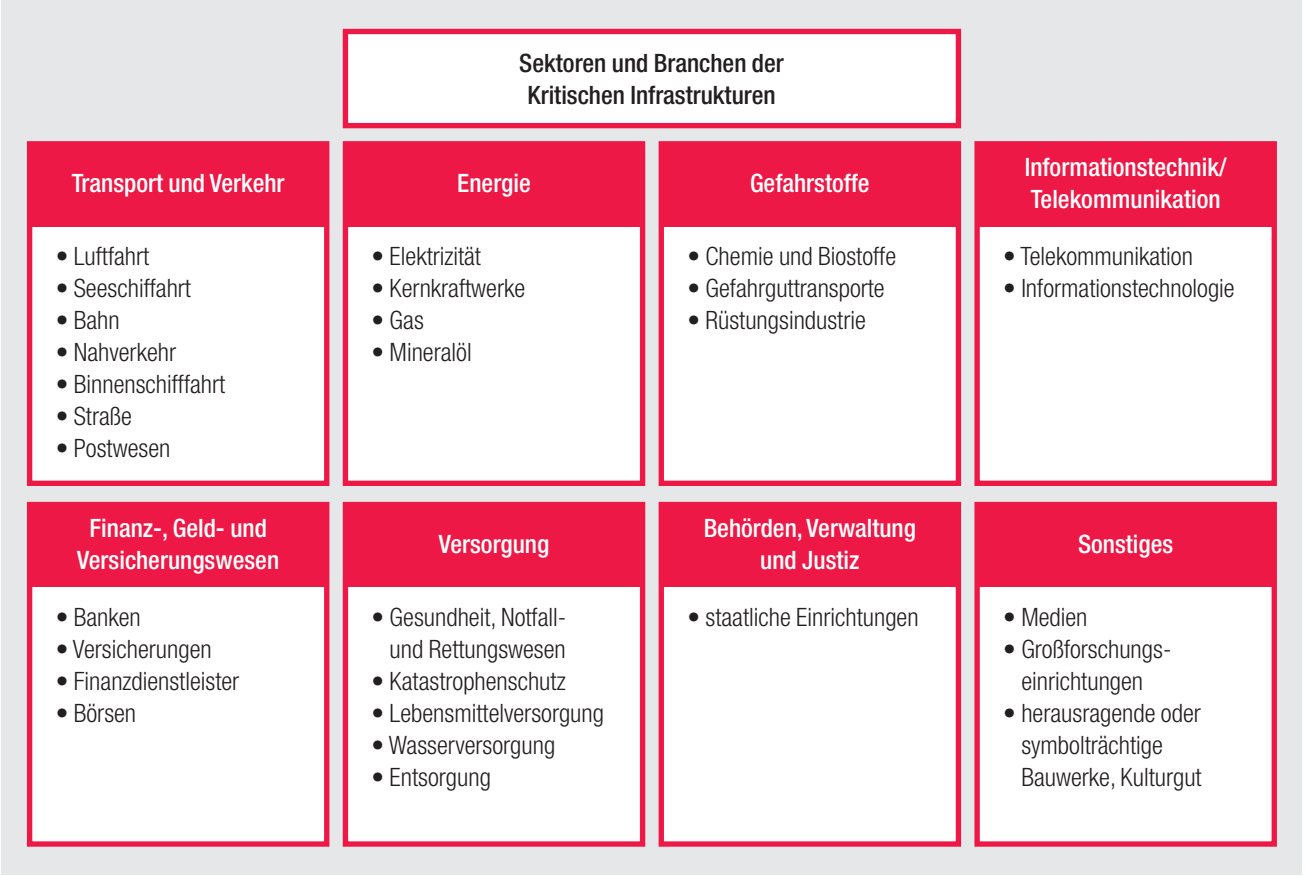
Cybersecurity – Komplexität von Informationssicherheit in sensiblen Versorgungsinfrastrukturen

Der Begriff Cybersecurity beschreibt mit seinen unterschiedlichen Maßnahmen die notwendigen Schritte zur Absicherung von IT-Systemen. Nachfolgend soll dieser Begriff auf kritische Versorgungsinfrastrukturen des Energie- und Wasser-Sektors angewendet werden. Im ersten Abschnitt werden die theoretischen Grundlagen dazu erläutert und im zweiten Abschnitt mit praktischen Maßnahmen zur Erhöhung der Informationssicherheit im Weiteren beschrieben.

