Deloitte.

Energiewirtschaft und Digitalisierung

Rechtsrahmen, Umsetzung und Geschäftsmodelle

28. September 2016

Anforderungen an den Netzbetrieb

Anforderungen an den Netzbetrieb

Umsetzung des IT-Sicherheitsgesetzes in der Praxis

Cyber Risiken sind kritische Risiken für die Energiewirtschaft

Hacker bringt deutsches Kraftwerk in zwei Tagen zum Stillstand

Angriff auf das Kraftwerk in Ettlingen (2014)

- "Friendly Attack" auf das Kraftwerk in Ettlingen
- In 2 Tagen verschaffte sich ein Hacker Zugriff auf die kritischen Systeme des Kraftwerkbetreibers
- Für den Angriff wurde keine komplizierte Hard- oder Software verwendet
- Ähnliche Angriffe gefährden andere Betreiber wichtiger Infrastrukturen wie z.B. deutsche Stahlwerke

2 Tage

Targeting	1st Stage Delivery	2nd Stage Delivery	Exploitation
			
Personen und Prozesse	**Applikationen**	**Netzwerk**	**Kraftwerk System**
Netzwerkzugriff nach Spearphishing Angriff per E-Mail auf einen Mitarbeiter	Kompromittierung der Hosts im Unternehmensnetzwerk	Ausweitung auf das Produktionsnetzwerk des Kraftwerks	Angriff endet an dieser Stelle ("Friendly Attack")
Zielsetzung	**Zielsetzung**	**Zielsetzung**	**Zielsetzung**
Zugriff auf die IT-Systeme	Ausweitung des Netzwerkzugriffs und Identifizierung autorisierter Nutzer.	Zugriff auf Steuerungssysteme des Kraftwerks	Angreifer hat die Kontrolle über das Kraftwerksystem erlangt und könnte gezielt z.B. einen Stromausfall auslösen.

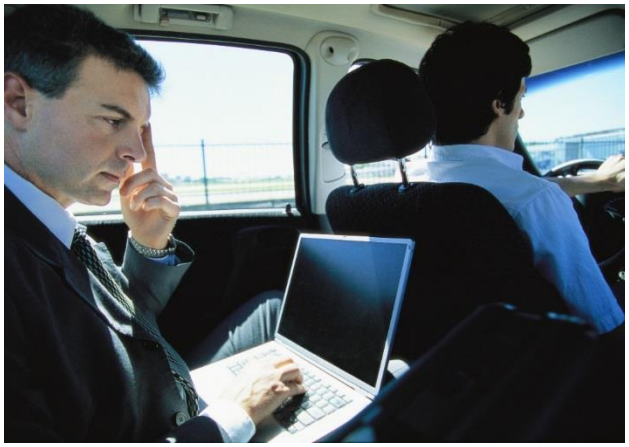
Quelle: http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen

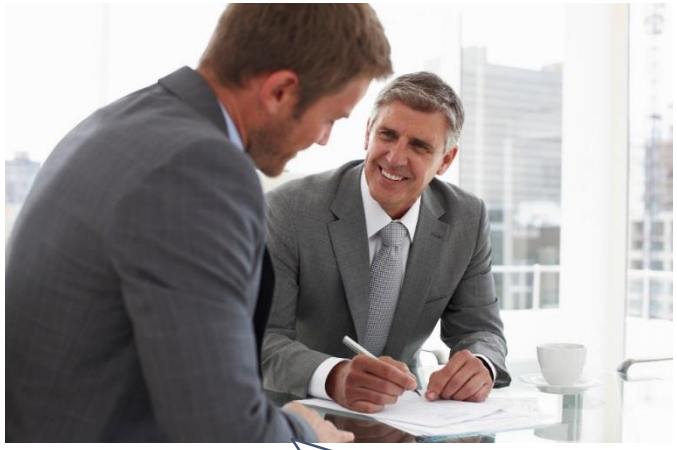
Cyber Risiken betreffen alle Unternehmensteile

Cyber Strategie und Capability Assessment

CEO:
"Es wurde in letzter Zeit sehr viel über Phishing Attacken berichtet. Sind wir gefährdet?"

Board:
"Wie gut sind wir gegen diese Cyber Risiken geschützt?"





Geschäftsbereich:
"Welche Cyber Bedrohungen sind für mein Geschäftsfeld relevant?"

CIO:
"Wie viel und wo muss ich investieren, um unsere Cyber Sicherheit zu stärken?"

