dena
Deutsche Energie-Agentur

Future Energy Lab

ENERCISE II

Empfehlungen zu praktischen Cybersicherheitsübungen für Verteilnetzbetreiber

Impressum

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

Autoren:
Marius Dechand, dena
Hendrik Zimmermann, dena
Dr. Martin Serror, Fraunhofer FKIE
Lennart Bader, Fraunhofer FKIE
Eric Wagner, Fraunhofer FKIE
Immanuel Hacker, Fraunhofer FIT
Markus Stroot, Fraunhofer FIT

Stand:
7/2024

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2024): EnerCise II – Empfehlungen zu praktischen Cybersicherheitsübungen für Verteilnetzbetreiber

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.

Vorwort

Das Thema Cybersicherheit bekommt weltweit eine immer größere Bedeutung – vor allem im Bereich der kritischen Infrastrukturen. Dies gilt insbesondere für das sich wandelnde Energiesystem und der damit nötigen voranschreitenden Digitalisierung. Im Kontext eines vermehrten Einsatzes digitaler Technologien auf allen Ebenen der Wertschöpfungsketten des Energiesystems vergrößern sich die Angriffsflächen für kriminelle Organisationen, die versuchen, das System zu infiltrieren oder anderweitig zu schädigen. Wir als Deutsche Energie-Agentur (dena) haben selbst erfahren müssen, was es bedeutet, Ziel eines Cyberangriffs zu werden.

Den Auftakt unserer Aktivitäten zur Cybersicherheit im Energiesystem bildete das 2021 veröffentlichte Gutachten „**EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft**“ (dena, 2021). In diesem Bericht werden sowohl Innovationspotenziale für Cybersicherheit im Rahmen der Energiewende als auch die Notwendigkeit von Cyberinnovationen für die Transformation des Energiesystems aufgezeigt. Ausgehend davon haben wir unter anderem die „**Branchenplattform Cybersicherheit in der Stromwirtschaft**“ ins Leben gerufen. Sie verbindet zentrale Akteure der Energie- und Digitalwirtschaft, um in einem institutionalisierten Format ein Verständnis der Bedürfnisse der jeweils gegenseitigen Branchen zu fördern und gemeinsame Entwicklungen anzustoßen. 2023 haben wir unter Einbezug der Projektpartner eine Themenroadmap veröffentlicht, die eine Übersicht über einige zum Zeitpunkt der Veröffentlichung relevante Themen bezüglich der Cybersicherheit in der Energiewirtschaft gibt (dena, 2023). Auch im internationalen Umfeld treibt die dena das Thema Cybersicherheit im Rahmen von **Energiepartnerschaften** mit verschiedenen Ländern voran.

Unter dem Titel „**EnerCise – Cybersicherheitsübungen für Netzbetreiber**“ haben wir zwei Cybersicherheitsübungen für deutsche Verteilnetzbetreiber ausgerichtet. Ziel der Übungen war es, Routinen und Response-Mechanismen zu entwickeln und zu erproben sowie die eingebundenen Akteure untereinander zu vernetzen. 2022 wurde die erste Cybersicherheitsübung **EnerCise I** für das Management und IT-Personal von Stromnetzbetreibern im Rollenspiel-Format durchgeführt (dena, 2022). Die zweite Übung, **EnerCise II**, fand unter Einbezug einer digitalen Simulationsumgebung im April 2024 statt und richtete sich an das Management, das IT/OT-Personal und das Leitwarten-Personal mittelgroßer Verteilnetzbetreiber.

In diesem Dokument informieren wir umfassend über EnerCise II. Das Übungskonzept und der Übungsablauf werden detailliert beschrieben und mit den Beobachtungen am Tag der Übung unterfüttert. Diese beziehen sich einerseits auf das Übungskonzept, andererseits auf das Vorgehen der Teilnehmerinnen und Teilnehmer. Auf Basis der Beobachtungen können wir das Konzept evaluieren und auf die relevanten Situationen im Vorgehen des Teilnehmerkreises (im positiven wie im negativen Sinne) aufmerksam machen. Hierdurch können Verteilnetzbetreiber – und andere Akteure im Energiesystem – Antworten auf zwei wesentliche Fragen finden:

1. **Was sollte bei der Konzeption eigener Cybersicherheitsübungen alles beachtet werden?**
2. **Worauf sollte bei Cybersicherheitsschulungen für das eigene Unternehmen besonderer Wert gelegt werden?**

Wir möchten uns auf diesem Wege bei unseren Projektpartnern des Fraunhofer FKIE (Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie) und des Fraunhofer FIT (Fraunhofer-Institut für Angewandte Informationstechnik) bedanken, die uns während dieses Vorhabens mit sehr großer fachlicher

Expertise begleitet und uns stets qualitativ hochwertige Arbeitsergebnisse zugeliefert haben. Ein besonderer Dank gilt auch dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK), das dieses Projekt ermöglicht hat. Selbstverständlich möchten wir auch den Teilnehmerinnen und Teilnehmern unserer Cybersicherheitsübungen für ihren Einsatz herzlich danken.

