VICCON

CONSULTING

# Energy Security Management

Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements in der Energiebranche

**IMPRESSUM**

Broschüre: Energy Security Management
Ein innovativer Ansatz für die Weiterentwicklung des Sicherheitsmanagements in der Energiebranche

## DIGITALE TRANSFORMATION

*Die Energiewende, die sich durch den Umstieg auf erneuerbare Energien auszeichnet, bedeutet im Kern eine Verlagerung der Erzeugung von zentralen auf dezentrale Einheiten.*

Energy im Kontext dieses Dokuments meint die Erzeugung, den Transport, den Handel, die Verteilung und die Nutzung von Energie. Dafür sind Geschäftsprozesse und Infrastrukturen vorhanden, die zentral oder dezentral organisiert sind. Der Energiesektor ist europäisch, schließt man die Rohstoffbeschaffung ein, sogar international vernetzt. Er umfasst konventionelle Rohstoffe wie Kohle, Gas oder Kernbrennstoffe als auch erneuerbare Energien wie Wasser, Wind oder Sonne und hat starke politische und sicherheitstechnische Bedeutung für Nationalstaaten. Aus diesem Grund ist der Sektor reguliert und nicht selten vollständig oder in Teilen in staatlicher Hand.

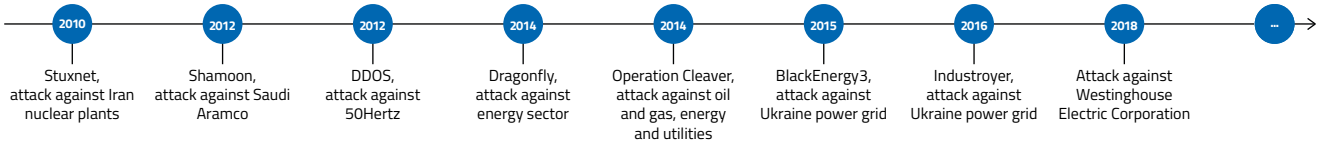
Die Energiewende, die sich durch den Umstieg auf erneuerbare Energien auszeichnet, bedeutet im Kern eine Verlagerung der Erzeugung von zentralen auf dezentrale Einheiten. Die voranschreitende Dezentralisierung der Produktion, der Speicherung und des Handels mit Energie verlangt nach vernetzter und digitaler Steuerung sowie immer mehr Datenaustausch. Die Konnektivität wächst mit jeder digitalen Komponente, egal ob im Kraftwerk oder im Haushalt. Ebenso bedeutet es eine Verlagerung der Stromerzeugung von großen Kraftwerksturbinen auf vielfältig verteilte Erzeugung. Diese Verlagerung geht mit der Entwicklung einher, dass die Energiesicherheit immer weniger von Systemen abhängt, die nach physikalischen und deterministischen Gesetzen arbeiten, sondern immer mehr von informationstechnischen Systemen, die diese Eigenschaften nicht besitzen, den Grad an Zuverlässigkeit nicht aufweisen und auf Grund ihrer inhärenten Schwachstellen eher probabilistischer Natur sind. Wurden früher analoge Systeme in konventionellen und nuklearen Bereichen auf 30 bis 40 Jahre ausgelegt, so sind heute digitale Komponenten nach 10 Jahren aus der Wartung der Hersteller. Und ohne Support und Wartung sind IT-basierte Systeme nicht langfristig sicher zu betreiben. Das Internet der Dinge (IoT), die maschinelle und auf Automatisierung basierte Vernetzung von Geräten bringen mehr Flexibilität und Effizienz, aber gleichzeitig neue Schwächen und Gefahren. Alles ist mit allem informationstechnisch verbunden. Eine oft fehlende technische Ausgereiftheit digitaler Systeme, die fehlende langfristige Auslegung von Komponenten und die Angreifbarkeit von inhärenten systemischen oder informationstechnischen Schwachstellen stellt für die gesamte Energiewirtschaft eine enorme Herausforderung bei der digitalen Transformation dar.

