FRI
Forschungsgruppe
Rechnernetze und Informationssicherheit

HSB
Hochschule Bremen
City University of Applied Sciences

# Zusammenfassung relevanter Informationssicherheitsstandards für deutsche Verteilungsnetzbetreiber

## Systemsicherheit von Energieversorgungsnetzen bei Einbindung von Informations- und Kommunikationstechnologien (SEnCom)

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

SEnCom

**Autoren:** Carl-Heinz Genzel, Olav Hoffmann, Prof. Dr. Richard Sethmann
Forschungsgruppe Rechnernetze und Informationssicherheit
Hochschule Bremen

**Datum:** 17.11.2017

---

# 1 Vorwort

Die IT-gestützte Leittechnik ist ein zentrales Element der Betriebsführung elektrischer Übertragungs- und Verteilungsnetze. Sie dient insbesondere der Informationsunterstützung des verantwortlichen (Netzleittechnik-)Personals zur zeitnahen, aktiven Antizipation von Fehlern und entsprechendem Fehlerklärungsverhalten sowie der reaktiven Fehlerbeseitigung nach Eintritt eines Netzfehlers (d. h. Fehlerursache, Fehlerzustand und Systemversagen). Vermehrt wird die Leittechnik auch zur aktiven Stützung bei der Auswahl zielführender Netzzustände im Rahmen einer Netzzustandsoptimierung verwendet. Im Gegensatz zum aktuellen Stand der Technik werden zukünftig weitere IT-gestützte Anwendungen im Rahmen des Ausbaus dezentraler Energieeinheiten sowie der gesetzlich vorgeschriebenen Zunahme von Smart-Metering-Systemen im Niederspannungsbereich antizipiert. Zu diesen Anwendungen gehören unter anderem neue bzw. erweiterte Verfahren zur Netzberechnung, Störanalyse oder Schaltauftragsverwaltung. Die hieraus entstehenden zusätzlichen Informationen und Anwendungen sind maßgeblich für das Gelingen der Energiewende in Deutschland. Hierbei ist jedoch sicherzustellen, dass die Versorgungssicherheit, von aktuell hoher Güte, durch die neuen Informationen und Anwendungen, vor allem im Niederspannungsbereich, nicht verringert wird.

Für den sicheren Betrieb von zukünftigen Verteilungsnetzen ist die Informationssicherheit deshalb von großer Bedeutung. Im Sinne des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) hat die Bundesnetzagentur (BNetzA) hierzu gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) den IT-Sicherheitskatalog gemäß §11 Absatz 1a Energiewirtschaftsgesetz (IT-Sicherheitskatalog) entwickelt [Bun15b].

In dem IT-Sicherheitskatalog definieren die beiden Behörden die folgende Kernanforderung zur Erhöhung der IT-Sicherheit in Energieversorgungsunternehmen (EVU):

*„Kernforderung des vorliegenden Sicherheitskatalogs ist die Einführung eines Informationssicherheits-Managementsystems [ISMS] gemäß DIN ISO/IEC 27001 sowie die Zertifizierung durch eine unabhängige hierfür zugelassene Stelle. […] Die Anforderungen des Sicherheitskatalogs sind unabhängig von der Größe oder der Anzahl der angeschlossenen Kunden von allen Netzbetreibern zu erfüllen, soweit diese über Systeme verfügen, die in den Anwendungsbereich des Sicherheitskatalogs fallen […].“*[Bun15]

Ziel dieser Kernanforderung ist die Erhöhung der Informationssicherheit technischer Anlagen sowie die Erhöhung der allgemeinen Versorgungssicherheit vor dem Hintergrund der eingangs angesprochenen immer stärkeren Durchdringung des Betriebs von EVU mit Informations- und Kommunikationstechnologie (IKT). Es wird ein angemessener Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme gefordert [Bun15]. Der angemessene Schutz wird dabei durch die Behörden wie folgt definiert:

*„Ein angemessener Schutz liegt gemäß § 11 Absatz 1a S. 4 EnWG vor, wenn der Katalog der Sicherheitsanforderungen vom Betreiber eines Energieversorgungsnetzes eingehalten wird. Der IT-Sicherheitskatalog stellt insofern einen Mindeststandard dar. Dabei hat der Netzbetreiber insbesondere auch den allgemein anerkannten „Stand der Technik“ in Bezug auf die Absicherung der jeweils eingesetzten Systeme zu beachten sowie die allgemeine IKT-Bedrohungslage und die spezifische Bedrohungslage für die eingesetzten Systeme zu berücksichtigen. Dazu sind geeignete, für den jeweiligen Anwendungsbereich formulierte, ggf. branchen- oder sektorspezifische*

*Sicherheitsstandards sowie relevante Empfehlungen, Anwendungsregeln etc. nach jeweils aktuellem Stand heranzuziehen."[Bun15]*

Zur Umsetzung dieser Vorgaben sind ausgeprägte Kenntnisse zur IT-Sicherheit in Form von Gefahren und Gegenmaßnahmen bei den für die IT verantwortlichen Personen eines EVU und speziell im Verteilungsnetz entscheidend. In der Praxis zeigt sich jedoch, dass das Wissen dieses Personenkreises im Bezug auf die Informationssicherheit sehr unterschiedlich ausgeprägt ist. Die Vielzahl bestehender Standards und Empfehlungen zum Thema IT-Sicherheit insbesondere zur Absicherung von IT-Infrastrukturen stellt darüber hinaus eine Herausforderung dar. Zuerst müssen die relevanten Standards identifiziert werden, die zu dem Anwendungsbereich passen. Anschließend müssen die Standards auch gelesen und verstanden werden. Diese Herausforderungen sind meistens nicht ohne ein entsprechendes Vorwissen zu bewältigen, da Standards oft allgemein formuliert sind. In der Folge entstehen, bei einem Anwender, während des Lesens meist Fragen nach konkreten Anwendungshinweisen.

Dieses Dokument soll eine Hilfestellung zu den genannten Problemen für Personen mit Verantwortung für IT bei EVU, insbesondere im Verteilungsnetz, bieten. Hierzu werden relevante Standards mit Bezug auf die Informationssicherheit im deutschen Energienetz, ausgehend von dem IT-Sicherheitskatalog, identifiziert und zusammengefasst. Die Zusammenfassung dient als Orientierung zu den Sicherheitsmaßnahmen in den untersuchten Standards für den oben genannten Personenkreis von EVU. Im Rahmen dieses Dokumentes werden organisatorische Aspekte eines ISMS dabei bewusst nur oberflächlich zur Einordnung betrachtet, da die Struktur und der Unternehmenscharakter eines EVU bei der Umsetzung organisatorischer Vorgaben eine wesentliche Rolle spielen. Eine Pauschalisierung ist an dieser Stelle nicht möglich. Stattdessen wird es als sinnvoller erachtet, dass ein EVU mit Hilfe von Experten (z. B. mit Hilfe eines Dienstleisters) eine entsprechende IT-Sicherheitsorganisation etabliert in deren Rahmen die einzelnen organisatorischen Aspekte gemäß ISO/IEC 27001 sowie die Werte und Risiken eines EVU erarbeitet werden. Hieraus entsteht dann zwangsläufig ein Bedarf nach technischen Sicherheitsmaßnahmen zum Schutz der festgestellten Werte und zur Minderung der erkannten Risiken. Der Bedarf muss jedoch nicht notwendigerweise bereits zu Beginn eines ISMS vollständig umgesetzt werden. Dies wird im Rahmen der Zertifizierung nicht verlangt, solang ein grundlegendes Sicherheitsniveau vorhanden ist. Vielmehr kann ein EVU einen Plan zur Umsetzung verschiedener Maßnahmen erstellen [Deu15]. Hierbei können im Gegensatz zu den organisatorischen Aspekten pauschalisierte Methoden wie Checklisten zur Auswahl von technischen Sicherheitsmaßnahmen eingesetzt werden. Dementsprechend soll dieses Dokument einem EVU helfen, eigenständig, technische Sicherheitsmaßnahmen erkennen zu können. Dieses Dokument dient zudem als Einstieg in die Vorgaben bestehender Standards für verantwortliche Personen im Bereich der IT eines EVU und Netzbetreibers.

# 2 Lebenszyklus und technische Maßnahmen im ISMS

Das Vorgehen in einem ISMS ist nach dem Plan-Do-Check-Act (PDCA)-Zyklus (vgl. [Bun15] u. [Deu15]) in Abbildung 1 organisiert.

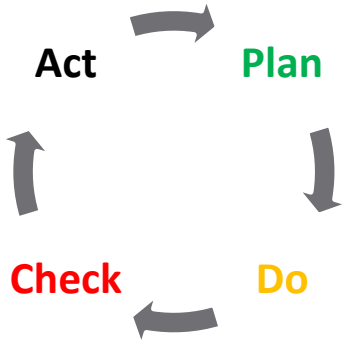


Abbildung 1: Plan-Do-Check-Act (PDCA)-Zyklus

Zu Beginn des Zyklus in der **Plan-Phase** werden relevante, zu schützende Prozesse und Werte identifiziert und inventarisiert. Ein sogenannter Scope oder Geltungsbereich wird hierzu festgelegt. Für EVU ist der minimale Geltungsbereich durch den IT-Sicherheitskatalog geregelt:

*„Der Geltungsbereich des vorliegenden IT-Sicherheitskatalogs umfasst alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind. Enthalten sind demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise. Daneben sind auch TK- und EDV-Systeme im Netz betroffen, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte. Darunter fallen z. B. Messeinrichtungen an Trafo- oder Netzkoppelstationen.“*

Innerhalb dieses Geltungsbereichs wird daraufhin eine Kommunikations- und Informationssicherheitspolitik definiert. Hierzu gehört die Festlegung von Leitlinien, Zielen, Prozessen sowie Verfahren für das Risikomanagement und die Verbesserung der Informationssicherheit. Außerdem müssen Verantwortlichkeiten festgelegt werden. Für die Umsetzung dieser organisatorischen Elemente ist eine Risikoanalyse zur Bestimmung der Informationssicherheit und der aktuellen Gefährdungslage im Geltungsbereich notwendig.

Hiernach folgt der Übergang in die **Do-Phase**. In dieser Phase werden fehlenden Überwachungs- und Schutzmaßnahmen eingeführt. Dies erfolgt auf der Basis von identifizierten Sicherheitsanforderungen der relevanten Werte und Prozesse in Verbindung mit der durchgeführten Risikoanalyse. Zudem wird das Personal geschult, um die neuen Anforderungen umsetzen und mögliche Informationssicherheitsprobleme erkennen zu können. Darüber hinaus wird ein Notfallplan zur Aufrechterhaltung des Geschäftsbetriebs (Business Continuity) und der Informationssicherheit etabliert.

In der **Check-Phase** werden die Regelungen und Prozesse überwacht und sicherheitsrelevante Vorkommnisse aufgezeichnet. Die Vorkommnisse werden zudem ausgewertet, um neue Risiken zu erkennen und Prozesse und Werte sowie deren Sicherheitsmaßnahmen anzupassen. Hierbei werden interne sowie externe Audits durchgeführt.

Mit der **Act-Phase** können erkannte Risiken und Sicherheitsprobleme reflektiert werden. Es können Maßnahmen zur Verringerung der Risiken und Lösung der Probleme sowie allgemeine Verbesserungsmaßnahmen eingeleitet werden. Hiermit beginnt der Zyklus von vorne, da mit der Einführung von Änderungen im ISMS eine erneute Prüfung des Geltungsbereichs und eine erneute

Risikobewertung notwendig werden. Des Weiteren müssen unter Umständen Sicherheitsmaßnahmen angepasst werden.

Die Etablierung technischer Maßnahmen zur Erhöhung der Informationssicherheit lässt sich gemäß PDCA-Zyklus am besten in die Do-Phase einordnen, da hier die tatsächliche Umsetzung organisatorisch sowie technisch stattfindet. Die Erkenntnisse aus der vorhergehenden Plan-Phase sind in dieser Phase ein ideales Hilfsmittel sowohl zur Ermittlung der in diesem Dokument zusammengefassten organisatorischen und insbesondere technischen Maßnahmen aus den ausgesuchten Standards als auch zur weiteren Recherche in den referenzierten Standards.

# 3 Eingrenzung der Standards

Durch die Aktualität des Themas Smart-Grid gibt es diverse Standards und Empfehlungen verschiedener Nationen, die sich mit dem Thema intelligente Energienetze auseinandersetzen. Das Oldenburger Forschungs- und Entwicklungsinstitut für Informatik-Werkzeuge und Systeme (OFFIS e.V.) hat hierzu einen zusammenfassenden Überblick veröffentlicht (vgl. [Roh10], [Usl10]). Ein Großteil der dort erfassten Standards sind umfängliche Betrachtungen des Smart-Grids und der verschiedenen Szenarien und Teilnehmer. Hierzu zählen, neben dem Verteilungsnetz und verschiedenen energetischen Komponenten, auch das Smart-Metering-System, E-Mobilität sowie verschiedene wirtschaftliche Teilnehmer inklusive der Energiemakler. Ergänzend dazu ist die Definition, was ein Smart-Grid ist, nicht in jedem Land identisch [Roh10], [Usl10]. Aus diesem Grund wurde für den Forschungsbereich von SEnCom eine Eingrenzung auf Standards, die für ein deutsches Verteilungsnetz relevant sind, vorgenommen. Im Rahmen dieser Eingrenzung wurden zwei Gruppen von Standards als besonders relevant für das deutsche Verteilungsnetz eingestuft.

Zum einen sind es die Empfehlungen der European Network and Information Security Agency (ENISA). Die ENISA hat in einem zeitlichen Abstand, neben einer sogenannten Bedrohungslandkarte [Eur13a], zwei Dokumente mit Sicherheitsempfehlungen für das Smart-Grid herausgegeben, die zur Orientierung für nationale Standards in Europa dienen sollen (vgl. [Eur12], [Eur13b]). Das erste Dokument [Eur12] besteht aus einer Sammlung von Sicherheitsmaßnahmen aus unterschiedlichen nationalen und internationalen Standards sowie aus verschiedenen weiteren Dokumenten beispielsweise von anderen staatlichen Organisationen oder Organisationen der Wissenschaft. Das zweite Dokument [Eur13b] baut auf den Vorarbeiten des ersten Dokuments auf und konsolidiert die Informationen des ersten Dokumentes zu einer Menge von Sicherheitsanforderungen, die mindestens notwendig sind. Hierbei wurden die Industrie sowie nationale Informationssicherheitsbehörden eingeladen, beratend mitzuwirken. Diese Sicherheits-anforderungen der ENISA fassen verschiedene internationale sowie nationale Standards, unter anderem der USA, zusammen und bilden daher einen guten allgemeinen Überblick zu notwendigen Informationssicherheitsmaßnahmen im Energiesektor. Der Inhalt des letztgenannten Standards fließt daher in diese Zusammenfassung relevanter Standards mit ein. Abbildung 2 zeigt hierzu einen Teil der durch die ENISA berücksichtigten Standards. Aufgrund der Verflechtungen zwischen den Standards besteht bei der Abbildung jedoch kein Anspruch auf Vollständigkeit, sie soll nur die Zusammenhänge verdeutlichen.

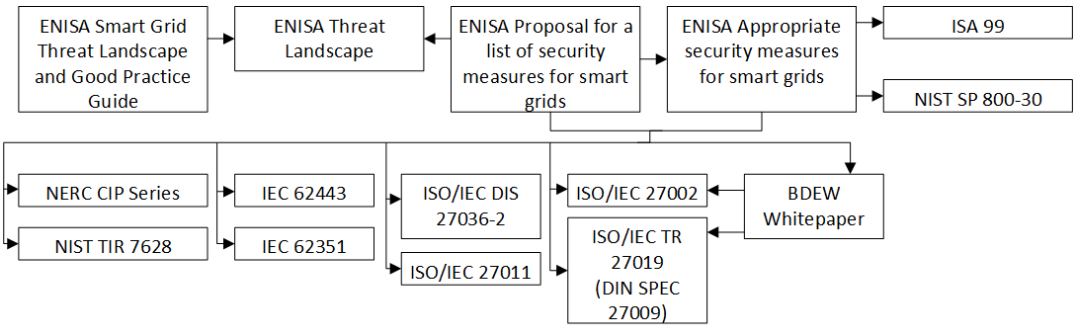


**Abbildung 2: Relevante Dokumente der ENISA und beeinflussende Standards**

Die Vorgaben der ENISA sind jedoch nur Empfehlungen. Im Gegensatz dazu sind die Vorgaben des IT-Sicherheitskatalogs in Deutschland, durch EVU verpflichtend umzusetzen und damit auch entsprechend relevant für die Zusammenfassung von Informationssicherheitsmaßnahmen in diesem Dokument. Im IT-Sicherheitskatalog wird auf Normen der internationalen Normenreihe ISO2700x (u. a. [Deu15], [Deu14]), auf den Bereich IT-Grundschutz (u. a. [Bun07], [Bun08]) und das sogenannte BDEW-Whitepaper [Bun15c] referenziert (vgl. [Bun15b]). Im Rahmen der Normenreihe ISO/IEC 2700x ist vor allem die Norm ISO/IEC 27001 ausschlaggebend, da sie die Anforderungen an ein sogenanntes Informationssicherheitsmanagementsystem (Information Security Management System (ISMS)) definiert. Gemäß IT-Sicherheitskatalog müssen EVU ein solches ISMS etablieren. Die anderen Normen dieser Normenreihe enthalten weiterführende Hinweise und Richtlinien zur Realisierung der Anforderungen an ein ISMS. Die Norm ISO/IEC 27002 konkretisiert in diesem Zusammenhang die Vorgaben der ISO/IEC 27001. Darüber hinaus beschreibt die Norm ISO/IEC TR 27019 ergänzend zur ISO/IEC 27002 spezielle Aspekte im Bereich der Energieversorgung und damit auch der Verteilungsnetze. Die genannten Normen werden dementsprechend im Rahmen der Zusammenfassung aufgegriffen. Durch ihren starken Praxisbezug sind das BDEW-Whitepaper und der IT-Grundschutz in Verbindung mit den Ergänzungen durch das in Abbildung 3 dargestellte ICS-Security-Kompendium (vgl. [Bun13]) für die Zusammenfassung von Informationssicherheits-maßnahmen von besonderer Bedeutung. Das BDEW-Whitepaper ist ein eigenständiges Dokument, das verschiedene grundlegende Sicherheitsanforderungen für EVU in Form eines Leitfadens enthält. Das BDEW-Whitepaper zielt insbesondere darauf ab, EVU bei der Formulierung von Sicherheitsanforderungen an Systemhersteller und Integratoren sowie Lieferanten in Form eines sogenannten Lastenheftes zu unterstützen. Das Dokument verweist dabei auch auf die ISO/IEC 27002 und ISO/IEC TR 27019 für zusätzliche Informationen [Bun15c]. Das BDEW-Whitepaper gilt in der deutschen Energiebranche als ein de facto Standard zur Umsetzung eines grundlegenden Sicherheitsniveaus und wird beispielsweise von Herstellern für Leittechnik entsprechend berücksichtigt [CT13]. Der IT-Grundschutz wurde dagegen für konventionelle IT-Verbünde entworfen. Er enthält eine Beschreibung für einen deutschen ISMS-Ansatz, der auf dem Standard ISO/IEC 27001 basiert und zertifizierbar ist [Bun07]. Teile dieses Ansatzes sind auch in den IT-Sicherheitskatalog eingeflossen (z. B. die Netzstrukturanalyse) [Bun15b]. Außerdem enthält der IT-Grundschutz einen Maßnahmenkatalog mit grundlegenden Sicherheitsmaßnahmen für konventionelle IT-Systeme [Bun08]. Durch den Fokus des IT-Grundschutzes auf konventionelle IT, ist dieser aber nur in Teilen auf die IKT eines Verteilungsnetzbetreibers anwendbar (z. B. auf Server der Leitwarte). Aus diesem Grund liegt der IT-Grundschutz im Gegensatz zu den anderen genannten Dokumenten nicht im Fokus der Zusammenfassung. Speziell für industrielle Steuerungssysteme (Industrial Control Systems (ICS)), wie die Systeme eines EVU im Feld, hat das BSI aber das sogenannte ICS-Security-Kompendium veröffentlicht, das Informationssicherheitsmaßnahmen für diese Systeme spezifiziert und anstelle

des IT-Grundschutzes für diese Zusammenfassung herangezogen wird. Das ICS-Security-Kompendium besitzt einen konkreten Zusammenhang (vgl. [Bun13]) zum IT-Grundschutz und Teile des Kompendiums sind im Rahmen der Modernisierung des IT-Grundschutzes (vgl. [Bun15a]) als sogenannte Bausteine (vgl. [Bun16]) wiederzufinden. Abbildung 3 zeigt einen Teil der durch den IT-Sicherheitskatalog berücksichtigten Standards. Aufgrund der Verflechtungen zwischen den Standards besteht auch hier kein Anspruch auf Vollständigkeit, es soll lediglich der Zusammenhang verdeutlicht werden.