Hendrik Zimmermann
Teamleiter Digitale Technologien
Deutsche Energie-Agentur (dena)

Marius Dechand
Seniorexperte Digitale Technologien
Deutsche Energie-Agentur (dena)

Executive Summary

Cyberangriffe stellen ein signifikantes Risiko für zunehmend digitalisierte kritische Infrastrukturen wie Stromnetze dar. Um diese Risiken zu minimieren, präventive Maßnahmen effektiv umzusetzen und für den Krisenfall hinsichtlich detektiver und reaktiver Maßnahmen vorbereitet zu sein, sind praktische Cybersicherheitsübungen für Netzbetreiber ein wichtiges Mittel. EnerCise II hat sich dieser Aufgabe angenommen, indem im Rahmen dieses Projekts ein Übungskonzept speziell für Verteilnetzbetreiber entwickelt und in einer praktischen Pilotübung erprobt wurde.

EnerCise II

Zielgruppe: Verteilnetzbetreiber

Teilnehmerkreis: 11 Personen

Dauer: 9 Stunden

Ort: Future Energy Lab

Rollen: Management, IT/OT, Leitwarte

Szenario: Ransomware

Ziele: Sensibilisierung, Praxistraining, Vernetzung

Das Konzept adressiert das Personal von Verteilnetzbetreibern aus den Bereichen der IT/OT, der Leitwarte und des Managements. In einer interaktiven Übung hat das Personal aus diesen Fachbereichen in einem fiktiven Szenario eines Verteilnetzbetreibers einen Cybersicherheitsvorfall erlebt und gemeinsam bewältigt. Hierzu hat das Konzept von EnerCise II eine realistische Simulationsumgebung, in der das Verteilnetz mit der zugehörigen IT und OT in Echtzeit nachgebildet wurde, mit Table-top-Elementen kombiniert, die die 11 Teilnehmerinnen und Teilnehmer in ihren Aufgaben und Lösungsideen unterstützt und angeleitet haben. Nach einer praktischen Einarbeitungsphase in das Übungsszenario und die technischen Umstände hat EnerCise II den Teilnehmerkreis mit einem realistischen Cyberangriffsszenario konfrontiert, das eine effektive Kommunikation innerhalb der und zwischen den Fachbereichen erfordert hat. So wurde die Unternehmensführung mit Erpresserschreiben, politischem und medialem Druck sowie Kundenbeschwerden konfrontiert, während das IT/OT- und das Leitwarten-Personal die technischen Auswirkungen des Cyberangriffsszenarios nachvollziehen, eindämmen und aufbereiten musste. Dieses bestand im Wesentlichen aus vier Stufen:

1. **Reconnaissance:** Scan aller gefundenen Subnetze auf aktive Hosts sowie potenzielle Dienste.
2. **Lateral Movement:** Hosts, auf denen ein SSH-Dienst erkannt wurde, werden mithilfe eines Brute-Force-Angriffs, also dem systematischen Erraten von Passwörtern oder -phrasen, attackiert. So können Zugangsdaten erbeutet werden.
3. **Blackmailing:** Die gesammelten Informationen werden genutzt, um Forderungen an die Unternehmensführung zu stellen. Im Zuge der Übung wird die Zahlung von ca. 1 Million Euro gefordert. Für den Fall eines Zahlungsversäumnisses wird mit weiteren Angriffen gedroht.
4. **Command and Control / Impact:** Als Reaktion auf ausbleibende Zahlungen werden kritische Dienste im OT-Netz gestört, manipuliert und abgeschaltet. Diese Aktionen haben direkten Einfluss auf den Betrieb des Stromnetzes.

Im Verlauf der praktischen Pilotübung wurde der Übungsbedarf zur Bewältigung eines Cyberangriffs vor allem bezüglich der Kommunikation der Gruppen untereinander sowie der Ausnutzung der zur Verfügung stehenden Handlungsoptionen deutlich. Insbesondere beim Auftreten der ersten Anzeichen eines Cyberangriffs zeigte sich, wie essenziell eine gruppenübergreifende Kommunikation im Krisenfall ist. Nur so kön-

nen Indizien für einen Angriff richtig gedeutet und gezielte Gegenmaßnahmen ergriffen werden. Hier übernimmt der Krisenstab der Management-Gruppe eine entscheidende Rolle, da er für den effektiven Informationsaustausch und die Bündelung der Kompetenzen verantwortlich ist. Positiv zu bewerten ist, dass sich die Teilnehmerinnen und Teilnehmer zügig in das unbekannte Szenario einarbeiten konnten, obwohl die Größe und die Komplexität des simulierten Verteilnetzes eine Herausforderung darstellten. Innerhalb der Gruppen wurden unterschiedliche Rollen verteilt und die anfänglichen Routineaufgaben effizient erledigt.