## CYBER ATTACKS

Da die Energieversorgung zu den Kritischen Infrastrukturen gehört, ist sie ein interessantes Ziel für professionelle nicht-staatliche und auch staatliche Akteure. Die Sabotage von Energieinfrastrukturen durch Cyber-Angriffe ist ein reelles Szenario, bei Strom häufig mit regionalen, nationalen oder auf Grund des europäischen Stromnetzverbunds auch mit transnationalen Auswirkungen.

In der Vergangenheit gab es immer wieder „Cyber-Unfälle", also den Befall von Systemen mit Schadsoftware durch unzureichende interne Prozesse, aber auch erfolgreiche Cyber-Angriffe von Hackergruppen auf die IT der Energieversorgung. Diese besteht aus Systemen zur Unterstützung von Geschäftsprozessen, der sogenannten Business-IT, sowie aus Betriebsmitteln zur Energieversorgung, der Mess-, Regel- und Steuerungssysteme, häufig auch als Operational IT (OT) bezeichnet. Besonders bekannt sind die Angriffe auf die iranischen Nuklearanlagen (Stuxnet) sowie die Angriffe auf das Stromnetz der Ukraine (BlackEnergy3, Industroyer), die jeweils bis zur OT vorgedrungen sind und erheblichen Schaden angerichtet haben.

Denkbare Angriffsszenarien im Energiebereich beziehen sich aber nicht nur auf Angriffe auf zentrale Komponenten oder Steuerungssysteme. Im Stromsektor sind auch Angriffe auf eine hohe Anzahl von IoT-Geräten denkbar, die Strom im Haushalt steuern, oder auf eine gewisse Anzahl von elektrisch betriebenen Autos während der Ladephase oder auf eine bestimmte Anzahl von Photovoltaik oder Windrädern. Solche Angriffe zielen darauf ab, das Stromnetz als Ganzes zum Erliegen zu bringen. Und auf Grund der fehlenden großen Kraftwerksturbinen, die gewisse Schwankungen im Stromnetz über die Gesetze der Physik wie zum Beispiel Trägheit der Masse ausgleichen können, wird diese Eigenschaft zukünftig nicht mehr gegeben sein und über intelligente IT-Logik ausgeglichen werden müssen. Von daher ist die singuläre Betrachtung von Cyber-Sicherheit einzelner Unternehmen wenig hilfreich. Will man Energiesicherheit, so muss diese im Energie-Ecosystem, zum Beispiel auf europäischer Ebene, organisiert sein.



*Um einen sicheren Betrieb zu gewährleisten, bedarf es ganzheitlicher Betrachtungsweisen*

Sicherheit bzw. Safety bedeutet der Schutz von Mensch und Umwelt. Sicherung bzw. Security bedeutet der Schutz vor schädigenden Handlungen. Datenschutz bzw. User Data Privacy schützt personenbezogene Daten vor Missbrauch. Betrachtet man die Funktionsweise von nuklearen Reaktoren, Umspannwerken oder Pipelines, so existieren dort digitale Komponenten, die Ventile steuern, Druck messen und regulieren oder Leitungen schalten. Solche Komponenten sind vor Ort durch angepassten Objektschutz zu schützen, aber gerade auch im Kontext einer vernetzen und digitalisierten Infrastruktur angemessen gegen Cyber-Attacken zu schützen.

Nicht nur der EU Single Market mit seiner europäischen Energiebörse EEX, auch viele Vorhaben der Energiewende verlangen Konnektivität zwischen den Beteiligten und massiven Datenaustausch, zum Beispiel zu Abrechnungs-, Wartungs- oder Vorhersagezwecken. Ein HGÜ-Konverterstandort, der funktionell einem Umspannwerk gleicht, benötigt zum Betrieb einige Dutzend 19"-Schränke an digitalem Equipment und stellt so ganz neue Anforderungen an die Betreiber. Damit werden Angriffsvektoren und Angriffswege geschaffen, die es vorher nicht gab. Um einen sicheren Betrieb zu gewährleisten und auszuschließen, dass IT-Komponenten zum Angriffsmittel, Angriffsweg oder Angriffsziel werden, bedarf es ganzheitlicher Betrachtungsweisen und Methodenansätze, unternehmensübergreifender Strukturen und Interaktionen sowie einer Zusammenarbeit aller Beteiligten im Energiesektor und an seinen Grenzen wie zum Beispiel zur Automobilindustrie.