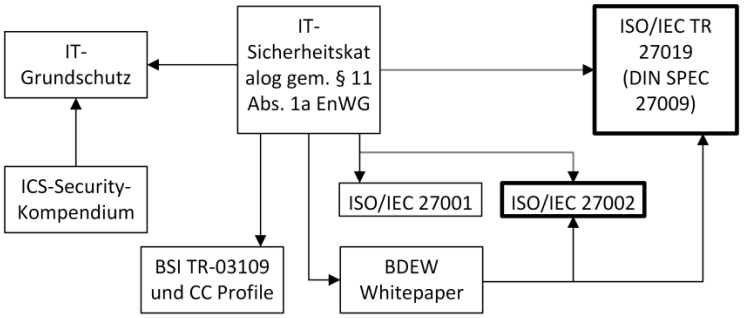


**Abbildung 3: Der IT-Sicherheitskatalog und beeinflussende Standards**

Im weiteren Verlauf werden somit die folgenden zuvor identifizierten Standards für die Zusammenfassung von Informationssicherheitsmaßnahmen in einem Verteilungsnetz herangezogen:

- ISO/IEC 27001 (Anforderungen an ein ISMS)
- ISO/IEC 27002 (Leitfaden für ein ISMS)
- ISO/IEC TR 27019 (Leitfaden für ein ISMS für die Energieversorgung auf Basis von ISO/IEC 27002)
- BDEW-Whitepaper (Anforderungen an sichere Steuerungssysteme und Telekommunikationssysteme)
- ICS-Security-Kompendium (Grundlagenwerk für die IT-Security in ICS des BSI)
- Proposal for a list of security measures for smart grids (Sammlung von Good Practices für Stakeholder im intelligenten Energienetz der ENISA)

Die Inhalte der genannten Standards wurden im Rahmen der Recherche im Forschungsprojekt SEnCom als besonders relevant für die Umsetzung von IT-Sicherheit, in einem deutschen intelligenten Verteilungsnetz, eingestuft. Ausländische Standards wurden nicht berücksichtigt, da die Inhalte zum größten Teil in den aufgelisteten Standards enthalten sind und dafür bereits für deutsche intelligente Energienetze adaptiert wurden. Im Allgemeinen ist allerdings zu beachten, dass eine hundertprozentige Informationssicherheit durch die Einhaltung von Standards allein nicht gewährleistet werden kann. Dies liegt zum einen daran, dass jede Umgebung eigene Besonderheiten besitzt, die gesondert berücksichtigt werden müssen. Zum anderen ist eine hundertprozentige Informationssicherheit durch das Vorhandensein von menschlichen und technischen Fehlern nicht erreichbar. Es können jedoch mit Hilfe der Sicherheitsmaßnahmen, in den ausgewählten Standards, viele Sicherheitslücken behoben bzw. vor der Ausnutzung geschützt werden.

# 4 Zusammenfassung der Maßnahmen

Die Norm ISO/IEC 27001 enthält die Basisanforderungen an ein ISMS. Alle im Rahmen dieses Dokumentes behandelten Standards referenzieren daher auf diese Norm. Die Inhalte der einzelnen Standards werden dabei meist den Anforderungen der ISO/IEC 27001 direkt oder indirekt zugeordnet

(vgl. [Bun13], [Bun15c], [Eur13b]). Zur besseren Orientierung stehen die folgenden Erläuterungen zu den technischen Maßnahmen in den einzelnen Standards deshalb auch immer in Beziehung zu den Punkten des Anhangs A der Norm ISO/IEC 27001 (s. [Deu15]). Für die Zusammenfassung der technischen Maßnahmen wurden daraus die folgenden Kategorien gebildet.

1) Grundlegende organisatorische Aspekte und Verwaltungsanforderungen
2) Erfassung und Umgang mit Unternehmenswerten
3) Aspekte und Anforderungen zur physischen Sicherheit von Objekten und Systemen
4) Aspekte und Anforderungen des IT-Betriebs
5) Ergänzende Sicherheitsmaßnahmen beim Umgang mit Dienstleistern
6) Safety vs. Security

Die genannten Kategorien werden im Folgenden als einzelne Kapitel, für die zusammenfassende Darstellung der einzelnen Standards und ihrer Maßnahmen, eingesetzt. Die Maßnahmen werden dabei in organisatorische und technische Maßnahmen unterschieden. Als **organisatorische Maßnahmen** werden im Rahmen dieses Dokumentes Maßnahmen, die hauptsächlich durch menschliche Handlungen realisiert werden müssen, angesehen. Die Dokumentation von Prozessen oder die Sensibilisierung von Mitarbeitern sowie die Erstellung von Richtlinien gehören hierzu. Als **technische Maßnahmen** werden dagegen Maßnahmen bezeichnet, die beispielsweise durch Computeranwendungen automatisiert oder durch physische Konstruktionen realisiert werden und demnach weitestgehend ohne menschliche Interaktion bestehen können.

Bei der zusammenfassenden Beschreibung der Maßnahmen werden Referenzen angegeben, um eine weiterführende Recherche in den jeweiligen Standards zu ermöglichen. Diese Referenzen weichen aus Gründen der Lesbarkeit von den allgemeinen Literaturangaben ab, die folgende Zuordnung wird verwendet: ISO27001/[Deu15], ISO27002/[Deu14], ISO27019/[Deu14], BDEW/[Bun15c], ICSSecK/[Bun13], ENISA/[Eur13b].

Zu Präzisierung der Referenzen werden nummerierte Elemente (z. B. Überschriftennummern) aus den jeweiligen Standards mit angegeben. An verschiedenen Stellen werden zudem erläuternde Beispiele und Schlüsselworte, zum Teil in Fußnoten, für zusätzliche Recherchemöglichkeit eingesetzt. Da der Fokus dieser Zusammenfassung auf den technischen Maßnahmen beruht, werden die verschiedenen technischen Hinweise aus den untersuchten Dokumenten detaillierter, als die organisatorischen Hinweise, beschrieben. Organisatorische Maßnahmen werden dagegen zur Einordnung oberflächlich erwähnt, aber nicht genauer dargestellt.

## 4.1 Grundlegende organisatorische Aspekte und Verwaltungsanforderungen

Zu den grundlegenden organisatorischen Aspekten und Verwaltungsanforderungen werden in diesem Dokument im Wesentlichen alle organisatorischen und technischen Maßnahmen zur Verbesserung der IT-Sicherheit eingeordnet, die allgemeine Anforderungen an ein Unternehmen stellen. Hierzu gehören die Erstellung und regelmäßige Kontrolle von übergeordneten Sicherheitsrichtlinien und die allgemeine Berücksichtigung von Informationssicherheit in allen Bereichen eines Unternehmens, insbesondere bei der Durchführung von Projekten [ISO27001 A.5.1.1, A.5.1.2, A.6.1.5], [ISO27002 5.1.1, 5.1.2, 6.1.5], [ICSSecK 2], [ENISA D1].

### 4.1.1 Allgemeine Rahmenbedingungen

Bei der Etablierung von allgemeinen Anforderungen sind insbesondere alle für ein Unternehmen geltenden rechtlichen Rahmenbedingungen zu betrachten. Hierzu zählen allgemeine als auch branchenspezifische Gesetze, Standards und vertragliche Vorschriften. Zu diesen Rahmenbedingungen gehören unter anderem Regelungen zum Umgang mit geistigem Eigentum, personenbezogenen Daten sowie der Privatsphäre des Einzelnen. Außerdem müssen kryptografischen Anforderungen im Umgang mit den vorhergenannten Aspekten beachtet und festgelegt werden. Die Einhaltung der gesetzlichen und anderweitigen Vorschriften ist dabei je nach Anforderung durch unabhängige Prüfer, interne leitende Angestellte und entsprechendes Fachpersonal auf technischer sowie organisatorischer Ebene zu überwachen und zu dokumentieren. Für technische Maßnahmen können dazu technische Werkzeuge zur automatisierten Prüfung herangezogen werden, sofern sie verfügbar sind. Daraus hervorgehende Audit-Protokolle (z. B. zum Stand der IT-Sicherheit im Unternehmen), wie auch andere Aufzeichnungen über oder zu gesetzlichen sowie anderweitig vorgeschriebenen Rahmenbedingungen, wie Geschäftsbücher oder Transaktionsprotokolle sind, wenn nötig, zu schützen. Die sensiblen Daten müssen hierzu unter anderem auf Medien aufbewahrt werden, die die nötigen Aufbewahrungsfristen unterstützen. Je nach Bedarf (vgl. 4.2.3 Klassifizierung) müssen Aufzeichnungen zudem kryptografisch vor Veränderung oder unbefugter Einsichtnahme geschützt werden und es können zusätzliche Prozesse zur Sicherstellung der Verfügbarkeit der Aufzeichnungen eingeführt werden [ISO27001 A.18.1.1, A.18.1.2, A.18.1.4, A.18.1.5, A.18.2.ff], [ISO27002 18.1.1, 18.1.2, 18.1.4, 18.1.5, 18.2.ff], [ISO27019 15.1.1], [BDEW 2.1.1.6, 2.4.6], [ICSSecK 9, 17, 18, 21, 58], [ENISA D1].

### 4.1.2 Verantwortlichkeiten und Rollen

Zur Umsetzung von Anforderungen an die Informationssicherheit müssen in einem Unternehmen entsprechende Verantwortlichkeiten auf verschiedenen Ebenen zugeordnet werden. Hierbei ist es wichtig, keine Interessenskonflikte zu erzeugen. Eine Trennung von widersprechenden Aufgaben in unterschiedliche Rollen und Personen ist notwendig [ISO27001 A.6.1.1, A.6.1.2], [ISO27002 6.1.1, 6.1.2], [ICSSecK 1, 10, 15], [ENISA D1]. Ein Beispiel hierfür ist die Aufteilung der Verantwortung für Unternehmens- oder Systemänderungen auf mindestens zwei Rollen und gleichermaßen auf mindestens zwei Personen. Eine Person ist für die Prüfung und Freigabe von Änderungen zuständig. Die andere Person ist für die Umsetzung von Änderungen zuständig [ICSSecK 11]. Für den technischen Bereich beschreibt das BDEW-Whitepaper im Detail, dass zur Verwaltung von Systemen mindesten die folgenden Rollen vorhanden sein sollten (s. [BDEW 2.4.1.1]):

1. Administrator-Rolle, die dazu berechtigt ist, ein System zu verändern.
2. Auditor-Rolle, die nur Informationen über ein System (z. B. Ereignisprotokolle) einsehen darf.
3. Operator-Rolle, die ein System im Rahmen der geschäftlichen Nutzung bedient.
4. Data-Display-Rolle, die den Status eines Systems und notwendige Betriebsdaten lesen darf.
5. Backup-Operator-Rolle (bei Bedarf), die für die Datensicherung aller relevanten Daten eines Systems zuständig ist.

### 4.1.3 Mitarbeiter

Um sicherzustellen, dass die Maßnahmen eines Unternehmens zur Informationssicherheit nicht von innen heraus unterwandert werden, ist es notwendig, Personen, die sich bei dem Unternehmen bewerben, einer Sicherheitsüberprüfung zu unterziehen. Die Art der Überprüfung sollte dabei an der zukünftigen Verantwortung einer Person ausgerichtet sein. Personen mit besonders hoher Verantwortung müssen auch genauer überprüft werden. Jede Person in einem Unternehmen sollte

zudem vertraglich auf ihre Rolle im Unternehmen sowie die damit verbundenen Rechte und Pflichten als auch auf eventuelle Konsequenzen für ihr handeln, insbesondere mit Bezug auf die Informationssicherheit (möglichst bei ihrer Einstellung), hingewiesen werden. Darüber hinaus müssen Personen im Rahmen ihres Verantwortungsbereichs entsprechend weitergebildet werden, so dass sie in der Lage sind, mit Werten des Unternehmens sicher umzugehen. Auch für das Ausscheiden einer Person aus dem Unternehmen müssen entsprechende Regelungen getroffen werden, um die Informationssicherheit, insbesondere nach dem Ausscheiden, durch die entsprechende Person nicht zu gefährden (z. B. Geheimhaltungsvereinbarung). Die genannten Maßnahmen sind besonders für den Energiesektor relevant, sofern es sich um Unternehmen handelt, die Teil einer kritischen Infrastruktur sind. Hier sind eventuelle schärfere Regeln und Überprüfungen (z. B. ausführliche Sicherheitsüberprüfungen und Regelungen zu höherer Belastung in Notsituationen) notwendig [ISO27001 A.7.1.ff, A.7.2.ff, A.7.3.ff], [ISO27002 7.1.ff, A.7.2.ff, 7.3.ff], [ISO27019 8.1.2, 8.1.3], [BDEW 2.1.2.2], [ICSSecK 14, 15, 16], [ENISA D4].

### 4.1.4 Informationssicherheitsvorfälle

Informationssicherheitsvorfälle können trotz guter Absicherung auftreten. Ein Unternehmen muss daher in der Lage sein, auftretende Informationssicherheitsvorfälle zu beherrschen. Hierzu müssen Prozesse und verantwortliche Personen bzw. Rollen definiert sein, die ein Unternehmen in die Lage versetzen, Informationssicherheitsvorfälle zu erkennen und möglichst nachvollziehbar zu behandeln. Bei der Erkennung von Informationssicherheitsvorfällen sind die verantwortlichen Personen dabei auf die Mitarbeit aller mit dem Unternehmen verbundenen Personen angewiesen (z. B. durch Meldung möglicher Vorfälle). Außerdem muss ein Unternehmen in der Lage sein, Erkenntnisse aus den Vorfällen für die Verbesserung der eigenen Informationssicherheit abzuleiten. Für eventuelle rechtliche Konsequenzen ist die Sammlung von Beweismaterial zudem ein wesentlicher Bestandteil der verantwortlichen Personen [ISO27001 A.16.1.ff], [ISO27002 16.1.ff], [BDEW 2.5.6], [ICSSecK 12], [ENISA D5, D3].

### 4.1.5 Widrige Situationen

Besonders in widrigen Situationen, Krisen oder Katastrophen, können Informationssicherheitsvorfälle auftreten. Das Sicherheitsniveau in einem Unternehmen sollte daher, durch eine entsprechende Planung und Umsetzung von organisatorischen und technischen Maßnahmen, soweit es möglich ist, auch in widrigen Situationen aufrechterhalten werden, um den Geschäftsbetrieb (z. B. die Versorgung mit Energie) nicht zu gefährden. Dabei sollten Informationssicherheitsmaßnahmen die während widriger Umstände ihre Wirkung verlieren durch weitere Maßnahmen ergänzt werden. Wichtige Systeme sollten dazu redundant ausgelegt werden, um Ausfälle zu vermeiden. Im Energiesektor ist es dabei beispielsweise besonders wichtig, ein System für die Notfallkommunikation aufrecht zu halten. Die Maßnahmen sollten darüber hinaus regelmäßig auf ihre Wirkung überprüft werden [ISO27001 A.17.1.ff, A.17.2.1], [ISO27002 17.1.ff], [ISO27019 14.1.1], [BDEW 2.1.1.1], [ICSSecK 13], [ENISA D2, D7, D11].

### 4.1.6 Kontakte

Zur rechtzeitigen Identifikation möglicher Gefahren für die Informationssicherheit eines Unternehmens sollte ein Unternehmen Kontakte zu Behörden oder thematischen Gruppen aufbauen, um regelmäßig Informationen über bestehende Informationssicherheitsrisiken zu bekommen. Diese Kontakte sollten aber auch für die Verbreitung eigener Erfahrungen und Informationssicherheitsvorfälle genutzt werden. Speziell für den Energiesektor wird beispielsweise die Anbindung an ein nationales Cyberüberwachungszentrum vorgeschlagen. Zudem wird eine

Kooperation mit Herstellern eingesetzter Systeme bis zu einem gemeinsamen, branchenweiten Computer Emergency Response Team (CERT)[1] angeregt. Dies gilt besonders für Unternehmen im Bereich einer kritischen Infrastruktur [ISO27001 A.6.1.3, A.6.1.4], [ISO27002 6.1.3, 6.1.4], [ISO27019 6.1.6, 6.1.7], [ICSSecK 12], [ENISA D5].

## 4.2 Erfassung und Umgang mit Unternehmenswerten

Das Ziel aller Maßnahmen in den ausgewählten Standards ist der Schutz von Werten eines Unternehmens vor Verlust oder Kompromittierung. Im Bereich der Informationssicherheit bezieht sich dies vor allem auf Werte in Form von Informationen oder Daten, die im Rahmen der Informationsverarbeitung im Unternehmen entstehen oder verarbeitet werden.

### 4.2.1 Inventarisierung

Um sich ihrer Werte bewusst zu sein, müssen Unternehmen zuerst eine Aufstellung aller Werte vornehmen und dokumentieren. Neben Dokumenten zu Prozessen oder spezifische Unternehmensdaten, wie Kundendaten, Konstruktionsanleitungen oder speziell im Energiesektor z. B. Netzpläne, Geodaten und Krisenpläne gehören hierzu auch Konfigurationsdaten und informationsverarbeitende Systeme, da deren Verlust oder Kompromittierung einen starken Einfluss auf die Geschäftstätigkeit eines Unternehmens haben kann. Im Bereich der Energieversorgung zählen hierzu unter anderem leittechnische Software, Management- und Überwachungssysteme sowie Leittechnik und Automatisierungskomponenten [ISO27001 A. 8.1.1], [ISO27002 8.1.1], [ISO27019 7.1.1], [BDEW 2.3.1.3], [ICSSecK 4, 5], [ENISA D3]. Der IT-Sicherheitskatalog schreibt zur Inventarisierung dieser Systeme vor, dass ein Netzstrukturplan der eingesetzten Systeme und deren Verbindungen bei einem Netzbetreiber für den Bereich der Prozesssteuerung eines Energienetzes erstellt werden muss, sofern dieser noch nicht existiert (vgl. [Bun15], [ICSSecK 4]).

### 4.2.2 Verantwortlichkeit

Neben der Inventarisierung der einzelnen Werte ist es notwendig, Verantwortlichkeiten für die Werte zu deren Verwaltung zuzuteilen. Ein Teil dieser Verantwortung besteht in der Etablierung, Dokumentation und Überwachung von Richtlinien für den zulässigen Gebrauch durch Personen, die mit dem Unternehmen verbunden sind, und für die Rückgabe von Werten, wenn sie nicht mehr benötigt werden [ISO27001 A.8.1.2, A.8.1.3, A.8.1.4], [ISO27002 8.1.2, 8.1.3, 8.1.4], [ISO27019 7.1.2], [ENISA D3, D4], [ICSSecK 16].