Mit der ersten Fassung des Anforderungskatalogs an Sicherheit in kritischen Infrastrukturen (KRITIS) des Bundesministeriums des Innern (BMI) begann im Jahre 2007 die Diskussion über deren Absicherung [1]. Spätestens seit diesem Zeitpunkt wird zunehmend über Informationssicherheit und deren Implementierung im Umfeld kritischer Infrastrukturen öffentlich diskutiert. Mit zunehmender Häufigkeit zeigen auch die Angriffe auf sensible Energieversorgungsinfrastrukturen sehr deutlich, wie notwendig die Berücksichtigung dieser Thematik ist.

Beschäftigt man sich eingehender mit diesen Sachverhalten, so ist es notwendig, mit den seit einigen Jahren auf nationaler und internationaler Ebene verabschiedeten Standards und Normen zu beginnen. Mit dem speziellen Fokus auf Energieversorgungsunternehmen ermöglichen diese, sich mit Hilfe der beschriebenen Maßnahmen und Anforderungen gegen die vielfältigen Bedrohungen gegenüber ihren IT-Infrastrukturen und Daten zu schützen. Die in diesem Zusammenhang wichtigste internationale Normenreihe ISO/IEC 27000 beschreibt die Maßnahmen für Informationssicherheit zur Absicherung kritischer Infrastrukturen. Des Weiteren sind in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem Umsetzungsplan KRITIS **(Abb. 1)** und der Allianz für Cybersecurity verstärkt dabei, die Informationssicherheitsanforderungen zu definieren. Weitere

Abb. 1: Umsetzungsplan KRITIS



Quelle: Bundesministerium des Innern

Verbände wie der DVGW e. V. und der VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V. haben sich des Themas ebenfalls in unterschiedlichen Arbeitskreisen und Publikationen angenommen. Als Ergänzung der ISO/IEC-27000-Reihe wurde im letzten Jahr eine Technische Richtlinie (TR) spezifiziert: der Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002.

Auch im internationalen Bereich wird der Thematik ein hoher Stellenwert zugeschrieben, wie z. B. in Amerika. Die Standards des National Institute of Standards and Technology (NIST) [2] und der North American Electric Reliability Corporation (NERC) [3] dienen dort als Grundlage. Beide Institutionen geben in ihren Veröffentlichungen, wie NIST SP800-82 „Guide to Industrial Control Systems (ICS) Security" oder den NERC Security Guidelines, detaillierte Verfahrensbeschreibungen zur Definition von Anforderungen an Informationssicherheit sowie Umsetzungs- und Konfigurationsempfehlungen.

Tabelle 1: Basismaßnahmen

Awareness
• Sensibilisierung und Schulung der Mitarbeiter • Kontrolle der Effektivität der Maßnahmen durch Kontrolle, wie Fragebögen oder Quiz
Schadsoftwareschutz
• Kompatibilität mit der Leitsystemsoftware/Systemverhalten im 24/7-Betrieb • Herstellersupport • Möglichkeit der Einbindung in das Patchmanagement/Aktualisierung • Zentrale Überwachungs- und Meldemechanismen, wie Monitoring der Clients
Patchmanagement
• Betriebssystem • Leitsystemsoftware • 3rd. Party Patchmanagement von Drittapplikationen • Systemkomponenten wie Firewall, Switche und Fernwirktechnik
Betriebssystemhärtung
• Notwendige Dienste nach Rolle des Systems • Basissoftware auf dem System und nicht benötigte Standardkomponenten • Konfigurationshärtung
Zonenmodell
• Firewall • Physikalische und logische Infrastrukturen
Physikalische Sicherheit
• Zutrittskontrolle • Hochverfügbarkeit
Grundlagen
• Risikomanagement • Schutzbedarfsfeststellung

