dena
Deutsche Energie-Agentur

Future Energy Lab

ANALYSE

Netzbetreiber-Umfrage Cybersicherheit

Zum Stand der Cybersicherheit im deutschen Stromnetz

Impressum

Herausgeber
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 (0)30 66 777-0
Fax: +49 (0)30 66 777-699
E-Mail: info@dena.de
Internet: www.dena.de

Autorinnen und Autoren:
Jasmin Wagner, dena
Dr. Oliver Chadenas, umlaut SE

Redaktion:
Marius Dechand, dena
Benedikt Pulvermüller, dena

Stand:
08/2022

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2022) „Netzbetreiberumfrage Cybersicherheit“

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Inhalt

Vorwort

Wie steht es um die Cybersicherheit im deutschen Stromnetz? Dieser Frage geht die Deutsche Energie-Agentur (dena) im vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderten Projekt EnerCise nach und hat hierfür die umlaut SE mit der Durchführung einer Umfrage unter Verteilnetzbetreibern beauftragt. Ziel der Netzbetreiberumfrage ist die Ermittlung des Status quo bei der Umsetzung von Cybersicherheitsmaßnahmen in Form von existierenden Gegenmaßnahmen gegen einen Angriff, bei der Nutzung von Cybersicherheits-Management-Systemen und Standards im Unternehmen sowie beim Vorhandensein von Response-Mechanismen. Dem voran wird eine Einschätzung der aktuellen Bedrohungslage aus Sicht der Netzbetreiber gegeben. Die Umfrage schafft mit ihren Ergebnissen eine Wissensbasis für die Identifizierung und Ausgestaltung weiterer Maßnahmen und setzt Anreize zu weiterführenden Diskussionen über die Bedeutung und Priorisierung des Themas Cybersicherheit.

Dem Thema Cybersicherheit kommt durch die Digitalisierung des Energiesystems eine immer größere Bedeutung zu. Durch den vermehrten Einsatz von digitalen Technologien auf allen Ebenen der Wertschöpfungskette vergrößert sich auch die Angriffsfläche für Hacker, die versuchen, das System zu infiltrieren oder anderweitig zu schädigen. Als besonders schützenswert gelten im Energiesystem die Kritischen Infrastrukturen (KRITIS). Kritische Infrastrukturen sind Organisationen oder Einrichtungen mit großer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[1] Im Energiesektor betrifft das Anlagen zur Erzeugung, zum Transport und/oder zur Verteilung von Strom, Gas, Mineralöl und Fernwärme ab einem in der BSI-Kritisverordnung definierten Schwellenwert. Anlagen, die nach der BSI-Kritisverordnung als Kritische Infrastruktur eingestuft werden, unterliegen besonderen Auflagen bezüglich der IT-Sicherheit und müssen im Falle einer massiven Versorgungsstörung geeignete Präventions- und Reaktionsmaßnahmen zur Minimierung des Ausmaßes der Folgen abrufen können.[2] Für einen reibungslosen Ablauf im Krisenfall sind regelmäßige Übungen zum Einstudieren der Protokolle hilfreich. Zudem können überregionale Sicherheitsübungen die Zusammenarbeit stärken und eine nachhaltige Stakeholder-Vernetzung fördern.

Vor diesem Hintergrund hat das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) die Deutsche Energie-Agentur (dena) mit den Projekten EnerCrypt und EnerCise beauftragt. EnerCrypt stellt in Form eines Innovationsgutachtens einerseits den Status quo der energiewirtschaftlichen Cybersicherheit in Deutschland dar und richtet andererseits den Blick in die Zukunft, indem es die aktuellen Trends zur cybersicheren Ertüchtigung von Betriebsmitteln durch digitale Zukunftstechnologien beleuchtet. Um die Marktstellung Deutschlands bei energiewirtschaftlichen Cyberinnovationen zu stärken, werden außerdem regulatorische, förderpolitische, wirtschaftliche und sicherheitskulturelle Hemmnisse für technische Innovationen im Bereich der Cybersicherheit sowie anhand internationaler Best-Practice-Beispiele Lösungsansätze zur Verbesserung der Cyber-Souveränität durch Cyberinnovationen aufgezeigt. Das Folgeprojekt EnerCise nimmt diesen roten Faden des EnerCrypt-Gutachtens auf. Durch eine Cybersicherheitsübung mit deutschen und internationalen Sicherheitsexpertinnen und -experten sowie Spezialistinnen und Spezialisten deutscher Netzbetreiber soll die Awareness für Cybersecurity erhöht und die Vernetzung der Branchen gestärkt werden. Ziele der ersten Übung sind die gemeinsame Entwicklung und Erprobung von Routinen und Response-

[1] § 2 Nr. 10 BSI-Gesetz; https://www.kritis.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html.
[2] https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/Energie/Energie_node.html.

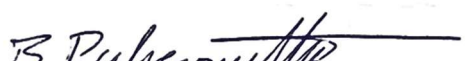
Mechanismen sowie die Vernetzung der eingebundenen Akteure untereinander. Die zweite Sicherheitsübung richtet, ähnlich wie das EnerCrypt-Gutachten, den Blick in die Zukunft und soll dazu eine Sandbox zur Erprobung digitaler Zukunftstechnologien in Bezug auf Cybersicherheit bei Netzbetreibern darstellen. Durch die Live-Testung dieser Zukunftstechnologien können Potenziale identifiziert, quantifiziert und dokumentiert werden. Dies soll eine solide Wissens- und Datengrundlage schaffen, auf Basis derer eine neue Stoßrichtung in der Diskussion zur Beseitigung regulatorischer, förderpolitischer, wirtschaftlicher und sicherheitskultureller Hemmnisse eingeschlagen werden kann.

Die Ergebnisse dieser Umfrage dienen innerhalb des Projekts EnerCise als Basis für eine effektive inhaltliche Ausrichtung der Cybersicherheitsübung, sollen darüber hinaus aber auch die Wissensbasis für folgende Projekte und Initiativen zum Thema Cybersicherheit des Future Energy Lab und der dena erweitern.

Herzlichst,

Andreas Kuhlmann

Vorsitzender der Geschäftsführung
der Deutschen Energie-Agentur (dena)



Benedikt Pulvermüller

Teamleiter Digitale Technologien & Start-up
Ökosystem der Deutschen Energie-Agentur (dena)

1 Einleitung und Motivation

Ziele des hier dokumentierten Projekts sind eine Erfassung der aktuellen Situation der Stromnetzbetreiber und die Identifikation von Schwerpunkten für Cyberübungen mittels einer Online-Umfrage und Experteninterviews. Das Kunstwort *Cyber*[3] wird dabei im Sinne von „die Informationstechnik bzw. IT-Systeme betreffend“ verwendet.

Das vorliegende Dokument beschreibt Kontext, Vorgehen und Ergebnisse des Projekts. Es gliedert sich wie folgt:

Kapitel 1 steckt den Rahmen für das Projekt ab und stellt die Situation der Netzbetreiber, die Bedeutung von Cybersicherheit sowie besondere Herausforderungen in diesem Zusammenhang dar.

Kapitel 2 beschäftigt sich mit der durchgeführten Online-Umfrage. Es werden Konzeption und Durchführung erläutert und die Ergebnisse dargestellt.

In Kapitel 3 werden die im Rahmen des Projekts geführten Experteninterviews dargestellt. Aufbau, Konzeption und Durchführung werden diskutiert und die wesentlichen Ergebnisse zusammengefasst.

Kapitel 4 stellt die Erkenntnisse aus Umfrage und Interviews dar. Es werden daraus resultierende Schlussfolgerungen und Empfehlungen formuliert sowie Schwerpunkte für eine zukünftige Cybersicherheitsübung identifiziert.

Das Literaturverzeichnis und ein Glossar ergänzen das Dokument.

1.1 Die EnerCrypt-Studie

Die vorliegende Studie ist im Rahmen des EnerCise-Projekts in einen größeren Kontext eingebettet, der mit der Studie **EnerCrypt** (dena, 2021) begonnen hat und einen Bogen von theoretischen Grundlagen der Cybersicherheit bis zur praktischen Anwendung schlägt.

Die EnerCrypt-Studie beschäftigt sich mit dem derzeit stattfindenden tiefgreifenden technologischen Wandel in der Energieversorgung. Dieser Wandel hat zwei wesentliche Treiber, nämlich zum einen die Energiewende und die damit verbundene Dezentralisierung in Stromnetzen, zum anderen die allgemeine technische Innovation.

EnerCrypt gibt eine Bestandsaufnahme der aktuellen Technologie, die derzeit in der Stromverteilung produktiv verwendet wird, sich in Entwicklung bzw. Evaluierung befindet oder aber für die Zukunft diskutiert wird. Dabei werden sowohl Kommunikationstechnik als auch Softwaremodelle, Algorithmen und Paradigmen ausführlich untersucht und vor allem im Hinblick auf ihre Sicherheitsmerkmale bewertet. Es wird dargestellt, dass Angriffe auf Computersysteme durchaus reale Auswirkungen bis hin zur Zerstörung von Netzkomponenten wie Generatoren haben können. Cyberbedrohungen und -gegenmaßnahmen werden analysiert, außerdem werden regulatorische und gesetzliche Rahmenbedingungen erläutert.

[3] Abgeleitet vom griechischen κυβερνήτης (kybernetes), auf Deutsch: „Steuermann“.

Als konkretes Fallbeispiel wird die Smart-Meter-Gateway-Infrastruktur (SMGW-Infrastruktur) herangezogen. Die Studie stellt dar, wie die für eine SMGW-Infrastruktur notwendige Technik und die erforderlichen Protokolle in eine cybersichere Umgebung überführt werden können. Hier besteht die Besonderheit, dass erstmals „nahezu alle relevanten Akteure der Energiebranche mit dieser verknüpft sind“[4]. Daraus lassen sich allgemein „grundlegende Anforderungen an die zulässigen bzw. notwendigen Kommunikationsmuster und die IT-Sicherheit ableiten“[5], unter anderem im Hinblick auf die Ladeinfrastruktur für Elektromobilität.

Die Studie sieht durchaus einen potenziellen Zielkonflikt zwischen Cybersecurity und Praxistauglichkeit. Sie hält „eine Abwägung von (kurzfristiger) Umsetzbarkeit und Risikominimierungspotenzial für entscheidend, um zu beurteilen, welche Maßnahmen in welchem Zeithorizont umgesetzt werden sollten“.[6] Unterstrichen wird die Wichtigkeit von einheitlichen Standards, praxistauglichen Schnittstellen und „Security by Design“. Der Schwerpunkt dieser Maßnahmen liegt dabei im Bereich der Elektrizitätsversorgung, da Stromverteilnetzen im Kontext von Cybersicherheit eine große Bedeutung zukommt. Ihre Spezifika und Einflussfaktoren werden im Folgenden näher erläutert.

1.2 Herausforderung Netzbetrieb

Die Netzbetreiber – und hier vor allem die Stromnetzbetreiber – haben im Hinblick auf Cybersicherheit eine besondere Stellung. Sie bieten durch ihre Rolle und ihr Handeln eine ganze Reihe von Angriffsflächen und sind so in mehrerer Hinsicht Risiken ausgesetzt.

Besondere **Risiken** ergeben sich vor allem durch die Zugehörigkeit der Stromnetze zur Kritischen Infrastruktur wie auch aus dem erhöhten Umfang der Datenerfassung und Datenverarbeitung:

- Stromnetzbetreiber sind unabhängig ihrer Größe durch § 11 Abs. 1a EnWG durch die BNetzA zur Einhaltung besonderer Mindestsicherheitsstandards in der IT Sicherheit verpflichtet. Ab einem Schwellenwert von 3.700 GWh/Jahr entnommener Arbeit zählen sie außerdem zur Kritischen Infrastruktur und sind daraus resultierend zu besonderer Berichterstattung gegenüber dem BSI verpflichtet. Ihr Ausfall führt unmittelbar zu massiven Beeinträchtigungen und wirtschaftlichen Schäden bis hin zu Gefahren an Leib und Leben. Je großflächiger und je anhaltender ein Stromausfall ist, desto schwerwiegender sind die Folgen und desto schwieriger wird eine Wiederaufnahme der Versorgung. Diese Anlagen haben einen sehr zentralisierten Charakter, sie werden über dedizierte Leitsysteme und spezielle Kommunikationsprotokolle gesteuert.
- Verteilnetz- sowie Messstellenbetreiber speichern meistens große Mengen an personenbezogenen Daten, da sie aufgrund ihrer Beziehung zu den Anschlussnehmern die relevanten Angaben zu Messpunkten, Lokationen, Verbräuchen, Namen etc. einschließlich Bankverbindungen und Zahlungsdaten verwalten müssen. Durch das Monopol der Verteilnetzbetreiber in ihrem jeweiligen Versorgungsgebiet sind dabei praktisch alle Haushalte und Firmen erfasst. Entsprechend bestehen Risiken für den Datenschutz und die Gefahr, unbeabsichtigt personenbezogene Daten zu „verlieren“.

Die möglichen **Angriffsflächen** nehmen vor allem durch die Systemtransformation stetig zu. Dies gilt insbesondere für die Digitalisierung und Dezentralisierung sowie die damit einhergehende Prozesskomplexität für die beteiligten Akteure:

[4] dena, 2021, Seite 48.
[5] ebd.
[6] ebd., Seite 58.

- Die Digitalisierung und Dezentralisierung des Energiesystems bringen eine Vielzahl neuer Komponenten wie Smart Meter, dezentrale Erzeugungsanlagen, lokale Steuerungsanlagen etc. mit sich, die untereinander vernetzt sind und durch ihre Fähigkeit zu kommunizieren als *intelligent* beschrieben werden. Charakteristisch für diese Anlagen ist, dass sie sich sehr nah an den Endverbraucherinnen und -verbrauchern befinden. In Hinsicht auf Digitalisierung unterscheiden sich Strom- von Gasnetzen, da diese bei Letzteren bei Weitem nicht so fortgeschritten ist.
- Netzbetreiber sowie Energieversorger und Stadtwerke, in die der gebietszuständige Netzbetreiber teilweise organisatorisch eingegliedert ist, sind Unternehmen mit einer Vielzahl von Aufgaben und heterogenen, historisch gewachsenen Strukturen. Sie beschäftigen eine große Zahl von Mitarbeiterinnen und Mitarbeitern, die in unterschiedlichen Funktionen tätig sind, von Technik und Instandhaltung über kaufmännische und buchhalterische Aufgaben bis hin zu Kundenservice, Außendarstellung und Marketing. Wie bei jedem derartigen Unternehmen entstehen dadurch Bedrohungen und Angriffsmöglichkeiten, die erhebliche Auswirkungen auf die Handlungsfähigkeit des Unternehmens haben können. Hier teilen also auch Netzbetreiber ein allgemein vorhandenes Risiko von Cyberangriffen.

Dementsprechend sind die **Motivationen** für Cyberattacken sehr unterschiedlich. Dies gilt auch für die zur Verfügung stehenden **Mittel** sowie die **Ziele**, die von den Angreifern erreicht werden wollen. Die Motivation eines Angriffs kann unter anderem auf folgende Gründe zurückgeführt werden:

- Ausländische Geheimdienste, die politisch motivierte Attacken oder Angriffe im Rahmen von Cyber-Kriegsführung einsetzen. Hier stehen teilweise sehr große Ressourcen und extrem großes Know-how zur Verfügung.
- Terroristische Anschläge mit dem Ziel, durch möglichst großen Schaden die Gesellschaft zu destabilisieren. Ein solches Szenario, wie es zum Beispiel fiktiv im Roman „Blackout“ (Elsberg, 2012) beschrieben ist, wird von der Bundesnetzagentur sehr ernst genommen (ZEIT, 2012).
- Wirtschaftlich motivierte Cyberkriminalität mit dem Ziel, Geld zu erpressen. Aktuelle Beispiele sind der Angriff auf die Stadtwerke Pirna am 3. Dezember 2021 (mdr, 2021) oder der auf den Dienstleister und Softwareanbieter KISTERS AG am 10. November 2021.
- Innere Angriffe, zum Beispiel durch Racheakte verärgerter Mitarbeiterinnen oder Mitarbeiter.

Die Entschiedenheit, mit der ein Angriff durchgeführt wird, nimmt in dieser Aufzählung von oben nach unten ab, die Wahrscheinlichkeit eines solchen Vorfalls dagegen nicht. Die tatsächliche Exposition diesen Angriffsarten gegenüber ist daher schwer zu bestimmen; ihre Einschätzung ist ein Ziel dieser Untersuchung.

Weitere Faktoren, die eine Wirkung auf die skizzierte Ausgangssituation im Stromnetzbereich haben, sind die aktuellen Entwicklungen zum Beispiel bei Marktprozessen und die damit einhergehende schrittweise notwendige Verknüpfung von Betriebsmittelsteuerung und IT-Prozessen, aber auch die eindeutige Ausgestaltung von Meldepflichten.

1.3 Herausforderung der Marktprozesse

Bei der Infrastruktur von Netzbetreibern spielt die Unterscheidung zwischen Prozessdatennetzen und Bürodatennetzen eine wesentliche Rolle. In diesem Zusammenhang wird auch von Kommunikationsnetzen der **Operativen Technik (OT)** bzw. der **Informationstechnik (IT)** gesprochen. Die OT erlaubt eine direkte

Steuerung und demzufolge auch Störung bzw. Beschädigung der Versorgungsinfrastruktur, die unter allen Umständen vermieden werden muss. Das IT-Netz dagegen ist für Verwaltungs- und Abrechnungsprozesse zuständig und wird dadurch als weniger kritisch betrachtet. Gleichzeitig gibt es wesentlich mehr Personen, die Zugriff auf das Netz haben, und ihre notwendigen Kontakte zur Außenwelt sind deutlich umfangreicher. Die Angriffe gegen das Prozessdatennetz (OT-Netz) richten sich sehr spezifisch gegen Netzbetreiber, während Angriffe auf das Bürodatennetz (IT-Netz) ganz allgemeine Bedrohungen für ein breites Spektrum von Unternehmen darstellen. Aus diesen Gründen werden im IT-Netz geringere Sicherheitsstandards angewandt. Sicherheitsanforderungen für beide Systeme werden im IT-Sicherheitskatalog der BNetzA definiert (BNetzA, 2015).