### 4.2.3 Klassifizierung

Zur Vereinfachung dieser Aufgaben sollen Werte anhand eines unternehmensweiten Klassifizierungsschemas durch die verantwortlichen Personen eingeordnet werden. Das Klassifizierungsschema bietet eine Orientierung für die verantwortlichen Personen bei der Etablierung von Richtlinien zum Umgang mit Werten anhand der Klassen. Eine Klassenspezifikation kann zum Beispiel bereits Vorgaben zur Zugriffsbeschränkung oder Aufbewahrung, der entsprechend klassifizierten Werte, enthalten. Die Klassifizierung sollte auf der Basis von gesetzlichen Vorgaben, der Kritikalität und der Empfindlichkeit einzelner Werte gegenüber Verlust oder Kompromittierung, von einem Unternehmen umgesetzt werden [ISO27001 A.8.2.ff], [ISO27002 8.2.ff], [ISO27019 7.2.1], [ICSSecK 2], [ENISA D9].

[1] Das BSI bietet zum Beispiel mit dem CERT-Bund eine *„zentrale Anlaufstelle für präventive und reaktive Maßnahmen mit Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in Computersystemen“* an.

## 4.3 Aspekte und Anforderungen zur physischen Sicherheit von Objekten und Systemen

Die physische Sicherheit von Werten ist die Basis für weitere technische Sicherheitsmaßnahmen. Ohne eine Abgrenzung der unternehmenseigenen Werte und Systeme zur Umwelt können viele organisatorische und technische Maßnahmen umgangen werden und sind damit wirkungslos. Mit Hilfe physischer Sicherheitsmaßnahmen soll vor allem ein Schutz vor unbefugtem Zugriff, Diebstahl, Feuer, Wasser und anderweitigen externen umweltbedingten Bedrohungen gewährleistet werden.

### 4.3.1 Betriebsgelände, Gebäude und Räume

Bereiche eines Unternehmens, in denen sich Werte befinden oder verarbeitet werden, müssen zum Schutz der Werte gegen die Außenwelt in Form von Sicherheitszonen abgegrenzt werden. Bei der Auswahl der physischen Maßnahmen zur Abgrenzung kann die Klassifizierung der Werte zur Hilfe genommen werden (vgl. 4.2.3 Klassifizierung). Zur effektiven physischen Abgrenzung sind bauliche Maßnahmen, wie eine Gebäude- und Raumaufteilung mit sicheren Türen sowie Fenstern als auch ggf. eine Abgrenzung des Betriebsgeländes durch Zäune oder Mauern, notwendig. Dabei muss darauf geachtet werden, dass diese Abgrenzungen lückenlos und unauffällig gestaltet sind. Nur autorisierte Personen sollten einen Zutritt zu den entsprechenden Sicherheitszonen haben und über diese informiert sein. Der autorisierte Zutritt zum Betriebsgelände, zu Gebäuden und zu Räumen sollte durch Personen (z. B. ein besetzter Empfang oder Pförtner) oder technische Einrichtungen (z. B. Zugangskarten, Schranken oder Drehkreuze) kontrolliert werden. Bereiche, bei denen ein Zutritt von unautorisierten Personen nicht ausgeschlossen werden kann (z. B. Empfangs- oder Anlieferungsbereiche), sollten so gestaltet sein, dass ein unautorisierter Zutritt zu anderen Bereichen mit höherem Sicherheitsniveau nicht möglich ist. Zur Unterscheidung zwischen autorisierten und unautorisierten Personen sollten Kennzeichen (z. B. Mitarbeiter- und Besucherausweis) eingesetzt werden. Externe Personen sollten dabei während ihres Aufenthalts kontrolliert und überwacht werden. In besonders kritischen Fällen sollten auch autorisierte Personen nur unter Beaufsichtigung in einem Sicherheitsbereich arbeiten (Vier-Augen-Prinzip). Die Zugangsberechtigungen der Mitarbeiter sollten außerdem regelmäßig und bei bestimmten Ereignissen (z. B. Änderung der Rolle oder der Verantwortlichkeiten) überprüft werden. Abgesehen von der Zutritts- und Personenkontrolle muss darauf geachtet werden, dass Werte – insbesondere sensible Informationen – nicht außerhalb ihrer Sicherheitsbereiche einsehbar sind (z. B. durch Ausspähen über ein Fenster oder lauschen an einer dünnen Wand oder einem geöffneten Fenster) und entsprechende Zutrittskontrollmaßnahmen zum Schutz der Werte ihre Wirkung nicht verlieren. Hierbei gilt unter anderem der allgemeine Grundsatz des aufgeräumten Schreibtischs. Der Grundsatz besagt, dass sensible Informationen am Arbeitsplatz in jedweder Form immer unter Verschluss gehalten werden sollten und nicht offen einsehbar sein dürfen. Dazu gehören beispielsweise die Sperrung des Bildschirms bei Abwesenheit und gegebenenfalls die Verwendung von Blickschutzmaßnahmen während der Arbeit als auch die Ablage von ungenutzten Akten in verschlossenen Schränken. Neben diesem Grundsatz ist eine unautorisierte Nutzung von Vervielfältigungssystemen (z. B. Drucker oder Kopierer) zu vermeiden. Wenn nötig, sollte zudem der Gebrauch von Aufzeichnungsgeräten, wie Kameras oder Smart-Phones, ohne spezielle Erlaubnis innerhalb eines Sicherheitsbereichs, untersagt sein. Türen, Fenster, Tore oder andere Öffnungen, wie Belüftungsschächte, sind zudem durch Verriegelungen, Alarmvorrichtungen und/oder Überwachungsmaßnahmen, wie Kameras, vor unbefugtem Eindringen zu schützen. Für Bereiche, an denen ein Austausch von Werten (z. B. Anlieferung von Waren zur Verarbeitung und Abgabe von Produkten zur Auslieferung) stattfindet, müssen darüber hinaus zusätzliche Sicherheitsmaßnahmen zur Kontrolle des Austauschvorgangs

getroffen werden. Es sollte getrennte Zonen für eingehende und ausgehende Werte geben. Außerdem sollten eingehende Werte auf ihre Echtheit und ihren Zustand geprüft und der Eingang festgehalten werden, bevor sie an andere Stellen eines Unternehmens weitergereicht werden. Darüber hinaus sind Schutzmaßnahmen gegen Feuer und andere Umwelteinflüsse zu etablieren. Hierzu zählen Brandabschnitte und Brandschutztüren oder Hochwasserschutzmaßnahmen sowie elektronische Abschirmmechanismen. Bei der Auswahl geeigneter Schutzmaßnahmen sind hierbei die rechtlichen Rahmenbedingungen, wie Gesetze und Standards, mit einzubeziehen. [ISO27001 A.11.1.ff, A.11.2.9], [ISO27002 11.1.ff, 11.2.9], [ICSSecK 31], [ENISA D8].

### 4.3.2 Dezentrale Standorte, Leitstellen und Technikräume

Für EVU gibt es die Besonderheit, dass sich die Werte und informationsverarbeitende Systeme nicht auf einen oder wenige zentrale Unternehmensstandorte beschränken. Die Systeme und Werte für den Energietransport sowie für die dezentrale Energieerzeugung befinden sich verteilt im Netzgebiet; meist in kleinen Gebäudeeinheiten, die zum Teil das Eigentum Dritter, nicht direkt mit dem Unternehmen verbundener Parteien, sind. Diese verteilten Standorte sind darüber hinaus nur sporadisch (z. B. in Fehlersituation) mit Personal besetzt. Aus diesem Grund sind die genannten technischen Aspekte zum physischen Schutz an dieser Stelle besonders wichtig. Vor allen Dingen ist es wichtig Standorte zu nutzen, bei denen Umwelteinflüsse, wie Erdbeben oder besonders starke Wetterphänomene sowie Hochwasser möglichst ausgeschlossen werden können. Alternativ müssen hierfür entsprechend starke Schutzmaßnahmen etabliert werden. Eine weitere Anforderung an diese Standorte ist eine, im besonderen Maße, automatisierte Kontrolle. Hierzu sollten die Umgebungsbedingungen, wie die Temperatur und Luftfeuchtigkeit sowie spezielle Gase, wenn nötig, überwacht werden. Störungen an Anlagen müssen erkannt und behoben werden können. Es sollte unter anderem eine automatische Brandbekämpfung möglich sein. Entsprechende Alarmsysteme gegen unbefugtes Eindringen sollten ebenfalls vorhanden sein. In Bereichen, die nicht Eigentum des Unternehmens sind aber Werte und informationsverarbeitende Systeme des Unternehmens beinhalten, sind entsprechende Trennungen, beispielsweise durch abgetrennte Schaltschränke, zu realisieren. Die Komponenten des Unternehmens und deren Kommunikationstechnik sollten physisch von den Komponenten anderer Parteien getrennt sein. Auch wenn Leitstellen nicht außerhalb eines zentralen Standorts von einem EVU betrieben werden, gelten aufgrund ihrer Kritikalität ähnlich verschärfte Regeln für deren Bereich und angeschlossene Technikräume [ISO27019 9.1.1, 9.1.2, 9.1.9, 9.1.7, 9.1.8], [ICSSecK 31], [ENISA D8, D11].

### 4.3.3 Platzierung von Systemen und Geräten

Neben der Ausgestaltung von Gebäuden und Räumen sollten die informationsverarbeitenden Systeme und andere Geräte, ihrem Sicherheitsniveau entsprechend, passenden Räumlichkeiten zugeordnet werden. Dabei ist darauf zu achten, dass Systeme mit unterschiedlichem Informationsanspruch und Sicherheitsniveau voneinander getrennt werden, so dass Bereiche mit homogenen Sicherheitsanforderungen geschaffen werden können. Hierdurch bekommen Personen, die mit den Systemen und Geräten umgehen keinen Einblick in Werte des Unternehmens, für die sie nicht autorisiert sind. Systeme zur dauerhaften Speicherung von Daten müssen zum Beispiel nur durch wenige Personen physisch erreichbar sein und besitzen einen besonderen Schutzbedarf, weshalb sie von anderen Systemen getrennt werden sollten. Ein anderes Beispiel sind die Systeme zur Prozesssteuerung, häufig müssen diese Systeme nicht für das kaufmännische Personal erreichbar sein. Dieses Vorgehen ermöglicht die Verringerung der Absicherungsaufwände im Allgemeinen, durch eine Reduzierung der Bereiche mit besonderem Schutzbedarf, da die anderen Systeme in Bereichen mit geringerem Schutzbedarf platziert werden können. Die Trennung muss dabei nicht

immer durch bauliche Strukturen geschehen. Es können auch spezielle Gehäuse, Schränke oder Tresore eingesetzt werden. Diese Trennelemente können darüber hinaus neben der Zugriffsbeschränkung zum Schutz von Geräten in Bereichen mit extremen Umgebungsbedingungen (z. B. Hitze, Kälte oder Staub) eingesetzt werden. Hierfür müssen sie erwartungsgemäß Schutzmaßnahmen gegen entsprechende Bedingungen (z. B. Isolationsmaterial oder Staubfilter) aufweisen [ISO27001 A.11.2.1], [ISO27002 11.2.1], [ISO27019 9.2.1], [ICSSecK 31], [ENISA D8, D11].

### 4.3.4 Systeme und Geräte in fremden Umgebungen

Informationsverarbeitende Systeme und Geräte außerhalb von Unternehmensgrenzen benötigen einen besonderen Schutz. Im Allgemeinen sollten Systeme und Geräte daher nur nach einer vorhergehenden Genehmigung aus dem Unternehmen entfernt werden. Um Informationen eines Unternehmens nicht ungewollt aus dem Unternehmen zu entfernen, sollten Systeme und Geräte, die aus einer sicheren Unternehmensumgebung kommen und zukünftig in einer fremden Umgebung eingesetzt werden sollen, generell zuvor genau geprüft werden. Wenn möglich sollten alle sensiblen Daten sicher und unwiederbringlich gelöscht oder überschrieben werden, bevor das System an einer anderen Stelle eingesetzt wird. Dies gilt im Allgemeinen auch für jedes andere System bzw. Gerät, das aus dem Unternehmen entfernt oder für eine andere Aufgabe wiederverwendet werden soll, damit Datenlecks durch eine Änderung der Einsatzumgebung vermieden werden. Beim Einsatz in einer fremden Umgebung sollten zudem vertragliche Vereinbarungen zum sicheren Betrieb der Systeme und Geräte in dieser Umgebung mit den Verantwortlichen geschlossen werden. Dabei sind analog zur Trennung von System und Geräten mit unterschiedlichem Schutzbedarf (vgl. 4.3.3 Platzierung von Systemen und Geräten) entsprechende Grenzen zwischen den eigenen Systemen und Geräten und der fremden Umgebung zu errichten. Hierbei können Maßnahmen zur Zugriffskontrolle auf physischer Ebene als auch auf logischer Ebene, wie in diesem Dokument beschrieben, umgesetzt werden (vgl. 4.3.3 Platzierung von Systemen und Geräten, 4.4.6 Anmeldeverfahren, 4.4.17 Sicherheit durch Netzsegmentierung). Die Kopplung mit der fremden Umgebung sollte dabei möglichst lose sein, so dass eine Trennung leicht möglich ist. Die eigenen Geräte und Systeme sollten zudem aus der Ferne mit Hilfe sicherer Protokolle überwacht werden können und Vorort sollte eine physische Manipulation durch Maßnahmen wie Siegel leicht erkennbar sein. Zudem gilt, wie für andere unbeaufsichtigte Systeme und Geräte, dass die Systeme gegen eine Benutzung durch unautorisierte Personen jederzeit gesperrt sind (z. B. mit einer Tastensperre und mit einem Kennwort geschützten Zugriff). [ISO27001 A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8,], [ISO27002 11.2.5, 11.2.6, 11.2.7, 11.2.8,], [ICSSecK 8, 30, 56], [ENISA D3, D8].

### 4.3.5 Versorgungseinrichtungen

Neben dem direkten physischen Schutz von Systemen und anderen Geräten sollte auch die Anbindung dieser an Versorgungseinrichtungen (wie Strom) und Kommunikationsnetze geschützt werden. Die notwendigen Leitungsarten sollten möglichst getrennt von der Umwelt verlegt sein. Eine unterirdische Leitungsführung und Schutzmechanismen wie Panzerrohre können beispielsweise als technische Sicherheitsmaßnahmen eingesetzt werden. Darüber hinaus sollten Anschlusspunkte, wie Anschlussdosen oder Verteilerkästen, vor unbefugtem Zugriff geschützt werden. Diese Punkte sollten zum Beispiel abschließbar sein. Sofern möglich, sollten automatisierte Maßnahmen zur Erkennung von Manipulationen oder dem Anschluss nicht autorisierter Geräte und Systeme an diesen Punkten eingesetzt werden. Besonders im Energiesektor sind an dieser Stelle weitere nicht physische Maßnahmen zur Erhöhung der Sicherheit zu betrachten (vgl. 4.3.3 Platzierung von Systemen und Geräten, 4.4.6 Anmeldeverfahren, 4.4.17 Sicherheit durch Netzsegmentierung). Außerdem müssen unter Umständen Redundanzen und alternative Versorgungsmöglichkeiten für den Fall des Ausfalls

einer Versorgungseinrichtung zur Verfügung gestellt werden (z. B. redundante Kommunikationsinfrastruktur und Geräte zur unterbrechungsfreien Stromversorgung). Für den Bereich der Energieversorgung gilt diese in besonderem Maße, da bei einem Stromausfall zirkuläre Abhängigkeiten entstehen, so dass Notstromaggregate zur Verfügung stehen müssen, um diese zu vermeiden. Die Versorgungseinrichtungen und alternativen Versorgungsmöglichkeiten sollten dabei genauso wie Systeme und Geräte regelmäßig geprüft und gewartet werden. Hierbei ist das Wartungspersonal gegebenenfalls zu überwachen (z. B. bei externen Wartungsdienstleistungen) [ISO27001 A.11.2.2, A.11.2.3, A.11.2.4], [ISO27002 11.2.2, 11.2.3, A.11.2.4], [ISO27019 9.2.2, 9.2.3], [ENISA D8, D11, D3].

## 4.4 Aspekte und Anforderungen des IT-Betriebs

Die Sicherheitsmaßnahmen für den sicheren Betrieb von informationsverarbeitenden Systemen sind thematisch in allgemeine Anforderungen, Anforderungen zum Schutz der Systeme, Anforderungen zum Schutz der Kommunikationsinfrastruktur sowie spezielle Anforderungen zu der Entwicklung und Anschaffung von Systemen unterteilt. Der sichere Betrieb von informationsverarbeitenden Systemen ist dabei der Bereich mit den meisten technischen Maßnahmen.

### 4.4.1 Dokumentierter Betrieb

Grundsätzlich müssen konsistente Betriebsabläufe für den sicheren Betrieb von informationsverarbeitenden Systemen etabliert werden. Wiederkehrende Bedienabläufe sollten für die jeweiligen Benutzer dokumentiert sein. Bei den Betriebsabläufen in einem Unternehmen kann dabei zwischen Administrationsabläufen und einfachen Benutzerabläufen unterschieden werden. Insbesondere bei den Administrationsabläufen sollten sicherheitsrelevante Aspekte wie die Voraussetzungen für den sicheren Betrieb, die Sicherheitseinstellungen und sicherheitsrelevanten Systemmeldungen eines Systems in die Dokumentation aufgenommen werden. Dies ist für den Energiesektor im Bereich der kritischen Infrastrukturen besonders wichtig, da in diesem Rahmen zudem festgelegt sein sollte, wann eventuelle Maßnahmen für Störungs- oder Krisenfälle in Kraft treten [ISO27001 A.12.1.1], [ISO27002 12.1.1], [ISO27019 10.1.1], [BDEW 2.1.2.ff], [ICSSecK 2, 6].

### 4.4.2 Änderungen am Betrieb

Wenn organisatorische oder technische Änderungen an dem Betrieb in einem Unternehmen notwendig sind, müssen diese gesteuert werden. Hierzu gehören die Feststellung notwendiger Änderungen, deren Beurteilung sowie die Planung und Umsetzung dieser Änderung als auch die Möglichkeit eine Änderung bei auftretenden Problemen wieder rückgängig zu machen. Durchgeführte Änderungen müssen außerdem dokumentiert und bestehende Abhängigkeiten angepasst werden. Änderungen sollten dabei auf ein erforderliches Maß beschränkt werden, um die etablierten organisatorischen und technischen Maßnahmen nicht zu gefährden und Sicherheitslücken zu vermeiden. Auf der technischen Seite sollte sich ein System immer in einem sicheren Zustand befinden, in dem unnötige Zugriffsrechte, Programme und Dienste deinstalliert oder zumindest deaktiviert sind. Dieser Zustand ist nach jeder Änderung an einem informationsverarbeitenden System entsprechend zu prüfen [ISO27001 A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4], [ISO27002 12.1.2, 14.2.2, 14.2.3, 14.2.4], [BDEW 2.5.1, 2.5.4, 2.5.5, 2.2.1, 2.1.1.10], [ICSSecK 7, 11, 52], [ENISA D3]. Für die Identifizierung notwendiger Änderungen ist neben anderen organisatorischen Maßnahmen wie der Risikoanalyse ein Kapazitätsmanagement notwendig, um eventuelle Engpässe bei der Leistung von Systemen in einem Unternehmen festzustellen. Hierzu sind neben organisatorischen Prozessen zur Überwachung und Prognose notwendiger Ressourcen auch, im weiteren Verlauf noch näher erläuterte, technische Maßnahmen zur Überwachung und

Protokollierung (vgl. 4.4.10 Ereignisprotokollierung) der Systemleistung einzelner Systeme notwendig [ISO27001 A.12.1.3], [ISO27002 12.1.3].