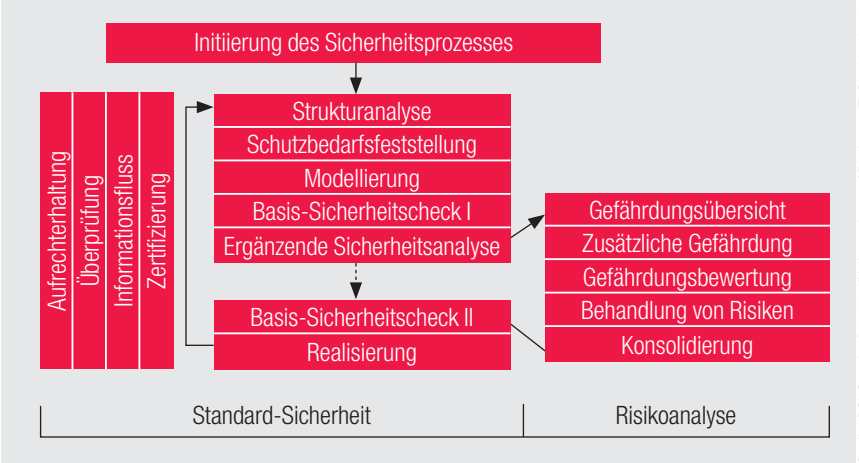
Quelle: CONSULECTRA Unternehmensberatung GmbH

Auf Basis der zuvor genannten Grundlagen ergibt sich die Fragestellung nach der Umsetzung. Wie viel Sicherheit ist tatsächlich notwendig? Die zwingend erforderlichen Basismaßnahmen **(Tab. 1)** lassen sich in der Praxis auf wesentliche Sicherheitsmechanismen reduzieren, um dadurch ein Basis-Informationssicherheitsniveau zu erreichen **(Abb. 2)**.

Die klassische Risikobewertung bildet einen guten Ausgangspunkt für eine angemessene Bewertung der Sicherheitsmechanismen zum Schutz des Leitsystems. Beispielsweise kann diese mit der BSI-Grundschutz-Methodik oder der in ISO/IEC 27005 beschriebenen Vorgehensweise durchgeführt werden.

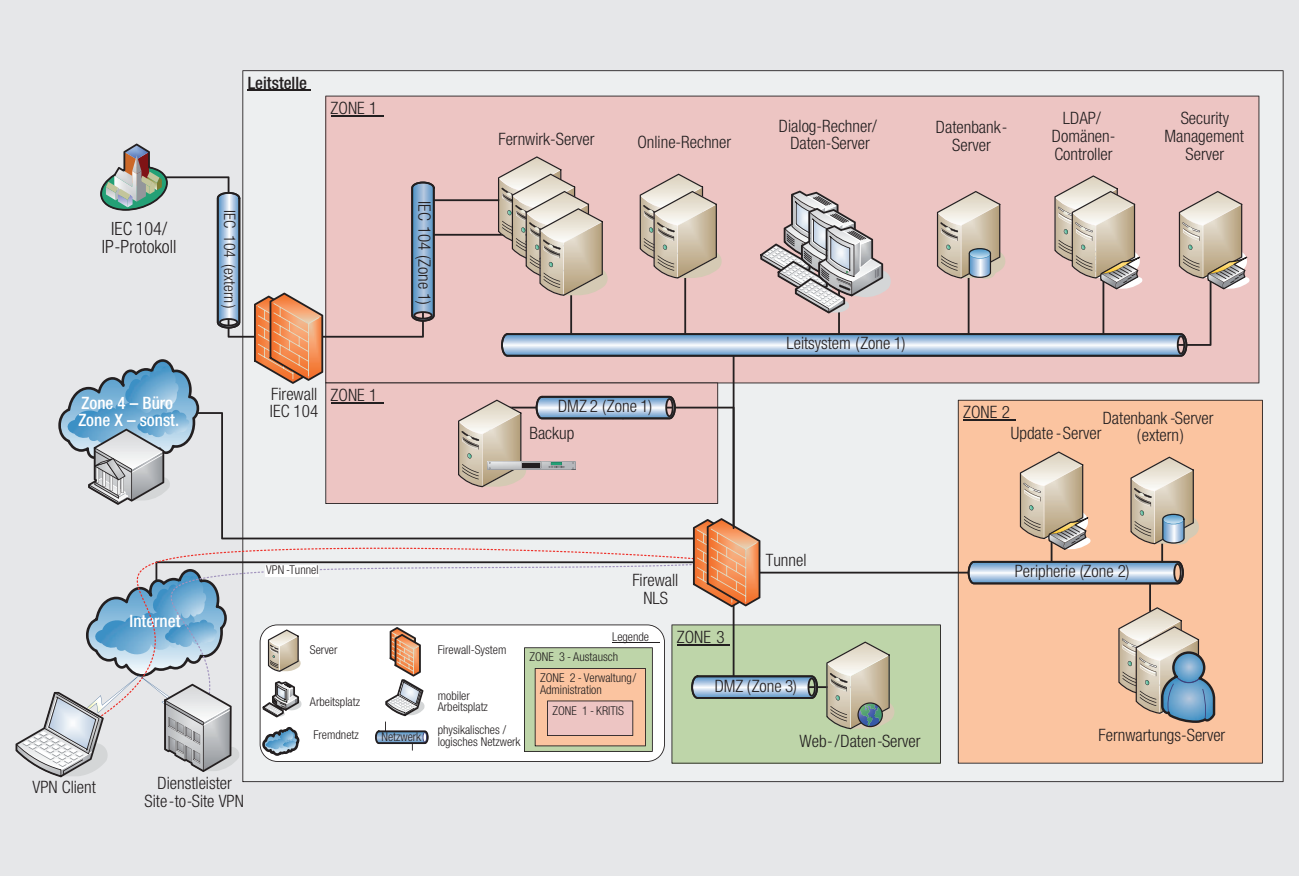
Mit den Ergebnissen aus der Risikoanalyse lassen sich sowohl der entsprechende Schutzbedarf als auch die Kritikalität für das System bzw. Teilkomponenten feststellen. Daraus können dann entsprechende Schutzmaßnahmen und deren Konfiguration abgeleitet werden, wie beispielsweise der Aufbau des nachfolgend genannten Zonenmodells **(Abb. 3)** und die notwendigen Sicherungsmaßnahmen.

