ITK Sicherheitsgesetz – Umsetzung mit verinice.PRO

verinice.XP- Grundschutztag

15.09.2015

SILA CONSULTING

IT-Security Consulting & Training & Qualifications

Überblick

- Kurze Vorstellung des IT-Sicherheitsgesetzes
- Konkretisierung des Gesetzes für Energieversorger
- Abbildung im verinice für den BSI Grundschutzview.

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

IT-Sicherheit – eigentlich nichts Neues!

BSI-Gesetz (2009-2013)

Informationstechnik,
die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch der Bundesbehörden untereinander oder mit Dritten dient…

IT-Sicherheitsgesetz

Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen

Ausgenommen Kleinstunternehmen: <10 Personen & <2Mio Jahresbilanz

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

IT-Sicherheitsgesetz ein „richtiges“ Gesetz

- Es ist ein Gesetz, aber „nur“ ein Artikelgesetz.
  - Ein Artikel- oder Mantelgesetz ist ein Gesetz, das gleichzeitig mehrere Gesetze oder sehr unterschiedliche Inhalte in sich vereint. Meist werden damit Änderungsgesetze bezeichnet, die eine bestimmte Thematik in einer ganzen Reihe von Fachgesetzen ändern. Für diese Gesetze ist auch die Bezeichnung „Omnibusgesetz“ gebräuchlich, wenn Änderungen, die inhaltlich nichts miteinander zu tun haben, in einem Artikelgesetz zusammengefasst werden. (Quelle Wikipedia)

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Wichtige Gesetze die geändert werden!

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Adressaten des IT-Sicherheitsgesetzes

- Betreiber von Webangeboten
- Telekommunikationsunternehmen
- Betreiber Kritischer Infrastrukturen
  - Absichern der erforderlichen IT zur Erbringung der Dienste nach dem „aktuellen Stand der Technik“
  - Melden von Sicherheitsvorfällen

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Forderungen des IT-Sicherheitsgesetzes (ITSiG)

- Angemessene organisatorischer und technische Vorkehrungen zur Vermeidung von Störungen (Eingesetzte Technik erfüllt die zugedachte Funktion nicht vollständig oder nicht mehr richtig oder es wurde versucht darauf einzuwirken)
- Angemessener Schutz, wenn Aufwand für den Schutz im Verhältnis zur Folge des Ausfalls oder Beeinträchtigung im Gelichgewicht ist
- Notfall und Business-Continuity-Konzepte
- Meldepflicht von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI)
- 2 Jahre Umsetzungsfrist (bis 07/2017)
- Alle 2 Jahre Nachweißpflicht in geeigneter Weise (z.B. Sicherheitsaudits, Zertifizierungen, Penetrationstests)
- Bei Nichterfüllung der Vorgaben Sanktionen bis 100.000 €

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Kritische Infrastrukturen...

Kritische Infrastrukturen

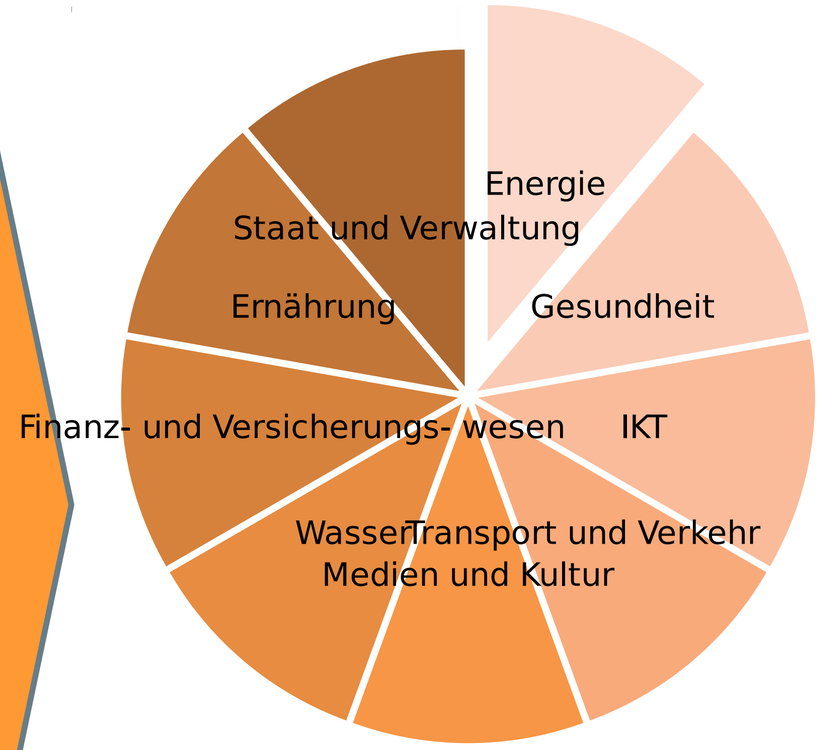
Alle Einrichtungen, welche ein Funktionieren einer arbeitsteiligen Volkswirtschaft garantieren und deren Ausfall enorme Beeinträchtigungen mit sich bringt.

