Foto: 2012 Dominic Schiller / Siemens Enterprise Communications

# KRITIS in der Energiewirtschaft

**Ein gemeinsames Beratungsangebot von**
**Siemens Enterprise Communications & enerson consulting**

enerson
www.enerson.de

**Siemens Enterprise Communications**
www.siemens-enterprise.com

SIEMENS
Siemens Enterprise Communications

***Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.***

„Strom fließt immer“ – diese pauschale Aussage ist in modernen Energienetzen längst überholt.

Stromleittechnik, also die Überwachung und Steuerung von Stromverteilungsnetzen, ist ebenso wie viele andere Bereiche in unserer Gesellschaft von einem stetig wachsenden Digitalisierungsgrad betroffen.

Informations- und Telekommunikationstechnik (ITK) sind zu einem wichtigen Werkzeug geworden, um die technische Stabilität bei der „Power Quality“ zu gewährleisten und den wirtschaftlichen Anforderungen zu genügen. Doch durch zunehmende Digitalisierung wächst das Risiko, dass davon abhängige Infrastrukturen so angegriffen werden, dass nicht nur wirtschaftlicher Schaden für das einzelne Unternehmen entsteht, sondern Dominoeffekte ganze Bereiche des öffentlichen Lebens lahmlegen. Die Energieversorgung ist dabei an vorderster Stelle eine kritische Infrastruktur.

| Sektoren kritischer Infrastrukturen |
|---|
| Energie |
| Informationstechnik und Telekommunikation |
| Gesundheit |
| Wasser |
| Ernährung |
| Transport und Verkehr |
| Finanz- und Versicherungswesen |
| Staat und Verwaltung |
| Medien und Kultur |

Die Einschränkungen der kritischen Infrastrukturen durch Distributed Denial of Service (DDoS) Angriffe bekam Estland im Mai 2007 zu spüren. Tagelang waren Banken und Kommunikation im Land lahmgelegt. Eindrucksvoll hat das Department of Homeland Security im Aurora-Projekt die Konsequenzen einer Hackerattacke auf die Energieinfrastruktur demonstriert. Der DDoS-Angriff auf einen deutschen Übertragungsnetzbetreiber Ende 2012 durch Hacker zeigt, dass Energieunternehmen durchaus im Fokus von Angreifern stehen können, auch wenn in diesem Beispiel die Energieversorgung nicht betroffen war. Aber unabhängig von mehr oder weniger

spektakulären Cyberangriffen schafft die zunehmende Durchdringung durch ITK zusätzliches Risikopotential, dessen möglicher Schaden unabhängig von krimineller Energie, technischen oder menschlichen Fehlern und sonstigen Einflussfaktoren enorm sein kann.

Diese Risiken sollten proaktiv in einem Information Security Management System (ISMS) minimiert werden, welches dann speziell auf die Process IT ausgedehnt werden muss. Mindestens ebenso wichtig ist im Rahmen von KRITIS auch die Schadensbegrenzung. Vor allem ist es notwendig, bei einem sogenannten Schwarzstart das Netz wieder geregelt hochfahren zu können. Im Rahmen der Energiewende entstehen durch die zunehmende Digitalisierung (Stichwort „smart grid“) neue Schwachstellen, auf die organisatorisch und technisch im eigenen Hause reagiert werden muss.