Nach der Ermittlung der Risiken und des Schutzbedarfs der Systeme und Systemkomponenten empfiehlt es sich, ein (IT-)Sicherheitskonzept aufzubauen. Um dabei sämtliche Punkte zu berücksichtigen, sollten die beschriebenen Umsetzungsempfehlungen angewendet werden.



Quelle: BSI-Standard 100-3 „Risikoanalyse auf Basis von IT-Grundschutz"

Abb. 2: *Integration der Risikoanalyse in den Sicherheitsprozess*



Quelle: BTC AG

Abb. 3: *Beispiel Zonenmodell*

Der Standort eines Leitsystems und seine physikalische Sicherheit sind dabei ein wichtiger Aspekt bei der Bewertung der Sicherheitsrisiken und Bedrohungen. Der Standort sollte so gewählt werden, dass durch entsprechende Sicherheitsmaßnahmen wie Zugangs- und Zutrittskontrolle, Brandschutz, Klimatisierung und Bewertung der Bedrohungen, wie durch Hochwasser, ein gleichbleibend hohes Sicherheitsniveau gewährleistet ist. Unter Einbeziehung der Bewertung der Kritikalität eines Systems kann dies für einen Standort beispielsweise die Trennung der Räumlichkeiten der kritischen Leitsystemkomponenten von den IT-Systemen der Büro-IT im Rechenzentrum implizieren, wenn diese nicht den notwendigen Anforderungen entsprechen.

