Effektive und effiziente Security auf Basis internationaler Standards

Nicht erst seit erfolgreichen Cyber-Angriffen auf die ukrainische Stromversorgung mit 225.000 vom Blackout betroffenen Kunden im Dezember 2015 halten wir unsere kritische Infrastruktur für verwundbar.
Die Gesetzgeber auf nationaler und internationaler Ebene haben auch schon vorher endsprechende regulatorische Anforderungen für den Schutz der kritischen Infrastruktur gegen Cyber-Angriffe auf den Weg gebracht.

Regulierungen

In Deutschland wurde das IT-Sicherheitsgesetz am 12. Juni 2015 vom Bundestag beschlossen. Darin fordert der Gesetzgeber vom Betreiber einer kritischen Infrastruktur einen ganzheitlichen Ansatz bezüglich der Risikoermittlung und Behandlung der Risiken. Dazu gehört auch die Implementierung eines Managementsystems für Informationssicherheit, für das die Konformität zur ISO/IEC 27001 durch eine Zertifizierung nachgewiesen werden muss.

Auf europäischer Ebene wurde die Richtlinie über die Sicherheit von Netzen und Informationssystemen (NIS-Richtlinie) am 6. Juli 2016 vom Europäischen Parlament verabschiedet und trat im August 2016 in Kraft. Die Mitgliedstaaten mussten die Richtlinie bis zum 9. Mai 2018 in nationales Recht umsetzen. Die Kriterien, welche Infrastrukturen unter die NIS-Richtlinie fallen, müssen die EU Mitgliedstaaten bis November 2018 festlegen.

Die wesentlichen Anforderungen sind:

- Festlegung einer nationalen Security-Strategie,
- Meldepflicht für Security Vorfälle,
- Festlegung von Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der europäischen Union.

Das deutsche IT-Sicherheitsgesetz musste im Jahre 2017 nur unwesentlich angepasst werden um der NIS-Richtlinie zu genügen.

Die europäische Datenschutz-Grundverordnung (DSGVO) gilt dagegen ab 25. Mai 2018 unmittelbar in der gesamten EU und muss nicht in nationales Recht umgesetzt werden. Die DSGVO adressiert den Schutz personenbezogener Daten. Die DSGVO ist damit auch eine Basisanforderung der beteiligten Rollen – Betreiber, Systemintegrator und Produktlieferant – in der Energieautomatisierung.

Allen Regulierungen gemeinsam ist, dass sie einen ganzheitlichen Ansatz verfolgen. Als ganzheitlicher Ansatz ist hier die Betrachtung von Menschen, Prozessen und Technologie gemeint. Das schwächste Glied in der Kette bestimmt immer die Gesamtsicherheit. Dieses schwächste Glied kann ein Mensch, ein Prozess oder eine technische Einrichtung sein.

Alle beteiligten Rollen müssen ihren Beitrag für eine sichere Infrastruktur leisten (*Bild 1*).

Dipl.-Ing. ***Andreas Kohl*** (links)**,** Lifecycle Manager Cyber Security, Energy Management Division, Digital Grid, Siemens AG, Nürnberg
Dipl.-Inf. ***Chaitanya Bisale,*** Product Lifecycle Manager, Senior Key Expert Cyber Security, Energy Management Division, Digital Grid, Siemens AG, Nürnberg

Betreiber

Die wesentliche Anforderung an den Betreiber ist die verpflichtende Implementierung eines ISMS (Informations Sicherheits Management Systems) gemäß ISO/IEC 27001. Dieser Prozess fordert den Betreiber, dem Risiko entsprechende Maßnahmen in der Infrastruktur zu implementieren.

Systemintegrator

Auch für den Systemintegrator und Dienstleister ist es essentiell, seine eigene Infrastruktur zu schützen. Dafür bietet sich ein ISO/IEC 27001 konformes ISMS an. Der Schutz der eigenen IT-Infrastruktur ist eine notwendige Voraussetzung um sichere Lösungen beim Betreiber zu installieren und zu warten. Die beim Systemintegrator gespeicherten Informationen zu einer Kundenanlage könnten im Falle einer Kompromittierung einen Angriff auf eine Kundenanlage erleichtern.

Die eigentlichen technischen Security-Anforderungen eines Systems sind im Standard IEC 62443-3-3 (siehe Kasten) formuliert. Der Integrationsprozess, also der Weg wie das System zu implementieren ist, ist im Standard IEC 62443-2-4 beschrieben.

Produktlieferant

Auch der Produktlieferant muss seine eigene Infrastruktur, am besten ISO/IEC 27001 konform, schützen. Kritische Daten beim Produktlieferant sind beispielsweise die Quelldateien der Software, die gegen unerlaubte Manipulation zu schützen sind. Ansonsten kann durch eine solche Manipulation dem potentiellen Angreifer eine »Hintertür« geöffnet werden.