IT-Sicherheitsgesetz

Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen

Ausgenommen Kleinstunternehmen: <10 Personen & <2Mio Jahresbilanz

Sektorspezifische Sicherheitsvorgaben (hier IT-Sicherheitskatalog der BNetzA)



SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Beispiel der Konkretisierung

Energiewirtschaftsgesetz (EnWG) § 11/1a

Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen.

EnWG-Novelle 2011:

Die Regulierungsbehörde (BNetzA) erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen.

Dezember 2013:

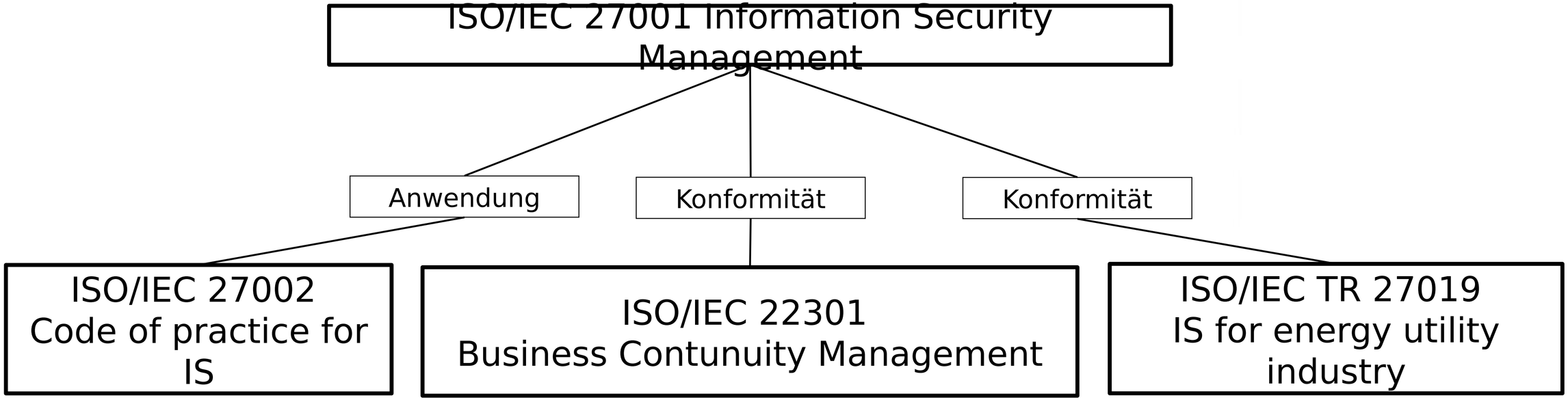
IT-Sicherheitskatalog (BNetzA)

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Wie hängen die Standards zusammen?

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Darstellung der normativen Umsetzung zur Erfüllung der Konformität zu § 11 EnWG (Strom)



- Beinhaltet Empfehlungen für diverse Kontrollmechanismen für die Informationssicherheit
- Eine Zertifizierung nach ISO/IEC 27002 ist grundsätzlich nicht möglich, da es sich bei der Norm um eine Sammlung von Vorschlägen handelt.

- Strategien, Pläne und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden – zu schützen bzw. alternative Abläufe zu ermöglichen.
- Im Rahmen des Managements der Informationssicherheit dient die Norm 22301 zur Implementierung eines BCM-Systems.

- Sektorspezifische Norm ISO/IEC TR 27019 für die EVU-Prozesstechnik
- Berücksichtigung im Rahmen eines ISMS nach ISO/IEC 27001

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Aber Moment mal....

- Eine Zertifizierung nach ISO 27001:2013 kann ein Nachweis sein im Sinne des ITSiG
  - OK kann man erreichen
- Anwendung der ISO 27002 oder anderer „Best Practises“ (BSI Grundschutz 100-2, 100-3)
- Konformität der DIN ISO/IEC TR 27019
  - Nicht ganz einfach denn der Standard verweist auf die ISO27002:2005
  - Die ISO 27001:2013 Annex A Controls sind im ISO27002:2013 beschrieben.
  - Hmm... Was tun sprach Zeus?

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Möglichkeit 1...

MIT VERINICE

- ISM View:
  - Herunterladen der VNA Dateien für ISO 27001:2005
  - Aktualisieren des ISM Verbundes mit der VNA für das Update auf die ISO 27001:2013
- GS-View
  - Verknüpfen der Controls mit den Maßnahmen des Grundschutzes nach der Matchingtabelle
  - Maßnahmen die bei dem Update entfallen sind als zusätzlich Bauteine/Maßnahmen zu erstellen

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Möglichkeit 2...