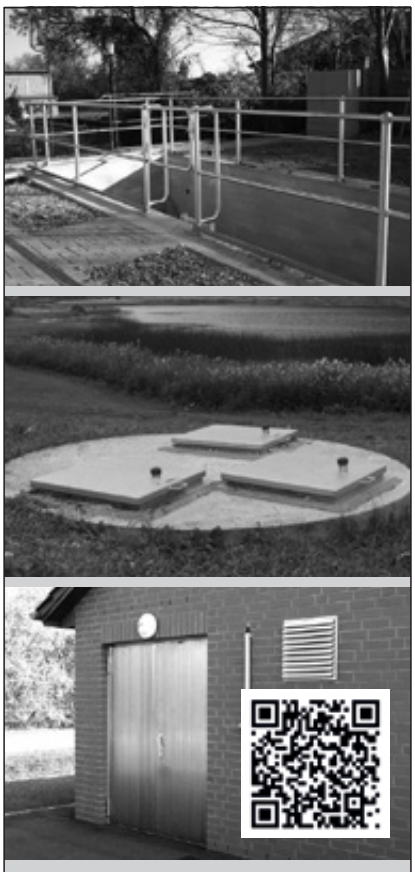
Wird mit dem Aufbau des Systems auf der Netzwerkebene begonnen, so ergibt sich als Erstes die Frage der öffentlichen Anbindung. In früheren Systemen war oftmals von einem Inselbetrieb oder „Air-Gap“ die Rede, bei dem das Leitsystem abgekoppelt von anderen Systemen, wie der Büro-IT oder dem Internet, betrieben wurde. Dieses ist heute durch die zunehmende Vernetzung sowie den notwendigen Datenaustausch mit anderen Einheiten in einem Energieversorgungsunternehmen kaum noch möglich. Der Datenaustausch erfolgt aus verschiedensten Gründen, wie etwa die zeitkritische Übermittlung von Abrechnungs- oder Prognosedaten aus dem Leitsystem in andere Geschäftsbereiche oder der administrative Zugriff zu Fernwartungszwecken für Dienstleister. Die Kommunikation mit Drittsystemen wird dabei in einem häufig als „Zonenmodell“ benannten Kommunikationsmodell beschrieben. Das Zonenmodell beschreibt auf Basis der notwendigen Kommunikationsbeziehungen einzelner Systeme bzw. Systemklassen den Datenaustausch auf Basis der eingesetzten Protokolle sowie Ports. Dabei sind sämtliche Kommunikationsbeziehungen zu berücksichtigen, wie der Datenaustausch mit der Bürowelt und den Abrechnungssystemen oder die Fernwartungsanbindung für Lieferanten oder Fernarbeitsplätze. Das Zonenmodell wird in der späteren Umsetzung durch entsprechende Firewallsysteme abgebildet, die gegebenenfalls hochverfügbar auszulegen sind. Erfolgt die Internetanbindung an das Leitsystem auf direktem Wege, wie durch die Bereitstellung eines DSL-Anschlusses, muss überlegt werden, an dieser Stelle eine gesonderte Firewall zu implementieren.

Betrachtet man als nächsten Schritt die Systeme des Leitsystems, so ist je nach Betriebssystem eine spezielle Anpassung notwendig. Dabei werden bei der sogenannten Betriebssystemhärtung alle nicht notwendigen Dienste deaktiviert, nicht notwendige Applikationen deinstalliert und die Konfiguration des Systems geprüft sowie die Installation aller zum Zeitpunkt der Inbetriebnahme vorhandener Aktualisierungen vorgenommen. Dies erfolgt in der Regel durch den Hersteller vor der Systemauslieferung. Dadurch wird es Angreifern erschwert, Sicherheitslücken im Betriebssystem der Applikationen auszunutzen und so unberechtigten Zugriff auf das System zu erhalten. Bei der Betriebssystemhärtung sollten sämtliche Systeme und Komponenten im Leitsystem betrachtet werden, da nicht nur Arbeitsplatzsysteme oder Server über unnötige Standarddienste verfügen. Zu diesen Systemen gehören neben Server und Arbeitsplatzsystemen auch die Peripherie, wie Firewall und Netzwerkkomponenten.

Um im späteren Betrieb vor Sicherheitslücken und Schwachstellen im Betriebssystem und den Applikationen geschützt zu sein, ist es notwendig, diese regelmäßig zu aktualisieren. Dieses Patchmanagement muss den Anforderungen der Kritikalität und des hochverfügbaren Systembetriebs gerecht werden. Sofern seitens des Systemherstellers ein solches Verfahren beschrieben wurde, sollte die Umsetzung im Betrieb geprüft werden. Die klassischen Verfahren, wie sie bereits für Systeme in der Büro-IT angewendet werden, führen im Leitsystem möglicherweise zum Ausfall des Systems, da dabei u. a. Systeme zu einem definierten Zeitpunkt heruntergefahren oder neu gestartet werden. Beim Patchmanagement sind dabei alle Systemkomponenten zu berücksichtigen, d. h. neben Arbeitsplatzsystemen auch Switche, Firewall und andere Peripherie, die möglicherweise über Sicherheitslücken Angreifern den Zugriff ermöglichen oder die Stabilität des Systems beeinflussen können.