In der Regel sind beide Netze logisch voneinander getrennt, sodass das Prozessnetz keine direkte Verbindung zum Internet hat (DIN e.V., 2017). Diese Trennung von OT- und IT-Netzen ist ein **wesentliches Sicherheitsmerkmal**. In der Regel besteht allerdings keine harte Trennung der Systeme bis auf die physische Ebene hinunter – also Kabel und Router. Das ist aus Praktikabilitätsgründen kaum möglich. Daher kann ein Überspringen einer Attacke von einem ins andere Netz oder der gleichzeitige Angriff auf beide nicht grundsätzlich ausgeschlossen werden.

Vor dem Hintergrund der mit der Energiewende verbundenen Prozessanpassungen wird diese klare Trennung aufgrund der fortschreitenden Verzahnung von Steuerungs-, Bilanzierungs- und Abrechnungsprozessen und der damit einhergehenden Verbindung zwischen technischen und kaufmännischen Systemen angepasst werden müssen. Eine solche notwendige Verbindung wird besonders am Beispiel der Regeln zum Redispatch 2.0 deutlich (BNetzA 059, 2020; BNetzA 060, 2021; BNetzA 061, 2021). Teil des Redispatch 2.0 ist eine Ausrichtung der Redispatch-Maßnahmen, also der steuernden Eingriffe ins Stromnetz als Teil des netzdienlichen Engpassmanagements, an gesamtwirtschaftlichen Erfordernissen. Wie bisher müssen präventive Eingriffe so wirtschaftlich wie möglich erfolgen, während kurative Eingriffe im Idealfall unnötig sein sollen. Die Umsetzung umfasst beim Redispatch 2.0 alle betroffenen Netzbetreiber und verlangt eine umfangreiche Kommunikation zwischen den Marktteilnehmern, insbesondere zwischen den Netzbetreibern sowie zwischen Netz- und Anlagenbetreibern. Genauso erforderlich ist eine Verknüpfung verschiedener Systeme, die traditionell unterschiedlichen Netzen zugeordnet sind: Das Redispatch-2.0-System muss sowohl Schnittstellen zum Leitsystem im OT-Netz als auch Bilanzierung, Abrechnung und Marktkommunikation im IT-Netz anbieten oder bedienen. Im Hinblick auf Cybersicherheit ist dies eine Situation, die besondere Herausforderungen an eine sichere Implementierung stellt: „Mit zunehmender Konnektivität steigt jedoch auch die Gefahr des Missbrauchs und der Manipulation. Cyberangriffe können direkte Auswirkungen auf die Steuerung der Anlagen haben.“ (BBH, 2020).

1.4 Meldepflichten

Für die Koordinierung von Cybersicherheitsmaßnahmen ist in Deutschland das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig. Die Frage, welche Vorfälle zwingend an das BSI gemeldet werden müssen, ist nicht immer ganz klar zu beantworten. Es gibt zwei gesetzliche Vorschriften, welche die Pflicht zum Melden von IT-Sicherheitsvorfällen für Netzbetreiber und allgemein für Energieversorger regeln, zum einen das Energiewirtschaftsgesetz (EnWG, 2005) und zum anderen das BSI-Gesetz (BSIG, 2009). Beide

Gesetze wurden mehrfach angepasst, in großem Umfang zuletzt 2021 durch das IT-Sicherheitsgesetz 2.0[7] und kleineren Novellierungen in 2022.

Das BSI-Gesetz macht verpflichtende Vorgaben für die Betreiber von Kritischen Infrastrukturen. Gemeldet werden müssen „Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben“ oder „*erhebliche* Störungen [usw.], die zu einem Ausfall [usw.] führen *können*“.[8] Welche Unternehmen in die Kategorie „Betreiber Kritischer Infrastruktur“ fallen, ist in der BSI-Kritisverordnung (BSI-KritisV, 2016) festgelegt.

Das Energiewirtschaftsgesetz (EnWG) hat seit der NIS-Verordnung (NIS, 2017) eigene Vorschriften für Meldungen an das BSI. Für Netzbetreiber ist darin die Einschränkung auf die Betreiber Kritischer Infrastruktur nach BSI-Kritisverordnung aufgehoben, es wird ausdrücklich von Störungen des Energieversorgungsnetzes gesprochen. Auf der anderen Seite sind Vorfälle, die nicht das Energieversorgungsnetz betreffen, darin nicht geregelt. Beeinträchtigungen von Bilanzierungs-, Marktkommunikations-, Prognose- oder sonstigen Systemen sind demnach nicht unbedingt meldepflichtig.

Eine Veröffentlichung der xmera e. K. bemängelt darüber hinaus die Formulierung „*erhebliche* Einschränkungen“ bzw. „*erhebliche* Störungen“, da dies kein hinreichend scharf definiertes Kriterium sei (xmera, 2017). Sie kommt zu dem Schluss, dass „rund 90 % der Strom- und Gasnetzbetreiber einen IT-Sicherheitsvorfall lediglich dann melden [müssen], wenn es deswegen zu einem Totalausfall in ihrem Versorgungsgebiet kommt oder kommen könnte“. Auf der einen Seite lässt sich vermuten, dass für viele kleinere und mittlere Netzbetreiber nicht immer zweifelsfrei zu bestimmen ist, ob eine harte Verpflichtung zu einer Meldung besteht. Auf der anderen Seite kann mit einigem Optimismus davon ausgegangen werden, dass ein Netzbetreiber sich im Zweifelsfall *für* die Erstattung einer Meldung entscheiden wird. Dem entgegen steht die Problematik, dass viele Betreiber aus falscher Scham Informationen zu Vorfällen nur zurückhaltend melden.

[7] Die aktuellen Fassungen stehen unter folgenden Links zur Verfügung: https://www.gesetze-im-internet.de/enwg_2005/EnWG.pdf sowie https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf.
[8] BSIG § 8b Absatz 4.

2 Online-Umfrage

2.1 Umfang und Durchführung

Vom 13. Dezember 2021 bis zum 28. Februar 2022 waren Netzbetreiber aufgefordert, an einer Befragung zum Thema Cybersicherheit teilzunehmen.

Die Online-Befragung wurde mittels eines Standard-Webtools (Microsoft Forms) umgesetzt, wobei der Fragebogen von den Teilnehmern per Browser am Rechner oder per Smartphone ausgefüllt werden konnte. Es waren insgesamt 33 Fragen enthalten, die in fünf Abschnitte eingeteilt waren. Zusätzlich wurde abschließend das Interesse an weiteren Aktionen (Auswertung der Umfrage, Telefoninterview, Cybersicherheitsübungen) erfragt.

Im Fragebogen wurden keine personenbezogenen Daten erfasst, sodass eine direkte Identifikation der Teilnehmer nicht möglich ist. Die freiwillige Angabe einer Mailadresse war vorgesehen, um den Abschlussbericht direkt zu erhalten, wobei alternativ auch eine kurze Mitteilung per Mail möglich war und ebenfalls akzeptiert wurde. Diese Mailadressen wurden zu keinem anderen Zweck verwendet und auch nicht an den Auftraggeber weitergeleitet.

Zielgruppe waren in erster Linie die Verteilnetzbetreiber (VNB) sowie die Übertragungsnetzbetreiber (ÜNB) in Deutschland. Zusätzlich wurden Arealnetzbetreiber, Stromnetzbetreiber im deutschsprachigen Ausland (Luxemburg und Schweiz) und vereinzelt Gasnetzbetreiber angeschrieben. Insgesamt haben 43 Unternehmen den Fragebogen bearbeitet und Antworten abgegeben.

2.2 Ziele und Inhalte

Das wesentliche Ziel der dena war es, Schwerpunkte und Inhalte für die geplante Cybersicherheitsübung zu ermitteln. Zu diesem Zweck wurde das Mittel der Umfrage gewählt, um den Netzbetreibern ein niederschwelliges Angebot zu machen und auf einfache Weise Informationen zu erhalten.

Weitere Ziele waren:

- Ermittlung von Ansprechpartnerinnen und -partnern für Cybersicherheit in den jeweiligen Unternehmen und Knüpfen von Kontakten
- Ermittlung und Bewertung des aktuellen Stands der Cybersicherheit im deutschen Stromnetzbetrieb
- Sensibilisierung der Netzbetreiber für das Thema der Cybersicherheit, soweit erforderlich

Der Fragebogen wurde von der umlaut SE in Abstimmung mit der dena erstellt und ist in folgende Abschnitte eingeteilt:

1. Fragen zum Unternehmen
2. Bedrohungslage
3. Gegenmaßnahmen zur Prävention
4. Cybersicherheits-Management und Standards
5. Response-Strukturen

Die Abschnitte beginnen in der Regel mit einer Frage zur subjektiven Einschätzung, worauf anschließend im Detail nach konkreten Aspekten gefragt wird.

Fragen zum Unternehmen

Die Abfrage von Unternehmenskenndaten war erforderlich, um die Zielgruppe zu strukturieren und vor statistischen „Verunreinigungen“ zu schützen. Insbesondere sollten in der engeren Auswertung ausschließlich Netzbetreiber berücksichtigt werden.

Im Vorfeld der Untersuchung wurde vermutet, dass größere Unternehmen tendenziell besser auf Cyberangriffe vorbereitet sind, da dort die entsprechenden Strukturen geschaffen wurden – teils aufgrund von bestehenden gesetzlichen Anforderungen, teils wegen besserer personeller Ausstattung. Um diese Vermutung zu überprüfen, wurde nach der Größe des Unternehmens gefragt.

Es wurde angenommen, dass die Komplexität der IT eines Energieversorgers mit der Anzahl der versorgten Menschen skaliert. Als Kennziffer für die Größe wurde deshalb die Anzahl von Anschlusspunkten herangezogen, wobei es nur um die ungefähre Einteilung in Stufen (20K, 100K, 500K, 2M) ging. In dieser groben Zuordnung spielt es letztlich keine Rolle, ob konkret Kunden, Zählpunkte, Mess- oder Marktlokationen gezählt werden. Weitere Strukturdaten wie Netzlänge, Aufteilung nach Spannungsebenen oder transportierte Energie wurden bewusst nicht erfragt.

Als ein wichtiger neuralgischer Punkt für Datenschutz und Cybersicherheit werden intelligente Messsysteme (iMSys, vulgo „Smart Meter“) gesehen. Nicht zuletzt gelten in Deutschland seitens des BSI strenge Anforderungen für die Zertifizierung und den Betrieb von Smart Metern und Smart Meter Gateways. Bei den Verteilnetzbetreibern ist der sogenannte Smart Meter Rollout jedoch noch lange nicht abgeschlossen. Aus diesem Grund wurde nach der Anzahl der aktuell im Netz eingebauten Smart Meter gefragt.

Ebenfalls interessant war die Anzahl von steuerbaren Ressourcen im Netz, etwa durch Controllable Local Systems (CLS), durch Rundsteuerung oder indirekt durch den Betreiber im Rahmen von Redispatch-Maßnahmen. Auf eine Erhebung dieser Zahlen wurde jedoch verzichtet, um den Aufwand für die Beschaffung der Daten seitens der teilnehmenden Unternehmen nicht zu hoch zu treiben. Der eventuelle zusätzliche Informationsgewinn wäre hier mit einer gewissen abschreckenden Wirkung erkauft worden.

Zudem wurde erfragt, ob das Unternehmen unter die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSIG, 2009) fällt. Als Kriterium für die Einordnung als KRITIS gilt, dass mehr als 500.000 Menschen durch das Unternehmen versorgt werden. Dies entspricht einer transportierten Jahresenergiemenge von 3,7 Terawattstunden bzw. einer maximalen Netzlast von 420 Megawatt, wobei gewisse Annahmen über Jahresverbräuche pro Person sowie Benutzungsstunden gemacht werden.

Die letzte Frage bezog sich auf die Rolle bzw. Position der den Fragebogen ausfüllenden Person. Daraus sollte abgeleitet werden, mit welcher fachlichen Kompetenz und/oder Entscheidungsbefugnis diese Person ausgestattet ist. Außerdem sollte dadurch auch hier die Möglichkeit vorbehalten werden, nachträglich offensichtliche Irrläufer bei der Beantwortung auszusortieren.

Bedrohungslage

Die reale Bedrohung durch Cyberangriffe ist schwierig zu bestimmen, da geeignete Messgrößen fehlen oder nicht zugänglich sind. Zudem besteht das Paradoxon, dass die schlimmsten Angriffe diejenigen sind, die

zunächst nicht bemerkt werden, denn bei diesen können über einen längeren Zeitraum Daten abfließen oder es kann Schadcode eingeschleust werden, um ihn zu einem späteren Zeitpunkt zu aktivieren. Folglich kann die Bedrohungslage nur ungefähr einerseits durch in der Vergangenheit erfolgte Angriffe, andererseits durch subjektive Einschätzung bemessen werden.

Die subjektive Einschätzung wurde zunächst summarisch auf einer fünfstufigen Skala abgefragt, die von „sehr niedrig“ (völliger Schutz vor Angriffen) bis „sehr hoch“ (erfolgreiche Angriffe sind bereits erfolgt) reicht. Eine weitere Differenzierung wurde hier noch nicht vorgenommen.

Zur Einschätzung der realen Gefährdung wurde um die Angabe der Anzahl der bekannt gewordenen Störfälle (Incidents) sowie der an das BSI gemeldeten Incidents gebeten. Da eine Meldung ans BSI entsprechend dokumentiert wird und also klar sein sollte, ob und wann eine solche Meldung erfolgt ist, wurde folglich in dieser Frage nicht nach ungefähren Größenordnungen, sondern nach der genauen Anzahl gefragt.

Ein „Incident“ wurde in der Fragestellung definiert als „ungeplante Unterbrechung oder Qualitätsminderung eines IT-Service bzw. ein Ereignis, das in der Zukunft einen IT-Service beeinträchtigen könnte“. Dies enthält also nicht nur aktive Angriffe von außen, sondern auch absichtlich oder versehentlich ausgelöste Vorfälle innerhalb des Unternehmens.

Zur besseren Einschätzung und Klassifizierung der Incidents sollte angegeben werden, ob und welche der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit dabei verletzt wurden. Bei einer Beeinträchtigung der Verfügbarkeit wurde zusätzlich nach der Wiederherstellungsdauer der verfügbaren Systeme gefragt, um eine quantitative Einordnung der Auswirkungen vorzunehmen.

Um einen detaillierteren Einblick zu bekommen, wurden zehn typische IT-Systeme bei Netzbetreibern genannt. Gefragt war jeweils nach einer Einschätzung der Gefährdung des Systems auf einer fünfstufigen Skala. Dabei wurde „Gefährdung“ so definiert, dass für das betreffende System entweder ein hinreichender Schutz nicht möglich ist oder dass eine potenzielle Störung massive schädliche Auswirkungen hätte. Beide Faktoren machen einen erfolgreichen Angriff wahrscheinlicher und tragen zu Cyberrisiken bei.

Bei den genannten IT-Systemen reichte die Spanne von den sehr netztechnisch orientierten Komponenten, etwa dem Leitsystem, bis hin zu kaufmännischen Systemen oder Arbeitsplatzrechnern, die in jedem Unternehmen existieren und nicht spezifisch für Netzbetreiber sind. Zusätzlich, so die Erwartung, würden Systeme genannt werden, an die bei der Erstellung der Umfrage nicht gedacht worden war.

Als wichtige Eigenschaft der Systeme wird das Hosting angesehen, also der physische Ort, an dem die jeweilige Hardware vorgehalten wird, und dementsprechend auch das logische Netzwerk, dem sie zugeordnet ist. Die Software ist entweder vor Ort („on premise“) installiert, sie kann bei einem Dienstleister in dessen Rechenzentrum laufen und dort betreut werden oder sie ist komplett in „die Cloud“, also auf die Ressourcen eines externen Drittanbieters, ausgelagert. Dies hat Einfluss zum einen auf die möglichen Angriffsszenarien, aber auch auf die Verantwortlichkeiten für Gegenmaßnahmen und Response-Strukturen.

Bei vielen Unternehmen liegt eine hybride Struktur vor, in der unterschiedliche Systeme an verschiedenen Orten gehostet werden, daher waren hier Mehrfachnennungen möglich. Auf eine Einzelaufschlüsselung je nach System wurde dagegen verzichtet, um die Antwortmöglichkeiten nicht unnötig komplex zu gestalten. Stattdessen wurde nach Plänen für die Zukunft gefragt, also ob etwa im Rahmen einer „Cloud-Strategie“ eine Verlagerung von Diensten auf externe Server vorgesehen ist.

Die letzten beiden Fragen im Abschnitt zur Gefährdungslage bezogen sich auf die Absicherung von Kommunikationskanälen, wobei nach externer und interner Kommunikation unterschieden wurde. Im Wesentlichen

lassen sich der Inhalt und der Transport verschlüsseln, wobei für beide Arten bestimmte Standardprotokolle vorgesehen sind. Auch hier waren Mehrfachnennungen möglich, da typischerweise verschiedenste Kommunikationskanäle verwendet werden und eine detailliertere Erfassung den Rahmen des Fragebogens gesprengt hätte.