Aus der Übung lassen sich Handlungsempfehlungen sowohl für die Durchführung von Cybersicherheitsübungen als auch für den generellen Umgang mit Cybersicherheitsvorfällen ableiten. Diese Empfehlungen beruhen jedoch ausschließlich auf den Erkenntnissen dieser speziellen Übung und bieten daher keine umfassende Garantie für die Cybersicherheit eines Unternehmens.

Handlungsempfehlungen für die Durchführung von Cybersicherheitsübungen

- Es sollte ein realistisches Szenario gewählt werden, das in der Komplexität variiert und auf die Kenntnisse und Fähigkeiten der Teilnehmerinnen und Teilnehmer zugeschnitten werden kann.
- Der Teilnehmerkreis sollte bereits vor der Übung Informations- und Schulungsmaterial zum Thema Cybersicherheit erhalten. Am Tag der Übung sollte die Einarbeitungszeit dynamisch angepasst werden können, damit sich alle Teilnehmerinnen und Teilnehmer ausreichend zurechtfinden und der jeweiligen Handlungsmöglichkeiten bewusst sind. Während der Übung sollte die Übungsleitung in angemessener Weise auf Fehler, Versäumnisse oder Handlungsmöglichkeiten hinweisen.
- Die Übung sollte direkt im Anschluss nachbereitet werden. Den Teilnehmerinnen und Teilnehmern sollte durch die Nachbereitung der genaue Ablauf des Angriffsszenarios sowie die Handlungsmöglichkeiten und ihre Auswirkungen bewusst sein. An geeigneter Stelle sollte konstruktives Feedback zu den gruppenspezifischen Handlungen gegeben werden.

Handlungsempfehlungen im Umgang mit Cybersicherheitsvorfällen

- EnerCise II hat gezeigt, dass während einer Krisensituation insbesondere die Kommunikation zwischen den eingebundenen Gruppen gestärkt werden muss, um einen effektiven Informationsfluss sicherzustellen.
- Für den Krisenfall sollten alle involvierten Personen dazu angehalten sein, Informationen zum aktuellen Lagebild im Krisenstab proaktiv mitzuteilen und zu versuchen, ein möglichst vollständiges Lagebild zu erhalten.
- Während der Durchführung von EnerCise II wurde deutlich, dass die Priorisierung von Aufgaben eine immense Bedeutung für die erfolgreiche Bewältigung von Krisensituationen hat.
- In allen Bereichen lassen sich mögliche Reaktionen vorbereiten, um sie im Krisenfall effizient und zeitnah einsetzen zu können. Dies umfasst organisatorische Maßnahmen wie Reaktionen auf Erpresserbotschaften, aber auch technische Gegenmaßnahmen.
- Eine wesentliche Erkenntnis aus EnerCise II ist, dass zwischen Theorie und Praxis im Bereich Incident Response und Krisenmanagement erhebliche Diskrepanzen bestehen: Selbst wenn umfassende IT-Sicherheitskonzepte und Notfallpläne erstellt wurden, ist deren korrekte und vollständige Umsetzung im Krisenfall nicht gewährleistet.

Die Durchführung von EnerCise II verdeutlicht den dringenden Bedarf an Cybersicherheitsübungen im

Energiesektor und die unverzichtbare Verknüpfung von interdisziplinärer Fachexpertise, resilienter Kommunikation und geordnetem Krisenmanagement. Cybersicherheitsübungen sind für Verteilnetzbetreiber ein angemessenes und wichtiges Mittel, um Risiken zu minimieren und die Betreiber auf den Umgang mit Krisensituationen vorzubereiten. Eine regelmäßige Durchführung – gegebenenfalls mit unterschiedlichen Schwerpunkten – wird daher empfohlen, um die Cybersicherheit in diesen kritischen Infrastrukturen langfristig zu erhöhen.