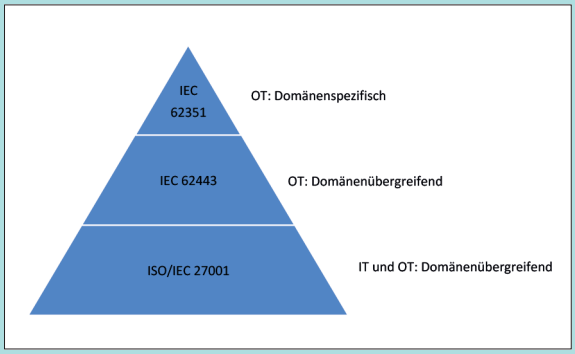
Die in den Komponenten implementierten Funktionen sollten dem Stand der Technik entsprechen und interoperabel sein. Das Gewährleistet die Implementierung konform zur Security Standardreihe IEC 62351.

Lieferantenmanagement

Ein Thema des Standards ISO/IEC 27001, dass die Absicherung der Schnittstellen zwischen den be-

Internationale Security Standards:

Die in diesem Artikel erwähnten Standards haben einen unterschiedlichen Fokus in Bezug auf den Adressaten, technische oder prozessuale Ausrichtung und technische Tiefe der Anforderungen.



Aufeinander aufbauende Standards

Die ISO/IEC 27001 beschreibt Anforderungen an ein Informations Sicherheits Management System (ISMS). Formal deckt das ISMS alle Informationen ab, also auch die gedruckten und die gesprochenen Informationen. Freier formuliert: Wie betreibe ich eine Infrastruktur um die Informationen entsprechend ihrer Kritikalität zu schützen. Ob es sich bei der Infrastruktur um eine IT oder OT (Operational Technology) Infrastruktur handelt spielt dabei keine Rolle. Auch ist die ISO/IEC 27001 domänenübergreifend. Sie ist auf ein Office Infrastruktur einer Spielzeugfabrik genauso anwendbar wie auf eine Stationsautomatisierung der Energieversorgung als Teil der kritischen Infrastruktur. Die ISO/IEC 27001 ist damit ein Basisstandard, der Prozessanforderungen definiert.

Die IEC 62443 mit ihren 13 Teilen fokussiert auf den Schutz eines industriellen Automatisierungssystems (Industrial Automation and Control System, IACS) und damit auf eine OT Infrastruktur. Die Adressaten sind hierbei alle beteiligten Rollen, der Betreiber der Anlage, der Systemintegrator und der Produktlieferant. Es werden Prozessanforderungen als auch technische Anforderungen an einzelne Komponenten und an das Gesamtsystem formuliert. Die technischen Anforderungen formulieren generische Anforderungen, also das „WAS“, und lassen die detaillierte technische Lösung weitgehend offen.

Die letzte Ebene der Security Standards sind die OT und domänenspezifischen Security Standards. Als Beispiel dient die IEC 62351, die auf Basis der technischen Anforderungen der IEC 62443 das „WIE“ beschreibt. Die IEC 62351 adressiert Anforderungen an den Produktlieferanten und beschreibt wie die technische Lösung zu realisieren ist. Das Ziel ist hier die Interoperabilität. Die technische Tiefe ist daher hier die höchste der verschiedenen Ebenen. Die IEC 62351 ist domänenspezifisch und beschreibt die verschiedenen Verfahren für die Energieautomatisierung, beispielsweise die Sicherung der in der Energieautomatisierung verwendeten Kommunikationsprotokolle wie IEC 61850 oder IEC 60870-5-104.

Am Beispiel der Zugangssteuerung und Benutzerverwaltung sehen wir das nahtlose Ineinandergreifen dieser Standards.

Die ISO/IEC 27001 fordert einen implementierten Prozess beim Betreiber, der das „Need-to-Know“ Prinzip sicherstellt.

Die IEC 62443-3-3 fordert auf Systemebene eine technische Lösung für die Benutzerauthentifizierung und Autorisierung. Die Schärfe der Anforderung ist dabei Abhängig ob Zugriff innerhalb einer sicheren Zone, oder via unsichere Netze erfolgt.

Der Part 8 der IEC 62351 hingegen beschreibt wie die technische Lösung des RBAC (Role Based Access Control) zu implementieren ist, um Interoperabilität zu erreichen.

Dies ist eine mögliche Kategorisierung der Security Standards, um die Anwendung der Standards besser zu verstehen. Weitere finden sich in [1].

Die Anwendung dieser Standards deckt die Anforderungen des BDEW-Whitepapers [2] ab und geht in vielen Bereichen darüber hinaus.

teiligten Rollen beschreibt, ist das Lieferantenmanagement. Der Systemintegrator tritt als Lieferant des Betreibers auf. Der Betreiber muss also bei der Auswahl des Lieferanten nicht nur die Anforderungen an die technische Lösung beschreiben, sondern auch die Anforderungen an die Prozesse des Lieferanten definieren. Das gleiche gilt für die Beziehung zwischen Systemintegrator und Produktlieferant und natürlich auch für die Beziehung eines Produktlieferanten zu Lieferanten, die Bauelemente oder Softwarekomponenten zu Produkten bereitstellen. Ein kompromittiertes Bauelement oder eine kompromittierte Softwarekomponente bestimmt am Ende die Gesamtsicherheit der Lösung.