Gegenmaßnahmen zur Prävention

Unter Gegenmaßnahmen werden hier vorbeugende Maßnahmen, die Angriffe verhindern oder wirkungslos machen sollen, verstanden. Dadurch grenzen sie sich ab von den Maßnahmen im Rahmen von Response-Strukturen, die auf Bekämpfung und Schadensbegrenzung im Nachhinein abzielen.

Der Abschnitt beginnt mit der Frage nach der subjektiven Bewertung der Wirksamkeit von bereits ergriffenen Gegenmaßnahmen. Im Anschluss wurden bestimmte konkrete Arten von Maßnahmen genauer beleuchtet. Dazu gehören Awareness-Maßnahmen für Mitarbeiterinnen und Mitarbeiter, Penetrationstests und Auditberichte.

Zusätzlich wurde nach einem Schwachstellen-Monitoring gefragt, also der Prüfung auf Existenz von bekannten Fehlern oder Angriffsmöglichkeiten in der eingesetzten Software. Während der Laufzeit der Interviews wurde die sogenannte log4j-Lücke gefunden, die weit über Fachkreise hinaus bis in die Abendnachrichten hinein zum Thema wurde (heise, 2021). Es konnte also erwartet werden, dass Sinn und Wichtigkeit eines Schwachstellen-Monitorings allgemein bekannt sind.

Cybersicherheits-Management und Standards

Unter Standards wurden nationale und internationale Vorgaben verstanden, die für die angesprochenen Unternehmen relevant sind.

Gefragt wurde konkret nach der Umsetzung von ISO 27001, das heißt nach der Einführung eines zertifizierten Informationssicherheitsmanagements (Information Security Management System, ISMS) im Unternehmen.

Für Unternehmen der Energiewirtschaft von Bedeutung ist ebenfalls das Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ des Bundesverbands der Energie- und Wasserwirtschaft (BDEW), das gemeinsam mit dem österreichischen Energieverband herausgegeben wurde (BDEW, 2018). Dieses Dokument enthält eine Vielzahl von Einzelanforderungen. Gefragt wurde nach dem Umsetzungsgrad (alle relevanten / teilweise / gar nicht) im Unternehmen.

Zuletzt wurde noch nach weiteren Vorgaben bzw. Rahmenwerken gefragt, die im Fragebogen nicht aufgeführt waren, aber im Unternehmen implementiert sind.

Response-Strukturen

Als „Response“ werden die Maßnahmen bezeichnet, die nach einem erfolgreichen Angriff ergriffen werden, um den Schaden zu begrenzen und die Operationsfähigkeit wiederherzustellen. Zur Verdeutlichung wurde im Fragebogen ein Beispielszenario angeführt, in dem durch eine Cyberattacke das SCADA-System kompromittiert wurde und dadurch komplett gelöscht und neu aufgebaut werden musste.

Im Anschluss an die Eingangsfrage nach der subjektiven Einschätzung der eigenen Response-Struktur, bei der wieder pauschal fünf Stufen („sehr gering“ bis „sehr hoch“) vorgesehen waren, folgten Fragen nach konkreten Maßnahmen. Genannt waren die Einrichtung eines Krisenstabs für Cyberangriffe sowie der Betrieb eines Security Operation Center (SOC) als permanente organisatorische Einrichtung (rund um die Uhr an allen Tagen des Jahres).

Weiter wurde nach einem Intrusion Detection System (IDS) gefragt, also einer Sammlung von Tools und Programmen, die Angriffe erkennen, alarmieren und dokumentieren sollen. In Anbetracht der verschiedenen Bereiche in der Unternehmens-IT mit ihren unterschiedlichen Bedrohungen und Sicherheitsanforderungen wurde hier separat nach Prozessdatennetzen (also Leitsystem und andere technische Systeme) und Intranet (Bürokommunikation und kaufmännische Systeme) unterschieden.

Ähnlich wie bei der Vorbeugung auf Cyberangriffe die Awareness-Übungen eine Rolle spielen, ist auch für die Bewältigung von Angriffen ein Training der Mitarbeiterinnen und Mitarbeiter sinnvoll. Es wurde daher nach der Durchführung und Frequenz solcher Übungen sowie nach deren Inhalten gefragt.

Die letzte Frage bezog sich auf regelmäßige Sicherheitskopien (Backups). Nach einem erfolgreichen Angriff mit schädlichen und gegebenenfalls unbekannten Auswirkungen sind diese essenziell, um Handlungsfähigkeit wiederherzustellen. Dabei ist wichtig, dass einerseits bekannt ist, welche Daten genau dem Backup unterliegen, und dass andererseits die Brauchbarkeit der Sicherheitskopien regelmäßig überprüft wird.

2.3 Auswertung und Ergebnisse

Fragen zum Unternehmen

Bei der Auswertung der Fragen zu Unternehmensgröße und -struktur zeigt sich, wie in Abbildung 1 zu erkennen, dass die teilnehmenden Unternehmen einen einigermaßen repräsentativen Querschnitt durch die deutsche Stromversorgungslandschaft darstellen. Das gilt sowohl für die Art des Netzbetreibers als auch für die Anzahl der Zählpunkte: von kleinen Stadt- und Gemeindewerken mit unter 20.000 Zählpunkten bis hin zu überregionalen Netzbetreibern mit mehr als 1 Million Zählpunkten und auch Übertragungsnetzbetreibern sind alle Größenordnungen in einem plausiblen Zahlenverhältnis vertreten. Aus der Kategorie Arealnetze nahmen keine Vertreter an der Umfrage teil, hierbei handelt es sich beispielsweise um geschlossene Stromnetzareale von Flughäfen oder Industrieparks. Vermutlich sehen deren Betreiber ihr Kerngeschäft nicht in der Energieverteilung, sodass sie sich nicht angesprochen gefühlt haben. Die Angabe „ÜNB und VNB“ wurde in dem Freitextfeld von einem Teilnehmer ergänzt.

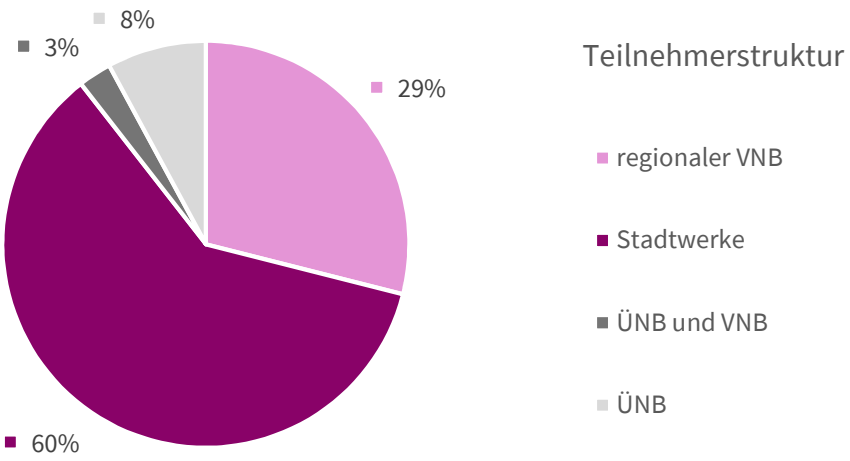


Abbildung 1: Struktur der teilnehmenden Netzbetreiber

Abbildung 2 zeigt, dass Querverbundunternehmen in der Umfrage am häufigsten vertreten sind. Die meisten Unternehmen, nämlich 87 Prozent der Teilnehmer, betreiben neben einem Stromnetz auch ein Gasnetz. Die Mehrheit transportiert auch Wasser (68 Prozent) und Fern- oder Nahwärme (63 Prozent). Etwa ein Drittel der Netzbetreiber fällt in die Kategorie KRITIS (vgl. Abbildung 3).

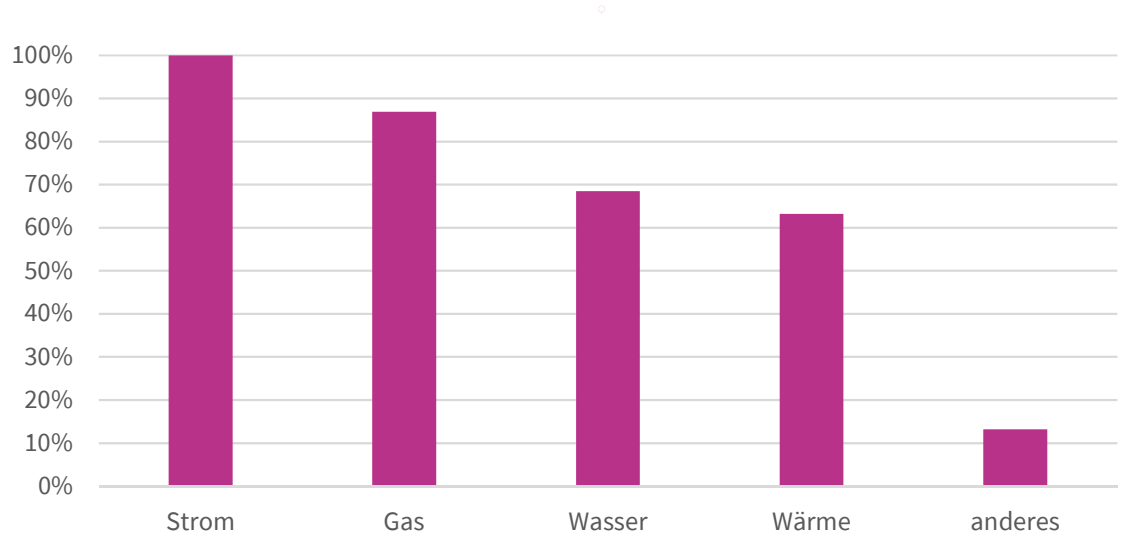


Abbildung 2: Aufschlüsselung nach Energiearten

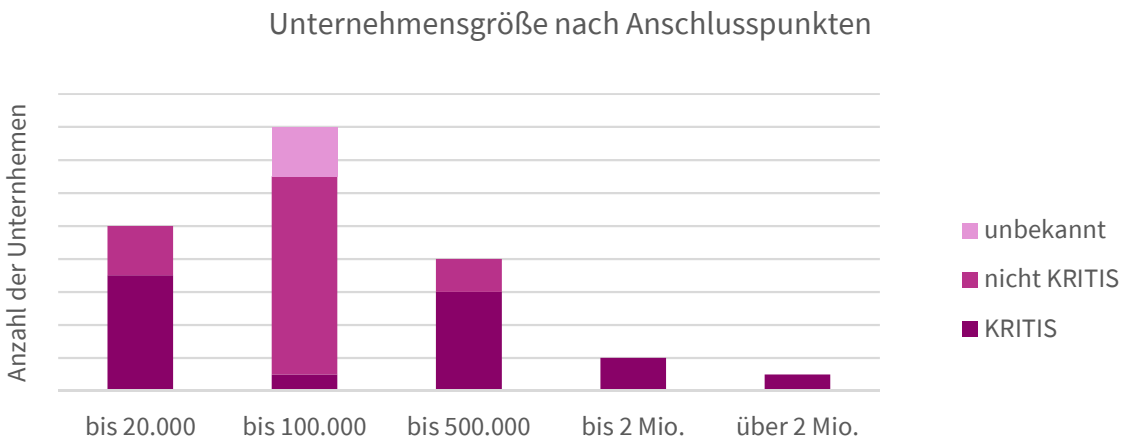


Abbildung 3: Größe nach Zahl der Anschlusspunkte

Interessant ist die große Bandbreite bei den Angaben zum Einsatz von Smart Metern, die in Abbildung 4 dargestellt sind. Hier wird eine große Zahlenrange genannt, ohne dass eine Häufung erkennbar wäre. Ein nennenswerter Anteil der Befragten hat keine oder nur relativ wenige intelligente Messsysteme (bis zu 50) im Einsatz, aber ein ebenfalls relevanter Anteil nennt deutlich höhere Zahlen im vier- bis sechsstelligen Bereich. Insgesamt lässt sich feststellen, dass der Smart Meter Rollout, soweit er überhaupt schon praktisch ausgeführt wird, bisher in der Betrachtung von Cybersicherheitsthemen bei den befragten Unternehmen keine Rolle spielt – eine Einschätzung, die in den Interviews bestätigt wurde.

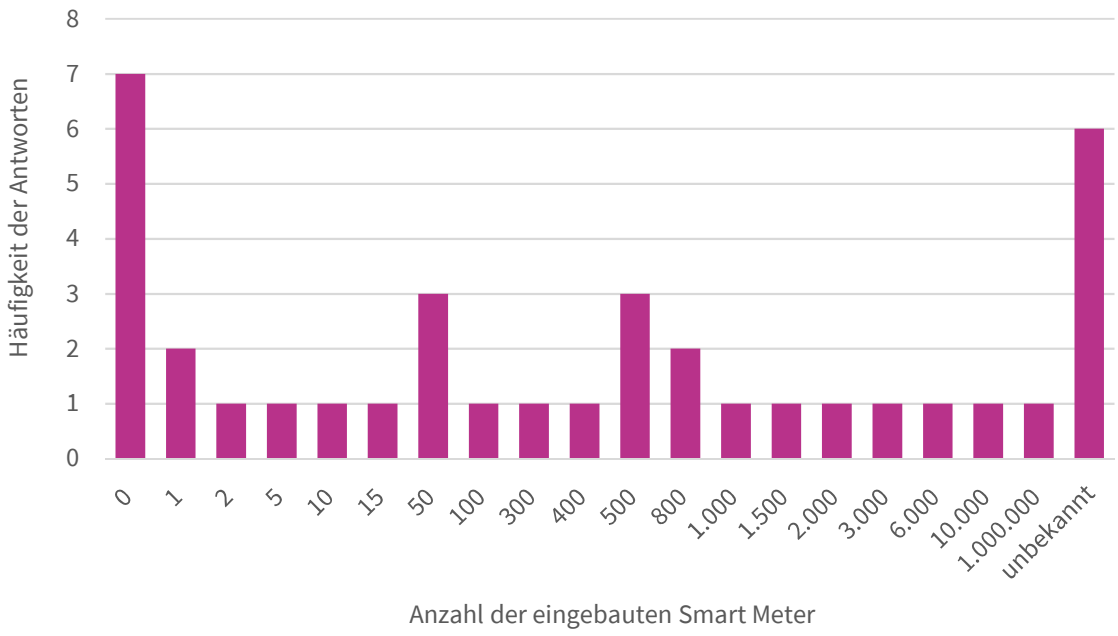


Abbildung 4: Anzahl der eingebauten Smart Meter

Bezogen auf die Zuständigkeit der antwortenden Personen im Unternehmen gaben 47 Prozent der Teilnehmenden an, als Datenschutz- oder IT-Sicherheitsbeauftragte bzw. -beauftragter oder als Chief Information Security Officer (CISO) tätig zu sein. Von den verbleibenden 53 Prozent ist der größere Teil in einer Management-Funktion, das heißt entweder in der Geschäftsführung oder in einer Abteilungsleitung. Insgesamt gaben 50 Prozent an, eine Leitungsposition innezuhaben, wobei zu beachten ist, dass aufgrund der möglichen Mehrfachnennungen die Werte in Abbildung 5 nicht addiert werden können. Die übrigen Teilnehmenden ordnen sich den Bereichen „Systemadministration“ oder „Fachexpertin/-experte“ zu.

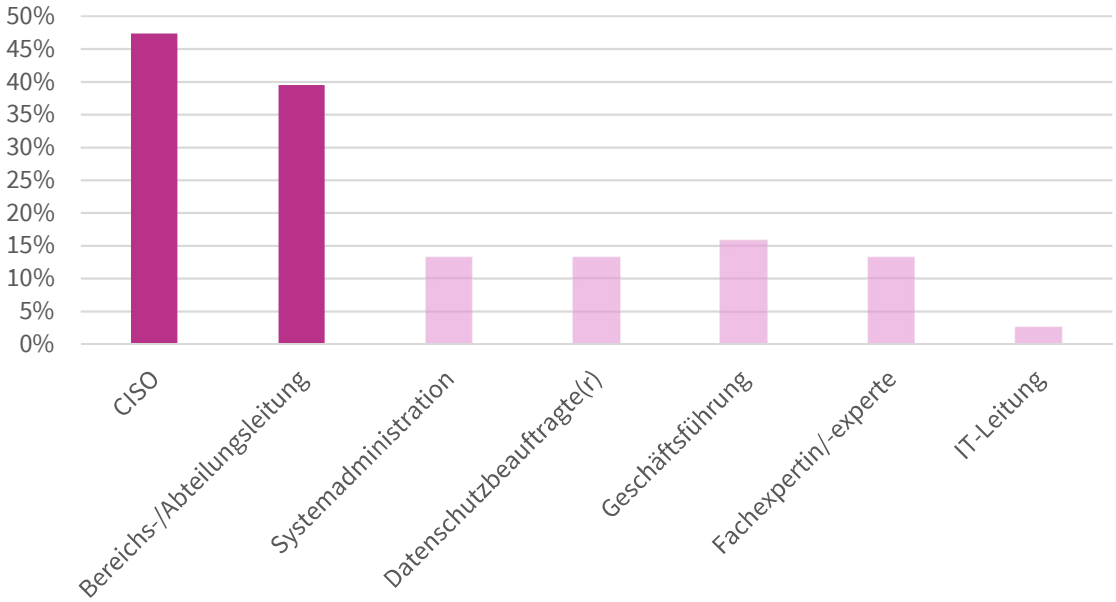


Abbildung 5: Funktion der antwortenden Personen im Unternehmen (Mehrfachnennungen möglich)

Bedrohungslage

Die Bedrohungslage wird von vielen Unternehmen als niedrig angesehen. Dieses Ergebnis wird in Abbildung 6 dargestellt. Insgesamt 58 Prozent geben an, dass erfolgreiche Angriffe „unwahrscheinlich“ oder „nicht sehr wahrscheinlich“ erscheinen. Es lässt sich aus den Antworten nicht unmittelbar ableiten, ob diese Unternehmen nicht mit ernsthaften Angriffen rechnen oder ob sie sich gut vorbereitet sehen. Auch die Antwort „Wir sind uns sicher, vor Cyber-Angriffen geschützt zu sein“, wurde gegeben – und zwar, wie aus dem Kontext der anderen Antworten hervorgeht, nicht unüberlegt, denn das entsprechende Unternehmen hatte durchaus schon mit Angriffen und Vorfällen zu tun gehabt.