Inhalt

1 Einleitung

Kritische Infrastrukturen (KRITIS), insbesondere im Energiesektor, sind einer wachsenden Bedrohung durch Cyberangriffe ausgesetzt, die potenziell verheerende Auswirkungen haben können. Dieser Herausforderung kann zuvorderst durch die konsequente Umsetzung effektiver Cybersicherheitsmaßnahmen begegnet werden. Hierfür ist eine enge Kooperation zwischen den betroffenen Akteuren sowie den zuständigen Behörden angeraten. Neben fundierter technischer Expertise für präventive Cybersicherheitsmaßnahmen ist es entscheidend, einen Cyberangriff frühzeitig zu erkennen und durch reaktive Maßnahmen effektiv einzudämmen, Resilienz aufzubauen und zum Normalbetrieb zurückzukehren. Hierbei reicht eine theoretische Wissensvermittlung allein nicht aus. Vielmehr müssen praktische Trainings durchgeführt werden, um Maßnahmen, Abläufe und Kommunikation im Krisenfall zu üben und zu festigen.

Der Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) von 2023 (BSI, 2023) unterstreicht die Bedrohungslage durch die detaillierte Analyse aktueller Cybervorfälle und identifizierter Schwachstellen im deutschen Energiesektor. Laut dem Bericht ist die Anzahl der Cyberangriffe auf kritische Infrastrukturen weiter angestiegen, wobei insbesondere Ransomware-Angriffe und die Ausnutzung von Schwachstellen in industriellen Kontrollsystemen stark zugenommen haben. Diese Entwicklungen erfordern eine proaktive und ganzheitliche Herangehensweise an Cybersicherheit.

Gesetzliche Vorgaben haben auf diese Bedrohungslage reagiert und fordern von Energieversorgern erhöhte Sicherheitsstandards. Das NIS2-Umsetzungsgesetz, das in Deutschland 2024 in Kraft treten soll, verstärkt die Cybersicherheitsanforderungen erheblich und erweitert die Pflichten für Betreiber kritischer Infrastrukturen. Das Gesetz setzt die EU-Richtlinie NIS2 um, die striktere Sicherheitsmaßnahmen und Meldepflichten für Sicherheitsvorfälle vorschreibt und die Implementierung umfassender Risikomanagementmaßnahmen fordert. In Verbindung mit dem IT-Sicherheitsgesetz 2.0 und dem KRITIS-Dachgesetz verpflichtet das NIS2-Umsetzungsgesetz Unternehmen des Energiesektors dazu, regelmäßig Cybersicherheitsübungen durchzuführen, Sicherheitsvorfälle unverzüglich zu melden und detaillierte Sicherheitskonzepte zu erstellen. Diese gesetzlichen Anforderungen zielen darauf ab, die Widerstandsfähigkeit der Infrastruktur gegen Cyberangriffe zu stärken und das Reaktionsvermögen bei Sicherheitsvorfällen zu verbessern.

Die nächsten Kapitel dieses Berichts geben eine detaillierte Beschreibung des Übungskonzepts, des Ablaufs der Übung sowie der gewonnenen Erkenntnisse und daraus abgeleiteten Handlungsempfehlungen. Es wird die Zielsetzung der Übung dargelegt und der konkrete Übungsablauf inklusive der verwendeten Technik und des Szenarios mit sämtlichen Schlüsselmomenten und den jeweiligen Detektions- und Reaktionsmöglichkeiten sowie den gruppenspezifischen Aufgaben und individuellen Lernzielen beschrieben. Die gewonnenen Erkenntnisse werden unterteilt in Erkenntnisse zur Gestaltung weiterer Cybersicherheitsübungen im Stile von EnerCise II und solche zum Verhalten der beteiligten Akteure bei einem Cybersicherheitsvorfall.

2 Übungskonzept

Für einen angemessenen Umgang mit Cybersicherheitsvorfällen im Verteilnetz sind Übungen für Verteilnetzbetreiber hinsichtlich der Prävention, Detektion und zielgerichteten Reaktion unabdingbar. So können Abläufe vorbereitet, Verantwortlichkeiten verteilt und Kommunikationswege etabliert werden.

2.1 Zielsetzung und Ablauf

Das Ziel von EnerCise II besteht darin, eine praktische Cybersicherheitsübung für Verteilnetzbetreiber durchzuführen, bei der effektive Reaktionen auf eine Krisensituation, insbesondere einen Cyberangriff, im Mittelpunkt stehen. Die Übung sollte für relevante Akteure innerhalb eines Verteilnetzes konzipiert werden, darunter IT/OT-Personal, Leitwarten-Personal und Management, die gemeinsam die auftretenden Herausforderungen bewältigen sollen. Besonderes Augenmerk liegt auf der Kommunikation zwischen den Akteuren und der Einleitung von Gegenmaßnahmen, die unter erschwerten Bedingungen wie Zeitdruck, unvollständigen Informationen und Teilausfällen in der Kommunikationsinfrastruktur stattfinden müssen.