Das Lieferantenmanagement sollte die gesamte Lieferkette vom Bauteil oder Software einer Komponente bis hin zum Gesamtsystem lückenlos abdecken.

Eine vorhandene Zertifizierung von Lieferanten und Unterlieferanten gemäß ISO/IEC 27001 kann hier Vertrauen schaffen und Aufwände für eigene Lieferantenaudits reduzieren.

Zusammenfassung

Das Folgen von internationalen Security-Standards ist effizient und stellt eine effektive Security sicher. Warum? Internationale Standards sorgen für in sich abgestimmte Anforderungen. Es sind bei der Verwendung der Standards weniger

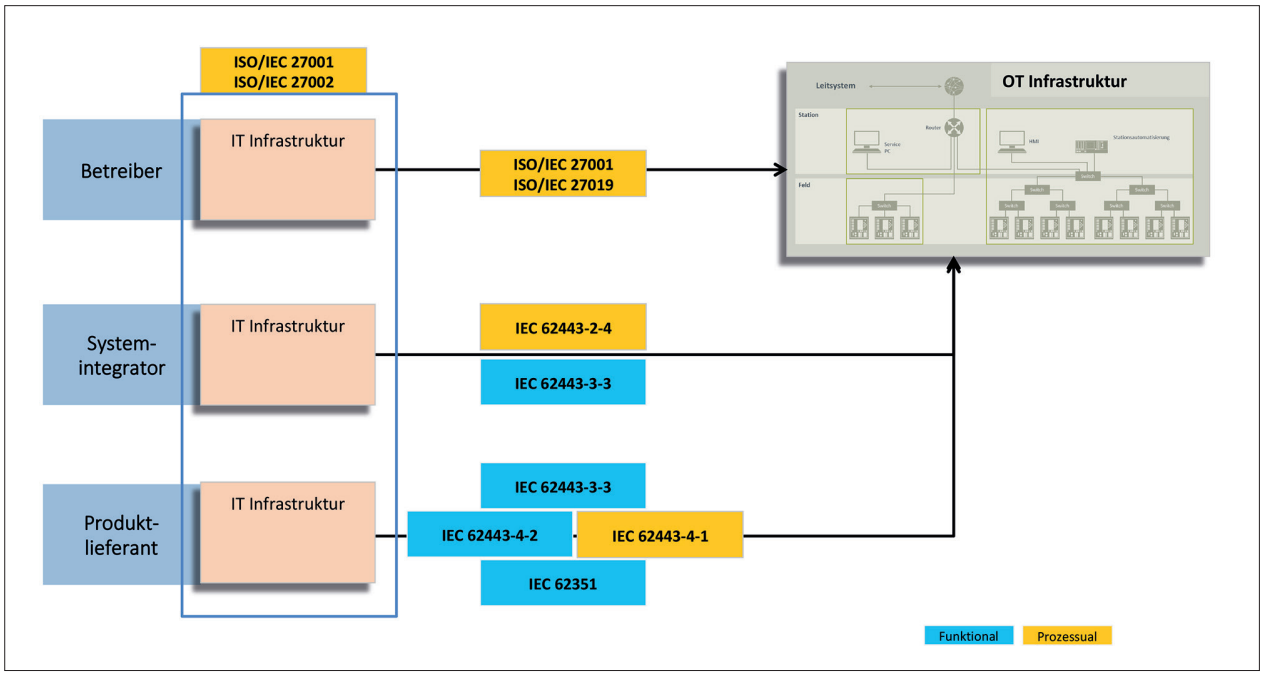


Bild 1: Anwendung der Standards für die beteiligten Rollen

Lücken zu erwarten als bei selbst definierten Anforderungen. Standards stellen Interoperabilität sicher. Das verweisen auf Standards wie IEC 62443 und IEC 62351 in einer Ausschreibung ist weniger fehleranfällig, beugt Missverständnissen vor und spart damit Zeit und Geld. Es würde auch niemand auf die Idee kommen, die Umweltanforderungen an Komponenten ohne die Verwendung von Standards zu definieren.

Die internationalen Standards bauen aufeinander auf, siehe auch Kasten »Internationale Security Standards«. Standards liefern eine klare Grundlage. Ein Lieferant der seine eigene Infrastruktur ISO/IEC 27001 konform betreibt, kann die Anforderungen eines Betreibers, der seine OT Infrastruktur konform zu ISO/IEC 27001 betreiben muss, besser verstehen.

Darüber hinaus ist eine Zertifizierung nur auf Basis internationaler Standards sinnvoll und vergleichbar. Die von Betreibern, begründet durch das Thema Lieferantenmanagement, zunehmend geforderte ISO/IEC 27001 Zertifizierung der Lieferanten kann dabei zusätzliches Vertrauen schaffen.

Schrifttum

[1] Cyber Security & Privacy; CEN-Cenelec-ETSI Smart Energy Grid Coordination Group; 2016-12

[2] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V; Österreichs Energie: Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme, Vollständig überarbeitete Version 2.0, 05/2018

andreas.kohl@siemens.com

Chaitanya.b@siemens.com

www.siemens.com