Es verbleiben also 42 Prozent, die ein Angriffsrisiko als hoch ansehen. Innerhalb dieser Gruppe sind auch Unternehmen, die schon Angriffe mit massiven Auswirkungen oder Schäden erfahren mussten.

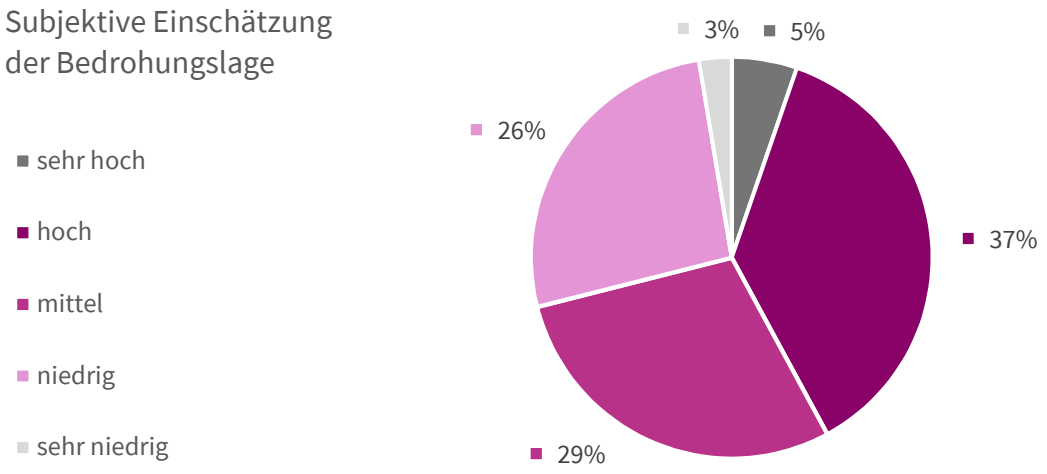


Abbildung 6: Subjektive Einschätzung der Bedrohungslage

Abbildung 7 zeigt die Anzahl der Meldungen an das BSI, diese ist insgesamt sehr niedrig. Zwei Drittel aller Unternehmen haben noch keinen Incident an das BSI gemeldet, weitere 16 Prozent haben einen Incident an das BSI melden müssen. Eine Unterscheidung ergibt sich zudem durch der Aufschlüsselung nach Netzbetreibergröße: Kleinere Stadtwerke (bis 20.000 Zählpunkte) haben bisher keine meldepflichtigen Vorfälle verzeichnen müssen, bei den Netzbetreibern mittlerer Größe (bis 100.000 Zählerpunkte) gab es bei einigen Unternehmen jeweils eine Meldung. Mehr als eine Meldung wurde lediglich bei Netzbetreibern ab 100.000 Zählerpunkten angegeben. Mehr als zehn Meldungen wurden bei keinem Netzbetreiber getätigt.

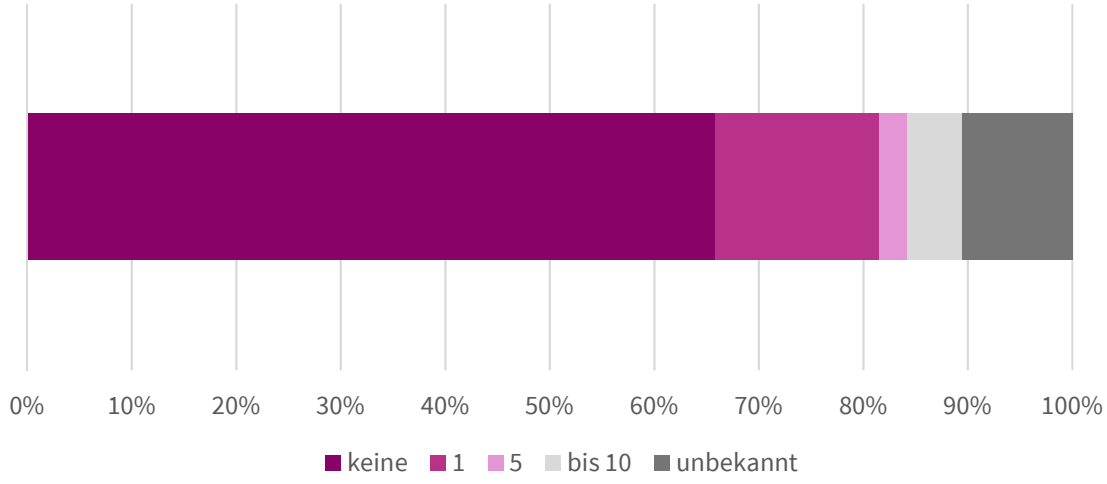


Abbildung 7: Anzahl der an das BSI gemeldeten Incidents

Bei den intern gemeldeten Incidents sieht es dagegen anders aus (Abbildung 8). Weniger als ein Drittel hat noch nie einen Vorfall gemeldet, dagegen haben 50 Prozent bereits mehr als einen, 18 Prozent sogar schon mehr als 10 Vorfälle gemeldet. Die Größe des Unternehmens spielt dabei zwar auch eine Rolle, allerdings ist der Effekt wesentlich weniger ausgeprägt als bei den BSI-Meldungen: Beschränkt man die Auswertung auf die kleinen und mittleren Stadtwerke (bis 100.000 Zählpunkte), so haben 42 Prozent noch nie einen Vorfall gemeldet, aber dieselbe Anzahl (also ebenfalls 42 Prozent) schon mehr als einen und fast 13 Prozent in dieser

Gruppe haben mehr als 10 Incidents gemeldet. Es wird demnach nicht jeder Vorfall, der intern bekannt wird, an das BSI weitergegeben. Dies kann durchaus seine Richtigkeit haben, wenn der Vorfall aufgrund fehlender wesentlicher Auswirkungen auf die Energieversorgung nicht meldepflichtig ist. Ein weiterer möglicher Grund könnte fehlendes Know-how für den komplexen Meldevorgang an das BSI darstellen.

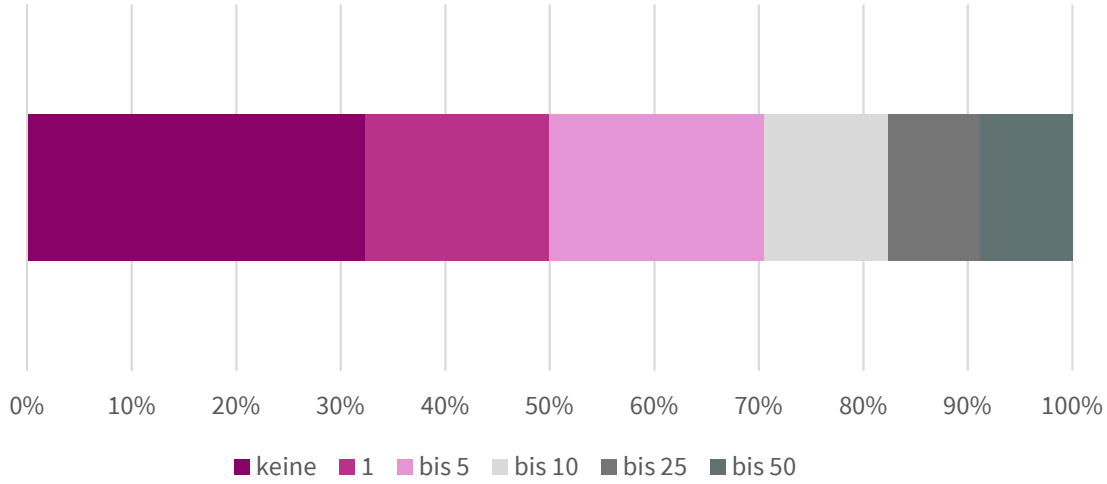


Abbildung 8: Ungefähre Anzahl der in den letzten beiden Jahren intern gemeldeten Incidents

Aus den Antworten zu der Art der verletzten CIA-Schutzziele (Confidentiality, Integrity and Availability – Vertraulichkeit, Integrität und Verfügbarkeit), die in Abbildung 9 aufgeführt sind, konnten keine brauchbaren Aussagen abgeleitet werden. Vermutlich war diese Frage zu wenig spezifisch gestellt; zudem haben die meisten teilnehmenden Unternehmen bisher keine konkrete Erfahrung mit Angriffen. Fast alle teilnehmenden Unternehmen haben „unbekannt“ oder gar keine Antwort angegeben. Auch auf die Frage nach der Wiederherstellungszeit konnten die meisten keine Antwort geben. Die Angaben, die gemacht wurden, liegen in der Größenordnung von einem Tag.

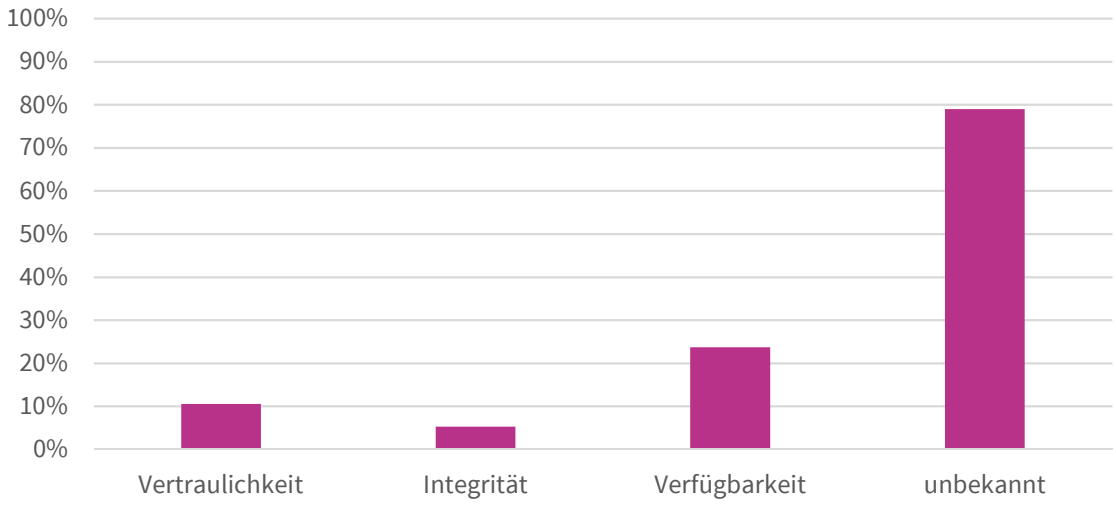


Abbildung 9: Verletzung konkreter CIA-Schutzziele bei bisherigen Angriffen

Bei der Frage nach den verschiedenen Systemen und ihrem jeweiligen Gefährdungsgrad gibt es zwei Systeme, die als besonders kritisch eingeschätzt werden. Dies sind zum einen die Mitarbeiterarbeitsplätze, gefolgt vom Website und Kundenportal (vgl. Abbildung 10). Mit einigem Abstand folgen unterschiedliche Systeme wie Marktkommunikationssoftware, interne Buchhaltung sowie Leitsysteme. Der Mittelwert bei der Bewertung ist jeweils ähnlich, die Streuung der Antworten allerdings nicht: Bei der Marktkommunikation konzentrieren sich die Antworten auf „hoch“ und „mittel“, während die extremen Einschätzungen praktisch nicht vorkommen. Anders bei den Leitsystemen: Hier sind alle fünf Antwortmöglichkeiten von „sehr hoch“ bis „sehr niedrig“ gleichmäßig vertreten, es herrscht also eine Uneinigkeit über die Exponiertheit der SCADA-Systeme (Supervisory Control and Data Acquisition).

Als weniger gefährdet gelten die Smart-Meter-Infrastruktur, das Energiedatenmanagement (EDM) und die Abrechnungssysteme. Hier wiederholt sich eine ähnliche Beobachtung: Bei der Smart-Meter-Technik gehen die Meinungen tendenziell auseinander, beim EDM geben die meisten „mittel“ als Gefährdung an. Das Schlusslicht bilden Rundsteuerungsanlagen und Asset Management; hier werden die geringsten Gefahren gesehen. Über die vorgegebenen Antworten hinaus wurden zusätzlich noch „Telefonanlagen etc.“ als gefährdete Systeme angegeben sowie in einem Fall die 450-Megahertz-Technik. Außerdem wird die Anbindung von Homeoffice-Arbeitsplätzen als Risiko angesehen.

Zusammenfassend lässt sich zu dieser detaillierten Frage sagen, dass die Gefahren tendenziell häufiger und stärker in der IT als in der OT gesehen werden. Die technisch orientierten Systeme (SCADA, SMI, Rundsteueranlagen etc.) werden überwiegend als wenig kritisch angesehen, wobei es jedoch einige abweichende Meinungen gibt, die genau das Gegenteil vertreten.

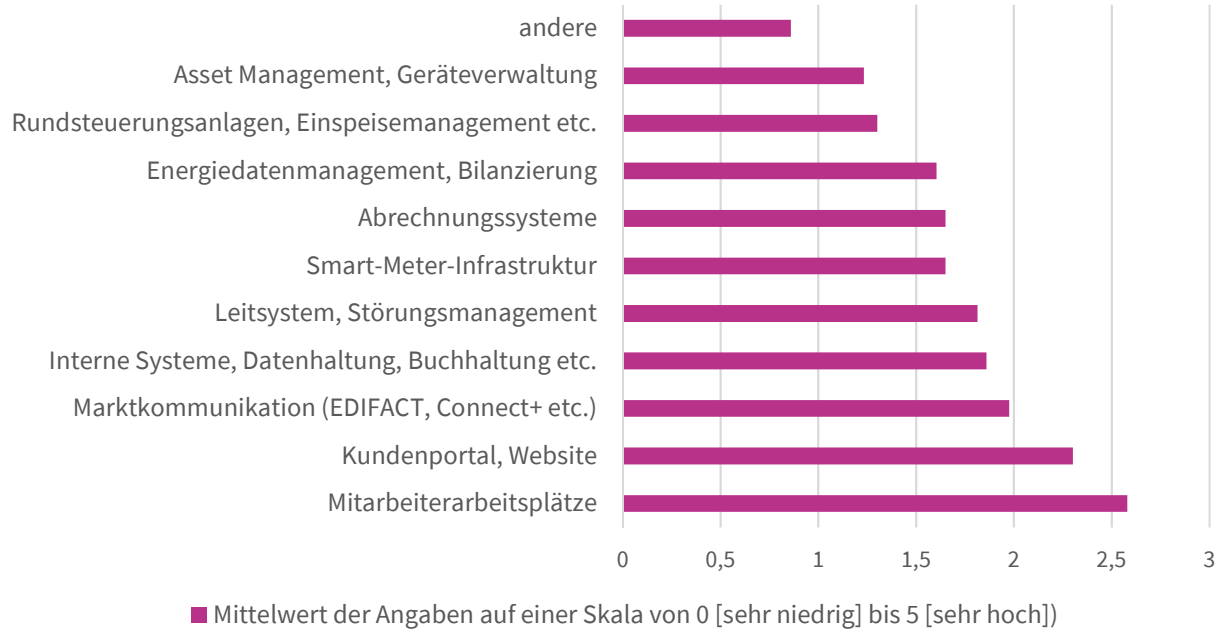


Abbildung 10: Gefährdungspotenzial unterschiedlicher IT-Systeme

Bei der Frage nach dem Hosting zeichnet sich ab, dass die große Mehrheit der Unternehmen nach wie vor Software im eigenen Rechenzentrum betreibt. In Abbildung 11 wird deutlich, dass 81,5 Prozent zumindest Teile ihrer Software im eigenen Unternehmen, also „on premise“, hosten. Das heißt, dass nur 18,5 Prozent vollständig auf externe Dienstleister oder Cloud-Lösungen setzen. Demgegenüber haben 31,5 Prozent keines

ihrer Systeme ausgelagert. Die übrigen Teilnehmer verfolgen eine hybride Strategie mit einer unterschiedlichen Mischung aus „on premise“, externen Dienstleistern und Cloud-Diensten. Daran wird sich in absehbarer Zeit auch nicht allzu viel ändern; nur wenige Unternehmen geben an, über einen Umzug in die Cloud nachzudenken.