### 4.4.3 Verhinderung von Schwachstellen

Organisatorische und vor allem technische Schwachstellen können auch in einem etablierten ISMS auftreten. Eine hundertprozentige Informationssicherheit ist durch ein unvermeidbares Restrisiko für menschliche und technische Fehler nicht erreichbar. Aus diesem Grund sind in den untersuchten Standards verschiedene Maßnahmen zur Vermeidung von Schwachstellen und zur Reaktion auf Schwachstellen beschrieben. Aus organisatorischer Sicht sollte diesbezüglich ein Schwachstellenmanagement im Unternehmen umgesetzt werden. Das Schwachstellenmanagement hat die Aufgabe Informationen über mögliche Schwachstellen von Herstellern und anderen Organisationen zu den Systemen, insbesondere den Systemen mit hohem Risiko, in einem Unternehmen einzuholen und zu bewerten. Des Weiteren plant es entsprechende Gegenmaßnahmen und führt deren Umsetzung durch. Das Schwachstellenmanagement muss dabei eng mit der Änderungsverwaltung zusammenarbeiten. Aus technischer Sicht gibt es zwei grundsätzliche Regeln zur Vermeidung von Schwachstellen und zum Umgang mit Schwachstellen; die Härtung von Systemen und die Etablierung eines Update-/Patchmanagements. Bei der Systemhärtung sollen alle Systeme, anhand anerkannter Best-Practices, in einen sicheren Zustand versetzt werden. Hierbei sollten vorhandene Funktionen zu Erhöhung der Systemsicherheit, wie eine Host-Firewall, aktiviert werden. Auftretende Datenflüsse sollten im Allgemeinen eingeschränkt und nicht benötigte Benutzer oder Standardbenutzer entfernt oder deaktiviert werden. Der Benutzerzugang zu den Systemen muss durch entsprechende Verfahren geschützt sein (s. 4.4.6 Anmeldeverfahren). Außerdem sollten Benutzerberechtigungen kontrolliert und nach dem Least-Privileges-Prinzip konfiguriert sein. Es müssen unnötige Anwendungen oder Dienste entfernt oder zumindest deaktiviert werden. Ergänzend hierzu sollte die Installation zusätzlicher Software in Zusammenarbeit mit dem Änderungsmanagement auf notwendige Programme reguliert werden. Hierzu ist der Einsatz eines Softwareverteilungssystems, mit dem die Installation von Software zentral gesteuert und überwacht werden kann, sinnvoll. Eine unautorisierte Installation von Software sollte unter anderem durch Benutzerrechte verhindert werden. Die Installation neuer Software sollte stattdessen nur nach einer Genehmigung durch fachkundige Administratoren durchgeführt werden können. Im Rahmen des Genehmigungsverfahrens sollten dabei zuvor umfangreiche Softwaretests (z. B. zur Benutzerfreundlichkeit, Sicherheit und zu Interdependenzen) in einer möglichst einsatznahen Testumgebung durchgeführt worden sein, um eventuelle Probleme im Voraus zu erkennen und zu bewerten. Darüber hinaus sollte es möglich sein, jede eingesetzte Software sowie deren Anwendungs- und Konfigurationsdateien im Betrieb regelmäßig auf ihre Integrität zu überprüfen[2]. Besondere Vorsicht gilt bei Software, die zur Anwendungsentwicklung eingesetzt werden kann. Es sollten sich weder Quellcode noch Compiler-Werkzeuge auf einem produktiven System befinden. Ergänzend zu den Maßnahmen für Software, sollten hardwarebasierte Schnittstellen abgeschaltet, entfernt oder blockiert werden, wenn sie für den täglichen Betrieb nicht notwendig sind. Hierzu zählen Anschlüsse, wie beispielsweise USB, oder Geräte zur Aufnahme von Wechselmedien, wie CD-ROM. Dies kann mit Hilfe von Software (z. B. Device-Control- Anwendungen sowie Betriebssystem spezifische Maßnahmen) oder direkte durch physische Maßnahmen (z. B. Ausbau oder irreversibles Blockieren einer Schnittstelle) erfolgen. Darüber hinaus sollte der Zustand eines Systems überwacht werden (s. 4.4.10 Ereignisprotokollierung). Neben der grundlegenden

[2] Eine Integritätsprüfung im Betrieb kann beispielsweise mit mit Hilfe von Trusted-Computing-Technologien umgesetzt werden.

Systemhärtung ist es besonders wichtig, kurzfristige auftretende Schwachstellen, sogenannte Zero-Day-Exploits, mit Hilfe eines aktiven Patchmanagements zu behandeln, da diese Schwachstellen meist auf Fehler im Programmcode eines Systems zurückzuführen sind. Hierzu kann ein zentrales System (wie das bereits genannte Softwareverteilungssystem) zum Bezug von Updates/Patches von einzelnen Herstellern für die im Unternehmen verwendeten Systeme genutzt werden. Nach einer entsprechenden Beurteilung der Patches durch die Verantwortlichen für das Sicherheitsmanagement, die Änderungsverwaltung und die zu patchenden Systeme, kann mit Hilfe dieses Systems eine automatisierte Installation ermöglicht werden. Zur besseren Beurteilung von Patches ist es, auch an dieser Stelle, sinnvoll eine Testumgebung zu betreiben. Außerdem können Datenbanken (z. B. mit Common Vulnerability Scoring System[3]) zur Einschätzung von Schwachstellen und der Kritikalität eines Patches verwendet werden. Ist die Kritikalität nicht so hoch, können auch Erfahrungen anderer Unternehmen, mit entsprechenden Patches, abgewartet werden. Um eventuell auftretende Probleme, beispielsweise durch Fehler bei der Installation von Updates, zu umgehen, sollten möglichst redundante Systeme eingesetzt und nacheinander aktualisiert werden. Hierdurch kann ein Gesamtausfall bei Problemen verhindert und eine hohe Einsatzbereitschaft der Systeme erreicht werden. Systeme ohne eine Herstellerunterstützung sollten immer vermieden werden. Wenn dennoch beispielsweise alte Systeme ohne Herstellerunterstützung mit bestehenden Schwachstellen existieren, die nicht ohne Weiteres ausgetauscht werden können oder Systeme vorhanden sind, die aus wichtigen Gründen nicht durch Patches aktualisiert werden dürfen, ist es notwendig, diese Systeme zusätzlich durch externe Maßnahmen zu schützen. Hierzu können sie in eigene Kommunikationsnetze ausgelagert und beispielsweise mit Hilfe von Firewalls und Intrusion Detection/Prevention Systemen (IDS/IPS) oder Anwendungs-Proxies vor bekannten Angriffen geschützt werden (vgl. 4.4.8 Erkennung von Schadsoftware) [ISO27001 A.12.5.1, A.12.6.1, A.12.6.2], [ISO27002 12.5.1, 12.6.1, 12.6.2], [ISO27019 10.11.1, 12.4.1], [BDEW 2.1.1.2, 2.1.1.3, 2.1.1.4, 2.1.1.5, 2.1.1.9, 2.1.1.10, 2.2.1, 2.5.4, 2.5.5, 2.5.6], [ICSSecK 5, 11, 26, 48, 49, 50, 52, 53] [ENISA D1, D3, D5].

### 4.4.4 Zugriffssteuerung auf Systeme, Netze und Dienste

Der Ausschluss des Zugriffs auf Systeme, Netze, Dienste und Informationen durch nicht autorisierte Personen ist ein wesentlicher Bestandteil der Informationssicherheit. Aus diesem Grund ist es notwendig, dass ein Unternehmen entsprechende Richtlinien zur Zugriffssteuerung definiert, in denen Zugangsrechte und Beschränkungen in Bezug auf Werte und Benutzerrollen sowie Maßnahmen zur Durchsetzung der Richtlinien festgelegt sind. Auf der Basis dieser Richtlinien müssen technische Maßnahmen zur Pflege von Zugriffsrechten für Benutzer auf Systeme, Netze, Dienste und deren Informationen umgesetzt werden. Hierzu gehören das Erstellen und Entfernen von Benutzern und die Bereitstellung von technischen Maßnahmen zur Zuteilung von Benutzerzugängen. Dabei ist es formal wichtig, dass Benutzer immer eindeutige Benutzerkennungen besitzen, um ihre Handlungen auf einem System, im Netz oder bei einem Dienst inklusive des Zugriffs auf Informationen nachvollziehbar zu machen. Aus diesem Grund sollten Benutzerkennungen beispielsweise nicht für andere Benutzer wiederverwendet werden. Für die Nachvollziehbarkeit ist es wichtig, dass Benutzer vor einem Zugriff immer erfolgreich authentifiziert werden müssen. Dies kann mittels Benutzerkennung und Passwort geschehen, zur Erhöhung der Sicherheit sind aber auch mehrere Faktoren einsetzbar. Man spricht hierbei von bis zu drei Authentisierungsmerkmalen oder

[3] Bekannte Datenbanken sind vor allem in den USA zu finden. Das Unternehmen MITRE Corporation betreibt beispielsweise die Datenbank Common Vulnerabilities and Exposure. Diese Datenbank ist zudem mit einer Datenbank der US-Regierung vom National Institute of Standards and Technology verknüpft, die U.S. National Vulnerability Database. In Deutschland bietet das BSI einen Warn- und Informationsdienst zu neuen Schwachstellen und Sicherheitslücken sowie aktuellen Bedrohungen für IT-Systeme über das CERT-Bund an.

Faktoren: Wissen (z. B. Passwort), Besitz (z. B. Schlüsselkarte) und körperliche Merkmale (z. B. Fingerabdruck). Benutzer müssen ihre Authentisierungsdaten geheim halten und sollten hierauf vertraglich hingewiesen werden. Insbesondere zur Geheimhaltung von Authentisierungsdaten aus dem Bereich Wissen sollten Benutzer nach der erstmaligen Zuweisung von Authentisierungsdaten, bei Verdacht auf Kenntnisnahme durch Dritte sowie falls möglich in regelmäßigen Intervallen (z. B. jährlich), dazu verpflichtet sein, die Daten zu verändern. Für die Wahl eines Passwortes durch einen Benutzer sollte es eine Richtlinie mit Regeln für sichere Passwörter geben, die Komplexitätsanforderungen wie

- Mindestlänge,
- Zeichensatz mit Buchstaben, Zahlen und Sonderzeichen,
- keine Verwendung von Sachverhalten mit Personenbezug (z. B. Geburtsdatum, Haustiernamen),
- keine Wörter aus einem Wörterbuch,
- keine einfachen Zeichenfolgen (z. B. abc, 123)

sowie die Gültigkeitsdauer eines Passwortes definiert. Zu Kontrolle dieser Anforderungen und zur Unterstützung bei der Verwaltung von Benutzern können hierbei zentrale Passwortmanagementsysteme eingesetzt werden. Ein solches Management ist oft in Verzeichnisdiensten (vgl. 4.4.5 Benutzerzugänge) integriert. Es ist zudem sicherzustellen, dass die Übermittlung der Authentisierungsdaten, für die erste Anmeldung auf sicherem Wege (z. B. Benutzername und Passwort getrennt voneinander per Post) durchgeführt wird. Zur Erleichterung des Umgangs mit Passwörtern kann Benutzern der Einsatz von etablierten gesicherten Aufbewahrungsmethoden wie Kennwortverwaltungsprogrammen [4] erlaubt werden. Die unverschlüsselte Aufbewahrung von Passwörtern (z. B. in Textdateien oder auf einem Zettel) ist dagegen nicht akzeptabel. Um Systeme, Netze und Dienste nicht durch ehemalige Benutzer zu gefährden, müssen Benutzer schnellstmöglich gelöscht werden, sobald kein Grund mehr für den Zugriff besteht. Im Bereich der Prozesssteuerung des Energiesektors können die bisher genannten Anforderungen zur Pflege von Benutzerzugängen jedoch nicht immer umgesetzt werden. Zum Teil gibt es beispielsweise nur einen fest vorgegebenen Benutzerzugang oder einen Zugang für eine Gruppe von Benutzern und nur den Faktor Wissen für die Authentisierung an diesem Zugang. Die Zuordnung von Handlung ist in diesem Fall nur auf eine Gruppe von Benutzern, denen dieser Zugang bekannt ist, möglich. In diesem Fall sollten zusätzliche Zugangsmaßnahmen getroffen werden, die getrennte Benutzerzugänge und ggf. mehrere Faktoren zur Authentisierung unterstützen (z. B. VPN). Die Authentisierungsdaten für eine Gruppe sollten zudem für einzelne Geräte oder Unternehmensbereiche unterschiedlich und besonders sicher (z. B. durch eine erhöhte Mindestlänge) gestaltet sein. Darüber hinaus ist es notwendig, bei Veränderung der Gruppe neue Authentisierungsdaten zu vergeben, damit ehemaligen Gruppenmitgliedern die Möglichkeit zur Authentisierung entzogen wird. Für die Verwaltung von Benutzerzugängen gilt darüber hinaus im Allgemeinen, dass sämtliche, öffentlich bekannte Standardbenutzerzugänge von Systemen, Netzen und Diensten, wenn möglich, gelöscht oder deaktiviert werden sollten. Alternativ müssen zumindest die Authentisierungsdaten, wie ein vorgegebenes, öffentliche bekanntes Password, geändert werden [ISO27001 A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.3], [ISO27002 9.1.1, 9.1.2, 9.2.1, 9.2.4, 9.2.6, 9.3.1, 9.4.3], [ISO27019 11.1.1, 11.3.1, 11.5.2], [BDEW 2.2.3, 2.3.1.1, 2.3.2.2, 2.4.1.1, 2.4.1.2], [ICSSecK 16, 25, 46, 47, 54, 55], [ENISA D4, D9].

[4] Eine bekannte, kostenfreie Anwendung zu Kennwortverwaltung ist z. B. die Anwendung KeePass Password Safe.

### 4.4.5 Benutzerzugänge

Für die Zuteilung der Benutzerzugänge sollte ein zentrales Verzeichnis eingesetzt werden, in dem die Benutzerzugänge mit ihren Rechten für informationsverarbeitende Systeme, Netze und Dienste sowie deren Informationen eines jeden Benutzers verwaltet werden. Im Energiesektor sollte hierbei darauf geachtet werden, dass die Zuteilung von Benutzerzugängen für das Prozessnetz getrennt von der Zuteilung für andere Bereiche (z. B. Büronetz) erfolgt. Das jeweilige Verzeichnis in einem Bereich kann hierbei durch einen Verzeichnisdienst[5] automatisiert sein, so dass Benutzerzugänge für verschiedene Systeme, Netze und Dienste an einer zentralen Stelle gepflegt werden können. Im Allgemeinen sollten zur Pflege dieses Verzeichnisses entsprechende Prozesse etabliert sein, die sicherstellen, dass die Rechte einzelner Benutzer angemessen sind und immer nach dem Least-Privileges- bzw. Minimal-/Need-To-Know-Prinzip zugeordnet werden. Die an einen Benutzerzugang gebundenen Rechte sollten deshalb auch regelmäßig und zu bestimmten Ereignissen (z. B. Versetzung oder Entlassung von Personen) überprüft und gegebenenfalls angepasst oder vollständig entzogen werden. Darüber hinaus muss ein Genehmigungsverfahren für Zugangsrechte etabliert sein, bei dem die Verantwortlichen für eventuell betroffene Werte beteiligt sind. Zur Vereinfachung der Rechteverwaltung sollte zudem, in Anlehnung an Abschnitt 4.1.2, ein Rollenkonzept mit vordefinierten Rechten (Role Based Access Control (RBAC)) verwendet werden, dem einzelne Benutzer zugeordnet werden können. Auch hier ist darauf zu achten, dass die zugeteilten Rollen für einen Benutzer nicht zueinander in Konflikt stehen. Ein Benutzer sollte zum Beispiel nicht die Rollen Auditor und Administrator für ein System besitzen, da die Kombination beispielsweise bei einer fehlerhaften Konfiguration eines Systems zu Interessenskonflikten führen kann. Das Beispiel zeigt des Weiteren auch, dass eine besondere Sorgfalt bei der Vergabe von privilegierten Rechten (d. h. Administrationsrechte) herrschen muss. Eine Vermischung allgemeiner Rechte (z. B. Operator- oder Data-Display-Rechte) und privilegierter Rechte in einem einzelnen Benutzerzugang muss vermieden werden. Ein Benutzer der privilegierte Rechte benötigt, sollte hierfür stattdessen einen zusätzlichen Benutzerzugang bekommen (vgl. 4.4.7 Privilegierte Programme und Schnittstellen) und diesen auch nur für die Durchführung privilegierter Aufgaben nutzen [ISO27001 A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1],[ISO27002 9.1.2, 9.2.2. 9.2.3, 9.2.5, 9.2.6, 9.4.1], [BDEW 2.1.1.1, 2.2.3, 2.3.1.2, 2.3.2.1, 2.3.2.2, 2.4.1.2, 2.4.1.1, 2.4.2], [ICSSecK 15, 16, 33, 57], [ENISA D4, D9, D10].

### 4.4.6 Anmeldeverfahren

Um die Zugangsrechte einzelner Benutzer zu Systemen, Netzen und Diensten durchzusetzen, müssen sichere Anmeldeverfahren eingesetzt werden, die Benutzer über die Existenz von Zugangsbeschränkungen belehren (z. B. mit Hilfe eines sogenannten Message-of-the-Day-Banner). Anmeldeverfahren können dabei sehr unterschiedlich ausfallen. Für den Zugriff auf ein System, einen Dienst oder eine Anwendung muss ein Benutzer beispielsweise eine Eingabemaske mit Anmeldedaten ausfüllen. Für den Zugriff auf ein Unternehmensnetz können dagegen auch maschinelle Methoden wie IEEE 802.1X zur Authentifizierung von Systemen an Netzanschlüssen oder das Portknocking eingesetzt werden. Grundsätzlich darf der Zugriff auf jedwede nicht öffentliche Information oder eine Durchführung von Aktionen, ohne eine erfolgreiche Anmeldung, nicht möglich sein. Dies gilt auch für etwaige Fehlermeldung bei der Anmeldung, um einem potenziellen Angreifer keine Informationen über mögliche Schwachstellen zu bieten oder eine Ableitung von Informationen über indirekte Hinweise zuzulassen. Sichere Anmeldeverfahren müssen in diesem Zusammenhang auch über einen Schutz vor Brute-Force-Methoden verfügen. Hierbei kommen beispielsweise

[5] Es gibt verschiedene Anwendungen zur technischen Realisierung eines Verzeichnisdienstes, ein Beispiel ist die proprietäre Software Microsoft Active Directory oder die quelloffene Software OpenLDAP.

Methoden, wie eine ansteigende zeitliche Verzögerung zwischen Anmeldeversuchen oder die Begrenzung von Anmeldeversuchen innerhalb eines Zeitintervalls bis zur Sperrung des Benutzerzugangs, in Frage. Speziell im Bereich der Prozesssteuerung im Energiesektor muss bei der Auswahl dieser Methoden jedoch immer abgewogen werden, ob z. B. eine Sperrung des Zugangs zu Problemen im Betrieb führen kann. Bei der Anmeldung selbst darf niemals das Kennwort im Klartext angezeigt oder übertragen werden. Speziell für die Übertragung der Anmeldedaten sowie für die weitere Kommunikation sind dabei sichere Protokolle einzusetzen. Diese müssen die Vertraulichkeit (z. B. durch Verschlüsselung) und die Integrität (z. B. durch Signaturen) der Anmeldedaten schützen. Erfolgreiche und nicht erfolgreiche Anmeldungen sollten dabei protokolliert werden. Ein Benutzer sollte zudem nach einer erfolgreichen Anmeldung erkennen können, ob jemand anderes einen Anmeldeversuch mit seinem Benutzerzugang versucht hat (z. B. Datum der letzten erfolgreichen Anmeldung und Anzeige der fehlgeschlagenen Anmeldungen seitdem). Nach einer erfolgreichen Anmeldung sollte zudem eine zeitlich eingeschränkte Gültigkeit der Anmeldung, in Form einer sogenannten Sitzung (Session), für den Benutzer aktiviert werden. Nach einer gewissen Zeit der Inaktivität sollte die Sitzung ablaufen und der Benutzer automatisch abgemeldet werden, um beispielsweise den Zugriff Dritter auf eine bestehende Sitzung aufgrund einer versehentlich vergessenen Abmeldung zu verhindern. Speziell im Bereich des Energiesektors muss eine Sitzung im Einzelfall jedoch dauerhaft aktiv sein (z. B. bei einer Mensch-Maschine-Schnittstelle zur Anzeige des Energienetzzustands). In diesem Fall sind eventuell physische Zugriffsbeschränkungen zu betrachten und der aktiven Sitzung sollten nur Data-Display-Rechte (vgl. 4.1.2 Verantwortlichkeiten und Rollen) zugeordnet sein. Um mit Informationen zu interagieren, bleibt eine zusätzliche Anmeldung notwendig. Für die Anmeldung von Benutzern außerhalb der Unternehmensgrenzen sollten ergänzende Anmeldeverfahren eingeführt werden (z. B. durch Einrichtung einer DMZ mit VPN oder Proxylösungen), so dass niemand von außen direkt auf Systeme, Netze und Dienste sowie deren Informationen, inklusive der dazu nötigen Anmeldung, zugreifen kann (vgl. 4.4.17 Sicherheit durch Netzsegmentierung) [ISO27001 A.9.4.2], [ISO27002 9.4.2], [ISO27019 11.5.5], [BDEW 2.2.3, 2.3.1.1, 2.3.2.1, 2.4.1.2], [ICSSecK 33], [ENISA D9].