EnerCise II verfolgt folgende Lernziele:

1. Sensibilisierung für Cybersicherheit und die Auswirkungen von Cyberangriffen
2. Praktische Anwendung von IT-Sicherheitsmaßnahmen
3. Stärkung der Kommunikation und Vernetzung der relevanten Akteure

Somit zählt neben der allgemeinen Sensibilisierung insbesondere auch die Vermittlung von praktischem Wissen zur Prävention und Erkennung von Cyberangriffen sowie zur Reaktion darauf zu den Kernaspekten der Übung. Sie soll die Integration innovativer Cybersicherheitslösungen und eine verbesserte Kommunikation im Krisenfall fördern sowie die Vernetzung zwischen den Teilnehmerinnen und Teilnehmern stärken, wobei die jeweiligen Kompetenzen des technischen und des nicht technischen Personals berücksichtigt werden.

Konzeptionell steht bei EnerCise II der praktische Teil der Cybersicherheitsübung im Vordergrund. Ein geringer theoretischer Anteil wird in Form eines vorbereitenden Online-Workshops sowie einer kurzen Einführung am Übungstag vermittelt. Inhaltlich beschränkt sich die Theorie auf eine prägnante Einführung zu Cybersicherheit im KRITIS-Sektor Energie, eine Kurzvorstellung des Szenarios und einige praktische Informationen zum Ablauf. Eine besondere Herausforderung besteht daher darin, dass die Teilnehmerinnen und Teilnehmer sich im praktischen Teil der Übung in ein weitgehend unbekanntes Szenario einarbeiten müssen. Ziel ist es, dass sie frühzeitig Rollen und Aufgaben verteilen und ihr Wissen durch effektive Kommunikation untereinander teilen.

Des Weiteren orientiert sich die praktische Übung grob am Konzept eines „Red Team versus Blue Team“-Ansatzes, bei dem das Red Team die Rolle der Angreifer und das Blue Team die Rolle der Verteidiger übernimmt. Eine Besonderheit von EnerCise II ist hierbei, dass die Teilnehmerinnen und Teilnehmer der Übung ausschließlich das Blue Team stellen und das Red Team von den Übungsorganisatoren gebildet wird. Der Fokus liegt daher auf der Verteidigerperspektive, wobei die bis zu 15 Teilnehmerinnen und Teilnehmer in verschiedene Gruppen (IT/OT-Personal, Leitwarten-Personal und Management) nach Kompetenzen und Verantwortlichkeiten differenziert werden. Dies soll die Kommunikation zwischen den Akteuren stärken und

eine schnellere und zielsichere Abwehr des Angriffs fördern, indem die Teilnehmerinnen und Teilnehmer in ihrem direkten Umfeld den unkomplizierten fachlichen Austausch finden können, gruppen- und somit fachübergreifende Kommunikation jedoch bewusster gesucht werden muss.

Unmittelbar im Anschluss an die Übung findet eine Nachbesprechung zwischen allen Teilnehmerinnen und Teilnehmern und den Übungsorganisatoren statt. Ziel sind die systematische Aufarbeitung und Analyse des erlebten Cybersicherheitsvorfalls sowie die Bewertung der Handlungsoptionen. Außerdem erfolgt eine Evaluation der Übung mittels einer offenen Feedback-Runde sowie eines Fragebogens, um das Übungskonzept für zukünftige Durchführungen zu verbessern.

Im Folgenden wird das Übungskonzept zum praktischen Teil von EnerCise II weiter ausgeführt und konkretisiert.

2.2 Szenariogestaltung und technische Umsetzung

Grundlage für das Übungsszenario in EnerCise II ist ein fiktiver Verteilnetzbetreiber für ein mittelgroßes Mittelspannungsnetz mit mehreren dezentralen Erzeugungsanlagen, das über ein einzelnes Umspannwerk an das übergeordnete Hochspannungsnetz angebunden ist. Für eine realitätsnahe Übung kommt in der Umsetzung die Co-Simulationsumgebung WATTSON (Bader et al., 2023) zum Einsatz, die das Stromnetz simuliert (modelliert) und das zugehörige Kommunikationsnetz mit Servern, Routern, Switchen und Fernwirkgeräten detailliert emuliert (nachbildet) sowie die Anbindung weiterer Geräte wie WLAN-Access-Points, Laptops oder auch Systemen zur Angriffserkennung ermöglicht. Bei der Simulation des Stromnetzes werden also dessen Eigenschaften und sein Verhalten modelliert, ohne dass diese tatsächlich vorhanden sind, während bei der Netzwerkemulation die Eigenschaften bzw. Funktionen so nachgebildet werden, dass sie auch von echten Anwendungen und echten Systemen genutzt werden können – so wird die Kommunikation nicht nur modelliert, sondern präzise durch virtuelle Interfaces und Geräte nachgebildet.