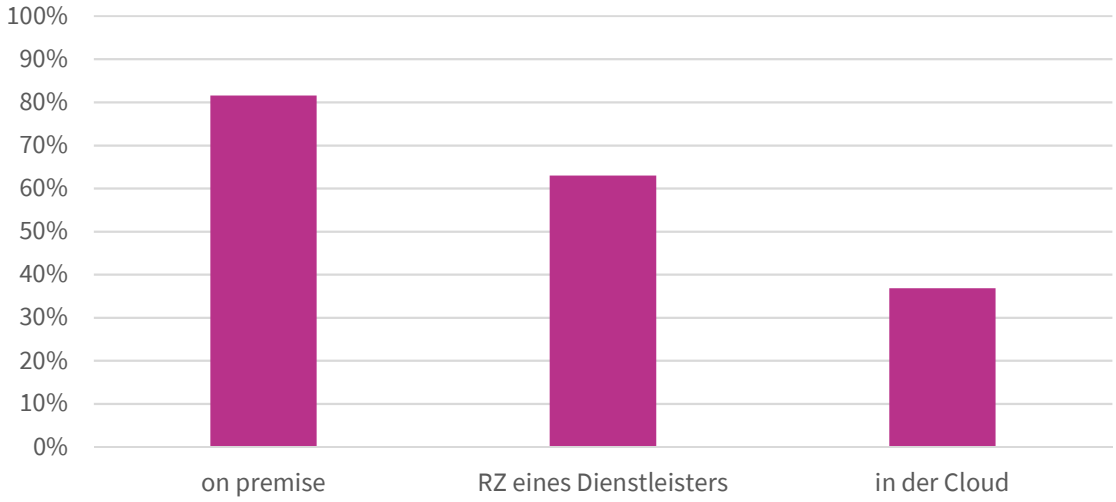


Abbildung 11: Hosting der Systeme (Mehrfachnennungen möglich)

Die letzten beiden Fragen im Abschnitt „Gefährdung“ bezogen sich auf die Absicherung interner und externer Kommunikation. Bei der Auswertung dieser Fragen (Abbildung 12) ist zu beachten, dass verschiedene Kommunikationskanäle unterschiedlich verschlüsselt sein können. Daher waren Mehrfachantworten möglich. Die Zahlen sind also zu interpretieren als „Gibt es überhaupt (mindestens) einen Kommunikationskanal, für den die genannte Verschlüsselungstechnik verwendet wird?“

Eine genauere Analyse der einzelnen Antworten (Abbildung 13) ergibt, dass für die externe Kommunikation bei den meisten Unternehmen bei mindestens einem Kanal eine Verschlüsselung angewandt wird. Nur 9 Prozent geben an, überhaupt keine Verschlüsselungstechnik zu verwenden. Ein relevanter Anteil der Verschlüsselung bezieht sich dabei nur auf die Transportwege. Eine Inhaltsverschlüsselung zumindest für Teile der Kommunikation wird von 74 Prozent der Unternehmen gewählt, eine generelle Inhaltsverschlüsselung für alle Kanäle geben 26 Prozent an.

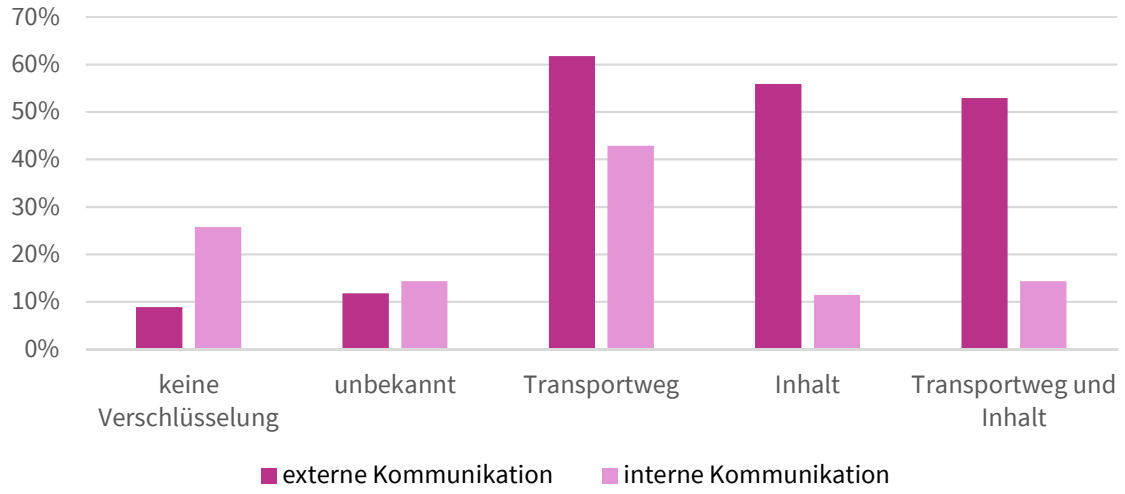


Abbildung 12: Absicherung für Kommunikationswege (Mehrfachantworten möglich)

Bei interner Kommunikation spielt die Verschlüsselung eine wesentlich geringere Rolle. Überhaupt verschlüsselt (wenigstens in Teilen) wird von 57 Prozent der Teilnehmer. Eine Auswertung auf Ebene der einzelnen Datensätze unter Berücksichtigung der möglichen Antwortkombinationen ergibt, dass sich innerhalb dieser Gruppe 34 Prozent mit einer Transportwegverschlüsselung begnügen. Dies ist aus praktischen Gründen verständlich und überrascht von daher nicht, bildet jedoch einen zusätzlichen Angriffsvektor.

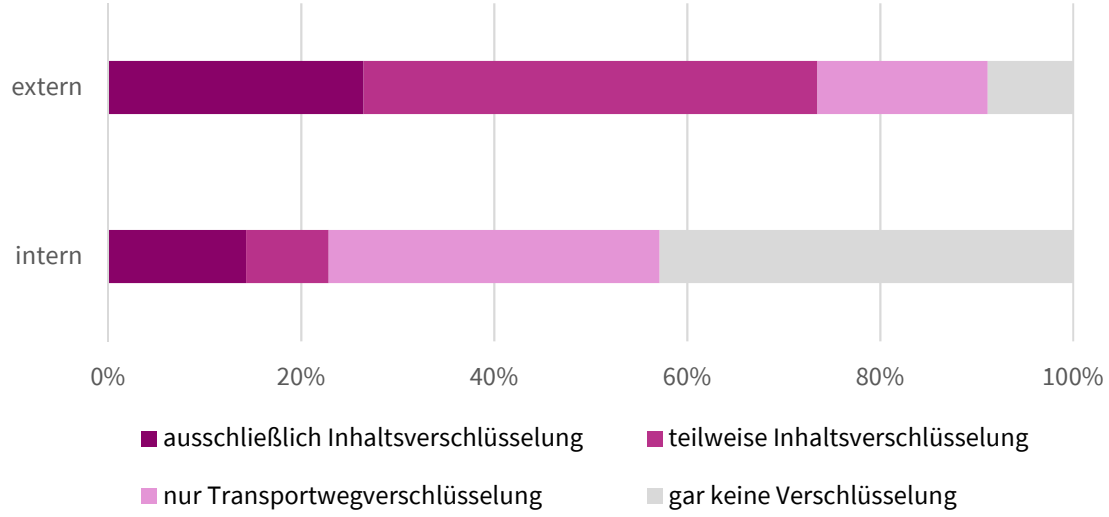


Abbildung 13: Absicherung für Kommunikationswege (aufgeschlüsselt nach Anteilen)

Anzumerken ist, dass die Absicherung insbesondere der externen Kommunikation über das hier betrachtete Thema der Cybersicherheit im Unternehmen hinausgeht und in den beiden Fragen nur angerissen werden kann. Genauere Untersuchungen bieten sich für nachfolgende Studien an. Dabei sollten verschiedene Arten der Kommunikation bei unterschiedlichen Empfängern untersucht sowie nach dem Vorhandensein einer echten Ende-zu-Ende-Verschlüsselung (End-to-End Encryption, E2EE) gefragt werden.

Gegenmaßnahmen zur Prävention

Über die Hälfte, nämlich 52 Prozent der Unternehmen, schätzen die Wirksamkeit ihrer Gegenmaßnahmen als „hoch“ oder „sehr hoch“ ein. Auf der anderen Seite sind 11 Prozent der Meinung, die Wirksamkeit ihrer Maßnahmen sei „gering“ (vgl. Abbildung 14). Eine Abhängigkeit von der Größe der Unternehmen ist nicht zu sehen.

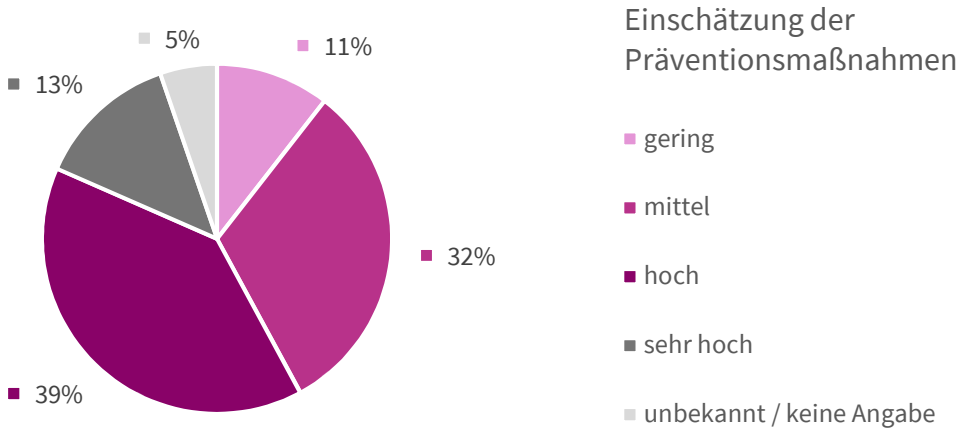


Abbildung 14: Einschätzung der Wirksamkeit bestehender Präventionsmaßnahmen

Abbildung 15 zeigt eine überwältigende Mehrheit von über 90 Prozent, die Awareness-Maßnahmen für die Belegschaft durchführt oder dies zumindest plant. Solche Maßnahmen sind also gängige Praxis. Der Haupt-Fokus liegt dabei auf Schulungen (meistens als Online-Kurse), Informationen per Rundmail oder im Intranet sowie Phishing-Simulationen. Seltener werden Präsenzschulungen durchgeführt, außerdem werden vereinzelt noch Informationen zu aktuellen Anlässen versendet sowie Testangriffe, „Life-Hacks“ und Übungen durchgeführt.

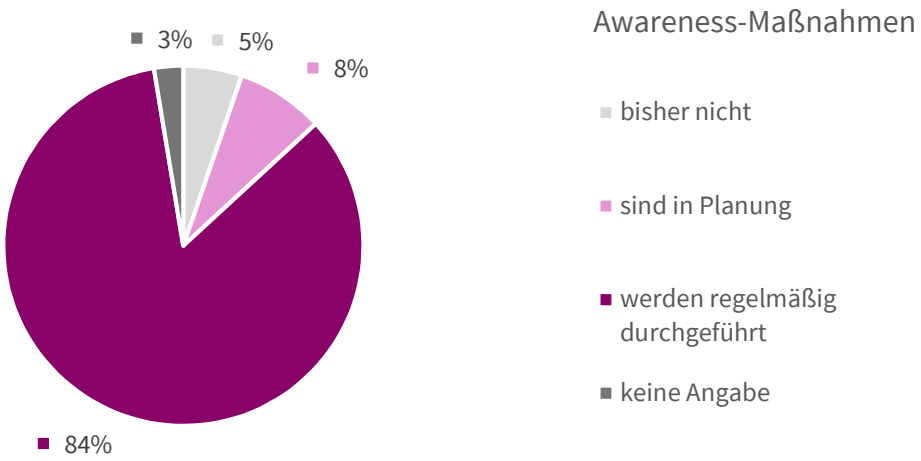


Abbildung 15: Durchführung von Awareness-Maßnahmen

Penetrationstests (Pen-Tests) sind deutlich weniger gängig. Wie in Abbildung 16 zu erkennen, bewerten nur 19 Prozent ihre Pen-Test-Abdeckung als „hoch“, auch hier interessanterweise quer über alle Unternehmensgrößen hinweg. Eine deutliche Mehrheit von 47 Prozent sagt, ein Teil der Systeme werde sporadisch mit Pen-Tests geprüft. Die restlichen Teilnehmer haben eine nur geringe oder gar keine Testabdeckung.

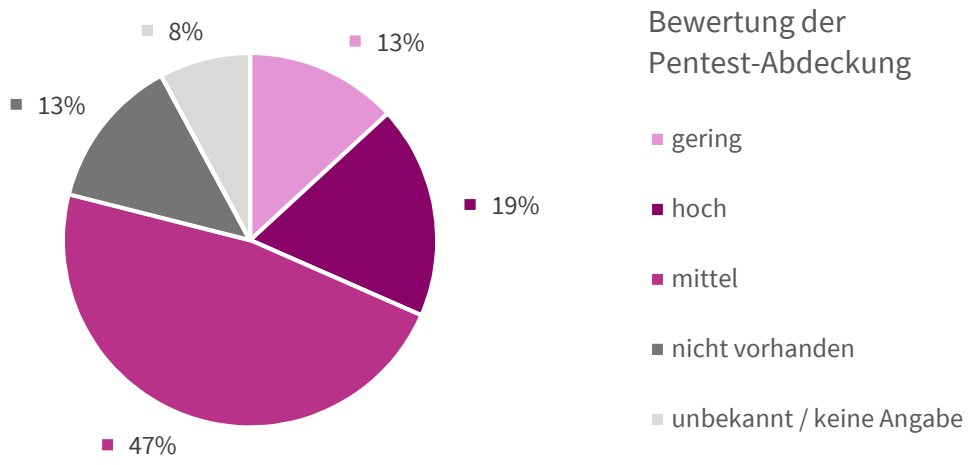


Abbildung 16: Bewertung der Pentest-Abdeckung

Cybersicherheits-Management und -Standards

Auditberichte nach ISO 27001 oder vergleichbaren Normen erstellen die meisten Unternehmen, nämlich mehr als drei Viertel. Etwa ebenso viele haben ein Information Security Management System (ISMS) eingerichtet. Wenig überraschend ist dabei, dass hierbei alle größeren Unternehmen vertreten sind, jedoch auch bei den kleinen Stadtwerken sind es noch mehr als 60 Prozent.

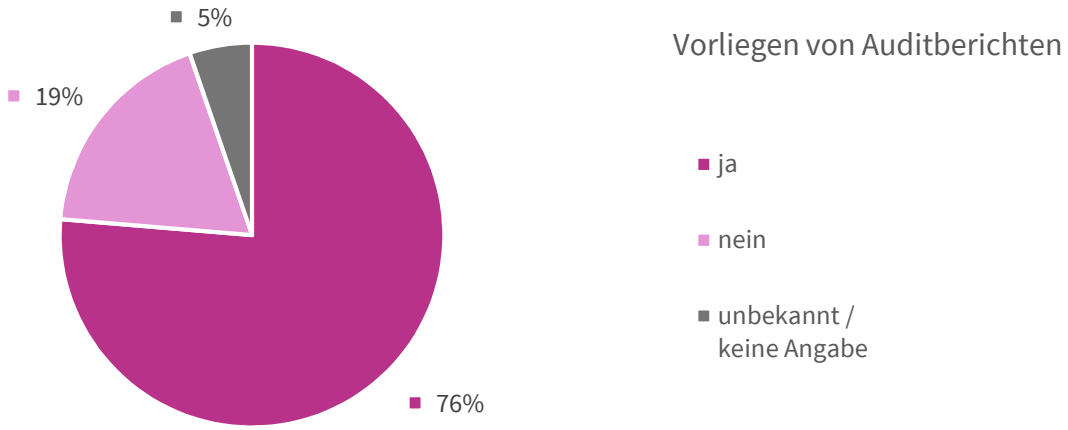


Abbildung 17: Vorliegen von Auditberichten (z. B. ISO-27001-Zertifizierung)

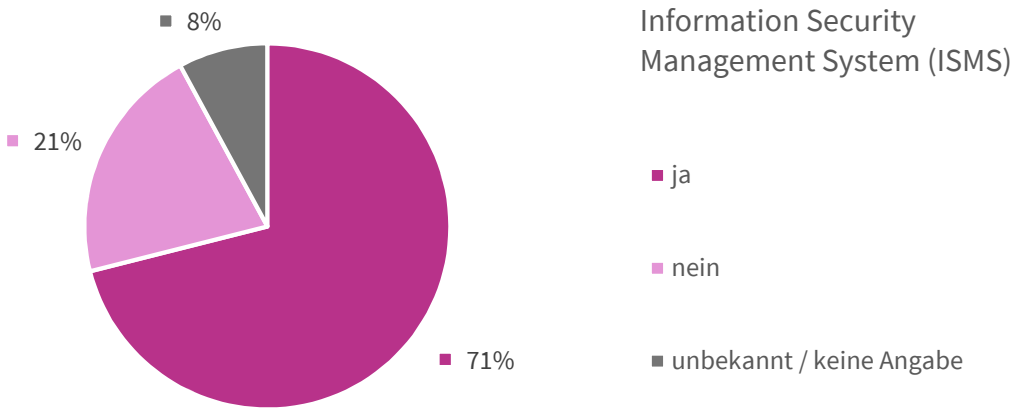


Abbildung 18: Information Security Management System (ISMS) nach ISO 27001 im Unternehmen

Erstaunlich hohe Werte werden für das in Abbildung 19 dargestellte Schwachstellen-Monitoring erreicht. Darunter wird die regelmäßige Überprüfung auf Software-Bibliotheken mit bekannten Angriffsmöglichkeiten verstanden. Nur 19 Prozent haben kein solches CVE-Monitoring (Common Vulnerabilities and Exposures) (oder wissen nicht, ob sie eins haben). Allerdings geben 55 Prozent an, das Monitoring werde nur in Teilbereichen und/oder in unregelmäßigen Abständen betrieben, wobei unklar bleibt, wie dies zu deuten ist.