### 4.4.7 Privilegierte Programme und Schnittstellen

Viele Systeme bieten Möglichkeiten an, die Anmeldung und andere Systemkontrollmaßnahmen mit Hilfe privilegierter Programme zu umgehen. Mit Hilfe des BIOS eines Computers ist es zum Beispiel möglich, über einstellbare Start-/Boot-Optionen ein anderes Betriebssystem von einem Wechseldatenträger zu starten und auf unverschlüsselte Daten des eigentlichen Betriebssystems, ohne eine vorherige Anmeldung, zuzugreifen. Aus diesem Grund ist es notwendig, den Einsatz dieser Programme zu beschränken und zu kontrollieren. Anmeldeverfahren sind zur Zugriffsbeschränkung auf diese privilegierten Programme zu nutzen. Der Zugriff auf ein BIOS lässt sich beispielsweise durch ein Passwort schützen. Privilegierte Programme sollten nur für einen eingeschränkten, vertrauenswürdigen Benutzerkreis und über dafür extra eingerichtete Benutzerzugänge zugänglich gemacht werden und nicht Teil der normalen Systemausstattung und Benutzerzugänge sein. Die Systeme und Dienste sollten stattdessen so abgesichert sein, dass solche Programme, wenn möglich, deinstalliert oder zumindest deaktiviert werden, wenn sie zum allgemeinen Betrieb nicht notwendig sind (zur Frage der Notwendigkeit ist ggf. der Hersteller zu konsultieren). Hierbei müssen möglicherweise auch externe Schnittstellen, wie USB oder Wechseldatenträger, entsprechend abgesichert werden, wenn mit ihnen Anmeldeverfahren und Kontrollmaßnahmen umgangen werden können (s. o. BIOS-Beispiel) [ISO27001 A.9.4.4], [ISO27002, 9.4.4], [BDEW 2.1.1.9, 2.2.1, 2.4.2], [ICSSecK 48, 69, 70], [ENISA D9].

### 4.4.8 Erkennung von Schadsoftware

Zur Ausnutzung einer bestehenden Sicherheitslücke wird häufig Schadsoftware benötigt, die auf einem angreifbaren System zur Anwendung kommt und eine bestehende Sicherheitslücke ausnutzt. Eine Schadsoftware kann über verschiedene Kanäle in ein Unternehmen gelangen (z. B. Wechseldatenträger, E-Mail oder Internet-Downloads). Aus organisatorischer Perspektive sollte ein Unternehmen deshalb, zum Schutz vor spezifischen Gefahren, regelmäßig Informationen zu aktuellen Bedrohungen im Rahmen des Schwachstellenmanagements (s. 4.4.3 Verhinderung von Schwachstellen) einholen und bewerten. Darüber hinaus sollten Mitarbeiter für die Gefahren sensibilisiert werden. Zur Beschaffung der notwendigen Informationen dürfen dabei nur als seriös geltende Quellen wie zum Beispiel Systemhersteller oder national anerkannte Sicherheitsgruppen verwendet werden. Zu den organisatorischen Aspekten gehören darüber hinaus Maßnahmen zur Wiederherstellung bei einem Schadsoftwarebefall, insbesondere zur Aufrechterhaltung des Geschäftsbetriebs. Hierbei sollten ebenfalls Hinweise von seriösen Quellen, wie zum Beispiel von Systemherstellern oder national anerkannten Sicherheitsgruppen, für die eingesetzten Systeme miteinbezogen werden. Da Schadsoftware normalerweise nicht zu den unternehmenskritischen Anwendungen zählt, muss zum Schutz vor Schadsoftware insbesondere darauf geachtet werden, dass, wie bereits in der Systemhärtung beschrieben, sowohl Maßnahmen in organisatorischer als auch technischer Form umgesetzt werden, um den Einsatz nicht autorisierter Software in einem Unternehmen zu verhindern (s. 4.4.3 Verhinderung von Schwachstellen). Neben den Maßnahmen zur allgemeinen Systemhärtung sollten des Weiteren spezielle Maßnahmen zur Erkennung und Vorbeugung von Schadsoftware umgesetzt werden. Hierzu gehören beispielsweise technische Maßnahmen zur Erkennung und Behandlung von Schadsoftware bzw. Schadcode in einer Software oder einer Website sowie in E-Mails. Dabei sollten auf allen Systemen sogenannte Anti-Malware-Anwendungen installiert sein, die höchstens durch einen Benutzer mit der Rolle Administrator (vgl. 4.1.2 Verantwortlichkeiten und Rollen) deaktiviert werden können. Mit Hilfe dieser Anwendungen sollten regelmäßige (z. B. täglich oder wöchentlich) Scans nach Schadsoftware auf dem jeweils umgebenden System durchgeführt werden. Darüber hinaus sollten ereignisbasierte Scans bei dem Zugriff auf Anwendungen und Dateien eingesetzt werden. Hierzu gehören unter anderem das Scannen von E-Mail-Anhängen beim Empfang aber auch das Scannen eines Downloads aus dem Internet oder das Scannen von Daten nach Anbindung eines USB-Sticks. In Ergänzung dazu können auch zusätzliche bzw. externe Anti-Malware-Anwendungen außerhalb geschäftskritischer Systeme eingesetzt werden. Mit Hilfe eines Internet- und eines E-Mail-Proxys können Webseiten und Downloads sowie E-Mails und deren Anhänge auf Schadsoftware untersucht werden, bevor die Daten an ein geschäftskritisches System weitergeleitet werden. Häufig bringen heutige Firewalls, sogenannte Next-Generation-Firewalls oder Application-Level-Gateways, diese Funktionen bereits mit. Speziell für Wechseldatenträger kann eine Wechseldatenträgerschleuse eingesetzt werden. Eine Wechseldatenträgerschleuse ist ein System, an das Wechseldatenträger zur Anti-Malware-Überprüfung angebunden werden, bevor sie mit einem kritischen System im Unternehmen in Verbindung gebracht werden. Bei der Verwendung ausgelagerter Anti-Malware-Anwendung können interne Scans in einem System für die ausgelagerten Bereiche ausgenommen werden, um geschäftskritische Systeme zu entlasten und die Effizienz der Schadsoftwareerkennung zu erhöhen. Dies gilt insbesondere für eingebundene Netzlaufwerke. Diese sollten immer von dem System gescannt werden, das die Netzlaufwerke bereitstellt. Im Allgemeinen sollte ein Scan von Daten immer so nah wie möglich an der Quelle dieser Daten durchgeführt werden, um eine unerkannte Verbreitung von Schadsoftware zu vermeiden. Zur Erkennung von Schadsoftware arbeiten alle Anti-Malware-Anwendungen vorwiegend mit Hilfe von Mustern (sogenannten Virensignaturen). Für eine

effektive Erkennung müssen diese Muster durch regelmäßige und zeitnahe Aktualisierungen immer aktuell gehalten werden. Dabei sollte ein direkter Bezug der Aktualisierungen durch einzelne Systeme aus dem Internet oder anderen Netzen von Dritten vermieden werden. Stattdessen sollte, analog zur Aktualisierung von Programmen (s. 4.4.3 Verhinderung von Schwachstellen), ein zentrales System zur Verwaltung und Verteilung der Aktualisierungen eingesetzt werden, um eine Kontrolle der Anti-Malware-Anwendungen zu gewährleisten. Diese Form der Steuerung hilft zudem dabei, Aktualisierungen vor dem Einsatz zu prüfen und eventuelle Unverträglichkeiten zu vermeiden [ISO27001 A.12.2.1], [ISO27002 12.2.1], [ISO27019 10.4.2], [BDEW 2.2.2], [ICSSecK 28, 59, 62, 63, 64, 67], [ENISA D9].

### 4.4.9 Erkennung von Schadsoftware in eingeschränkten Umgebungen

Die allgemeinen Empfehlungen zum Einsatz von Anti-Malware-Anwendungen aus den ausgewählten Standards (s. 4.4.8 Erkennung von Schadsoftware) sind jedoch nicht überall im Energiesektor einsetzbar. Insbesondere bei industriellen Steuerungssystemen ist es aufgrund der Systemgestaltung nicht immer möglich, eine Anti-Malware-Anwendung zu installieren und zu betreiben. Durch die zusätzliche Systemlast, die durch eine solche Anwendung erzeugt wird, können zum Beispiel Ressourcenengpässe auftreten. Diese können die Verfügbarkeit eines Systems gefährden. Auch ein regelmäßiges Update der Virensignaturen ist in manchen Fällen nicht möglich, so dass eine Anti-Malware-Anwendung, nach kurzer Zeit, wirkungslos wird. Die Beachtung der Herstellerangaben ist an dieser Stelle notwendig. Dabei ist zu prüfen, ob eine Anti-Malware-Anwendung ggf. teilweise eingesetzt werden kann, indem Scans zum Beispiel nur in ausgewiesenen Wartungsfenstern stattfinden und möglicherweise manuell durchgeführt werden. Die Systeme, bei denen der uneingeschränkte Einsatz von Anti-Malware-Anwendungen nicht möglich ist, sollten in ein eigenes Netzsegment (vgl. 4.4.17 Sicherheit durch Netzsegmentierung) ausgelagert werden. Ein solches Netzsegment sollte keinen Zugriff auf das Internet ermöglichen. Wenn ein Zugriff auf das Internet doch nötig ist, müssen bereits beschriebene externe Lösungen (z. B. Internet- oder E-Mail-Proxy) zum Schutz vor Schadsoftware eingesetzt werden. Des Weiteren kann auf den Systemen gegebenenfalls eine spezielle Software eingesetzt werden, die das Ausführen nicht genehmigter Programme, wie Schadsoftware, verhindert. Das sogenannte Application-Whitelisting nutzt hierfür spezifisch Merkmale von genehmigter Software, wie zum Beispiel Signaturen, Hashwerte oder den Dateisystempfad, um nicht genehmigte Software zu identifizieren und deren Ausführung zu regulieren. Neben dem Application-Whitelisting gibt es weitere Maßnahmen, die nicht nur für Systeme mit eingeschränkter oder ohne Anti-Malware-Anwendungen zum Einsatz kommen können. Wie bereits erwähnt, (vgl. 4.4.3 Verhinderung von Schwachstellen) sollte eine Host Firewall aktiviert und restriktiv konfiguriert sein, wenn sie auf einem System vorhanden ist. Darüber hinaus können Intrusion-Detection- oder Prevention-Systeme (IDS/IPS) eingesetzt werden. Diese Systeme arbeiten ähnlich wie Anti-Malware-Anwendungen vorwiegend mit Mustern. Diese Muster beziehen sich jedoch nicht explizit auf Schadsoftware sondern auf die Erkennung von anomalem Verhalten (Anomalien) in ihrer Einsatzumgebung. In diesem Zusammenhang kann ein IDS Anomalien frühzeitig erkennen, während ein IPS darüber hinaus vorgegebene Aktionen zur Unterbindung des anormalen Verhaltens durchführen kann. Diese beiden Varianten lassen sich, je nach ihrer Platzierung, zudem in zwei Arten unterscheiden. Ein Host-based-IDS/IPS (HIDS/HIPS) wird direkt auf einem System eingesetzt und kann zum Beispiel ungewöhnliche Dateizugriffe oder Netzwerkzugriffe, mit Bezug auf das umgebende System, überwachen. Einige HIDS/HIPS ermöglichen in dieser Beziehung auch ein Application-Whitelisting. Ein Network-based-IDS/IPS (NIDS/NIPS) wird dagegen in einem Kommunikationsnetz platziert, so dass es die Datenströme in diesem Netz mitlesen kann, um

beispielsweise ungewöhnliche Muster in einem Protokollablauf zu erkennen. NIDS/NIPS werden hierzu meist an zentralen Übergängen zwischen einzelnen Netzen platziert. Sie sind eine geeignete Maßnahme zur zusätzlichen Absicherung von Systemen mit eingeschränkten Möglichkeiten zum Betrieb von Anti-Malware-Anwendungen. In besonders kritischen Bereichen wird jedoch nur der Einsatz der IDS-Varianten empfohlen, da die, durch eine IPS-Variante, automatisch ausgeführten Aktionen den Betrieb gefährden könnten. Durch die Verwendung von Mustern zur Erkennung von Anomalien müssen diese bei IDS/IPS für deren effektiven Einsatz, ähnlich wie bei Anti-Malware-Anwendungen (s. 4.4.8 Erkennung von Schadsoftware), regelmäßig aktualisiert werden. Darüber hinaus ist die Administration eines IDS/IPS wesentlich aufwendiger als die Administration andere Sicherheitsmaßnahmen, wie einer Firewall oder einer Anti-Malware-Anwendung. Dies liegt vor allem an der komplexen Anforderung zwischen gewöhnlichem Verhalten und Anomalien, in der jeweiligen Einsatzumgebung, zu unterscheiden. Jede Einsatzumgebung ist anders und ein IDS/IPS muss dementsprechend in einem langen Prozess auf diese Umgebung eingestellt und bei jeder Änderung der Umgebung erneut angepasst werden. Eine entsprechende wirtschaftliche Betrachtung ist an dieser Stelle notwendig [ISO27019 10.4.1], [ICSSecK 39, 42, 51, 59, 60, 61, 65], [ENISA D9].

### 4.4.10 Ereignisprotokollierung

Für den sicheren Betrieb einer IT-Infrastruktur ist ein möglichst umfangreicher Überblick über den Status der Infrastruktur und ihrer einzelnen Netze, Systeme und Dienste entscheidend. Dies sollte möglichst mit Hilfe eines automatisierten Überwachungssystems[6] an einer zentralen Stelle erfolgen. Das Überwachungssystem sollte in der Lage sein, Ereignisse mit Informationen über den Status der IT-Infrastruktur aus verschiedenen Quellen aufzubereiten und eine Möglichkeit zur Konfiguration von Alarmen für besonders kritische Ereignisse bereitstellen. Speziell für den Bereich der industriellen Steuerungssysteme, wie in der Energieversorgung, sollte dabei ein dediziertes Überwachungssystem für die Prozessumgebung eingesetzt werden. Die eingesetzten Systeme und Dienste in einer IT-Infrastruktur müssen für ihre Überwachung in der Lage sein, Ereignisse aus ihrem Einsatzbereich, in Form eines Ereignisprotokolls, zeitlich geordnet zu erfassen, zu speichern und sie mit Hilfe standardisierter Übertragungsprotokolle (z. B. Syslog oder SNMP) an ein zentrales Überwachungssystem zu übertragen. Beispiele für Ereignisquellen in einer IT-Infrastruktur sind Betriebssysteme, Firewalls, Router sowie Switche oder IDS und Anit-Malware-Anwendungen. Die folgende Liste zeigt zudem Beispiele für relevante Ereigniskategorien im Zusammenhang mit überwachten Netzen, Systemen und Diensten:

- Benutzeraktionen (z. B. Ausführung von Anwendungen oder Befehlen)
- Zugriffsaktionen (z. B. erfolgreiche und fehlgeschlagene Anmeldeversuche oder Zugriffs-versuche auf Informationen)
- Ausnahmen und Fehler (z. B. hohe Ressourcen-Auslastung (z. B. CPU-Auslastung) oder eine ausgefallene Netzanbindung sowie Hardwaredefekte)
- Privilegierte Aktionen (z. B. Änderung der Systemkonfiguration und Ausführung privilegierte Befehle sowie Aktivierung/Deaktivierung von Schutzmaßnahmen)

Zu einem Ereignis sollten neben seiner Beschreibung weitere Metadaten durch die jeweilige Quelle erfasst werden. Zu den Metadaten gehören unter anderem Datum und Uhrzeit, Kritikalität sowie die

[6] Hierzu können beispielsweise spezielle Systemüberwachungswerkzeuge wie Nagios und Logging-Systeme, zur Speicherung und Untersuchung von Ereignissen, oder intelligente Security-Information-and-Event-Management-(SIEM)-Systeme, zur Normalisierung unterschiedlicher Ereignisinformationen und einer automatisierten Korrelation von Ereignissen zur Erkennung spezieller Systemzustände, eingesetzt werden.

Ereignisquelle (z. B. Anwendung, System, Benutzer, Standort) selbst. Hierbei muss jedoch auf bestehende Datenschutzbestimmung geachtet werden [ISO27001 A.12.4.1], [ISO27002 12.4.1], [ISO27019 10.10.1], [BDEW 2.4.6], [ICSSecK 33, 73], [ENISA D6]. Laut Bundesdatenschutzgesetz (BDSG) §31 muss unter anderem sichergestellt werden, dass:

*„Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, […] nur für diese Zwecke verwendet werden [dürfen].“* [BDSG §31]

### 4.4.11 Zeitsynchronisation

Für die Erfassung der Metadaten Datum und Zeit bei der Überwachung von Netzen, Systemen und Diensten muss eine einheitliche Zeitvorgabe für alle Elemente gelten. Ohne eine einheitliche Zeitvorgabe sind eine später Untersuchung von Ereignissen und der Nachweis zeitlicher Zusammenhänge schwierig und gegebenenfalls nicht für die Durchführung einer rechtlichen Verfolgung von Informationssicherheitsvorfällen geeignet. Für eine einheitliche Zeitvorgabe muss es eine Referenzzeitquelle in einem Unternehmen geben, mit der sich die Systeme entsprechend synchronisieren. Für die Synchronisation der Systeme mit der Referenzzeitquelle kann das Network Time Protocol (NTP) eingesetzt werden. Da NTP keine Maßnahmen zum Schutz der Integrität von Zeitinformationen bereithält, ist jedoch zu beachten, dass zusätzliche kryptografische Maßnahmen eingesetzt werden sollten, um eine Manipulation der Zeitsynchronisationsvorgänge zu verhindern. Als Alternative zu NTP kann zudem das Precision Time Protocol (PTP) eingesetzt werden, auch hier sind zusätzliche Maßnahmen zum Schutz vor Manipulationen zu empfehlen [ISO27001 A.12.4.4], [ISO27002 12.4.4], [ISO27019 10.10.6], [BDEW 2.4.6], [ICSSecK 45].