2.2.1 Szenariogestaltung

Um aktuelle und insbesondere zukünftige Angriffsszenarien in der Übung abzudecken, wird auf der Stromnetzseite des Szenarios eine Durchsetzung mit erneuerbaren Energien gewählt, die dem voranschreitenden Ausbau entspricht und voraussichtlich in naher Zukunft besondere Relevanz haben wird. Analog wird auf der zugehörigen Kommunikationsseite eine fortgeschrittene Digitalisierung mit einer gegenüber der heutigen Anzahl angebundener Stationen von üblicherweise bis zu 30 Prozent erhöhten Quote fernwirktechnischer Anbindung von Ortsnetzstationen (ONS) angenommen und im Gesamtszenario umgesetzt.

Das resultierende Stromnetz-Szenario basiert auf einem *SimBench*-Mittelspannungsnetz (Meinecke et al., 2020) und umfasst 122 Knoten (Sammelschienen, Ortsnetzstationen), ein Umspannwerk mit zwei Transformatoren und zwei Doppelsammelschienen zur Anbindung an das Hochspannungsnetz, sieben Windparks zwischen 1,5 und 14 MWp, vier Photovoltaik-Anlagen (PV-Anlagen) auf Mittelspannungsebene zwischen 0,075 und 1,42 MWp, eine Biogasanlage mit 540 kWp sowie ein Wasserkraftwerk mit 920 kWp. Die untergeordnete Niederspannungsebene wird aggregiert und abstrahiert im Szenario abgebildet. Eine Übersicht über die Stromnetztopologie findet sich in **Abbildung 1**.

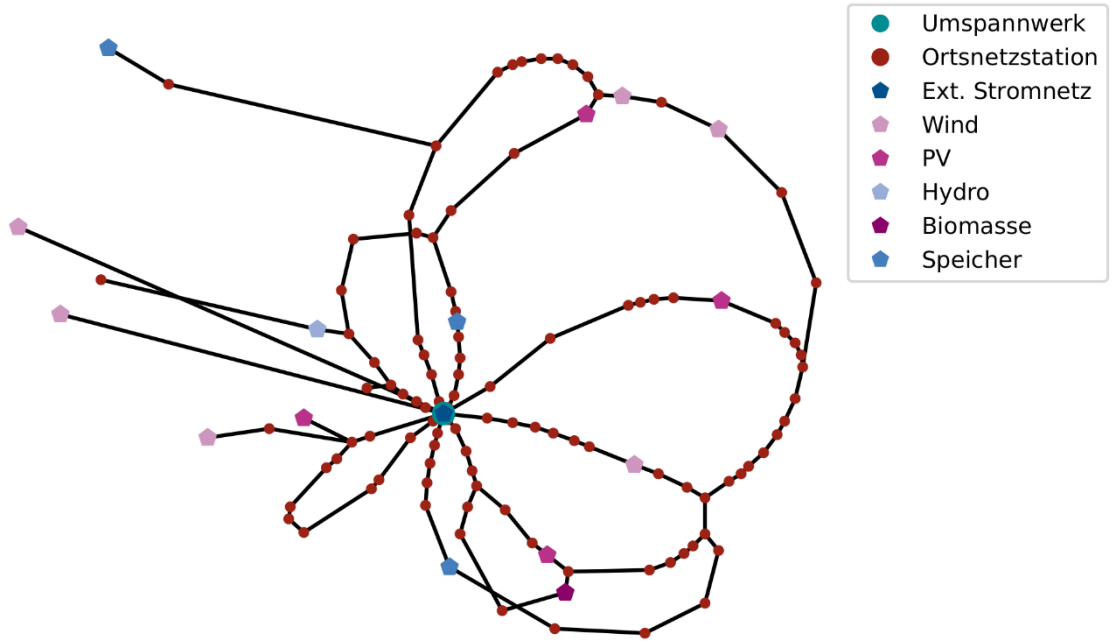

Abbildung 1: Übersicht über die verwendete Stromnetz-Topologie, die auf einem *SimBench*-Mittelspannungsnetz basiert.

Die Topologie besteht aus mehreren geöffneten ringartigen Strukturen, die nach Bedarf geschlossen oder an anderen Stellen geöffnet werden können. Prinzipiell kann im Simulationsmodell jeder Abgang des Umspannwerks und der ONS geschaltet werden. Die Transformatoren des Umspannwerks werden mitsimuliert und sind in der Lage, eine Spannungsregelung mittel *On-Load Tap Changer* (OLTC) durchzuführen.