NATÜRLICH AUCH VERINICE

- GS-View
  - Erstellen eines IT-Verbundes für das SRK
  - Erstellen eines IT-Verbundes für die Steuer und Leittechnik
  - Erstellen eines IT-Verbundes für die Office IT
  - Maßnahmen der ISO 27019 und der verwiesenen ISO27002:2005 als zusätzlich Bauteine/Maßnahmen zu erstellen nach Mapping Tabelle

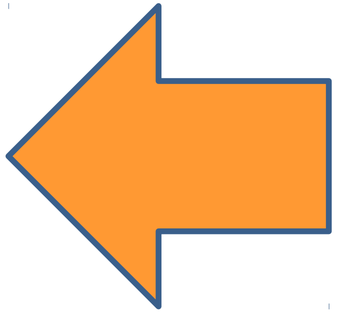
SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Nach Vorgehen des Grundschutzes...

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Beispiel 2

- EVU Dummy IT-Verbund [a917c7]
  - DIN SPEC 27009:2012 0.6.1.1 Engagement des Managements für Informationssicherheit [a917c7]
  - DIN SPEC 27009:2012 0.6.1.2 Koordination der Informationssicherheit [a917c7]
  - DIN SPEC 27009:2012 0.6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit [a917c7]
  - DIN SPEC 27009:2012 0.6.1.4 Genehmigungsverfahren für Informationsverarbeitende Einrichtungen [a917c7]
  - DIN SPEC 27009:2012 0.6.1.5 Vertraulichkeitsvereinbarungen [a917c7]
  - DIN SPEC 27009:2012 0.6.1.6 Kontakt zu Behörden [a917c7]
  - DIN SPEC 27009:2012 0.6.1.7 Kontakt zu speziellen Interessengruppen [a917c7]
  - DIN SPEC 27009:2012 0.6.1.8 Unabhängige Überprüfung der Informationssicherheit [a917c7]
  - DIN SPEC 27009:2012 0.6.2.1 Identifizierung von Risiken in Zusammenhang mit externen Mitarbeitern [a917c7]
  - DIN SPEC 27009:2012 0.6.2.2 Adressieren von Sicherheit im Umgang mit Kunden [a917c7]
  - DIN SPEC 27009:2012 0.6.2.3 Adressieren von Sicherheit in Vereinbarung mit Dritten [a917c7]
  - DIN SPEC 27009:2012 0.7.1.1 Inventar der organisationseigenen Werte (Assets) [a917c7]
    - EM 0.7.1.1 [] Inventar der organisationseigenen Werte (Assets) [a917c7]
    - M 2.1 [A] Festlegung von Verantwortlichkeiten und Regelungen [a917c7]
    - M 2.2 [C] Betriebsmittelverwaltung [a917c7]
    - M 2.4 [B] Regelungen für Wartungs- und Reparaturarbeiten [a917c7]
    - M 2.5 [A] Aufgabenverteilung und Funktionstrennung [a917c7]
    - M 2.6 [A] Vergabe von Zutrittsberechtigungen [a917c7]
    - M 2.7 [A] Vergabe von Zugangsberechtigungen [a917c7]
    - M 2.8 [A] Vergabe von Zugriffsrechten [a917c7]
    - M 2.13 [A] Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln [a917c7]
    - M 2.16 [B] Beaufsichtigung oder Begleitung von Fremdpersonen [a917c7]
    - M 2.18 [Z] Kontrollgänge [a917c7]
    - M 2.37 [C] Der aufgeräumte Arbeitsplatz [a917c7]
    - M 2.39 [B] Reaktion auf Verletzungen der Sicherheitsvorgaben [a917c7]
    - M 2.40 [A] Rechtzeitige Beteiligung des Personal-/Betriebsrates [a917c7]
    - M 2.139 [A] Ist-Aufnahme der aktuellen Netzsituation [a917c7]
    - M 2.177 [Z] Sicherheit bei Umzügen [a917c7]
    - M 2.195 [A] Erstellung eines Sicherheitskonzepts [a917c7]
    - M 2.217 [B] Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen [a917c7]
    - M 2.225 [B] Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten [a917c7]
    - M 2.393 [A] Regelung des Informationsaustausches [a917c7]
    - M 5.33 [B] Absicherung von Fernwartung [a917c7]



Maßnahmen aus der ISO 27019 und der ISO27001:2013

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

ISO27019 mit BSI Grundschutz

- Möglich mit einigen Kniffen
- Beste Möglichkeit:
  - Nutzung der Verknüpfungsmöglichkeiten von verinice
  - Neue Reportingfunktionen für den Nachweis einer Umsetzung
  - Einfach neue Informationen durch neue Bausteine und Maßnahmen erstellen

SILA CONSULTING
IT-Security Consulting & Training & Qualifications

Fragen?!

- ITSiG
- ISO27019 und Grundschutz vereinbar?
- Verinice Anpassungen

- Vielen Dank!

SILA CONSULTING
IT-Security Consulting & Training & Qualifications