### 4.4.12 Schutz von Ereignissen und Ereignisprotokollen

Die Statusinformationen in einem Ereignis bilden die Grundlage für die Überwachung einer IT-Infrastruktur. Aus diesem Grund ist der Schutz von Ereignissen eine wesentliche Voraussetzung für eine verlässliche Überwachung. Dies gilt für die Übertragung von Ereignissen an ein zentrales Überwachungssystem sowie bei der Speicherung von Ereignissen in lokalen Ereignisprotokollen der Ereignisquellen und des zentralen Überwachungssystems. Ereignisse sollten durch kryptografische Maßnahmen vertraulich und integritätsgesichert übertragen werden (z. B. mit Hilfe von Verschlüsselung und Signaturen). Darüber hinaus sollten die gespeicherten Ereignisprotokolle vor Veränderungen und dem Löschen geschützt werden (z. B. durch Zugriffsberechtigungen und Signaturen). Sofern sich in den Ereignisprotokollen zudem sensible Daten befinden, müssen zusätzliche kryptografische Maßnahmen zum Schutz der Vertraulichkeit (z. B. Verschlüsselung, Anonymisierung, Pseudonymisierung) eingesetzt werden. Des Weiteren sind, beispielsweise aus gesetzlichen Gründen, Backup-Konzepte zur eventuellen langfristigen Speicherung der Daten notwendig (vgl. 4.4.13 Backup). Ereignisse die auf privilegierten Handlungen, z. B. durch die Rolle Administrator (s. 4.1.2 Verantwortlichkeiten und Rollen) basieren, müssen darüber hinaus besonders geschützt werden. Grundsätzlich sollte deshalb sichergestellt werden, dass die Ereignisse und Ereignisprotokolle weder durch normale Benutzer noch durch privilegierte Benutzer verändert werden können. Nur die Rolle Auditor sollte in der Lage sein, Ereignisse einzusehen und zu archivieren, aber nicht zu ändern [ISO27001 A.12.4.2, A.12.4.3], [ISO27002 12.4.2, 12.4.3], [BDEW 2.1.1.6, 2.4.6], [ICSSecK 73], [ENISA D6].

### 4.4.13 Backup

Für die Archivierung bzw. Sicherung von Informationen, wie Ereignisprotokolle, Konfigurationsdaten, oder Anwendungs- und Prozessdaten, gibt es in den untersuchten Standards allgemeine Vorschriften. Es können verschiedene Backup-Methoden eingesetzt werden. Zum einen ist ein vollständiges Backup aller Informationen möglich. Um Speicherplatz zu sparen, können aber auch sogenannte inkrementelle oder differenzielle Backups durchgeführt werden, bei denen nur die neuen oder geänderten Informationen, seit dem letzten Backup, gesichert werden. Darüber hinaus kann ein Backup regelmäßig oder ereignisbasiert erfolgen. Die ereignisbasierte Variante ist dabei vor allem bei Daten sinnvoll, die sich nur sehr selten zu bestimmten Ereignissen ändern. Die Veränderung der Basiskonfiguration eines Switches wird hierfür als Beispiel genannt. Je nach Methode ergeben sich verschiedene Vorgehensweisen für eine Wiederherstellung, die entsprechend berücksichtigt und dokumentiert werden müssen. Um eine Wiederherstellung jederzeit zu ermöglichen, müssen Backup-Daten sehr gut geschützt sein. Dies gilt auf physischer sowie logischer Ebene. Backup-Daten sollten hierzu physisch, je nach Kritikalität, in einer passenden, abgeschlossenen Aufbewahrungsstätte beispielsweise in einem feuerfesten Tresor, auf möglichst langlebigen Medien (z. B. Magnetband), außerhalb ihres Entstehungsortes aufbewahrt werden. Außerdem sollten die Integrität und, wenn nötig, auch die Vertraulichkeit der Daten auf der logischen Ebene (z. B. durch Signaturen und Verschlüsselung) sichergestellt werden. Die Integrität und Unversehrtheit der Backups ist darüber hinaus regelmäßig physisch sowie logisch zu überprüfen. Auch die festgelegten Wiederherstellungsverfahren sollten dabei regelmäßig überprüft werden. Die Backups sowie deren Prüfung und eventuelle Fehler sind entsprechend zu dokumentieren. Wenn Wechseldatenträger zur Speicherung von Backups eingesetzt werden, sollten zudem die Vorschriften zum allgemeinen Umgang mit Wechseldatenträgern beachtet werden (vgl. 4.4.14 Wechseldatenträger) [ISO27001 A.12.3.1], [ISO27002 12.3.1], [BDEW 2.6.1], [ICSSecK 13, 71, 72].

### 4.4.14 Wechseldatenträger

Wechseldatenträger stellen ein besonderes Risiko dar, weil diese schnell den Besitzer wechseln, verloren gehen oder entwendet werden können. Die Verwendung von Wechseldatenträgern ist deshalb im Allgemeinen auf das Nötigste zu beschränken, um ein Datenverlust durch den Verlust eines Wechseldatenträgers zu vermeiden. Darüber hinaus sollte der Verbleib von Wechseldatenträgern eines Unternehmens überwacht und dokumentiert werden. Aus technischer Sicht, sind Wechseldatenträger in sicheren Umgebungen aufzubewahren und die Vertraulichkeit der enthaltenen Daten ist gegebenenfalls zu schützen (z. B. mit Hilfe von Verschlüsselung). Während eines Transports von Wechseldatenträgern sollten zudem schützende Verpackungen und vertrauensvolle Transportwege (z. B. spezielle Sicherheitskuriere) eingesetzt werden. Daten, die nicht mehr auf einem Wechseldatenträger gebraucht werden, sollten sicher, beispielsweise durch mehrfaches Überschreiben, gelöscht werden, damit sie nicht unautorisiert wiederhergestellt werden können. Wechseldatenträger, die nicht mehr im Unternehmen verwendet werden sollen, sind entsprechend sicher zu entsorgen. Dies gilt insbesondere für Wechseldatenträger mit sensiblen Daten oder Daten, die zusammengenommen zu sensiblen Daten werden (Kumulierungseffekt), enthalten. Zu entfernende Wechseldatenträger sollten zentral gesammelt und vernichtet werden (z. B. durch physisches Schreddern oder logisches, irreversibles Löschen der Daten). Hierfür können, eine entsprechende Vertrauenswürdigkeit vorausgesetzt, auch externe Dienstleistungen in Anspruch genommen werden. Da Wechseldatenträger verschiedenen Umwelteinflüssen und einer Medienalterung ausgesetzt sein können, sollten die Daten eines Wechseldatenträgers regelmäßig auf ihre Integrität überprüft werden. Sofern es sich um wichtige Unternehmensdaten handelt, sollten

des Weiteren zusätzliche Backups der Daten an anderen Stellen aufbewahrt werden [ISO27001 A.8.3.ff], [ISO27002 8.3.ff], [BDEW 2.5.2], [ICSSecK 66], [ENISA D9].

### 4.4.15 Mobilgeräte

Mobilgeräte wie Laptops oder Smartphones können teilweise analog zu Wechselmedien betrachtet werden. Wie Wechselmedien können sie schnell den Besitzer wechseln, verloren gehen oder entwendet werden. Im Gegensatz zu Wechselmedien enthalten Mobilgeräte jedoch neben Informationen auch häufig Zugangsberechtigungen, beispielsweise zu internen Netzen oder E-Mail-Konten eines Unternehmens. Aus diesem Grund müssen sie über die allgemeinen Schutzmaßnahmen für informationsverarbeitende Systeme hinaus genauer betrachtet werden. Hierzu ist vor allem eine Sensibilisierung der Mobilgerätebenutzer für diese spezielle Situation und den damit verbundenen Gefahren notwendig. Technisch müssen Mobilgeräte besonders starke Zugriffsschutzmaßnahmen aufweisen (vgl. 4.3.4 Systeme und Geräte in fremden Umgebungen, 4.4.6 Anmeldeverfahren). Zudem müssen alle Zugriffsmöglichkeiten auf ein Unternehmensnetz, durch ein Mobilgerät aus der Ferne (vgl. 4.4.17 Sicherheit durch Netzsegmentierung), durch starke Authentifizierungs- (vgl. 4.4.4 Zugriffssteuerung auf Systeme, Netze und Dienste) und Verschlüsselungsmaßnahmen geschützt werden. Sensible Daten sollten auf einem Mobilgerät nur in verschlüsselter Form vorliegen. Dabei ist gegebenenfalls eine vollständige Verschlüsselung des Mobilgerätes in Betracht zu ziehen. Neben dem logischen Zugriffsschutz sollten ergänzende physische Maßnahmen zum Schutz vor Diebstahl[7] umgesetzt werden. Darüber hinaus kann es sinnvoll sein, eine Anwendung zum Lokalisieren eines Mobilgerätes sowie eine Anwendung zum sicheren Löschen des Gerätes aus der Ferne einzusetzen. Die private Nutzung eines Mobilgerätes sollte, wenn möglich, ausgeschlossen werden oder getrennt von den geschäftlichen Informationen erfolgen (z. B. Multi-Boot-System). Ein spezieller Fall von Mobilgeräten im Energiesektor sind Wartungslaptops. Da diese direkt im Bereich der Prozesssteuerung eingesetzt werden und die Möglichkeit besteht, dass durch ihren Einsatz Sicherheitsmaßnahmen umgangen werden, müssen diese Geräte besonders restriktiv gestaltet sein. Neben den allgemeinen Vorgaben für informationsverarbeitende Systeme im Unternehmen, insbesondere der Maßnahmen zur Vermeidung von Sicherheitslücken und Schadsoftware (vgl. 4.4.3 Verhinderung von Schwachstellen, 4.4.8 Erkennung von Schadsoftware), sollte sich nur Software zur Durchführung der Wartung auf diesen Laptops befinden. Diese Geräte sollten zudem nie außerhalb der Prozesssteuerung verwendet oder eingebunden werden, um beispielsweise eine Verschleppung von Schadsoftware in die Prozessteuerung zu vermeiden [ISO27001 A.6.2.1], [ISO27002 6.2.1], [ICSSecK 68], [ENISA D10].

### 4.4.16 Telearbeit

Eine weitere Besonderheit im Bereich eines Unternehmens stellt die Telearbeit dar. Sie besitzt Analogien zu den Mobilgeräten, mit der Einschränkung, dass die Systeme zur Telearbeit nur in einer festgelegten Umgebung außerhalb des Unternehmens eingesetzt werden und ihren Standort üblicherweise nicht häufig verändern. Ein Mitarbeiter arbeitet hierbei aus der Ferne, typischerweise von zu Hause aus, für ein Unternehmen. Es kommt zu einer Überlagerung des heimischen Arbeitsplatzes mit dem Arbeitsbereich eines Unternehmens und möglicherweise zu einer Vermischung von privaten und unternehmensinternen Daten. In diesem Fall sind deshalb besondere Regeln zu beachten. Das Unternehmen sollte informationsverarbeitende Systeme und Sicherheitsmaßnahmen bereitstellen, die an die genannten Besonderheiten der

[7] Die meisten Laptops besitzen beispielsweise eine Aussparung zur Anbringung sogenannter Kensington-Schlösser, die wiederum mit einer Vorrichtung (z. B. eine Drahtschlaufe) zur Fixierung an festen Objekten versehen sind.

Telearbeitsumgebung angepasst sind. Auf der logischen Ebene können spezielle Netzsegmente für den Zugriff aus der Ferne und eine virtuelle Desktopumgebung[8] dazu beitragen, dass Informationen nicht aus dem Unternehmen abfließen. Genau wie bei Mobilgeräten muss darüber hinaus ein starker Zugriffsschutz auf den Systemen sowie zur Kommunikation mit dem Unternehmen vorhanden sein (vgl. 4.4.15 Mobilgeräte). Die Verbindung in ein Unternehmensnetz muss dabei ebenfalls verschlüsselt erfolgen. Der Zugang zum Unternehmensnetz kann beispielsweise mit Hilfe eines Tunnels über die private Internetverbindung oder über dedizierte Hardware und unternehmenseigene Kommunikationsschnittstellen hergestellt werden. Physisch muss der Zugriff auf Informationen und Systeme zum Beispiel mit Hilfe von physischen Schutzmaßnahmen, wie verschließbaren Türen und Schränken, umgesetzt werden (vgl. 4.3.1 Betriebsgelände, Gebäude und Räume, 4.3.4 Systeme und Geräte in fremden Umgebungen). Darüber hinaus muss es Prozesse zur Bereitstellung der, in diesem Dokument beschriebenen, verwaltungstechnischen bzw. administrativen Tätigkeiten, wie Sicherheitsüberwachung, Wartung, Backup sowie Benutzerverwaltung in der Ferne geben [ISO27001 A.6.2.2], [ISO27002 6.2.2], [BDEW 2.5.2].

### 4.4.17 Sicherheit durch Netzsegmentierung

Zur Übertragung von Informationen zwischen Systemen und Diensten sind Kommunikationsnetze notwendig. Bei der Gestaltung dieser Netze sind die Anforderungen der einzelnen Systeme, Dienste und Informationen zu berücksichtigen. Zur Gewährleistung dieser Anforderungen, insbesondere mit Bezug auf die Sicherheit, von Systemen, Diensten und Informationen, sollten Sicherheitszonen in einem Kommunikationsnetz, sogenannte Netzsegmente, zur Trennung der Systeme mit unterschiedlichen Sicherheitsanforderungen genutzt werden. Ein Netzsegment erfüllt dabei bestimmte Sicherheitsanforderungen und enthält alle Systeme, die diese Sicherheitsanforderungen benötigen bzw. ebenfalls erfüllen. Die Unterteilung der Netzsegmente kann dabei z. B. anhand von Systemcharakteristika erfolgen, so dass Desktop-Systeme von Server-Systemen getrennt sind. Alternativ kann eine Unterteilung nach Organisationseinheiten im Unternehmen erfolgen, so dass die Systeme der Personalabteilung von Systemen der Vertriebsabteilung getrennt sind. Eine Mischung verschiedener Charakteristika ist ebenfalls denkbar (z. B. Desktop-Systeme der Vertriebsabteilung). Man spricht hierbei auch von einer vertikalen Netzwerksegmentierung. Darüber hinaus sollte eine sogenannte horizontale Netzwerksegmentierung eingeführt werden, in dem die Kommunikationsnetze einzelner Standorte voneinander getrennt sind. Netzsegmente können physische durch dedizierte Netzwerkhardware oder auch logisch zum Beispiel mit Hilfe virtueller Netze (z. B. VLAN oder VPN) umgesetzt werden. Bei besonders kritischen Netzsegmenten sollte dabei auf eine physische Trennung mit dedizierter Hardware zurückgegriffen werden. Die Kommunikationsbeziehungen der Systeme in einem Netzsegment können weitestgehend unreguliert, nur durch die eigenen Sicherheitsmaßnahmen der Systeme und Dienste beschränkt, verlaufen. Aus diesem Grund ist es besonders wichtig darauf zu achten, dass sich nur die Systeme in einem Netzsegment befinden, die für das Netzsegment vorgesehen sind. Gegebenenfalls sind hier entsprechende Maßnahmen zum Zugriffsschutz einzuführen (vgl. [Zugriffsschutz, Anmeldeverfahren]). Dagegen werden Kommunikationsbeziehungen zwischen Systemen und Diensten in unterschiedlichen Netzsegmenten an den Grenzen dieser Segmente reguliert. Hierzu können Firewalls, Proxies oder andere (Anwendungs-)Gatewaylösungen sowie filternde Router mit möglichst restriktiven Einstellungen eingesetzt werden. Diese Sicherheitssysteme begrenzen die möglichen Kommunikationsbeziehungen zwischen den Netzsegmenten auf die notwendigen Systeme

[8] Sogenannte virtuelle Desktopumgebungen sind für den Informationsschutz bei der Telearbeit hilfreich, da ein virtueller Desktop das Unternehmen aus technischer Sicht nicht verlässt, sondern nur optische in der Ferne dargestellt wird.

und Dienste sowie deren eingesetzte Kommunikationsprotokolle. Dies sollte möglichst immer nach dem Whitelist-Prinzip erfolgen. Die Kontrolle kann hierbei, bis zur Anwendungsebene, mit Hilfe spezieller Proxies oder (Anwendungs-)Gateways durchgesetzt werden. Bei besonders kritischen Netzsegmenten können zudem zusätzliche Netzsegmente als Pufferzonen (Demilitarisierte Zone (DMZ)) eingesetzt werden, um eine stärkere Trennung zu anderen Netzsegmenten zu erreichen. In einer DMZ werden dann typischerweise Proxies oder Gateways integriert, die eine direkte Verbindung in ein kritisches Netzsegment verhindern, indem sie eine Vermittlerrolle bei der Kommunikation mit kritischen Netzsegmenten einnehmen. Durch den beschriebenen Einsatz von Netzsegmenten und entsprechenden Sicherheitssystemen kann beispielsweise die Verbreitung von Schadsoftware besser vermieden werden. Durch eine weitestgehende Einschränkung der grenzüberschreitenden Kommunikation zwischen Netzsegmenten, mit Hilfe der genannten Sicherheitssysteme, können darüber hinaus unnötige Abhängigkeiten zwischen Netzsegmenten vermieden und Kaskadeneffekte beim Ausfall eines Netzsegmentes minimiert werden. Sollte eine Kommunikation über mehrere Netzsegmente nötig sein, ist darauf zu achten, dass die Kommunikation möglichst nur von Netzsegmenten mit einem höheren Sicherheitsniveau in Netzsegmente mit einem niedrigeren Sicherheitsniveau stattfinden kann, um den Übergriff von Gefährdungen aus einem Netzsegment mit einem niedrigeren Sicherheitsniveau nach Möglichkeit auszuschließen. In allen anderen Fällen sind dementsprechend zusätzliche Netzsegmente, wie eine DMZ, mit entsprechenden Proxy- oder Gatewaylösungen einzusetzen. Eine spezielle Rolle bei der Netzsegmentierung spielen Netze, die mit Hilfe von Funktechnologien realisiert werden. Diese Funknetzsegmente sollten besonders gut von anderen Netzsegmenten getrennt werden, da Funktechnologien als Übertragungsmedium nur schwer einzugrenzen sind, wodurch das Risiko eines Zugriffs von außen auf ein Funknetzsegment, im Vergleich zu anderen Netzsegmenten, steigt. Eine DMZ ist an dieser Stelle besonders wichtig. Für kritische Systeme sollten Funktechnologien darüber hinaus generell vermieden werden. Insbesondere für Netzsegmente auf der Basis von Funktechnologien aber auch für Netzsegmente im Allgemeinen gilt zudem, dass sichere Protokolle und kryptografische Verfahren für die Kommunikation eingesetzt werden müssen. Verschlüsselungsprotokolle wie TLS und VPN-Technologien sollten, wann immer möglich, genutzt werden. Zudem sollten über Netzgrenzen hinweg möglichst nur Protokolle eingesetzt werden, die von den eingesetzten Sicherheitssystemen, wie Firewall, Proxy oder NIDS/NIPS, auch unterstützt werden, um eine möglichst feine Erkennung von unerwarteten Kommunikationsvorgängen zu ermöglichen (z. B. Deep-Packet-Inspection). Bei Anwendungsdiensten, die über die Unternehmensgrenzen hinweg über ein Kommunikationsnetz erreichbar sein müssen, liegt überdies ein besonderer Fokus auf der Vertraulichkeit und Integrität von Daten, gemessen an ihrer Klassifizierung und dem daraus resultierenden Schutzniveau (vgl. 4.2.3 Klassifizierung). Hierbei ist es von besonderer Bedeutung, ein Vertrauensniveau zwischen den beteiligten Benutzern, Diensten und Systemen mit Hilfe von Authentifizierungs- und Autorisierungsmaßnahmen herzustellen und den rechtmäßigen Empfang von unveränderten Daten nachweislich zu garantieren. Dementsprechend müssen Signatur- und Verschlüsselungsverfahren von allen Beteiligten zur Sicherung der Kommunikation und des Kommunikationswegs eingesetzt werden, damit die Transaktionen zwischen den Beteiligten vertraulich bleiben und die Datenschutzbestimmung gewahrt werden. Der Einsatz von Zertifikaten und einer dazu passenden Public-Key-Infrastruktur ist hierfür zu empfehlen. Ergänzend dazu muss sichergestellt werden, dass sensible Daten durch eine entsprechende Transaktion nicht an einen öffentlichen Ort gelangen. [ISO27001 A.13.1.3, A.14.1.2, A.14.1.3], [ISO27002 13.1.3, 14.1.2, 14.1.3], [ISO27019 11.4.5], [BDEW 2.1.1.1, 2.3.1.1, 2.3.1.2, 2.3.3], [ICSSecK 32, 35, 36, 37, 38, 41, 43], [ENISA D9, D10].