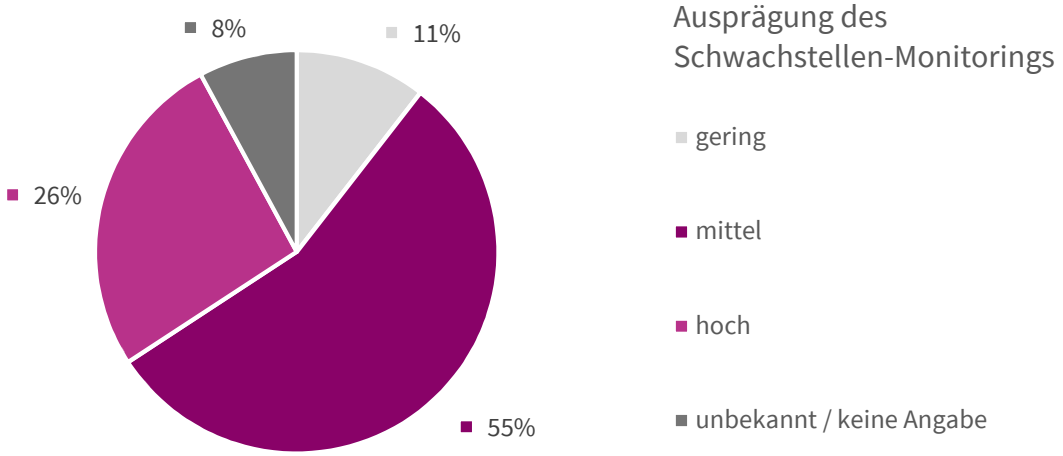


Abbildung 19: Ausprägung des Schwachstellen-Monitorings

Das BDEW-Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ ist drei Vierteln der Unternehmen ein Begriff. Insgesamt 29 Prozent haben alle relevanten Aspekte umgesetzt, weitere 45 Prozent geben eine teilweise Umsetzung an (vgl. Abbildung 20). Zu weiteren Rahmenwerken, die von den Unternehmen berücksichtigt und umgesetzt werden, gehören:

- IT-Sicherheitskatalog der BNetzA (ITSiKat, 2015)
- Technische Regel TR-3109-6 des BSI zur Smart-Meter Gateway-Administration (BSI, 2015)

- Branchenspezifischer Sicherheitsstandard für Aggregatoren (BDEW, 2021) und dessen Pendants für Wasser und Fernwärme
- VGB-Standard „IT-Sicherheit für Erzeugungsanlagen“ (VGB, 2014)
- Einschlägige Normen DIN EN ISO 27001, DIN EN ISO 27002, DIN EN ISO 27011 und DIN EN ISO 27019
- BSI-Grundschutz (BSI, 2022).

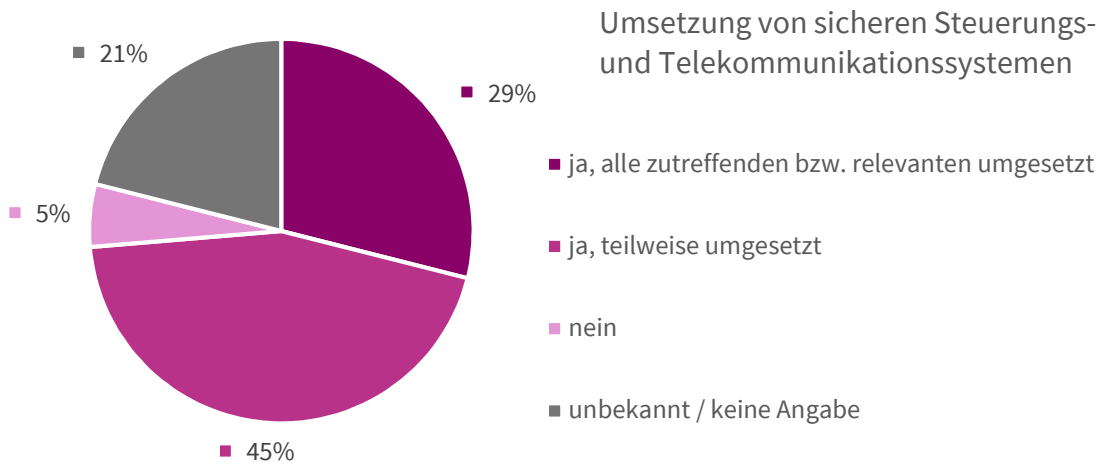


Abbildung 20: Umsetzung von Aspekten des BDEW-Whitepapers „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“

Response-Strukturen

In Abbildung 21 sind die Ergebnisse zur Einschätzung der eigenen Response-Struktur aufgeführt. Bei dieser Einschätzung sind die meisten Unternehmen optimistisch. Als „hoch“ oder „sehr hoch“ wird sie von 34 Prozent eingestuft, weitere 40 Prozent schätzen ihre Response-Struktur als „mittel“ ein, dies entspricht der Angabe: „Die Reaktion auf und die Behebung von Cyberangriffen ist möglich, allerdings noch ausbaufähig.“

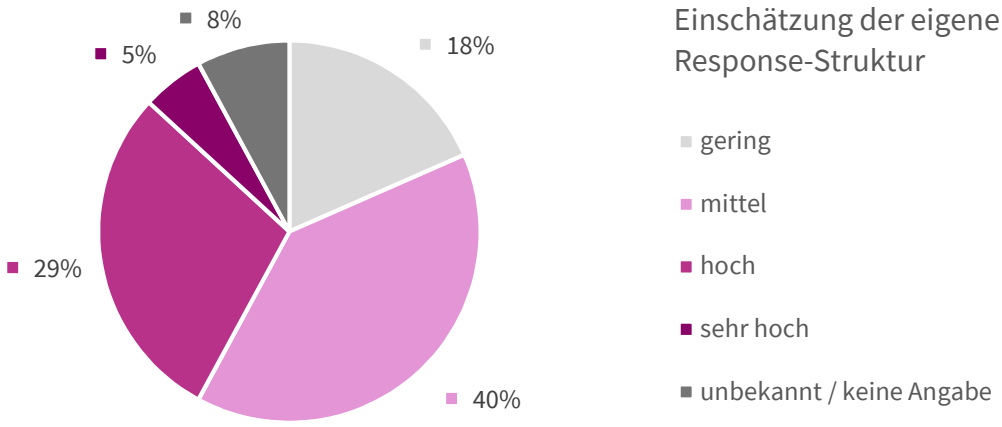


Abbildung 21: Subjektive Einschätzung der eigenen Response-Struktur

Bei den folgenden Fragen nach den konkreten Strukturen zur Angriffsbewältigung sind die Unternehmen allerdings weniger optimistisch, wie in Abbildung 22 und 23 zu sehen. Nur die Hälfte hat einen Krisenstab für Cyberangriffe benannt, hierbei ist im Verhältnis kein Unterschied von kleinen und mittleren zu großen Netzbetreibern (über 100.000 Zählpunkte) feststellbar. Ein Security Operations Center wird nur von 13 Prozent betrieben und auch hier gibt es zwischen kleinen, mittleren und großen Netzbetreibern keine signifikanten Unterschiede.

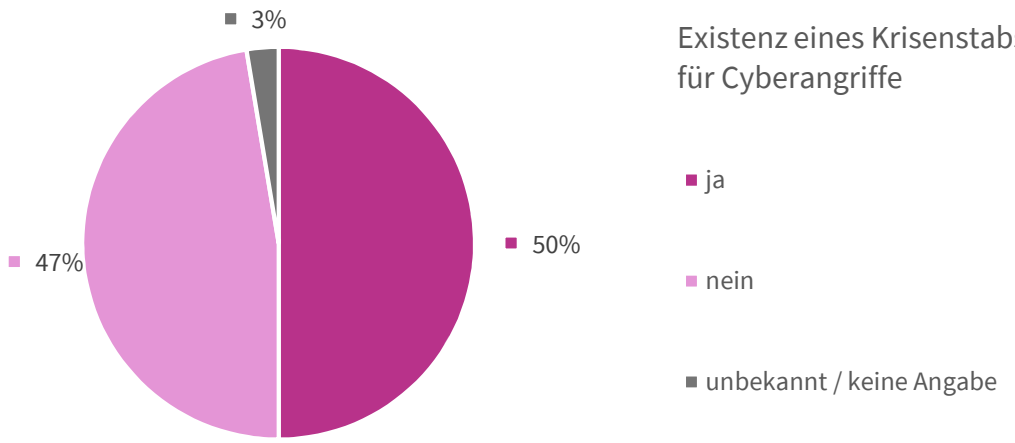


Abbildung 22: Existenz eines Krisenstabs für Cyberangriffe

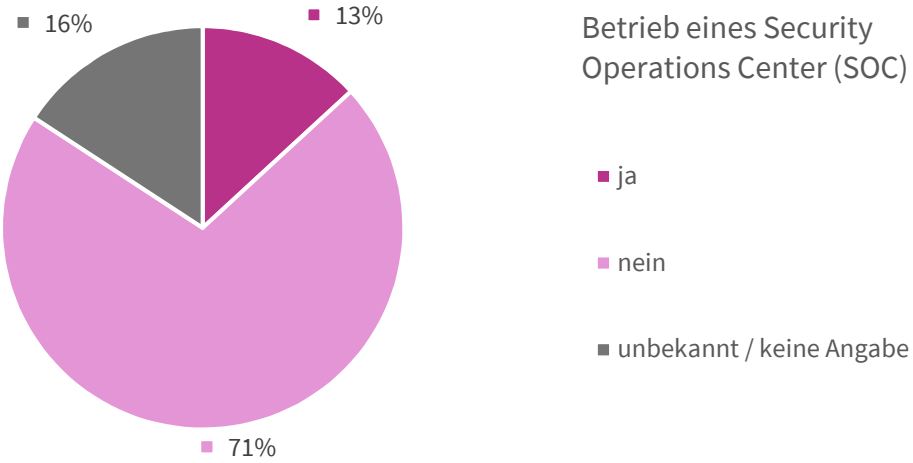


Abbildung 23: Betrieb eines Security Operations Center (SOC)

Der Einsatz eines Intrusion Detection System (IDS) ist einigermaßen weit verbreitet. Abbildung 24 zeigt, dass bei 16 Prozent ein IDS für das IT-Netz existiert, bei 5 Prozent für das OT-Netz und bei 24 Prozent im gesamten Unternehmen. Insgesamt betreiben damit 45 Prozent der Unternehmen ein IDS.

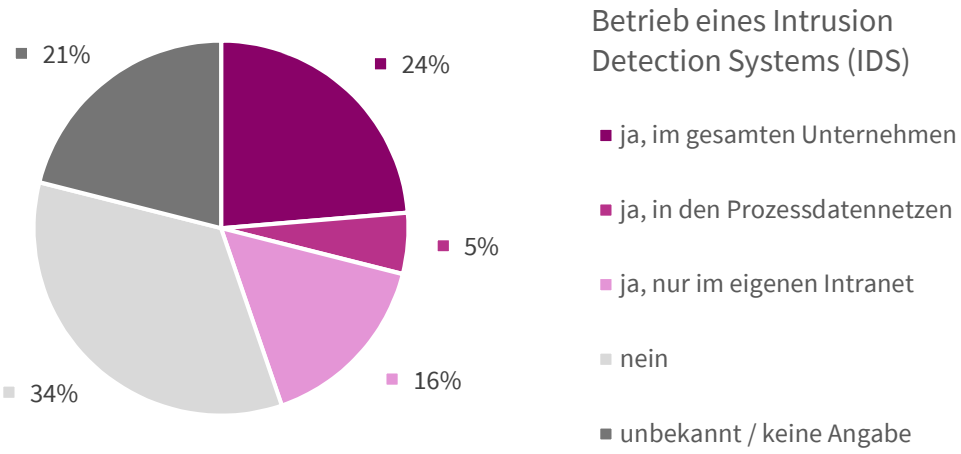


Abbildung 24: Betrieb eines Intrusion Detection System (IDS) innerhalb des Unternehmens

Übungen zur Reaktion auf Cyberangriffe werden deutlich seltener durchgeführt als solche zur Prävention. Dieses Ergebnis wird in Abbildung 25 wiedergegeben. In deutlichem Kontrast zu den 95 Prozent der durchgeführten oder geplanten Awareness-Maßnahmen führen lediglich 11 Prozent regelmäßig Response-Übungen durch. Weitere 24 Prozent geben „unregelmäßig oder einmalig“ durchgeführte Übungen an. Alle übrigen Teilnehmer haben bisher noch nie eine Übung durchgeführt, jedoch ist eine solche bei 26 Prozent in Planung. Ein mittelgroßes Stadtwerk gibt konkrete Inhalte für die Schwerpunkte der Übungen an: „Meldeketten, Test der Funktionsfähigkeit der aufgestellten Regelungen etc.“. Einige weitere Antworten sind eher unspezifisch („Umgang mit Cyberkrisen“, „schnelle und angemessene Reaktion“), während die übrigen Antworten eher auf eine hohe inhaltliche Überschneidung mit Awareness-Übungen hindeuten.

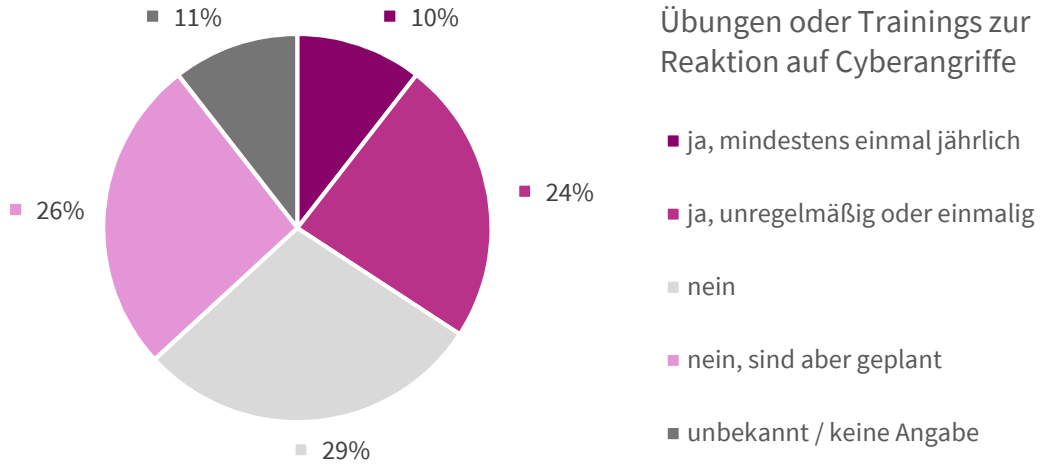


Abbildung 25: Übungen oder Trainings zur Reaktion auf Cyberangriffe

In praktisch allen Unternehmen werden regelmäßig Sicherheitskopien erstellt. Deutlich weniger, nämlich etwa zwei Drittel, prüfen jedoch, ob diese Backups tatsächlich existieren – die Erstellung von Backups kann unter Umständen durch Tippfehler, geänderte Pfade und Verzeichnisse, vollgelaufene Platten etc. verhindert

werden. Bei 42 Prozent der Unternehmen wird das Wiederherstellen mithilfe von Backups geübt. Bei ebenfalls 42 Prozent der Unternehmen (nicht zwingend denselben) wissen die Mitarbeiterinnen und Mitarbeiter, welche Datenbestände wie oft gesichert werden – dies ist wichtig, weil es möglicherweise wichtige Daten geben kann, von denen die Systemadministration nichts weiß oder deren Bedeutung sie nicht erkannt hat (vgl. Abbildung 26).

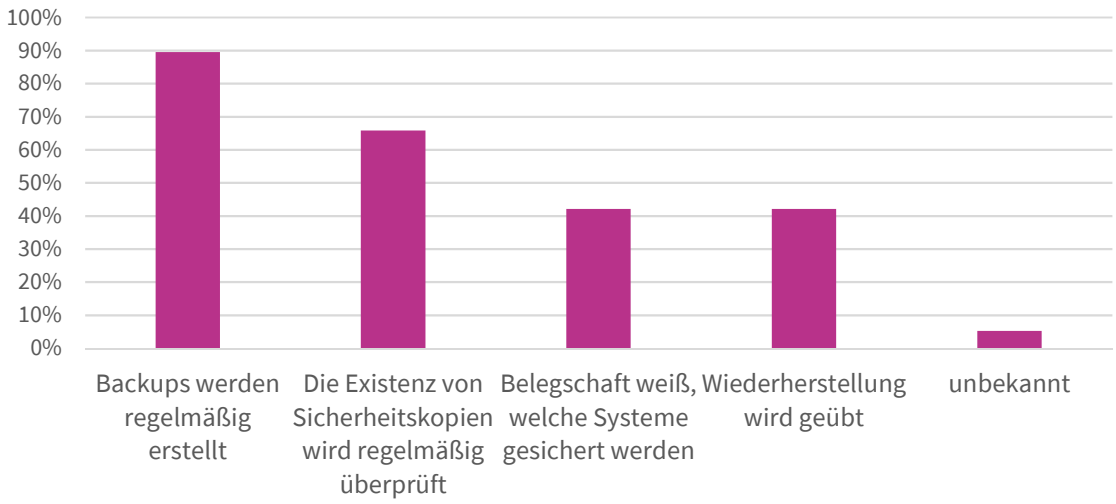


Abbildung 26: Backup-Strategie des Unternehmens

In Abbildung 27 ist zu erkennen, dass knapp die Hälfte aller teilnehmenden Unternehmen Interesse hat, an einer Cybersicherheitsübung teilzunehmen. Konkrete Wünsche für die Schwerpunkte werden eher nicht genannt, es wird jedoch allgemein ein hoher Praxisbezug gewünscht. Ansonsten sind die potenziellen Teilnehmer für alle Inhalte offen.