| | | |
|---|---|---|
| Plant and Grid Functional Safety | Plant and Grid Operations | User Data Privacy |
| Plant and Grid Security | | |

## ENERGY SECURITY MANAGEMENT

*VICCON verfolgt einen übergreifenden Ansatz in Form eines Energy Security Management System® (ESMS) für Energieversorger, das das Ecosystem berücksichtigt.*

Der Energiesektor ist zwar reguliert und die Beteiligten sind durch Energieinfrastrukturen miteinander verbunden, aber trotzdem gibt es keine ausgeprägte Zusammenarbeit über den gesamten Sektor. Ein einheitliches Verständnis von Bedeutung, Aufbau und Struktur eines Security Management Systems fehlt. Deshalb werden aktuell neue Ansätze und Ideen diskutiert, wie ein unternehmensübergreifendes Sicherheitsmanagement erreicht werden kann. Der Bedarf ergibt sich aus dem notwendigen Zusammenwirken von unterschiedlichen Unternehmenseinheiten, der gemeinsamen Zielsetzung nach dem Schutz physischer Sicherung (Physical Protection), funktioneller Sicherheit (Functional Safety) sowie der Konnektivität und Verschmelzung der digitalen Systeme mit der Business-IT. Somit wird ein Sicherheitsmanagementansatz gesucht, der die Bereiche Business, Systemführung, Kommunikation und dezentrale Infrastrukturen miteinander verbindet. Gleichzeitig existieren zahlreiche Anforderungen, die sich zum Beispiel aus Datenschutz, Zertifizierungen oder Compliance-Audits ergeben können wie zum Beispiel bei ISO 27001, IT-Sicherheitskatalog oder SEWD-IT. Hinzu kommen europäische oder internationale Rahmenwerke und Standards.

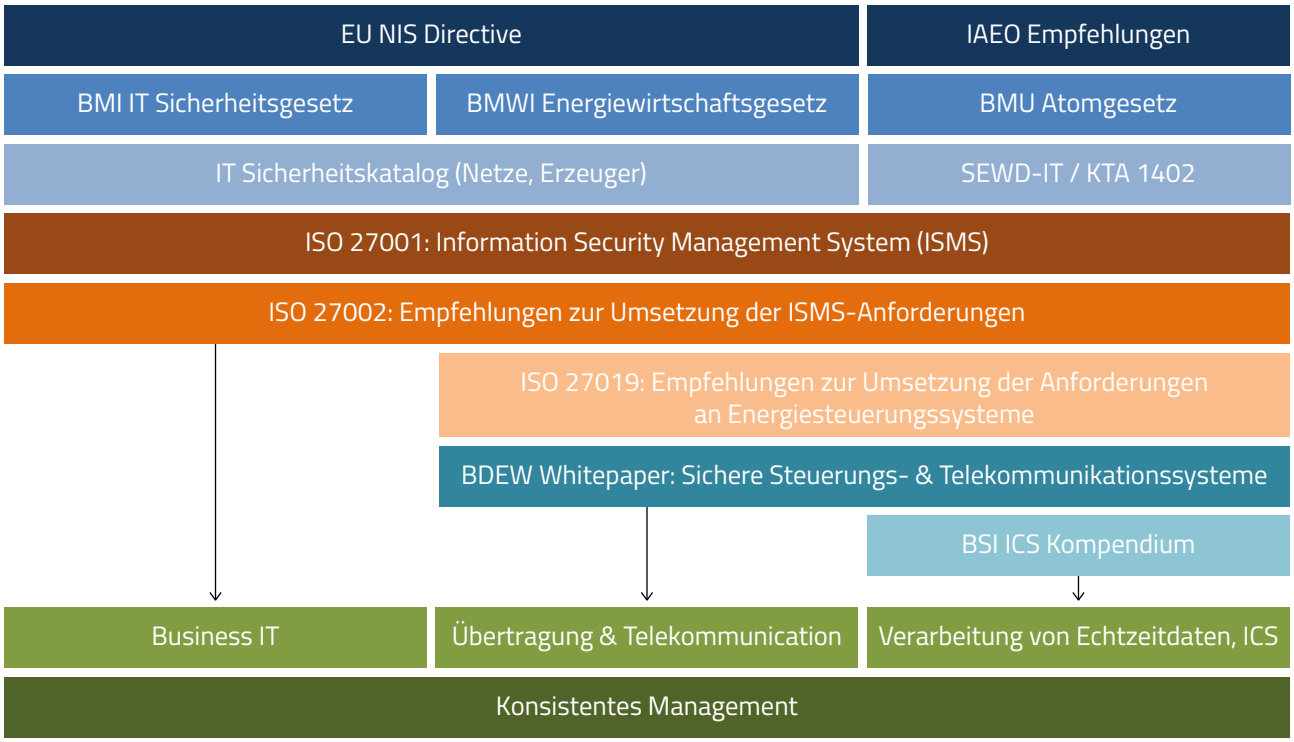
VICCON verfolgt einen übergreifenden Ansatz in Form eines Energy Security Management System® (ESMS) für Energieversorger, der das Ecosystem berücksichtigt. Die Versorgung mit Energie wird durch verschiedene digitale Systemwelten unterstützt, die eng mit Geschäftsprozessen interagieren. Ein gemeinsamer und effizienter Schutz über alle Geschäftseinheiten, Versorgungsinfrastrukturen und Standorte sollte gegeben sein, um das übergreifende Ziel einer sicheren digitalisierten Versorgung zu erreichen. Dazu werden existierende und kommende Standards für Cyber Security und Informationssicherheit verbunden und angewendet.