### 4.4.18 Netzsegmentierung in der Prozesssteuerung

Speziell für den Energiesektor gelten für Kommunikationsnetze weitere Einschränkungen, die sich vor allem auf die Prozesssteuerung beziehen. Da Systeme in der Prozesssteuerung einen besonders hohen Schutzbedarf haben und selbst oft nur geringe Schutzmaßnahmen besitzen, sind entsprechend restriktive Netzsegmente an dieser Stelle besonders wichtig. Dies kann soweit führen, dass einzelne Systeme in eigene Netzsegmente ausgegliedert werden, um ihrem Schutzbedarf (Schutz vor anderen Systemen) oder auch ihren Schwächen (Schutz der anderen Systeme) gerecht zu werden. Die Netzsegmente für die Prozesssteuerung sollten von anderen Unternehmensnetzen, am besten physisch, getrennt sein und die industriellen Steuerungssysteme sollten des Weiteren möglichst keine Verbindung zu externen Netzen bzw. aus externen Netzen, wie dem Internet haben. Sollte eine Verbindung nötig sein, so sind an dieser Stelle zusätzliche Netzsegmente als DMZ mit entsprechenden Proxy- oder Gatewaylösungen einzusetzen, um einen direkten Zugriff zu vermeiden. Sofern ein Zugriff nur sporadisch notwendig ist, sollte die Verbindung zudem physisch, zum Beispiel durch einen Schalter, oder zumindest logisch durch einen Benutzer mit einer entsprechenden Administratorrolle (vgl. 4.1.2 Verantwortlichkeiten und Rollen) für alle anderen Zeiten, im Unternehmen erkennbar, unterbunden werden. Ein besonderer Fall stellt die Fernwartung bei industriellen Steuerungssystemen dar. In vielen Fällen wird hierfür ein direkter Zugang, beispielsweise vom Hersteller, verlangt. Zuvor genannten Regeln im Umgang mit externen Netzen sind hierbei besonders wichtig, wobei gefordert werden sollte, dass das Fernwartungsnetz dasselbe Sicherheitsniveau hat, wie das Netzsegment in dem das zu wartende System eingeordnet ist. Darüber hinaus sollte insbesondere bei diesem Anwendungsfall auf eine starke Authentifizierung durch z. B. zwei Faktoren (vgl. 4.4.4 Zugriffssteuerung auf Systeme, Netze und Dienste) und dem bereits im Allgemeinen genannten Einsatz von sicheren, im Speziellen verschlüsselten, Kommunikationsbeziehungen geachtet werden (vgl. 4.4.19 Sicherheit der elektronischen Übertragung). Ein weiteres Szenario ist die Kopplung mit Netzen dritter aus betrieblichen Gründen. Hier sind ähnliche Maßnahmen anzuwenden. Zudem sollten alle externen Verbindungen besonders genau überwacht werden. Hierbei kann die Regulierung des Zugriffs bis auf einzelne Befehle oder Daten notwendig sein [ISO27019 9.3.3, 11.4.8], [BDEW 2.3.2.2], [ICSSecK 29, 35, 38, 43], [ENISA D8].

### 4.4.19 Sicherheit der elektronischen Übertragung

Für die Übertragung von Informationen über ein Kommunikationsnetz müssen allgemeine Maßnahmen zum Schutz der drei wesentlichen Sicherheitsattribute Vertraulichkeit, Integrität und Verfügbarkeit etabliert werden. Informationen müssen im Allgemeinen jederzeit nachvollziehbar von einer Quelle, ohne die Einsicht unbefugter Personen und unverändert, an ihrem Ziel ankommen. Hierzu ist der Einsatz von kryptografischen Maßnahmen zur Verschlüsselung und Signatur von Daten notwendig. Aus diesem Grund sollten zur elektronischen Übertragung nur aktuelle, standardisierte Protokolle sowie dazugehörige Sicherheitsmaßnahmen eingesetzt werden[9]. Bei der Wahl von Sicherheitsmaßnahmen sind dabei eventuell gesetzliche Vorgaben zu beachten. Bei der elektronischen Übertragung muss des Weiteren sichergestellt werden, dass Daten nicht unautorisiert aus dem Unternehmen abfließen. Zur Verhinderung solcher Datenlecks können bereits genannte Proxylösungen, wie E-Mail-Proxies, (vgl. 4.4.8 Erkennung von Schadsoftware, 4.4.17 Sicherheit durch Netzsegmentierung) eingesetzt werden, um sensible Daten, in diesem Beispiel in einer E-Mail oder dem Anhang einer E-Mail, zu erkennen und ggf. eine unautorisierte Weitergabe der Daten zu

[9] Im Bereich des Energiesektors gehören die Protokolle ISO/IEC 60870-5/6 oder ISO/IEC 61850 beispielsweise zu den aktuell zu bevorzugenden Protokollen. Da diese Protokolle keine Sicherheitsmaßnahmen definieren, sollte für dieses Beispiel zudem der Standard ISO/IEC 62351 betrachtet werden, der Sicherheitsmaßnahmen, für die genannten und weitere Protokolle, im Energiesektor definiert.

verhindern. Für den Bereich der Prozesssteuerung werden zudem sogenannte Datendioden oder One-Way-Gateways empfohlen, die eine Datenübertragung in nur eine Richtung zu lassen. So können zum Beispiel Statusdaten zur Darstellung eines Lagebildes direkt empfangen werden, Steuerungsdaten können aber nicht direkt an Steuerungssysteme gesendet werden. Neben der Vermeidung von Datenlecks sollten außerdem schadhafte Daten, wie Schadsoftware, von legitimen Daten bei der elektronischen Übertragung unterschieden und unterbunden werden können. Hierfür gibt es verschiedene Ansätze (s. 4.4.8 Erkennung von Schadsoftware). Aus organisatorischer Sicht müssen Mitarbeiter darüber hinaus für den Umgang mit digitalen Informationen und den technischen Übertragungsmedien sowie möglichen Schwachstellen und Datenlecks sensibilisiert werden und es sollten Vereinbarungen mit externen Parteien getroffen werden, wenn sensible Daten über Unternehmensgrenzen hinaus (z. B. über Kommunikationsnetze) ausgetauscht werden sollten. Hierzu gehören unter anderem Vereinbarungen zur Vertraulichkeit und Geheimhaltung. [ISO27001 A.13.2.ff], [ISO27002 13.2.ff], [ISO27019 10.6.3], [BDEW 2.1.1.7, 2.3.1.1, 2.3.1.2, 2.5.2], [ICSSecK 15, 19, 40, 43], [ENSIA D9, D2].

### 4.4.20 Netzstrukturplan und Verwaltung

Bei der Gestaltung und Umsetzung von Netzen in einem Unternehmen muss darauf geachtet werden, dass keine Umgehung der Netzsegmentierung und der eingesetzten Sicherheitssysteme durch unkontrollierte oder nicht dokumentierte Netzverbindungen sowie fehlerhaft konfigurierte Sicherheitssysteme zur Trennung der Netzsegmente (z. B. Firewall) möglich ist. Die Netze eines Unternehmens müssen aus diesem Grund verwaltet und gesteuert werden. Hierzu sollten die Netze, wie andere Werte eines Unternehmens auch, erfasst und inventarisiert werden. Ein Netzstrukturplan auf physischer (mit Bezug zu der realen Welt und der realen elektrotechnischen Infrastruktur) und logischer Ebene (mit Bezug zu den Netzsegmenten und darin zusammengefassten Systemen) muss unter anderem gemäß IT-Sicherheitskatalog durch EVU dafür umgesetzt werden (s. [Bun15b]). Dieser Plan sollte auf den entsprechenden Ebenen Systeminformationen, wie IP-Adresse, MAC-Adresse, Systemname und Standort enthalten. Neben der Erfassung und Inventarisierung mit Hilfe eines Netzstrukturplans müssen verantwortliche Personen sowie Verfahren zur Planung und Verwaltung der Netze etabliert werden. Dabei kann es sinnvoll sein, den Betrieb der Netze von dem Betrieb anderer Systeme und Dienste, wie Desktop-Systemen, personell zu trennen. Die in diesem Dokument dargestellten Maßnahmen zur allgemeinen Absicherung von Systemen im Betrieb sind allerdings auch auf Netzkomponenten anzuwenden. Netzkomponenten müssen zudem ebenfalls in der Lage sein, Ereignisse zu protokollieren und ggf. an ein zentrales Überwachungssystem zu übertragen, um eine effektive Überwachung zu ermöglichen. Zum Betrieb der Netze sollten darüber hinaus zentrale Dienste bereitgestellt werden. Hierzu gehören vor allem ein entsprechendes Konfigurationsmanagement, ein System zur Namensauflösung (Domain Name System) – sofern Namen zur Adressierung der Systeme verwendet werden – sowie ein System zur zentralen Vergabe von IP-Adressen und Kommunikationsparametern (z. B. mit DHCP) – sofern eine dynamische Konfiguration eingesetzt werden darf. Im Bereich der Prozesssteuerung sollte in diesem Zusammenhang eine statische Konfiguration der Kommunikationsparameter bevorzugt werden. Hierfür sollten Konventionen und Prozesse für ein vereinfachtes Management erstellt und eingehalten werden. Komponenten zur Netztrennung könnten zum Beispiel immer die ersten IP-Adressen in einem Netzsegment bekommen. Wenn DNS eingesetzt wird, sollte für die Prozesssteuerung eine eigene, von anderen Unternehmensbereichen unabhängige Domäne genutzt werden, um die Prozesssteuerung vor Einflüssen von außen zu schützen. Darüber hinaus muss eine sichere Konfiguration des DNS vorhanden sein, um Ausfälle sowie verschiedene DNS-Angriffe zu

vermeiden. Dazu können unter anderem kryptografische Maßnahmen eingesetzt werden. Bei besonders kritischen Netzen kann es zudem notwendig sein, das technische Management dieser Netze, aufgrund von Sicherheits- oder Verfügbarkeitsbedenken, auszulagern. Man spricht hierbei von einem Out-Of-Band-Management. Bei dieser Form werden die Kernsysteme eines Netzes über dedizierte Managementnetze verwaltet. Die Durchführung der Netzverwaltung und die damit verbundene Vermischung von Netzmanagement- und Geschäftsdaten „In-Band“ über das eigentliche Kommunikationsnetz wird damit ausgeschlossen [ISO27001 A.13.1.1, A.13.1.2], [ISO27002 13.1.1, 13.1.2], [ISO27019 9.3.3, 11.4.5], [BDEW 2.1.1.6, 2.2.1, 2.3.1.1, 2.3.1.2, 2.3.2.1, 2.3.3, 2.4.3], [ICSSecK 4, 33, 34, 43, 44, 48, 49, 73], [ENISA D9, D10].

### 4.4.21 Beschaffung und Entwicklung

Um den vielfältigen Sicherheitsanforderungen für Werte eines Unternehmens gerecht zu werden, ist eine Berücksichtigung dieser bereits bei der Beschaffung von Systemen, Geräten und Anwendungen notwendig. Dasselbe gilt bei der Erweiterung der Genannten. Hierzu sollten allgemeine Anforderungen eines Unternehmens in Design-Dokumenten festgehalten werden. Davon ausgehend sollten für die Beschaffung von Systemen, Geräten oder Anwendungen sogenannte Lastenhefte mit spezifischen (Sicherheits-)Anforderungen für diese erstellt und als Kriterienkatalog bei der Auswahl von Systemen, Geräten oder Anwendungen eingesetzt werden. Dies gilt neben der Beschaffung von kommerziellen Produkten aus dem Regal (englisch: commercial-off-the-shelf (COTS)-Produkte) eines Herstellers auch für die Entwicklung von spezialisierten Systemen und Software im Unternehmen oder durch externe Dienstleister. Bei der Entwicklung von spezialisierten Systemen und Software muss in diesem Zusammenhang besonders auf den Einsatz sicherer Entwicklungsmethoden geachtet werden. Hierzu sind entsprechende Richtlinien zu formulieren, die eine sichere Entwicklung und Entwicklungsumgebung gewährleisten. Die in diesem Dokument dargestellten Sicherheitsmaßnahmen für eine sichere IT-Infrastruktur sollten dabei neben der Betriebsumgebung auch zur Absicherung der Entwicklungsumgebung eingesetzt werden, da eine sichere Entwicklungsumgebung mit dem Ziel betrieben wird, die entstehenden Systeme oder die entstehende Software vor unautorisierten Einflüssen zu schützen. Eine Entwicklungsumgebung sollte deshalb möglichst dasselbe Sicherheitsniveau aufweisen, wie der Bereich in dem die entwickelten Systeme oder die entwickelte Software eingesetzt werden sollen. Unter Umständen ist sogar ein höheres Sicherheitsniveau sinnvoll. Darüber hinaus sollten Vorgaben zur Entwicklung selbst, wie Richtlinien zur Verwendung von Softwarebibliotheken, Programmiersprachen und Techniken sowie Testverfahren im Unternehmen definiert werden. Sogenannte Grundsätze für den gesamten Entwicklungsprozess, von der Analyse über die Entwicklung bis zum Test und der Pflege der Systeme, müssen vorhanden sein. Die Grundsätze definieren Vorgehensweisen und Entwicklungsprinzipien für ein sicheres System oder eine sichere Software. Hierbei ist unter anderem eine sichere Architektur notwendig, die ein System so definiert, dass es auch in einem Ausnahmefall nicht in einen unsicheren Zustand wechselt. Sicherheitsmechanismen für Ein- und Ausgabekanäle, wie die zwingende Validierung der ein- bzw. ausgehenden Daten, stellen in diesem Zusammenhang zum Beispiel eine wichtige Anforderung dar. Fehlerhafte Eingaben dürfen nicht zu einem unsicheren System führen. Das System oder die Software müssen stattdessen robust gestaltet sein. Bei der Umsetzung sollten hierfür unter anderem standardisierte und langlebige Verfahren und Algorithmen eingesetzt werden. Aufgrund der langen Einsatzzeit von Systemen zur Prozessteuerung ist dies für den Energiesektor besonders relevant. Vor allem im Bereich der Kryptografie sollten nur gut getestete

Softwarebibliotheken eingesetzt werden, deren Algorithmen langfristig als sicher gelten[10]. Darüber hinaus ist es sinnvoll überflüssige Funktionen in einem System oder einer Software im Sinne der Sicherheit zu vermeiden. Stattdessen sollten zusätzliche Sicherheitsmaßnahmen wie Self-Tests und Integritätsprüfungsmechanismen berücksichtigt werden, um den Betriebszustand eines Systems oder einer Software jederzeit nachvollziehen zu können. Dies gilt insbesondere für Systeme im Energiesektor, die außerhalb der Unternehmensgrenzen eingesetzt werden. Je nach Einsatzziel können zudem weitere Grundsätze für eine sichere Entwicklung hinzukommen[11]. Neben der Definition und Anwendung der Grundsätze für eine sichere Entwicklung ist die Einhaltung dieser Grundsätze mir Hilfe von Tests zur Systemsicherheit während der Entwicklung und später im Rahmen von Systemabnahmetests zu überprüfen. Dabei ist es sinnvoll, dass die Tests, besonders bei der Entwicklung durch Dienstleister, nach dem Vier-Augen-Prinzip, von dem Auftragnehmer und dem Auftraggeber gleichermaßen durchgeführt werden. Hierbei können z. B. Code Reviews aber auch automatisierte Tests mit Code-Analyse-Tools und Test-Frameworks zum Einsatz kommen. Die Ergebnisse sollten dokumentiert werden, um bei Mängeln entsprechende Anpassungen vornehmen zu können. Für die Durchführung der Tests sind meist möglichst realistische Prüfdaten aus dem Geschäftsbetrieb eines Unternehmens notwendig. Diese Daten können Werte eines Unternehmens darstellen und sollten deshalb entsprechend ihrer Klassifizierung wie im allgemeinen Betrieb geschützt und zum Ende der Entwicklung unwiderruflich aus der Entwicklungsumgebung entfernt werden. Ein besonderer Schutz ist darüber hinaus für den Quellcode einer Software oder eines Systemteils notwendig. Er bildet die Basis für den späteren produktiven Einsatz. Unautorisierte Änderungen an dem Quellcode können einen besonders weitreichenden Schaden anrichten und sind im fertigen System oder in der fertigen Software nur noch schwer zu erkennen. Im Allgemeinen sollten deshalb nur ausgewählte, fachkundige Mitarbeiter einen Zugriff auf den Quellcode haben. Jeder Zugriff und die dabei ausgeführten Aktionen sind dabei unbestreitbar zu verfolgen. Hierbei ist eine Anwendung zur Kontrolle des Quellcodes und dessen Änderungen mit Hashsummen und Signaturen hilfreich, die nur authentifizierten Benutzern einen Zugang erlaubt[12]. Sämtliche Änderungen müssen darüber hinaus autorisiert werden. Hier ist eine Zusammenarbeit mit dem Änderungsmanagement sinnvoll (vgl. 4.4.2 Änderungen am Betrieb). Quellcode sollte außerdem niemals auf einem Produktivsystem vorhanden sein. Dies gilt auch für andere Entwicklungswerkzeuge wie Compiler (vgl. 4.4.3 Verhinderung von Schwachstellen). Im Allgemeinen sollten Entwicklungs-, Test- und Betriebsumgebung immer voneinander getrennt sein, um den Betrieb nicht zu stören und die Sicherheit bei der Entwicklung nicht zu gefährden. Sollten Situationen vorhanden sein, in denen eine Trennung nicht möglich ist, müssen entsprechende Sicherheitsvorkehrungen getroffen werden, so dass das benötigte Sicherheitsniveau für die einzelnen Bereiche gewahrt bleibt und keine Datenlecks oder unautorisierten Zugriffe zwischen den Bereichen entstehen. Ein solches Szenario muss jedoch die Ausnahme sein. Sollte die Entwicklung an einen Dienstleister ausgelagert sein, sind die vorausgehend genannten organisatorischen und technischen Maßnahmen sowie die Entwicklung im Allgemeine durch das beauftragende Unternehmen zu überwachen, um Sicherheitsmängel zu vermeiden und ggf. gesetzliche Anforderungen zu erfüllen

[10] Im Bereich der Kryptografie wird heute beispielsweise bereits über die sogenannte Post-Quanten-Kryptografie diskutiert, da man davon ausgeht, dass die Sicherheit einiger heutiger Algorithmen mit der Etablierung von Quantencomputern nicht mehr gewährleistet ist (vgl. [Bun16a]).

[11] Web-Applikationen müssen zum Beispiel nach anderen Grundsätzen entwickelt werden als Desktop-Applikationen. Bei einer Web-Applikation ist beispielsweise der gleichzeitige Zugriff durch mehrere Benutzer zu berücksichtigen, so dass, im Gegensatz zu einer Desktop-Anwendung, die nur von einem Benutzer zurzeit benutzt wird, besonders hohe Anforderungen an die Leistung, die Ausfallssicherheit und vor allem die Benutzertrennung gestellt werden müssen.

[12] Versionsverwaltungssysteme wie Git oder Subversion können zur Kontrolle des Quellcodes eingesetzt werden.

[ISO27001 A.9.4.5, A.12.1.4, A.14.1.1, A.14.2.1, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1], [ISO27002 9.4.5, 12.1.4, 14.1.1, 14.2.1, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1], [27019 12.1.1], [BDEW 2.1.1.1, 2.1.1.5, 2.1.1.8, 2.1.1.9, 2.1.1.10, 2.1.2.1, 2.3.3, 2.4.4, 2.4.5, 2.4.7, 2.5.1, 2.5.2, 2.5.3, 2.5.4, 2.5.5, 2.5.7, 2.6.2, 14.2.5], [ICSSecK 2, 7, 18, 20, 22, 23, 24, 27, 50], [ENISA D3, D11].