## Was ist zu tun?

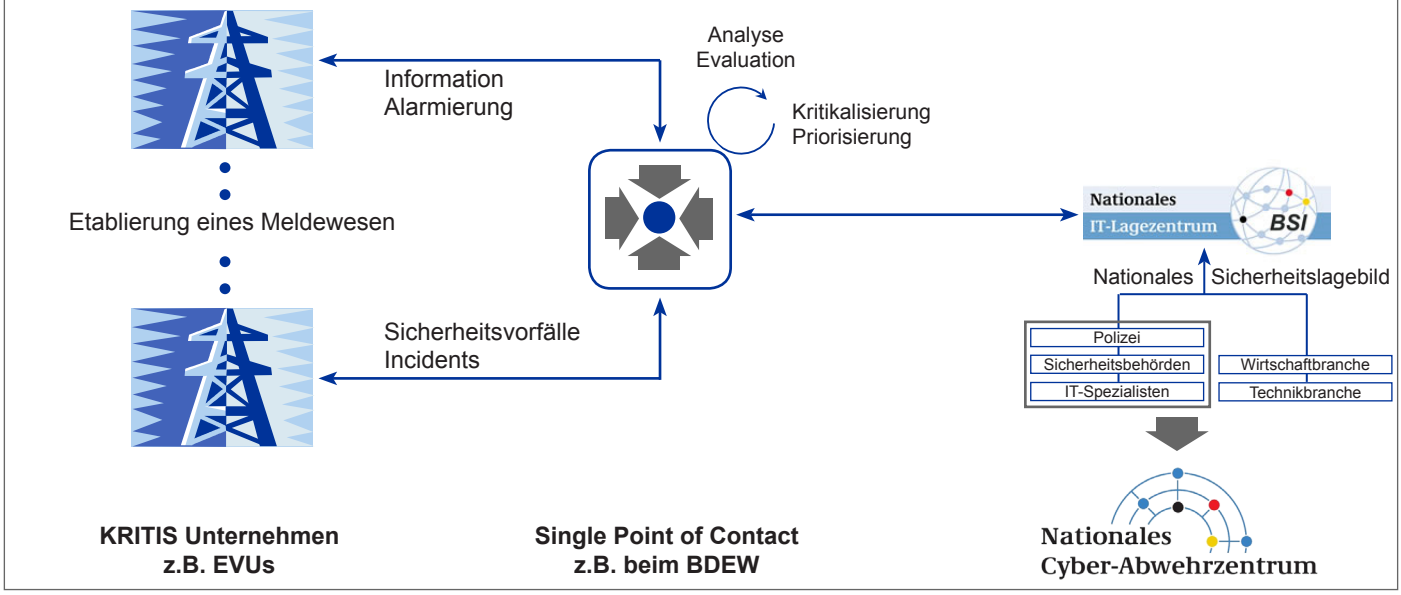
Für den „Nationalen Umsetzungsplan für Kritische Infrastrukturen“ (UP KRITIS) ist das Bundesministerium des Innern (BMI) verantwortlich. Mit der konkreten Umsetzung sind zwei Bundesämter durch den Innenminister beauftragt worden, nämlich das Bundesamt für Bevölkerungsentwicklung und Katastrophenschutz und wegen der besonderen Bedeutung der Cybersicherheit im Rahmen von KRITIS, das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Nach dem Willen des BMI hat jedes Unternehmen bzw. jede betroffene Organisation in der Energieversorgung deshalb ein Meldewesen zu etablieren, mit dem relevante Sicherheitsvorfälle an einen Single Point of Contact gemeldet werden müssen. Dieser Kontaktpunkt wird voraussichtlich der Bundesverband der Energie- und Wasserwirtschaft (BDEW) sein. Dort wird bewertet, ob der Vorfall repräsentativ ist und ggf. an die Bundesbehörden weitergeleitet werden muss. Dies kann bis hin zum Cyberabwehrzentrum des Bundes erfolgen. Andererseits müssen umgekehrt Hinweise und Meldungen der Behörden und des Verbandes auf eigene Relevanz ausgewertet werden und entsprechende Maßnahmen eingeleitet werden. Dies setzt eine Sicherheitsorganisation mit Regelwerk, Bewertungskriterien und Meldewesen voraus. Diese Organisation ist zumindest politisch in hohem Maß gewollt, wird vom Verband begrüßt und für seine Mitgliedsunternehmen ausdrücklich gefordert.

## Anforderungen an die Sicherheitsorganisation?

Zur Verbesserung der IT-Sicherheit sind Betreiber wichtiger kritischer Infrastrukturen angehalten IT-Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik zu ergreifen und ihre Einhaltung sicherzustellen. Hierfür können brancheninterne Standards entwickelt werden, die das BSI als Konkretisierung der gesetzlichen Verpflichtung anerkennt.

## klassische Internet-Security erreicht EVU's: KRITIS-Anforderungen werden verbindlich




Betreiber kritischer Infrastrukturen sind in der Pflicht dem BSI unverzüglich erhebliche IT-Sicherheitsvorfälle, wie z.B. der unerlaubte Zugriff auf Systeme mit Auswirkung auf die Versorgungssicherheit oder die öffentliche Sicherheit, über hierfür etablierte Wege zu melden. Dadurch erhält das BSI ein valides, nationales Lagebild, um Betreiber bei der Bewältigung gegebener Vorfälle unterstützen zu können.

Wieweit die Berichtspflicht gehen wird, ist noch nicht festgelegt. Größe der Bedrohung und Ausmaß des Schadens (z.B. Anzahl betroffener Einwohner) werden ausschlaggebend sein. Es ist aber schon im Eigeninteresse sinnvoll, sich im eigenen Hause entsprechend aufzustellen. Für die Realisierung dieser zentralen Regelungsinhalte müssen Unternehmen daher u.a. ein ISMS aufbauen. Dies kann nach den Vorgaben des BSI erfolgen, die im Standard BSI 100-1 festgelegt sind. Dieser ist auf den klassischen IT-Betrieb (z.B. in Rechenzentren) zugeschnitten.

Weiterhin kann der internationale Standard ISO 27000 angewendet werden, der größere Freiräume gestattet und seit kurzem mit einer eigenen Ausprägung für die Prozessleittechnik der Energiebranche entgegen kommt. Diese Ergänzung von ISO 27002 ist bereits in Deutschland verabschiedet, und wurde im Fast Track Verfahren als ISO/IEC/DTR 27019 international normiert. Eng verwandt mit diesen Vorgaben ist das BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme". Siemens Enterprise Communications und enerson consulting haben gemeinsam ein Beratungskonzept ausgearbeitet, das Kunden aus der Energiewirtschaft neben umfassender IT-Kompetenz auch tiefergehendes Prozess-Know-how bietet. Mit diesem Beratungsansatz – der Symbiose aus Betriebsprozesskompetenz von enerson consulting in der Energiewirtschaft und der strategischen IT-Sicherheits-Kompetenz von Siemens Enterprise Communications sind wir somit ein ganzheitlicher Partner für die aufkommenden KRITIS-Anforderungen.