In der Mittelspannungsebene sind ca. 50 Prozent der Ortsnetzstationen fernwirktechnisch angebunden. Davon können einige ONS lediglich Messwerte übertragen, während andere auch Steuerungsmöglichkeiten bieten. Die Messwerte begrenzen sich hierbei auf die mittelspannungsseitigen Spannungswerte sowie die Strommessung der einzelnen Abgänge, woraus sich auch die bezogene Leistung des unterlagerten Niederspannungsnetzes ergibt. Die Steuerungsmöglichkeiten beziehen sich primär auf das fernwirktechnische Ein- oder Ausschalten der Abgänge und das Einspeisemanagement für mittelspannungsseitige Erzeugungsanlagen. Auch eine Verschiebung von Trennstellen im Mittelspannungsring kann fernwirktechnisch realisiert werden.

Im Gegensatz zu den Erzeugungsanlagen sind Verbraucher nicht steuerbar. Sie verhalten sich entsprechend einer für das Szenario spezifischen realitätsorientierten Lastkurve, die für jeden Verbraucher individuelle Werte vorschreibt. Auch die Erzeugungsanlagen folgen einer entsprechenden Kurve, die für PV- und Windkraftanlagen die eingespeiste Leistung abhängig von Tageszeit und Wetterbedingungen limitiert und für Wasserkraft- und Biogasanlagen einen Fahrplan vorgibt, der durch fernwirktechnische Ansteuerung überschrieben werden kann.

Für die fernwirktechnische Anbindung der Stationen an die Leitwarte, die Anbindung von Nutzerendgeräten sowie die Bereitstellung von IT-Diensten wie Telefonie, Dateiablage, DHCP, DNS oder E-Mail und dem allgemeinen Internetzugang ist auch eine entsprechende Netzwerkinfrastruktur Teil des Übungsszenarios. Sie wird basierend auf den Anforderungen hinsichtlich benötigter IT-Dienste, der fernwirktechnischen Anbindungsdichte und weiterer Faktoren wie des Netzwerksegmentierungslevels durch das Stromnetz-Modellie-

rungs-Tool PowerOwl (Bader, 2024) erstellt. Das resultierende Netzwerk besteht aus den folgenden drei Hauptnetzgebieten:

- *Office-Bereich*, dem Nutzerendgeräte, Server, WLAN-Access-Points und Internetzugang zugeordnet sind
- *OT-Bereich*, der in mehrere Subnetze unterteilt ist und alle Remote Terminal Units (RTUs) umfasst
- *Leitwarten-Bereich*, der, durch eine eigene Firewall geschützt, die Anbindung an den OT-Bereich realisiert

Das Netzwerk umfasst 139 Switche, sechs Router mit Firewall-Funktion, fünf Server sowie 89 RTUs. Ein Schema des resultierenden Netzwerks ist in **Abbildung 2** dargestellt.