Das Patchmanagement steht in direkter Verbindung mit dem Schadsoftwareschutz eines Leitsystems. In der klassischen Büro-IT erfolgt die Auswahl eines Schadsoftwareschutzes oder auch Virenscanners häufig anhand der Erkennungsrate und anderen leistungsbezogenen Parametern. Im Leitsystemumfeld hingegen ist zu differenzieren. Hier wird vor allem auf die Verträglichkeit des Schadsoftwareschutzes und den störungsfreien Betrieb ein hoher Stellenwert gelegt. Sollte es durch diesen, beispielsweise während des Updates der Definitionsdateien oder des Programmes, zu einer Störung im Betrieb kommen, so ist dieser für eine „real-time"-Umgebung ungeeignet. Bei der Einführung einer Schadsoftwareschutzlösung ist es notwendig, die Supportzusage des Leitsystemherstellers zu erhalten bzw. diesen mit der Installation und Betreuung, beispielsweise in Form eines Wartungsvertrages, zu beauftragen. Die Aktualisierung der Definitionsdateien und der Softwarekomponente ist dabei in das Patchmanagement-Verfahren zu integrieren.

Sämtliche technische Maßnahmen reduzieren ihre Wirksamkeit, wenn mit übermäßigen Rechten am System gearbeitet wird und dadurch möglicherweise das System durch einen Innentäter oder Unvorsichtigkeit kompromittiert wird, beispielsweise durch die Verwendung eines nicht zugelassenen USB-Sticks am System. Um dies zu vermeiden, empfiehlt es sich, ein Berechtigungskonzept auf Basis der Benutzerrollen im System zu etablieren. Dabei sollte mindestens zwischen der Dispatcher- oder Benutzerrolle und dem Administrator getrennt werden. Der Dispatcher sollte dabei nur über die für den Betrieb und seine Rolle vorgesehenen Berechtigungen im System verfügen. Für die Umsetzung können dazu die auch aus der Büro-IT bekannten Verzeichnisdienste wie LDAP oder Microsoft-Active-Directory Anwendung finden. Diese ermöglichen es, die Berechtigungen zentral zu steuern sowie kurzfristig auf Änderungen zu reagieren.



Mit Edelstahl perfekt ausgerüstet...

... für Wasserversorgung, Abwasserentsorgung und Biogaserzeugung

Wir liefern höchstwertige Produkte aus Edelstahl für die verschiedensten Anwendungsbereiche.

Unsere Produkte sind:

- korrosionssicher
- dauerhaft
- wirtschaftlich
- sicher für Mensch und Umwelt

IFAT **Besuchen Sie uns auf der IFAT vom 5.–9. Mai 2014 in Halle A2, Stand 333**

info@huber.de
www.huber.de

HUBER TECHNOLOGY
WASTE WATER Solutions

Die vorhergehend beschriebenen Maßnahmen gewährleisten die Basissicherheit des Leitsystems. Die Praxis zeigt, dass neben den IT-Bedrohungen ein Großteil der Sicherheitsprobleme von Personen im Umfeld des Leitsystems selbst ausgeht, beispielsweise durch Verwendung von Wechseldatenträgern, unsicheren Kennwörtern oder Publizieren von sensiblen Daten durch Unwissenheit über deren Sensibilität. Daher ist es unerlässlich, Mitarbeiter im Umfeld der kritischen Infrastrukturen auf diese Anforderungen hin zu sensibilisieren und zu schulen. Das ist bereits mit einfachen Maßnahmen wie prägnanten Plakaten oder Marketingmaterial möglich und kann bis zum Einsatz eines entsprechenden Systems zur Mitarbeiterschulung und Verständniskontrolle ausgeweitet werden.