Herausforderungen im Energiesektor aus CRS Sicht

Die veränderte Cyber-Gefahrenlage, regulatorische Anforderungen und Veränderungen der digitalen Umwelt werden immer relevanter für E&R Unternehmen

Es sind wachsende Risiken durch Cyber Attacken zu beobachten, die zielgerichtet aber auch ziellos auftreten.
Bsp.: Locky-Trojaner (gezielte Verschlüsselung von Festplatten zur Erpressung von Unternehmen)

Die in der Fernwirktechnik und der Netzleitstelle verwendet Informations- und Kommunikationstechnologie besteht häufig aus Altsystemen, die der modernen digitalen Welt nicht gerecht werden.

IT-Sicherheitsgesetz: KRITIS-sektorübergreifende Betroffenheit in Mehrspartenunternehmen (jedes Stadtwerk)
Gesetz zur Digitalisierung der Energiewende: Einführung des Smart Metering

Diesem unterliegen insbesondere mittelständischen Stadtwerke, die häufig in mehreren Sparten und das IT-Sicherheitsgesetz fallen und denen geringes Budget zur Umsetzung zur Verfügung steht.

Cyber Risk Services

Ausblick

Cyber Readiness (MSS)

Seit Mai 2016 verfügt Deloitte in Deutschland über ein Cyber Intelligence Center (CIC), welches zukünftig auch mit den Unternehmen aus dem Bereich E&R verknüpft werden soll.

Unsere Services:

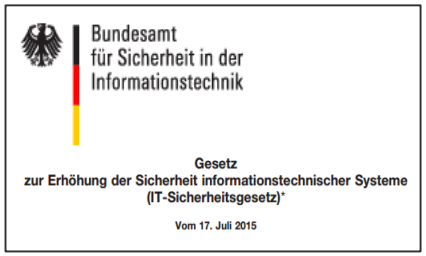
- Cyber Watch
- Cyber Monitor
- Cyber Check
- Cyber Protect
- Cyber Response
- Cyber Govern
- Cyber Academy

Smart Metering

Das Gesetz zur Digitalisierung der Energiewende fordert die Einführung intelligenter Messsysteme, die aus einem digitalen Stromzähler und einer Kommunikationseinheit, dem so genannten Smart Meter Gateway, bestehen.

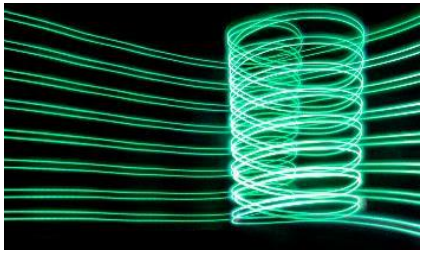
Mögliche Gefahren hierbei sind:

- Manipulation von Daten
- Diebstahl von sensiblen Daten
- Vorbereitung von weiteren Straftaten, z.B. Einbruch



IT-Sicherheitsgesetz

Das kürzlich verabschiedete IT-Sicherheitsgesetz fordert explizit von Unternehmen im Energiesektor die Einführung von Informationssicherheitsmanagementsystemen (ISMS) zum Schutz ihrer Informations- und Kommunikationssysteme vor den stetig wachsenden digitalen Bedrohungen.



Smart Home (Internet of Things)

- Malware in den Smart Home Endgeräten ermöglichen die Manipulation von z.B. Öffnen von geschlossenen Türen oder Ausschalten des Feueralarm [1].

Smart Grid

- Zur effizienten Lastenverteilung werden in intelligenten Netzen (Smart Grids) ITK-Systeme genutzt um diese zu Steuern. Im Fall eines Cyber Angriff könnte z.B. das gesamte Netz zum Stillstand gebracht werden.

[1] Quelle: https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/

Deloitte Cyber Risk Services

SECURE.VIGILANT.RESILIENT.™

Wir bieten die gesamte Bandbreite von Cyber Risk Leistungen, die Strategie und Steuerung mit den Kernelementen des **Secure.Vigilant.Resilient.™** Ansatzes integriert und sich damit über den gesamten Lifecycle von Beratung, Implementierung und Managed Services erstreckt.

Offerings

Cyber Strategy & Transformation		
• Board Education: Cyber Governance • Cyber Risk Strategy	• Cyber Architecture • Third Party Cyber Risk Management	• Cyber Governance, Risk & Compliance • Data Privacy

SECURE	VIGILANT	RESILIENT
• Identity & Access Management • Enterprise Application Integrity • Application Security • Data Protection • Network & Infrastructure Security	• Threat Intelligence • Vulnerability Management • Application Security Monitoring • Security Operations Center	• Cyber War Gaming • Cyber Incident Response • Technology Resilience • Deloitte Cyber Intelligence Centers (CIC)

Delivery methods

Advise			Implement			Manage		
SECURE	VIGILANT	RESILIENT	SECURE	VIGILANT	RESILIENT	SECURE	VIGILANT	RESILIENT

Mittelständischer Energieversorger: ISMS Design & Implementierung

Das IT-Sicherheitsgesetz im Energiesektor

Warum jetzt?