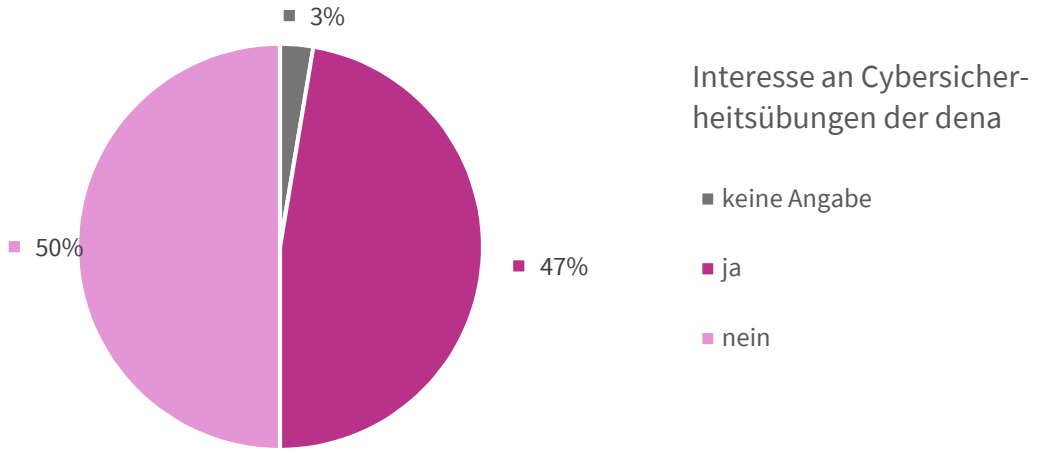


Abbildung 27: Interesse an Cybersicherheitsübungen der dena

3 Interviews

3.1 Umfang und Durchführung

Im Anschluss an die Umfrage wurden Experteninterviews mit IT-Sicherheitsverantwortlichen von insgesamt sieben ausgewählten Netzbetreibern geführt. Bei der Auswahl wurde darauf geachtet, dass sowohl kleine als auch große Netzbetreiber beteiligt waren. Dennoch sind größere Unternehmen hier überrepräsentiert, da aufgrund der besseren personellen Ausstattung der IT-Abteilungen tendenziell mehr Ansprechpersonen mit entsprechendem Fachwissen und entsprechenden Kompetenzen zu finden sind.

Der Zeitraum der Interviews lag zwischen dem 27. Januar 2022 und dem 31. März 2022.

3.2 Themencluster

Bei den Gesprächen wurde grundsätzlich unterschieden, ob das betreffende Unternehmen bereits einen tatsächlichen Angriff erfahren hatte oder nicht. Je nachdem konnte in den nachfolgenden Fragen entweder auf den konkreten Fall eingegangen werden oder es wurde über allgemeine Einschätzungen und Vorkehrungen gesprochen.

Bei den Themen wurden vier Haupt-Cluster angesprochen:

Maßnahmen im Vorfeld

Welche spezifische Art von Bedrohungen sehen Sie für Ihr Unternehmen? Welche Angriffsvektoren/Angriffsflächen/Einfallstore gibt es? Welche Präventionsmöglichkeiten bestehen? Falls es einen tatsächlichen Fall gab: Was war in diesem konkreten Beispiel der Angriffsvektor? Wie hätte der Angriff verhindert werden können?

Handeln während eines Angriffs

Haben Sie für den Fall eines Angriffs einen konkreten Notfallplan? Gibt es ein Framework, nach dem Sie sich ausrichten? Wie soll eine Informationsstrategie aussehen? Gibt es eine vorgeplante Kommunikation? Falls es ein konkretes Beispiel für einen Angriff gibt: Welche Systeme waren hauptsächlich betroffen? Wie haben Sie reagiert? Welche Maßnahmen haben geholfen?

Folgenbewältigung

Wie können Folgen beseitigt werden? Was muss im Nachhinein getan werden? Wenn Sie bereits Opfer eines erfolgreichen Angriffs waren: Was musste getan werden, um das System wiederherzustellen? Welche Komponenten waren am schwierigsten wieder hochzufahren? Welche Maßnahmen haben dabei geholfen? Welche Lehren wurden gezogen, welche Verbesserungen konnten erzielt werden?

Allgemeine Beurteilung

Wie sehen Sie grundsätzlich die Cybersicherheit im deutschen Energiemarkt? Stimmen Sie sich mit anderen Netzbetreibern und den Behörden (BSI) ab? Gibt es Informationsaustausch, gemeinsame Aktionen etc.? Welche Schwierigkeiten (organisatorisch/technisch) gibt es bei der Implementierung von Sicherheitsmaßnahmen? Was wären sinnvolle Inhalte einer Cybersicherheitsübung?

3.3 Ergebnisse

Aus der Vielzahl der so gewonnenen Informationen werden hier einige Hauptpunkte zusammengestellt, die entweder besonders oft genannt wurden oder aber besonders wichtig erscheinen.

Angriffsvektoren

Die Mehrzahl der befragten Netzbetreiber hatte noch keinen erfolgreichen Angriff erlebt. Einige berichten über kleinere Incidents, die sich lokal eingrenzen und relativ schnell beheben ließen. In einem Fall jedoch war ein Netzbetreiber von einem massiven Angriff mit Schäden in Millionenhöhe betroffen.

In allen Fällen erfolgte der Angriff über Phishing-Mails mit anschließendem Nachladen von Schadcode. Die Mails wiesen teilweise einen hohen Qualitätsstandard auf und erschienen auf den ersten Blick durchaus plausibel. In praktisch allen Fällen hatten die betreffenden Anwenderinnen oder Anwender kurz vorher erst eine Unterweisung oder Schulung erhalten.

Das Eindringen wurde wesentlich dadurch erleichtert, dass große Teile der betroffenen Unternehmen „Excel-basiert“ sind. Noch immer scheinen Microsoft-Standardprodukte insbesondere mit ihrer Makro-Verwaltung ein gutes Einfallstor für Cyberangriffe zu sein. Beobachtet wurde in der Regel ein „klassisches“ Vorgehen: Nach der initialen Infektion versucht der Angreifer, sich weitere Rechte zu erarbeiten und andere Rechner zu infizieren.

Als weiterer Angriffsvektor wurden ungepatchte Schwachstellen in den eingesetzten Softwareprodukten gesehen, also Programmierfehler in öffentlichen oder weit verbreiteten Bibliotheken und Komponenten, die von Angreifern zum Eindringen genutzt werden können. Ein bekanntes Beispiel ist die log4j-Lücke (heise, 2021). Ein tatsächlicher Angriff über diesen Weg ist aber nicht bekannt.

Durchweg war die Einschätzung aller Interviewpartner, dass sich ein erfolgreicher Angriff letztlich nicht verhindern lässt. Selbst „gewöhnliche“ Cyberkriminelle haben genug Möglichkeiten, sich Zugang zum IT-Netz zu verschaffen, hinzu kommen anders motivierte Angriffe, wie beispielsweise von Geheimdiensten.

Angriffe auf Dienstleister

Insbesondere die Ransomware-Attacke am 11. November 2021 auf die KISTERS AG hat die Gefahr eines indirekten Angriffs über im Unternehmen eingesetzte Drittsoftware verdeutlicht. Das betrifft sowohl extern gehostete Systeme als auch vor Ort eingesetzte Software, vor allem aber auch Fernwartungszugänge.

Im Fall KISTERS fühlten sich mehrere der Befragten schlecht über den Status informiert. Warnungen oder zusätzliche Informationen kamen erst spät, nur vereinzelt wurden die Netzbetreiber direkt durch ihre Kundenbetreuerinnen und -betreuer angerufen, in den meisten Fällen erfuhren die Unternehmen erst durch die Meldung des BSI von dem Vorfall. Dies lag nicht an einem bewussten Zurückhalten von Informationen, sondern daran, dass bei der KISTERS AG durch den Systemausfall auch die Kommunikationskanäle ausfielen, zusätzlich standen dadurch Adresslisten und Kundendaten nicht mehr zur Verfügung.

Zusammenarbeit mit dem BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird durchgängig als kompetent und engagiert beschrieben. Es wird anerkannt, dass das BSI nicht als Kontrollbehörde, sondern eher unterstützend als Dienstleister auftritt, und ihm wird eine Kommunikation „auf Augenhöhe“ bescheinigt, auch wenn die Vorgaben als eher theoretisch wahrgenommen werden. Auch die vom BSI angebotenen regelmäßigen „Stammtische“ werden angenommen und besucht.

Bemängelt wird, dass die Bulletins des BSI über aktuelle Sicherheitsprobleme zu umfangreich sind. Es fällt schwer, in der schieren Menge der Informationen die relevanten Punkte herauszusuchen. Hier wäre es sinnvoller, eine bessere Vorfilterung nach Schweregrad vorzunehmen, oder, wie es ein Interviewpartner ausdrückte, „nur dann Feuer zu rufen, wenn es auch brennt“.

Die Berichte an das BSI, die im Falle eines Incident abzugeben sind, werden als sehr kompliziert und aufwendig angesehen. Dies mag ein Grund sein, warum freiwillige Meldungen von nicht meldepflichtigen Vorfällen eher selten sind. Von den befragten Personen haben nur die allerwenigsten bereits eine formelle Meldung an das BSI durchgeführt.

Angriffe

In allen Fällen erfolgte der Angriff über das Büronetz. Die operative Technik war bislang bei keinem Netzbetreiber betroffen. Hier wurde also die Einschätzung aus der Umfrage bestätigt.

In einigen Unternehmen bestehen strikte Regeln, wie OT- und IT-Netz im Falle eines Incident voneinander getrennt werden, und es sind Personen benannt, die eine solche Trennung veranlassen können. Dies ist in einigen Fällen auch tatsächlich erfolgt.

Kommunikation

Die Kommunikation im Unternehmen während eines Angriffs ist ein extrem kritischer Punkt. Bei einem erzwungenen Herunterfahren der IT-Systeme stehen alle üblichen Kommunikationskanäle nicht mehr zur Verfügung. Der Zugriff auf wichtige Informationen ist ebenfalls nicht mehr möglich. Dies kann die Handlungsfähigkeit massiv einschränken. Außerdem ist die Kommunikation mit der Außenwelt ebenfalls erschwert.

An dieser Stelle hilft eine erfolgreiche Eindämmung auf das Büronetz und die Verhinderung eines Übergreifens auf die Netzleittechnik nichts, da die Kommunikation im IT-Netz angesiedelt ist. Zu den von den Stadtwerken ergriffenen oder vorgesehenen Maßnahmen gehören:

- Ausweichen auf externe Dienstleister für Mail (zum Beispiel posteo) und Instant Messaging (WhatsApp etc.)
- Direkter telefonischer Kontakt
- Vorhalten von Betriebsfunk
- Feste Leitungen zu Polizei, Feuerwehr und Behörden

Teilweise wird ein „Notfallkoffer“ in der Leitstelle vorgehalten, der Organisationsanweisungen, Handys oder Satellitentelefone, Telefonlisten etc. enthält, gegebenenfalls auch „saubere“ Notebooks.

Eine nicht zu unterschätzende Rolle für die Kommunikation mit der Öffentlichkeit spielen Social-Media-Kanäle. Darüber können einerseits Informationen verteilt werden, zum anderen sind die Überwachung und gegebenenfalls das Einwirken auf diese Kanäle wichtig. Im Fall eines Angriffs mit erheblichen Auswirkungen hatte eines der an den Interviews teilnehmenden Unternehmen durch einen hohen Aufwand auf Social Media erfolgreich einen „Shitstorm“ vermieden.

Wahrnehmung im Unternehmen

Eine erhebliche Rolle bei der Umsetzung von Cybersecurity-Maßnahmen spielt die Akzeptanz bei den Kolleginnen und Kollegen sowie die Rückendeckung durch die Geschäftsleitung.

Cybersecurity-Maßnahmen werden von Anwenderinnen und Anwendern als umständlich und lästig empfunden. Hinzu kommt, dass manche lieb gewonnenen Gewohnheiten aufgegeben werden müssen, wie etwa Administratorrechte auf Arbeitsplatzrechnern. Die Erfahrung zeigt, dass sich Widerstände erheblich verringern lassen, wenn zum einen der Sinn der Maßnahmen gut erklärt wird und wenn zum anderen mehr pragmatisch als dogmatisch vorgegangen wird. So ist es zum Beispiel durchaus möglich, Admin-Rechte zu gewähren, wenn diese für die tägliche Arbeit gebraucht werden, hierfür muss allerdings eine ausreichende Begründung vorliegen. Optimal ist, wenn das Security-Team nicht als Aufpasser, sondern als Unterstützung wahrgenommen wird, analog zum Bild der Polizei als „Freund und Helfer“.

Entscheidend ist letztendlich die Unterstützung der Geschäftsleitung, denn daran hängt insbesondere die personelle Ausstattung. Ohne ein entsprechendes Standing im Unternehmen ist eine schlagkräftige Cyberabwehr kaum möglich. Daher ist es wichtig, dass Cybersecurity nicht als Kostenfaktor wahrgenommen wird, sondern als Investition. Hier hilft in erster Linie der Verweis auf die enormen Kosten, die im Schadensfall entstehen. In gewissem Maße gibt es auch sekundäre Nutzen, wenn zum Beispiel die Einführung eines ISMS zu generell besserer und saubererer Dokumentation von Assets, Strukturen und Prozessen führt. Generell ist der direkte Gewinn durch solche Kollateralnutzen jedoch überschaubar. Eine direkte positive Auswirkung auf das Bild des Unternehmens in der Außendarstellung wird eher nicht gesehen, dafür ist das Thema zu abstrakt.

Weitere Gefahren / Neuartige Strukturen

Durchweg als gering angesehen wird die Gefahr, die von intelligenten Messsystemen und ähnlichen Vorrichtungen ausgeht. Solange Smart Meter nur messen und nicht steuernd eingreifen, wird hier kein Potenzial für Angriffe ausgemacht. Die größte Gefahr ist in diesem Bereich, dass Hersteller ihre eigenen, proprietären Protokolle zur Gerätesteuerung entwickeln, weil dadurch die Vorgaben des BSI zur Sicherheit umgangen würden und kein gemeinsamer, definierter Sicherheitsstandard besteht.

Deutlich gefährlicher ist das Zusammenwachsen von Stromnetzen und Marktprozessen, wie es derzeit beispielsweise im Rahmen der Einführung des Redispatch 2.0 (BNetzA 059, 2020) stattfindet. Hier erfolgt ein Eingriff in die technische Netzsteuerung auf Basis von Anforderungen anderer Netzbetreiber, was zu einer kostengünstigeren Gestaltung des Redispatch in Deutschland führen soll, aber aus Sicht der Cybersicherheit kontraproduktiv ist: Die Verknüpfung von operativer Technik mit Marktnachrichten, die aus Sicht von Redispatch 2.0 notwendig und gewollt ist, hebt gerade das zentrale Sicherheitsfeature der Netzbetreiber in Teilen auf. Eine Attacke, die zu einer unbefugten Steuerung von Erzeugungsanlagen führen kann, wird auf verschiedene Weise als möglich gesehen, zum Beispiel durch einen Angriff auf die Infrastruktur der zentralen

Plattform des *Data Providers*, der Einsatzverantwortlichen oder der Netzbetreiber oder – am einfachsten – durch Einspeisen von falschen Nachrichten in das System.

Einige Interviewpartner weisen darauf hin, dass nach wie vor ein physischer Angriff auf Strukturen der Energie- und Wasserversorgung weitaus wahrscheinlicher und erfolgversprechender ist als ein Cyberangriff. Das gilt sowohl für einfache, ungerichtete Kriminalität (Kupferklau) als auch für Terroranschläge. Auch Naturkatastrophen wie die Überschwemmungen in Westdeutschland im Jahr 2021 können zu erheblichen Ausfällen in Transport- und Verteilnetzen führen.

4 Schlussfolgerungen und Empfehlungen

4.1 Empfehlungen

Eine wesentliche Erkenntnis der Umfrage und Interviews ist, dass es keine hundertprozentig sichere Prävention gibt. Selbst auf Unternehmen, die großen Wert auf Cybersicherheit legen und ihre Belegschaft regelmäßig schulen, gibt es erfolgreiche Angriffe. Es ist davon auszugehen, dass jeder Arbeitsplatzrechner, bei dem ein Mailclient und ein Webbrowser Zugang zum Internet haben, potenziell infiltriert werden kann. Die Gefährdung steigt zusätzlich bei Verwendung von Office-Software wie zum Beispiel Microsoft Excel.

Vor diesem Hintergrund ist die Konzentration allein auf präventive Schutzmaßnahmen wie Awareness-Kampagnen kritisch zu hinterfragen, da sich durch sie keine absolute Sicherheit erreichen lässt. Günstigstenfalls schärfen diese Kampagnen bei den Beteiligten das Bewusstsein für das Thema Cybersicherheit, es ist aber auch möglich, dass ein Gefühl falscher Sicherheit entsteht („Mir kann das nicht passieren!“) oder Misstrauen zwischen den Anwenderinnen und Anwendern einerseits und der Systemadministration andererseits gesät wird („Die versuchen, mich reinzulegen“).

Daher sollte bei Cyberübungen der Schwerpunkt nicht ausschließlich auf die Verhinderung von Infektionen gelegt werden, sondern vor allem darauf, Schäden zu begrenzen, Handlungsfähigkeit zu bewahren und den operativen Betrieb schnellstmöglich wieder aufzunehmen.

Letztendlich soll auch die Möglichkeit von Störungen im IT- und OT-Betrieb, die nicht auf Cyberangriffe zurückgehen, berücksichtigt werden. Auch durch Unfälle, Naturkatastrophen oder physische Sabotage können erhebliche Teile des Netzes lahmgelegt werden. Für viele dieser Störungen sind ähnliche Maßnahmen angebracht, sodass auch sie in einer Übung mit betrachtet werden sollten.