| Energy Security Management System® | | | |
|---|---|---|---|
| Business Process Information Security | | | |
| Business IT | Communication | Operation | Support & Maintenance |
| Protection of IT Systems | Protection of Telecommunication Systems, WAN | Protection of Control Systems, Safety Systems, Operational Systems | Protection of Operational Systems, Maintainance Data |

## DIGITALES VERTRAUEN UND SICHERHEITSSTRATEGIE

Die Regulierung im Energiesektor ist in den meisten Nationalstaaten stark ausgeprägt, insbesondere, wenn Kernenergie zur Energieerzeugung gehört. In Deutschland sind verschiedene Behörden in die Regulierung der IT-Sicherheit des Energiesektors eingebunden, um das notwendige Vertrauen für die Bevölkerung zu schaffen. Zukünftig werden auch europäische und internationale Organisationen mehr Einfluss auf eine Harmonisierung von IT-Sicherheit haben und Regeln für Mindeststandards und Zusammenarbeit fortschreiben und besser durchsetzen.

Trends und Themen wie Industrie 4.0, Digitales Vertrauen, Resilienz, Vernetzte Gesellschaft und New Work müssen in zukünftige Überlegungen einfließen. VICCON verarbeitet solche Anforderungen in einer Sicherheitsstrategie, in der mit einem methodischen Ansatz konkrete Maßnahmen für die zukünftige Arbeit der Sicherheitsabteilungen und des gesamten Unternehmens abgeleitet werden.




## ADVICE - DIALOG - KNOWLEDGE TRANSFER - IMPLEMENT - EDUCATE

VICCON unterstützt seit rund 20 Jahren Organisationen darin, sicherheitsrelevante Entwicklungen zu verstehen, die notwendigen Kompetenzen und Prozesse dafür aufzubauen und sie so sicher zu beherrschen.

VICCON entwickelt mit Ihnen gemeinsam Ideen und sucht im Dialog mit allen Unternehmensebenen eine passende Orientierung zur Sicherheitspolitik im Lichte der unterschiedlichen Anforderungen.

VICCON entwickelt Strategien für sichere und resiliente Organisationen, begleitet die digitale Transformation und berät bei der Implementierung dieser Strategien in Form eines Next Generation Security Managements.

VICCON verfolgt das Ziel, Security im Sinne des Managements und Business im Unternehmen strategisch zu verankern. Besondere Schwerpunkte liegen im Informationssicherheitsmangement sowie im Management von Cyber-Risiken und im Prototypen- und Know-how-Schutz.

### KONTAKT

Für weitere Informationen kontaktieren Sie:

VICCON GmbH

Ottostraße 1
76275 Ettlingen
Deutschland

Tel.: +49 7243 719734
Fax: +49 7243 719704

E-Mail: info@viccon.de
www.viccon.de

VICCON

CONSULTING