Der voranschreitende Digitalisierungstrend und die damit einhergehenden Cyber Sicherheitsrisiken haben zu neuen Regulierungen geführt, die die Sicherheit kritischer Infrastrukturen gewährleisten sollen. In diesem Kontext fordert das neue IT-Sicherheitsgesetz (IT-SiG) Betreiber kritischer Infrastrukturen dazu auf, ein Informationssicherheitsmanagementsystem (ISMS) nach dem internationalen Standard ISO 27001/27019 und Sektor-spezifischen Regelungen zu implementieren. Das ISMS muss bis Ende Januar 2018 zertifiziert werden.

Die wichtigsten Anforderungen auf einen Blick:

- Ein ISMS auf Basis der Anforderungen des IT-SiG und spezifischen Risikomanagement Prozessen
- Ein ISMS Netzwerkstrukturplan auf Basis der Anforderungen des IT-SiG und eine Bestandsaufnahme aller Assets
- Eine Kontakt-/Meldestelle zur Meldung von Cyber Security Incidents und zum Informationsaustausch mit der Bundesnetzagentur (BNetzA)

Unsere Vorgehensweise

Vorgehensweise für ein erweitertes ISMS

Analyse	Entwicklung	Implementierung
Analyse von Cyber Kompetenzen basierend auf bereits bestehender IT-Sicherheitsstruktur	Auswertung von Sicherheitsrisiken und Entwicklung präventiver Maßnahmen mit Hinblick auf Restrisiken	Implementierung der Maßnahmen und Entwicklung eines Plans zum Übergang in ein betriebsfähiges Managementsystem

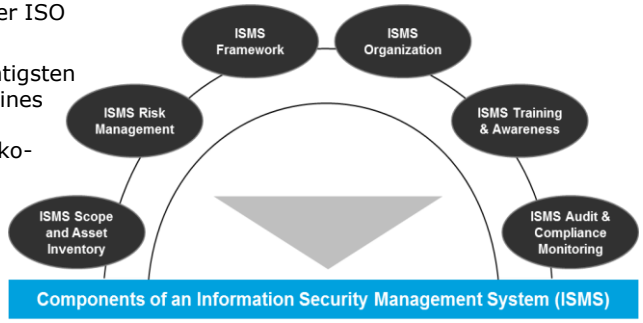
Vorteile

Schutz gegen Cyber Sicherheitsrisiken	Erfüllung der Anforderungen des IT-SiG	Zusammenwirken mit bereits bestehenden Prozessen

Methodik

ISMS im Energiesektor

- Ein ISMS beinhaltet 6 Kernkomponente und beruht auf ISO / IEC 27001
- Diese Komponenten werden ergänzt durch Sektor-spezifische Anforderungen und weitere Regelungen der ISO / IEC 27019
- Eines der wichtigsten Bestandteile eines ISMS ist ein effektives Risiko-management



Beispielprojekt: ISMS für ein mittelständisches städtisches Versorgungsunternehmen

Analyse des IST-Zustands und Aufbau eines ISMS

Sektor	Elektrizität-, Gas-, Wasser- und Heizungsversorgung, Telekommunikation
Scope	Betrieb von Gas- und Elektrizitätsnetzen (minimaler gesetzlicher Geltungsbereich)
Dauer	3 Monate
Ansatz	1. IST-Analyse: Gespräche mit zuständigen Fachbereichen und Auswertung von Dokumenten (2 Wochen). 2. ISMS Aufbau: Durchführung einer Risikoanalyse, die eine Bestandsaufnahme kritischer Assets und einen Entwurf von internen Regelungen beinhaltet (2 ½ Monate). 3. Das ISMS wird anhand einer Roadmap eigenständig vom Kunden implementiert.

Ihre Ansprechpartner für Deloitte Cyber Risk Services sind …

Deloitte.

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
Dammtorstraße 12
20354 Hamburg
Deutschland

Peter Wirnsperger
Partner
Cyber Risk Services

Tel: +49 (0)403 2080 4675
Mobil: +49 (0)172 3690 675
pwirnsperger@deloitte.de
www.deloitte.com/de/cyber

Deloitte.

Deloitte GmbH
Wirtschaftsprüfungsgesellschaft
Schwannstr. 6
40476 Düsseldorf
Deutschland

Zoltan Kerekes
Director
Cyber Risk Services

Tel: +49 (0)211 8772 2426
Mobil: +49 (0)151 5807 1067
zkerekes@deloitte.de
www.deloitte.com/de/cyber