### Was sind unsere Leistungen?

- Darstellung der politischen/gesetzlichen Anforderungen für KRITIS in kompakter Form
- Definition der individuellen globalen Schutzziele für Ihr Haus
- Individuelle Risikoanalyse mit wesentlichen Bewertungen für die Geschäfts- und Betriebsprozesse
- Individuelles Assessment zur Identifikation des Gefährdungspotenzials, der Risiken und ihrer Bewertung unter betriebswirtschaftlichen (Business Impact Analyse) und volkswirtschaftlichen Gesichtspunkten (KRITIS)
- Identifikation konkreter Maßnahmen gemäß Schutzzielen und Risikoanalyse
- IST-Analyse Ihres Hauses zum Stand eines Information Security Management Systems (ISMS)
- Optional: Ergänzung eines ISMS-Konzept für Ihr Haus im Einklang mit politischen/gesetzlichen Anforderungen und geschäftlichen Anforderungen
- Erarbeitung von Organisationsstrukturen, Regelwerken und technischen Maßnahmen unter Berücksichtigung von Process IT, Telekommunikation und Commercial IT

### Was ist Ihr Nutzen ?

- Alle Verantwortlichen Ihres Hauses werden sensibilisiert und in den Veränderungsprozess einbezogen
- Konkrete Definition Ihrer strategischen Schutzziele
- Risiken werden identifiziert und gemäß ihrem Schadenspotenzial bewertet
- Aufbau präventiver Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit eines Schadensfalls
- Realitätsnaher Prüfungsplan für den Schadensfall zur beschleunigten Fehlererkennung
- Maßnahmenkatalog zum verbesserten Wiederanlauf der Energieversorgung
- Reduzierung indirekter Schäden und Haftungsrisiken durch Verringerung der Ausfallzeit im Schadensfall
- Bestehende oder zu schaffende organisatorische Rollen und Prozesse im Hause zur Gewährleistung der Informationssicherheit werden mit den Anforderungen an ein externes Meldewesen verknüpft.
- Systematischer Informationsautausch mit den Behörden

## Siemens Enterprise Communications

Siemens Enterprise Communications ist ein führender Anbieter von End-to-End-Lösungen für die Unternehmenskommunikation. Offene, standardbasierte Architekturen sorgen für die Konvergierung von Kommunikations- und Unternehmensanwendungen und ermöglichen so die nahtlose Zusammenarbeit im gesamten Unternehmen. Dank unserer preisgekrönten „Open Communications"-Strategie können wir Anwendern einfach implementierbare Lösungen bieten, die sich reibungslos in vorhandene IT-Umgebungen einbinden lassen und damit nicht nur die Produktivität steigern, sondern auch Kosten senken. Darauf basiert das OpenPath-Angebot der SEN Group, das Kunden die Minimierung von Risiken und die wirtschaftliche Einführung von Unified Communications ermöglicht. Wir unterstreichen unser Engagement mit dem OpenScale Service-Portfolio, das internationale, Managed Service- und Outsourcing-Angebote enthält. Siemens Enterprise Communications gehört einem Joint Venture von The Gores Group und der Siemens AG. Auch Enterasys Networks liefert als weiterer Teil des Joint Ventures Netzwerkinfrastrukturen und Sicherheitssysteme, die die perfekte Grundlage für einheitliche Kommunikationslösungen bieten.

Die in dieser Broschüre enthaltenen Informationen beinhalten im Wesentlichen allgemeine Beschreibungen oder Leistungseigenschaften, die in der Praxis nicht unbedingt wie beschrieben gelten oder die sich infolge von Produktentwicklungen ändern können. Eine Verpflichtung zu den genannten Eigenschaften gilt nur dann, wenn dies ausdrücklich vertraglich vereinbart wurde. OpenScape, OpenStage und HiPath sind eingetragene Warenzeichen von Siemens Enterprise Communication & Co KG. Alle anderen Unternehmens-, Marken-, Produkt- und Service-Bezeichnungen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Hersteller.

## enerson consulting

enerson consulting ist eine Strategie- und Managementberatung für die Energiewirtschaft. Unsere Schwerpunktthemen sind IT-Management, Netze, Vertrieb und dezentrale Erzeugung. Wir besitzen langjährige Erfahrungen in Linie und Beratung der Energiewirtschaft. Zu unseren Kunden zählen Stadtwerke, Regionalz und überregionale Energieversorger, die wir mit unserem fundierten Fachwissen bei aktuellen Herausforderungen in der Energiewirtschaft unterstützen.



enerson
www.enerson.de


www.siemens-enterprise.de

SIEMENS
Siemens Enterprise Communications