Der Leitsystemhersteller und die eingesetzten Komponenten spielen ebenfalls eine entscheidende Rolle bei der Sicherstellung eines sicheren Systembetriebs. Aktuelle Leitsysteme verfügen in der Regel über Fernwartungsverbindungen zum Leitsystemhersteller und möglicherweise anderen Lieferanten. Dabei ist es wichtig, diese Verbindungen in das vorhergehend beschriebene Zonenmodell zu integrieren und kritisch zu betrachten. Es ist mit einfachen Mitteln möglich, das Leitsystem über eine solche Verbindung zu kompromittieren. Deshalb sollten die Hersteller selbst über die notwendige Sensibilität verfügen. Grundsätzlich sollte bei der Fernwartung der Kern des Leitsystems nicht im direkten Zugriff über die Fernwartung stehen, beispielsweise die Systeme der Dispatcher. Für die Fernwartung bietet sich hier ein durch die DMZ (eigenständige und gesicherte Netzwerkzone) getrenntes System explizit als Zwischenschritt zur Fernwartung an. Dies kann beispielsweise in Form eines Terminalservers realisiert werden. Für den Verbindungsaufbau sollten grundsätzlich nur als sicher einzustufende Verfahren verwendet werden – ein VPN mit hoher Verschlüsselung. Der klassische Wartungsvertrag mit dem Hersteller des Leitsystems oder der Komponenten sollte zukünftig auch die Informationssicherheitsmechanismen und den Datenschutz mitberücksichtigen, um so ein hohes Sicherheitsniveau zu gewährleisten.

Als Basis für einen angemessenen Schutz von Versorgungsinfrastrukturen können somit durchaus die klassischen Sicherheitsmechanismen wie das Patchmanagement und der Schadsoftwareschutz eingesetzt werden. Ergänzt durch entsprechende Berechtigungskonzepte auf Basis von Benutzerrollen, abgebildet durch einen zentralen Verzeichnisdienst zur Berechtigungsverwaltung, wie z. B. das LDAP-Protokoll oder Microsoft-Active-Directory und Patchmanagement. Diese Komponenten sind in der klassischen IT-Welt bereits hinreichend erprobt. Durch die Kritikalität der Systeme können diese aber nicht so übernommen werden. Es ist daher wichtig, die einzusetzenden Maßnahmen und Prozesse kritisch auf die Anwendbarkeit im Leitsystemumfeld zu überprüfen und entsprechend anzupassen.

In der Praxis zeigt sich, dass viele Leitsystemhersteller bereits Sicherheitsmaßnahmen in ihre Leitsysteme implementiert haben, dies geht zum Teil bis in die sichere Anwendungsentwicklung. Es ist ebenfalls festzustellen, dass einige Hersteller bereits Sicherheitszertifizierungen nach den genannten Sicherheitsstandards anstreben bzw. schon durchgeführt haben, wie z. B. der ISO/IEC 27001.

Für die Zukunft lässt sich feststellen, dass es durch den Einsatz intelligenter Netzkomponenten und IP-basierter Protokolle wichtig sein wird, einen kritischen Blick auf die Netzwerkinfrastruktur zu werfen. Auf dem Weg zu einem intelligenten Energienetz wird die klassische Informations- und Kommunikationstechnik (IKT) weiter Einzug in die Versorgungsnetze halten. Die damit verbundenen Bedrohungen haben wir heutzutage schon in anderen Infrastrukturen, wie der Büro-IT. Daher ist es wichtig, die Informationssicherheit von vornherein mitzuberücksichtigen. Ein Beispiel dafür sind die im Leitsystemumfeld eingesetzten Kommunikationsprotokolle, die heute über keine implementierten Sicherheitsmechanismen verfügen. Die Kommunikation verläuft dabei unverschlüsselt bei einem transparenten Protokollaufbau. Mittelfristig sollte hier auf sichere Protokolle und eine verschlüsselte Kommunikation umgestellt werden.

Nur eine ganzheitliche Betrachtung oder auch „defense-in-depth"-Strategie aller Komponenten, Prozesse und Systeme einer kritischen Infrastruktur kann den Schutz der Versorgungsinfrastruktur nachhaltig sicherstellen. ■

Quellen:
[1] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2007/Kritis.html
[2] www.nist.gov
[3] www.nerc.com

Der Autor

Michael Pietsch ist Projektleiter – CISSP, C|EH, E|CSA, L|PT, ISO 27001 Auditor – bei der CONSULECTRA Unternehmensberatung GmbH.

Kontakt:
CONSULECTRA Unternehmensberatung GmbH
Weidestr. 122 a
22083 Hamburg
Tel.: 040 27899-256
E-Mail: m.pietsch@consulectra.de
Internet: www.consulectra.de