Über eine konkrete Übung hinaus sind weitere Maßnahmen und Strategien sinnvoll. In den Interviews hat sich gezeigt, dass eine positive Wahrnehmung von IT-Sicherheit im Unternehmen – sowohl bei den Mitarbeiterinnen und Mitarbeitern als auch bei der Geschäftsführung – essenziell wichtig ist. Dazu braucht es ein gewisses internes Lobbying. Einerseits müssen dazu die im Ernstfall vermiedenen hohen Kosten beziffert werden, andererseits sollte sich das IT-Sicherheitsteam als Dienstleister im Unternehmen positionieren.

4.2 Schwerpunkte für die Übung EnerCise

Im Folgenden werden inhaltliche Themen benannt, die aufgrund der gewonnenen Erkenntnisse bei einer Übung als Schwerpunkte berücksichtigt werden sollten. Für Form und Durchführung der Übung lassen sich unterschiedliche Varianten denken, etwa ein Training an speziell dafür konzipierten Softwaresystemen als Simulationsumgebung, aber auch Planspiele als Gruppenarbeit ohne direkte Computerunterstützung.

Sofortmaßnahmen der IT-Administration

Es wird ein Szenarium entworfen, bei dem ein erfolgreiches Eindringen von außen in die IT-Infrastruktur entdeckt wird. In diesem Moment ist das Ausmaß des Cyberangriffs überhaupt noch nicht bekannt. Es muss zunächst davon ausgegangen werden, dass das gesamte IT-Netzwerk kompromittiert und potenziell auch das OT-Netz betroffen ist.

Für die ersten Sofortmaßnahmen ist es wichtig, dass die IT-Administration über einen von ihr ausgearbeiteten Notfallplan verfügt und dass dieser auf Papier existiert und allen relevanten Personen bekannt und zugänglich ist. Dieser Plan muss Fragen adressieren wie:

- Wie werden Systeme vom Netz getrennt und heruntergefahren? Gibt es eine Reihenfolge, in der dies geschehen muss?
- Welche Zugänge und Schnittstellen nach außen müssen gekappt werden?
- Wie können Informationen über das Ausmaß der Störung bzw. des Angriffs eingeholt werden?
- Wer ist zu benachrichtigen?

Diese Punkte sind hier nur exemplarisch aufgeführt. Eine detaillierte Ausarbeitung muss im jeweiligen Unternehmen erfolgen, allerdings darf der Plan nicht so kompliziert und umfangreich werden, dass er in Stresssituationen nicht mehr zu bewältigen ist. Die Verständlichkeit des Notfallplans soll Bestandteil der Übung sein.

Kommunikationsstrukturen

Für die Übung soll davon ausgegangen werden, dass die bestehende Kommunikationsstruktur komplett ausgefallen ist. Sowohl der Mailserver als auch die Telefonanlage sind heruntergefahren, VPN-Zugänge (Virtual Private Network) sind gekappt. Zusätzliche Instant-Messenger- oder Chatprogramme (etwa Microsoft Teams) sind nicht mehr verfügbar. Ein Zugriff auf Informationen im Intranet ist nicht möglich.

Vor diesem Hintergrund soll ein Schwerpunkt der Übung darin liegen, eine funktionierende Kommunikation aufzubauen. Dazu gehören unter anderem Fragen wie:

- Gibt es Telefonlisten auf Papier und wissen alle, wo diese zu finden sind?
- Kann die Belegschaft im Homeoffice erreicht werden?
- Auf welche alternativen Kommunikationskanäle (etwa externer Anbieter) soll ausgewichen werden? Findet sich die Belegschaft auf diesen Kanälen zusammen?
- Wie erfolgt die Kommunikation mit der Außenwelt?

Sinnvoll ist, ein komplett unabhängiges Medium wie etwa Betriebsfunk vorzusehen. In diesem Fall muss sichergestellt und in einer Übung überprüft werden, ob die Geräte funktionstüchtig und zugänglich sind und ob eine hinreichende Zahl von Mitarbeiterinnen und Mitarbeitern mit der Technik vertraut ist.

Organisation

Eng verbunden mit der Kommunikation ist die Frage der Organisationsstrukturen. Entsprechend soll in einer Übung ein Schwerpunkt auf ihre Wiederherstellung bzw. Aufrechterhaltung unter schwierigen Bedingungen gelegt werden.

- Wer muss mit wem reden? Wie können die zuständigen Personen erreicht werden? Sind Listen der Teams und ihrer Mitglieder vorhanden und offline verfügbar?
- Wissen insbesondere Technikerinnen und Techniker sowie die IT-Administration, was sie zu tun haben?

- Wer übernimmt die Koordination und die Organisation? Wer gibt Anweisungen?
- Wer kommuniziert mit Behörden – Polizei, Feuerwehr, BSI, Stadtverwaltung?

Eine sinnvolle Einrichtung ist das Vorhalten eines „Notfallkoffers“ mit allen notwendigen Dokumentationen und Arbeitsanweisungen sowie technischen Geräten für den Notbetrieb (etwa Funkgeräte oder vorbereitete, „saubere“ Laptops). Der Notfallkoffer muss zugänglich und sein Inhalt den relevanten Personen bekannt sein.

Handbetrieb

Bei einem Komplettausfall muss es möglich sein, die Versorgung vollständig manuell zu sichern bzw. wiederherzustellen. In einer Übung soll daher beispielsweise geprüft werden:

- Lassen sich die wichtigen Elemente des Versorgungsnetzes (Strom, Gas, Wasser) vor Ort von Hand bedienen? Sind die entsprechenden Räume zugänglich? Wo werden Schlüssel aufbewahrt?
- Welche elektronischen Zugangssysteme gibt es und können diese manuell übersteuert werden?
- Dasselbe gilt für die IT-Administration: Können Server, Switches etc. physisch erreicht werden? Können Rechner einzeln heruntergefahren, hochgefahren, vom Netzwerk getrennt und verbunden werden?

Angriffsanalyse und Cyberabwehr

Bei einem Angriff auf das OT-Netz müssen Ausmaß und Auswirkungen der Störung festgestellt und unmittelbare Gegenmaßnahmen eingeleitet werden. Dies wird in der Übung unter Verwendung einer Trainings- und Simulationsumgebung durchgeführt. Eine solche Umgebung wurde zum Beispiel im Projekt MEDIT unter Federführung des Fraunhofer-Instituts (FIT, 2022) entwickelt.

- Woran lassen sich Fehlerzustände erkennen und wie unterscheiden sich Cyberangriffe von zufälligen Gerätedefekten?
- Welche Techniken und Methoden können eingesetzt werden, um Lösungen für kritische Szenarien zu finden?
- Wie werden die bestehenden Incident-Response-Leitfäden umgesetzt, können sie validiert und gegebenenfalls weiter konkretisiert werden?

Weitergehende IT-Maßnahmen

Zu den dringenden Aufgaben gehört aus zwei wesentlichen Gründen die Kommunikation mit dem BSI: Zum einen müssen Auswirkungen über das Unternehmen hinaus geprüft und gegebenenfalls Warnungen ausgesprochen werden. Zum anderen bietet das BSI Hilfestellung und Unterstützung bei der Bewältigung von Angriffen und ihren Folgen. Die Meldung eines Incident an das BSI bedarf allerdings einer gewissen Erfahrung und eines entsprechenden Fachwissens.

Zur Einübung der Kommunikation soll ein Incident-Report über den simulierten Angriff erstellt werden. Sinnvollerweise soll diese Meldung auch tatsächlich zur Übung versandt werden. Dies setzt eine Einbeziehung des BSI im Vorfeld voraus.

Disaster Recovery / Backup and Restore

Zur Aufnahme des Regelbetriebs gehört ganz wesentlich die Wiederherstellung verlorener oder kompromittierter Daten. Daher muss geprüft werden, ob Daten aus Sicherheitskopien zurückgespielt werden können. Es muss zudem bestimmt werden, welche Daten mit welchem Zeithorizont wieder verfügbar sein müssen, und gegebenenfalls eine Priorisierung festgelegt werden.

In der Praxis wird dieser Punkt oft vernachlässigt, da ein „Recovery zur Probe“ mit erheblichem Aufwand verbunden ist. Dennoch sind Backup und Restore von eminent großer Bedeutung für die betriebliche Kontinuität, sodass ein realer Test auf jeden Fall durchgeführt werden sollte. Für die Übung kann eine begrenzte Datenmenge verwendet werden, die zufällig aus einer vorher aufgestellten Liste ausgewählt wird, zum Beispiel Kundenanfragen, Mailverkehr, Telefon- und Organisationslisten oder Abrechnungsdaten.

4.3 Zusammenfassung

Eine eindeutige Aussage, ob die Cybersicherheit der Netzbetreiber in Deutschland als „gut“, „zufriedenstellend“ oder „besorgniserregend“ bewertet werden muss, lässt sich nicht abschließend treffen. Die Mehrheit der befragten Netzbetreiber sieht sich jedoch verhältnismäßig gut aufgestellt.

Auf der einen Seite gilt mit ziemlicher Sicherheit, dass ein Angriff auf die IT-Infrastruktur nicht in jedem Fall abgewehrt werden kann, auch nicht bei großen Netzbetreibern, die hohe Investitionen in Cybersicherheit tätigen. Ein entschlossener und mit ausreichenden Mitteln versehener Angreifer wird mit großer Wahrscheinlichkeit Möglichkeiten finden, zumindest Teile des IT-Netzes zeitweise lahmzulegen.

Auf der anderen Seite ist eine flächendeckende erfolgreiche Attacke auf die Stromversorgung schwierig. Die Netzbetreiber verfügen über eine mehr oder weniger ausgeprägte Trennung von OT- und IT-Netzen und sind zudem in der Regel fähig, ihre Stromnetze manuell zu schalten und zu steuern. Zudem existiert in Deutschland eine sehr heterogene IT- und Sicherheitslandschaft unter den Netzbetreibern. Ein großflächiger Blackout allein durch Cyberangriffe scheint daher relativ wenig wahrscheinlich.

Eine besondere Herausforderung stellt die im Rahmen der Energiewende erwünschte Verzahnung von Erzeugungsanlagen und Netzen dar, die durch die zunehmende Digitalisierung im Energiemarkt bedingt wird und aktuell unter anderem im Rahmen von Redispatch 2.0 vorangetrieben wird. Dadurch werden zusätzliche Schnittstellen des Leitsystems zu Drittsystemen und zum Energiemarkt bedingt, sodass die strikte Trennung zwischen OT und IT schwieriger wird. Es müssen Mittel gefunden werden, wie die Cybersicherheit trotzdem sichergestellt werden kann. Unter anderem sollte bei der Ausgestaltung der Marktprozesse seitens BSI, BNetzA und BDEW darauf geachtet werden, dass die Sicherheit der Netze nicht den Erfordernissen des Marktes untergeordnet wird.

Übungen zur Cybersicherheit sind auf jeden Fall sinnvoll. Sie sollen für Netzbetreiber aller Größenordnungen angeboten und zur Teilnahme empfohlen werden. Dabei sollten die Schwerpunkte auf einer angemessenen und wirkungsvollen Antwort auf Angriffe liegen. Im Fokus sollten die Aufrechterhaltung der Versorgung, die Wiederherstellung der Geschäftsprozesse und die Minimierung von Schäden stehen. Dabei darf ungeachtet aller Wichtigkeit von IT- und OT-Systemen nicht vergessen werden, dass gerade die nicht computerisierten Prozesse im Krisenfall für die Handlungsfähigkeit eine wesentliche Rolle spielen.

Abbildungsverzeichnis

Literaturverzeichnis

Becker Büttner Held (BBH, 2020): Konvergenz statt Insellösungen: Vernetzung im Energiesektor. In: BBH Blog, 14.12.2020, abgerufen unter https://www.bbh-blog.de/alle-themen/digitalisierung/konvergenz-statt-inselloesungen-vernetzung-im-energiesektor

Bundesamt für Justiz (EnWG, 2005): Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz) vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 5 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1325) geändert worden ist

Bundesamt für Justiz (BSIG, 2009): Gesetz zeur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist

Bundesamt für Justiz (BSI-KritisV, 2016): Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163) geändert worden ist

Bundesamt für Justiz (NIS, 2017): Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) vom 23. Juni 2017. Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 40

Bundesamt für Justiz (IT-SiG 2.0, 2021): Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021. Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 25

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2015): BSI-TR-03109-6: Smart-Meter-Gateway-Administration. Version 1.0 vom 26.11.2015

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2021): BSI-Standard 200-4: Business Continuity Management. Community Draft (Entwurf), veröffentlicht unter www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4_CD.pdf

Bundesamt für Sicherheit in der Informationstechnik (BSI, 2022): IT-Grundschutz-Kompendium. Reguvis Fachmedien GmbH, 2022, ISBN 978-3-8462-0906-6

Bundesnetzagentur (BNetzA, 2015): IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG. Bundesnetzagentur, 12.08.2015

Bundesnetzagentur (BNetzA 059, 2020): Festlegungsverfahren zum bilanziellen Ausgleich von Redispatch-Maßnahmen sowie zu massengeschäftstauglichen Kommunikationsprozessen im Zusammenhang mit dem Datenaustausch zum Zwecke des Redispatch. Beschluss BK6-20-059 vom 06.11.2020

Bundesnetzagentur (BNetzA 060, 2021): Festlegungsverfahren zur Informationsbereitstellung für Redispatch-Maßnahmen. Beschluss BK6-20-060 vom 23.03.2021

Bundesnetzagentur (BNetzA 061, 2021): Festlegungsverfahren zur Netzbetreiberkoordinierung bei der Durchführung von Redispatch-Maßnahmen. Beschluss BK6-20-061 vom 12.03.2021

Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW, 2018): Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“, abgerufen unter www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf

Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW, 2021): Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung (B3S Aggregatoren). Version 1.1 vom 15.02.2021

Cybersecurity and Infrastructure Security Agency (CISA, 2016): ICS Alert (IR-ALERT-H-16-056-01). Cyber-Attack Against Ukrainian Critical Infrastructure, abgerufen unter www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01

Deutsche Energie-Agentur (Hrsg.) (dena, 2021): EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft

Deutsches Institut für Normung e.V. (Hrsg.) (DIN e.V., 2017): DIN EN ISO/IEC 27001:2017-06, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015)

Elsberg, Marc (Elsberg, 2012): Blackout – Morgen ist es zu spät: Roman. Blanvalet Verlag 2012, ISBN 978-3764504458

Europäisches Parlament und Rat der Europäischen Union (EU, 2016): Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rats vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. Amtsblatt der Europäischen Union L 194 vom 19.7.2016, S. 1

Fraunhofer-Institut für Angewandte Informationstechnik FIT (FIT, 2022): MEDIT. Prävention, Detektion und Reaktion bei IT-Angriffen und -Ausfällen. https://medit-projekt.de/

Hampe, Liane (xmera, 2017): BSI-Kriterium hebelt Meldepflicht für Energieversorger wieder aus. Digitale Broschüre, November 2017, abgerufen unter https://xmera.de/wp-content/uploads/2017/10/2017-11-14_bsi-kriterium-hebelt-meldepflicht-fuer-energieversorger-wieder-aus.pdf

Kutte, Inge, und Rauner, Max (ZEIT, 2012): Das wäre ein Riesenproblem. Interview mit Jochen Homann und Marc Elsberg, 6. Dezember 2012, DIE ZEIT Nr. 50/2012

heise online (heise, 2021): Kritische Zero-Day-Lücke in Log4j gefährdet zahlreiche Server und Apps. Meldung vom 10.12.2021, abgerufen unter heise.de/-6291653

mdr Sachsen (mdr, 2021): Cyberangriff auf Stadtwerke Pirna. Meldung vom 6. Dezember 2021, abgerufen unter www.mdr.de/nachrichten/sachsen/dresden/freital-pirna/cyberangriff-stadtwerke-pirna-100.html

VGB Powertech (VGB, 2014): IT-Sicherheit für Erzeugungsanlagen. VGB Verlag technisch-wissenschaftlicher Schriften, 06.05.2014, ISBN 978-3-86875-754-5

Glossar

Begriff	Definition
Arealnetz	Lokal begrenztes Gebiet aus privaten Grundstücken mit einem Niederspannungsverteilnetz. Konkret: Flughäfen, Bahnhöfe, Industrieparks etc.
BCM	Business Continuity Management (Betriebliches Kontinuitätsmanagement)
BDEW	Bundesverband der Energie- und Wasserwirtschaft e. V.
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritisverordnung
CIA-Triade	Confidentiality, Integrity, Availability (die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit)
CLS	Controllable Local Systems
CVE	Common Vulnerabilities and Exposures (bekannte Schwachstellen und Anfälligkeiten
cyber-	Abgeleitet vom griechischen κυβερνήτης (kybernetes), auf Deutsch: „Steuermann“. Hier: die Informationstechnik bzw. IT-Systeme betreffend
DR	Disaster Recovery (Katastrophenwiederherstellung)
E2EE	End-to-End Encryption
EDM	Energiedatenmanagement
EnWG	Energiewirtschaftsgesetz
IDS	Intrusion Detection System
iMSys	Intelligentes Messsystem
Incident	Ungeplante Unterbrechung oder Beeinträchtigung eines IT-Service
ISMS	Information Security Management System
IKT	Informations- und Kommunikationstechnik
IT	Informationstechnik
IT-Störung	Liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann
KRITIS	Kritische Infrastruktur gemäß BSI-KritisV: Unternehmen, die mehr als 500.000 Menschen versorgen

Begriff	Definition
NIS	Netzwerk- und Informationssicherheit
OT	Operational Technology (Operative Technik, im Gegensatz zu IT)
RD	Redispatch
SCADA	Supervisory Control And Data Acquisition (Leitsystem)
SMGW	Smart Meter Gateway
SOC	Security Operations Center
ÜNB	Übertragungsnetzbetreiber
VNB	Verteilnetzbetreiber
VPN	Virtual Private Network

www.dena.de

dena
Deutsche Energie-Agentur