### 4.4.22 Kryptografische Maßnahmen

Der Einsatz kryptografischer Maßnahmen zum Schutz der Vertraulichkeit (Verschlüsselung) sowie der Integrität (Signaturen und Hashwerte) als auch zur Sicherstellung der Unbestreitbarkeit von Handlungen und der hierzu notwendigen Authentifizierung von Benutzern (Verschlüsselung und Signaturen) ist eine wiederkehrende Konstante in den Maßnahmen zur erfolgreichen Absicherung einer IT-Infrastruktur und den darin enthaltenen Netzen, Systemen, Diensten und Informationen. Zur Orientierung in diesem breiten Anwendungsfeld sollten Verantwortlichkeiten und Richtlinien zum Einsatz und dem Umgang mit kryptografischen Maßnahmen in einem Unternehmen festgelegt werden. In Abhängigkeit zu vorhandenen gesetzlichen Bestimmungen und dem Schutzbedarf der Unternehmensdaten, entsprechend ihrer Klassifizierung und ihrer erwarteten Mobilität, erleichtern generelle kryptografische Vorgaben, in Bezug auf Stärke und Qualität, die Auswahl von Verschlüsselungstechnologien und damit den Einsatz von Kryptografie in einem Unternehmen. Bei der Auswahl der Verfahren ist dabei immer der aktuelle Stand der Technik zu berücksichtigen. Außerdem sollten nur anerkannte Verschlüsselungsalgorithmen und Bibliotheken zur Umsetzung verwendet werden. Im Allgemeinen sollten möglichst immer Protokolle und Technologien eingesetzt werden, die den kryptografischen Schutz von Daten unterstützen, um kryptografische Maßnahmen bei einem entsprechenden Schutzbedarf jederzeit, ohne größeren Aufwand einführen zu können. Darüber hinaus müssen Prozesse zum Umgang mit kryptografischen Maßnahmen eingeführt werden. Ein wichtiger Aspekt ist hierbei die Wiederherstellung von verschlüsselten Daten. Des Weiteren ist die Verwaltung von Schlüsseln von besonderer Bedeutung. Eine sichere Erzeugung von Schlüsseln muss gewährleistet werden. Eventuell ist eine sogenannte Public-Key-Infrastruktur (PKI) zur Verwaltung von Zertifikaten (z. B. zur Authentisierung) notwendig. Neben der Erzeugung von Schlüsseln muss zudem eine sichere Schlüsselverteilung und Speicherung möglich sein. Hierzu können beispielsweise hardwarebasierte Sicherheitsmaßnahmen wie Smartcards eingesetzt werden. Außerdem müssen Verfahren zum Umgang mit zeitlich abgelaufenen oder anderweitig kompromittierten Schlüsseln umgesetzt werden[13] [ISO27001 A.10.1.ff], [ISO27002 10.1.ff], [BDEW 2.1.1.7, 2.3.1.1, 2.3.3, 2.4.3, 2.5.2], [ICSSecK 43, 58], [ENISA D9].

### 4.4.23 Audit

Zur Aufrechterhaltung der Aspekte und Anforderungen des IT-Betriebs und zur Erfüllung gesetzlicher Vorgaben oder zur Zertifizierung sollten in regelmäßigen Abständen Audits durchgeführt werden, mit denen die Umsetzung und Wirksamkeit von Sicherheitsmaßnahmen überprüft wird. Die Auditmaßnahmen müssen dabei so gewählt sein, dass sie den IT-Betrieb nicht stören. Sollte dies nicht möglich sein, müssen Auditmaßnahmen außerhalb der Betriebszeiten durchgeführt werden. Ein Auditor sollte für ein Audit immer nur lesenden Zugriff auf informationsverarbeitende Systeme zur Kontrolle der Aspekte und Anforderungen haben. Das Audit selbst sollte überwacht und dokumentiert werden, um einen konsistenten, vergleichbaren Prüfungsablauf zu erreichen [ISO27001 A.12.7.1], [ISO27002 12.7.1], [ICSSecK 9, 17], [ENISA D6].

[13] Im Fall einer PKI sind Zertifikate beispielsweise rechtzeitig vor Ablauf auszutauschen und kompromittierte Zertifikate müssen anderen Systemen unter anderem mit Hilfe einer Certificate-Revocation-List (CRL) bekannt gemacht werden.

## 4.5 Ergänzende Sicherheitsmaßnahmen beim Umgang mit Dienstleistern

Externe Dienstleister sind häufig auf Informationen durch ein beauftragendes Unternehmen angewiesen. Hierzu müssen sie zum Teil auf Netze, Systeme oder Dienste eines Unternehmens zugreifen. Dies kann auf dem Gelände eines Unternehmens aber auch aus der Ferne passieren. Zur Aufrechterhaltung der Sicherheit im Unternehmen müssen deshalb Richtlinien zum Umgang mit Dienstleistern, wie Lieferanten, auf der Basis der Sicherheitsanforderungen und Maßnahmen in einem Unternehmen definiert werden. In diesen Richtlinien sollen Vorgaben zum Umgang mit Informationen für Dienstleister festgelegt werden. Hierzu gehören beispielsweise Vorgaben darüber, wie der Informationszugriff für verschiedene Arten von Dienstleistern erfolgen darf und welche Anforderungen an einen Dienstleister für den Umgang mit Informationen gestellt werden. Des Weiteren muss es Prozesse zur Kontrolle des Umgangs und zur Rückführung der Informationen in das Unternehmen geben, wenn diese nicht mehr von einem Dienstleister benötigt werden. Diese und weitere Inhalte, insbesondere spezifische und situationsabhängige Regelungen, sollten in Verträgen mit Dienstleistern rechtlich bindend festgehalten werden. Dabei ist sicherzustellen, dass die Vorgaben eines Unternehmens an einen Dienstleister auf die gesamte Kette seiner Leistungserbringung angewendet werden. Dies gilt auch für Unterauftragnehmer aufseiten eines Dienstleisters. Dienstleister sollten hierzu regelmäßig durch das beauftragende Unternehmen überprüft werden. Ggf. kann auch verlangt werden, dass ein Dienstleister regelmäßige externe Audits vorweisen muss (z. B. gemäß ISO/IEC 27001). Hierzu sind entsprechend Verantwortliche im Unternehmen zu bestimmen. Anpassungen von Dienstleistungen durch das Unternehmen oder Änderungen aufseiten eines Dienstleisters sowie der Wechsel eines Dienstleisters sind darüber hinaus als Teil des Änderungsmanagements im Unternehmen zu sehen und sollten entsprechend behandelt werden. Hierzu gehört wie unter Abschnitt 4.4.2 beschrieben die Feststellung notwendiger Änderungen, deren Beurteilung, sowie die Planung und Umsetzung der Änderung als auch die Möglichkeit eine Änderung bei auftretenden Problemen wieder rückgängig zu machen [ISO27001 A.15.1.ff, A.15.2.ff], [ISO27002 15.1.ff, 15.2.ff], [ISO27019 6.2.3], [BDEW 2.3.2.2, 2.1.1.8], [ICSSecK 2, 10, 19, 21, 27], [ENISA D2].

## 4.6 Safety vs. Security

Im Rahmen dieses Dokuments werden Sicherheitsmaßnehmen für Netze, Systeme, Dienste und deren Informationen betrachtet. Die daraus resultierende Sicherheit kann dem Oberbegriff Security zugeordnet werden. Security wird im Rahmen dieses Dokumentes als Sicherheit von Unternehmenswerten vor unautorisierten Einflüssen definiert. Safety wird in diesem Dokument dagegen als Sicherheit von Leib und Leben im Allgemeinen und speziell der Personen eines Unternehmens definiert. Safety wird in den untersuchten Standards nur selten direkt erwähnt, auch wenn Security eine wichtige Voraussetzung für Safety darstellt. Die Folgen einer Manipulation eines Steuerungssystems in der Prozesstechnik können beispielsweise in den Bereich Safety fallen, wenn hierdurch eine Situation erzeugt wird, die eine Gefahr für Leib und Leben darstellt. Safety ist im Energiesektor von besonderer Bedeutung, so dass im Rahmen der [ISO27019 10.12.1] zumindest definiert wird, dass Netze, Systeme und Dienste so ausgelegt werden müssen, dass Safety nie gefährdet wird. Hierzu sollte gegebenenfalls ein eigenes Kommunikationsnetz für Safety-bezogene Informationen etabliert werden, um eine Beeinträchtigung der Kommunikation durch andere Systeme zu vermeiden. Darüber hinaus müssen Safety-Systeme auch ohne eine zentrale Steuerung automatisiert funktionieren, um Schäden zu jeder Zeit abwenden zu können. Des Weiteren sollen Änderungen an diesen Systemen besonders genau geprüft und dokumentiert werden, damit es nicht zu unvorhergesehenen Gefahren kommen kann. Safety besitzt im Allgemeinen immer eine höhere

Priorität als Security. Dies heißt wie oben angedeutet jedoch nicht, dass Security vernachlässigt werden kann, da sie eine Voraussetzung für Safety darstellt.

# 5 Schlusswort

Die Zusammenfassung der ausgesuchten Standards und ihrer Maßnahmen mit dem Fokus auf die technischen Aspekte zeigt, dass die Standards zusammengenommen bereits einen umfangreichen Maßnahmenkatalog enthalten. Einige Maßnahmen sind dabei in allen Standards zu finden, während andere Maßnahmen, insbesondere konkretere Vorgaben, nur in einzelne Standards auftauchen. Dies hat zur Folge, dass eine verantwortliche Person für die Informationssicherheit bei einem EVU durchaus mehrere Standards zur Beantwortung der Frage, wie ein Unternehmen abgesichert werden kann, heranziehen muss. In jedem Fall ist die Normenreihe ISO/IEC 2700x ein guter Ausgangspunkt für die Lektüre von Standards, da sich die meisten Standards an einer Stelle auf diese Normenreihe beziehen. Dennoch sollten EVU im Verteilungsnetz auch die branchenspezifischen Informationen, die durch den BDEW und zum Teil auch durch das BSI herausgegeben werden, beachten. Hier finden sich Lösungen für die Eigenheiten bei den EVU, insbesondere mit Bezug auf die notwendige Prozesssteuerung. Durch die Lektüre und Anwendung der Maßnahmen in den Standards lässt sich somit ein gutes Sicherheitsniveau in einem Verteilungsnetz erreichen.

Während das Bewusstsein für Informationssicherheit auf der Ebene der Übertragungsnetze sehr hoch ist, lässt sich aus Beobachtungen in der Realität der Verteilungsnetze jedoch ableiten, dass Standards in vielen Fällen nur teilweise oder gar nicht berücksichtigt werden. Dies liegt vor allem an der Historie dieser Netze. Die informationsverarbeitenden Systeme, die dort in der Vergangenheit eingesetzt wurden, waren in den meisten Fällen proprietär mit proprietären Kommunikationsverbindungen und normalerweise nicht mit Netzen, wie dem Internet, verbunden. Eine sogenannte Air-Gap trennte die Prozesssteuerung von anderen Bereichen in einem Unternehmen. In dieser Situation waren Maßnahmen zur Informationssicherheit von geringer Bedeutung, da man annahm, dass allgemeine Gefahren aus typischen Computernetzen an dieser Stelle nicht zum Tragen kommen könnten. Diese Annahme wurde von den EVU auch auf die Hersteller der Steuerungssysteme übertragen, in dem nur ein geringer Bedarf für Informationssicherheit durch EVU bestand, besaßen die Systeme der Hersteller auch nur geringe Sicherheitsmaßnahmen.

Mit dem Beginn der Energiewende wird diese Situation jedoch immer weiter verändert. Es etablieren sich standardisierte Protokolle und dezentrale Systeme werden aus Kostengründen über ein öffentliches Kommunikationsnetz, wie das Internet, zur Steuerung mit einem EVU verbunden. Dabei werden jedoch erst nach und nach Sicherheitsfunktionen in Steuerungssysteme integriert und traditionelle Sicherheitsmaßnahmen aus den typischen Computernetzen müssen erst auf die notwendigen Protokolle und technischen Anforderungen der neuen Steuerungssysteme adaptiert werden, bevor sie zur Absicherung von Prozessnetzen eingesetzt werden können. Dies führt dazu, dass Sicherheitsprobleme entstehen. Ein Beispiel hierfür, dass sich im Rahmen des Forschungsprojektes SEnCom gezeigt hat, ist die Überwachung der informationsverarbeitenden Systeme. Die Überwachung der neuen Steuerungssysteme auf informationstechnische Fehler wird zum aktuellen Zeitpunkt nur wenig adressiert, obwohl dies, unter anderem durch das BDEW-Whitepaper, von den Herstellern gefordert wird. Sowohl die Prognose zukünftiger Verteilungsnetze, als auch aktuelle Ereignisse weisen aber darauf hin (vgl. [HEI16]), dass Fehlerursachen zukünftig auch vermehrt in der IKT zu finden sein werden. Hierdurch entsteht eine Art „Blinder Fleck“, der zur Folge

hat, dass zukünftige Fehler im Stromnetz nicht mehr mit bisherigen Mitteln zu identifizieren sind. Es besteht die Gefahr, dass ein Fehler der eigentlich durch die IKT verursacht wird, durch eine fehlende Überwachung nicht auf die IKT zurückgeführt werden kann und in der Energietechnik gesucht wird. In der Folge kann eine zuverlässige Unterscheidung zwischen Fehlern der IKT und der Energietechnik erst durch aufwendige Diagnosevorgänge vor Ort erreicht werden. Eine Erhöhung der Ausfallzeiten kann die Folge sein. Die Notwendigkeit von umfassenden Überwachungsmaßnahmen wird zudem durch die im IT-Sicherheitskatalog festgelegte Meldepflicht von informationstechnischen Sicherheitsvorfällen gegenüber dem BSI bekräftigt (s. [Bun15b]).

Mit der Energiewende ist es daher auf Seiten der EVU sowie aufseiten der Hersteller notwendig, das Sicherheitsbewusstsein zu erhöhen. Bestehende Standards müssen anerkannt und umgesetzt werden. Insbesondere bei der Informationssicherheit geht es dabei nicht um eine rein technische Betrachtung, sondern um eine ganzheitliche Beurteilung der Situation in einem Unternehmen und die besonnene Ableitung notwendiger organisatorischer und technischer Maßnahmen. Im Rahmen der Deepsec-Konferenz 2016, einer der führenden Informationssicherheitskonferenzen, hat beispielsweise der IT-Sicherheitsexperte Markus J. Ranum hierzu betont, dass der Kauf von Sicherheitstechnologien alleine nicht ausschlaggebend für eine sichere IT-Infrastruktur sei. Für eine sichere IT-Infrastruktur sei eine ganzheitliche Betrachtung der Probleme und ihrer Quellen notwendig, die in einer gezielten Planung und Umsetzung für Verbesserungsmaßnahmen münden müsse [Gi16].

Oft können bereits wenige, teils nur organisatorische, Maßnahmen eine signifikante Erhöhung des Sicherheitsniveaus in einem Unternehmen bewirken, wenn sie an der richtigen Stelle umgesetzt werden. Bei den EVU im Verteilungsnetz müssen dazu weiterführende Kompetenzen für IKT und Informationssicherheit eingebracht werden. Dies kann durch eigenes Personal und Schulungen oder durch Dienstleister geschehen. EVU müssen, als Kunden von Systemherstellern, außerdem eine höhere Informationssicherheit für die Produkte fordern, damit Probleme wie der „Blinde Fleck“ nicht auftreten und die Maßnahmen aus den Standards auch technisch umgesetzt werden können. Ohne die Unterstützung durch die eingesetzten Systeme kann Informationssicherheit durch EVU im Verteilungsnetz technisch zumindest nur eingeschränkt umgesetzt werden.

Abschließend ist noch einmal zu betonen, dass Informationssicherheit kein einmaliges Projekt ist. Durch menschliche und technische Fehler können trotz aller Bemühungen immer Sicherheitslücken auftreten, so dass Informationssicherheit ein andauernder Prozess sein muss. Glücklicherweise lässt sich der Aufwand an dieser Stelle stark reduzieren, wenn ein ISMS umgesetzt wird und entsprechende Informationskanäle etabliert sind. Es müssen dann hoffentlich nur kleine Eingriffe stattfinden, die zum Teil automatisiert sind und somit keine hohen Ressourcen im Unternehmen binden. Dieses Dokument bietet durch die Zusammenfassung hierzu einen Einstieg. Das Dokument soll außerdem zur weiteren Lektüre von Standards und anderen Informationsquellen zur Informationssicherheit über die hier ausgesuchten Standards hinaus anregen.

# 6 Literaturverzeichnis

[Bun07] Bundesamt für Sicherheit in der Informationstechnik. BSI Standard 100-1 – Information Security Management System (ISMS). Bonn, 2007.

[Bun08] Bundesamt für Sicherheit in der Informationstechnik. BSI Standard 100-2 – IT-Grundschutz-Vorgehnsweise. Bonn, 2008.

[Bun13] Bundesamt für Sicherheit in der Informationstechnik. ICS-Security-Kompendium. Bonn, 2013.

[Bun15] Bundesnetzagentur. IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. Bonn, 2015.

[Bun15a] Bundesamt für Sicherheit in der Informationstechnik. Struktur_Modernisierung.pdf. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Struktur_Modernisierung.pdf?__blob=publicationFile, letzter Aufruf 25.01.2016, Bonn, 2015.

[Bun15b] Bundesnetzagentur. IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz. Bonn, 2015.

[Bun15c] Bundesverband der Energie- und Wasserwirtschaft e. V.. Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme. Berlin, 2015.

[Bun16] Bundesamt für Sicherheit in der Informationstechnik. IND.1: Betriebs- und Steuerungstechnik (IT-Grundschutz-Baustein). Bonn, 2016.

[Bun16a] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Bonn, 2016.

[CT13] M. Conrad, R. Thomas. BDEW White Paper in practice: IT security in the secondary systems. Internationaler ETG-Kongress 2013 – Energieversorgung auf dem Weg nach 2050 - Symposium 1: Security in Critical Infrastructures Today, Berlin, 2013.

[Deu14] Informationstechnik – Sicherheitsverfahren – Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014). Berlin, 2014.

[Deu15] Deutsches Institut für Normung. Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014). Berlin, 2015.

[Eur12] European Network and Information Security Agency. Appropriate security measures for smart grids - Guidelines to assess the sophistication of security measures implementation. Heraklion, 2012.

[Eur13a] European Network and Information Security Agency. Smart Grid Threat Landscape and Good Practice Guide. Heraklion, 2013.

[Eur13b] European Network and Information Security Agency. SMART GRID TASK FORCE 4 EG2 DELIVERABLE 5 - Proposal for a list of security measures for smart grids. Heraklion, 2013.

[Gi16] H. Gierow. Was IT-Sicherheit mit Diätnahrung zu tun hat. http://www.golem.de/news/deepsec-keynote-was-it-sicherheit-mit-diaetnahrung-zu-tun-hat-1611-124408.html, letzter Aufruf 01.12.2016, Golem.de, 2016.

[HEI16] F. Rötzer. Ukraine: Hackerangriff verursachte Blackout. Heise Medien GmbH & Co. KG. Hannover, 2016

[Roh10] S. Rohjans, M. Uslar, R. Bleiker, J. González, M. Specht, T. Suding, T. Weidelt. Survey of Smart Grid Standardization Studies and Recommendations. *2010 First IEEE International Conference on Smart Grid Communications (SmartGridComm)* vol., no., S. 583-588, Oktober, 2010.

[Usl10] M. Uslar, S. Rohjans, R. Bleiker, J. Gonzalez, M. Specht, T. Suding, T. Weidelt. Survey of Smart Grid standardization studies and recommendations — Part 2. *Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES* , vol., no., S.1-6, Oktober, 2010.