein und auf Grundlage des B3S-Wasser/Abwasser)
- Zertifizierung „Smart-Meter-Gateway-Administration“ gemäß BSI

Vielen Dank