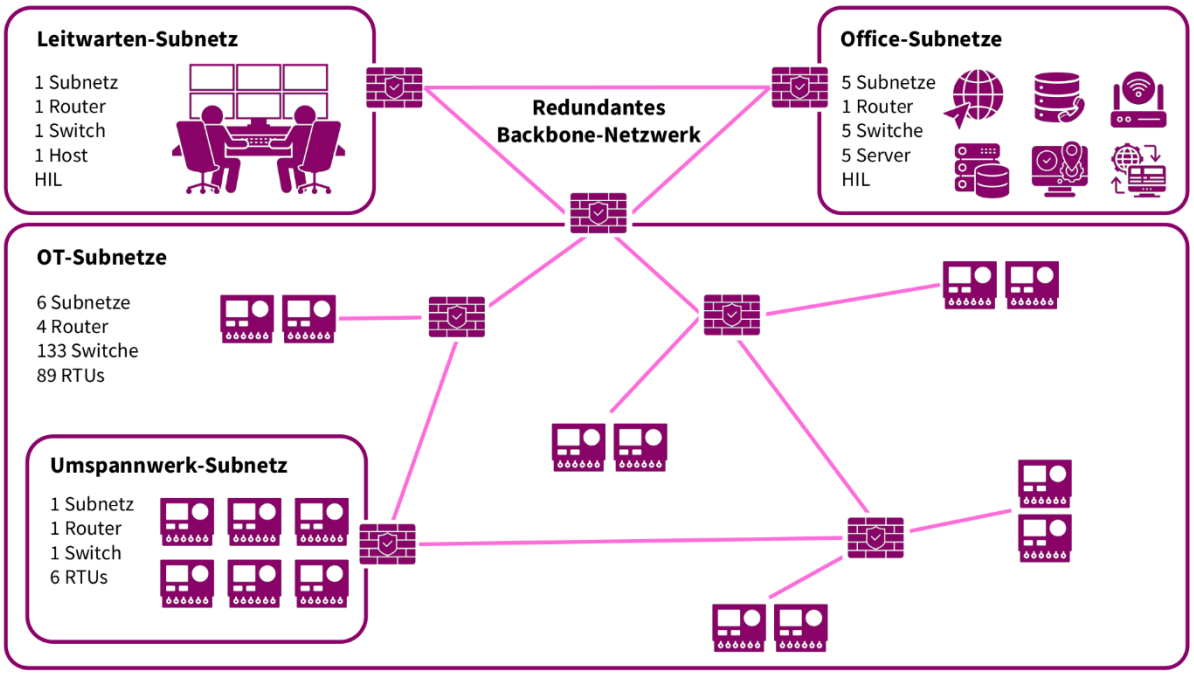

Abbildung 2: Das Kommunikationsnetz umfasst sowohl den Bereich der Leitwarte und den Office-Bereich als auch das klassische OT-Netz. Einige Subnetze enthalten von Beginn an physische Geräte (Hardware in the Loop (HIL)).

2.2.2 Technikkonzept

Das Konzept für die technische Umsetzung der Übung umfasst vier Kernaspekte:

1. **Räumliche Verteilung:** Die Teilnehmerinnen und Teilnehmer werden in die drei Gruppen Management, Leitwarten-Personal und IT/OT-Personal aufgeteilt. Jede dieser Gruppen arbeitet in einem eigenen, abgetrennten räumlichen Bereich. Hierdurch wird ein realistischer Rahmen für die Kommunikation innerhalb der und zwischen den Gruppen geschaffen.
2. **Realistische Dokumentation:** Für jede Gruppe werden Hilfsmittel bereitgestellt, die die gruppenspezifische Arbeit erleichtern und unterstützen. Hierzu zählen beispielsweise Pläne des Stromnetzes und des Kommunikationsnetzes. Diese Dokumentation kann im Verlauf der Übung durch die Teilnehmerinnen und Teilnehmer ergänzt und verändert werden.
3. **Aufgaben- und Aktionskarten:** Während der Übung erhalten die Teilnehmerinnen und Teilnehmer Hilfestellungen, Aufgaben und Hinweise zu Ereignissen in Kartenform. Dieses Table-top-Element erleichtert es den Teilnehmerinnen und Teilnehmern, sich auf relevante Aspekte im Übungsablauf zu fokussieren.
4. **Co-Simulationsumgebung WATTSON:** Um eine realistische Interaktion mit dem fiktiven Szenario zu ermöglichen, kommt die Co-Simulationsumgebung WATTSON (Bader et al., 2023) zum Einsatz, die das Stromnetz und das Kommunikationsnetz sowie ihre Wechselwirkungen realitätsnah abbildet und die Teilnehmerinnen und Teilnehmer in die Simulation einbindet.

Für die Durchführung empfiehlt sich eine räumliche Aufteilung in zwei oder drei Abstufungen. So sollte die Management-Gruppe vorerst in einem separaten Raum untergebracht werden, während die IT/OT-Gruppe sowie die Leitwarten-Gruppe entweder ebenfalls vollständig getrennt arbeiten oder gemeinsam einen größeren Bereich nutzen können, der durch Raumtrenner die Aufteilung der Gruppen in separate Raumbereiche ermöglicht und dennoch eine direkte Kommunikation zwischen den beiden Gruppen fördert. Bei Bedarf sollte ebenfalls die Möglichkeit für die Management-Gruppe bestehen, den Krisenstab räumlich näher an die technischen Gruppen zu verlegen, falls sie dies für vorteilhaft befindet.

Um insbesondere den technisch-orientierten IT/OT- und Leitwarten-Gruppen die Einarbeitung in die Systeme des fiktiven Verteilnetzbetreibers zu erleichtern, steht ihnen eine entsprechende Dokumentation zur Verfügung, die vorab von den Übungsorganisatoren erstellt und zu Beginn der Übung besprochen wird. Weiterhin helfen Aufgaben- und Aktionskarten, die Übung sowie den Fokus der Teilnehmerinnen und Teilnehmer zu steuern und bedarfsabhängig zusätzliche Hinweise zu geben.

Die Co-Simulationsumgebung WATTSON ist die Grundlage für die realitätsnahe Umsetzung der Übung. WATTSON simuliert das Stromnetz basierend auf seiner aktuellen Topologie und der Konfiguration einzelner Assets wie Lasten und Erzeuger. Weiterhin wird das Kommunikationsnetz bis auf ISO/OSI-Schicht 2 (Ethernet) nachgebildet. Diese Netzwerkemulation ermöglicht Echtzeitkommunikation unter Nutzung normaler Netzwerkprotokolle und erlaubt zudem das Einbinden physischer Geräte wie Laptops, WLAN-Access-Points oder auch Systemen zur Angriffserkennung. WATTSON bildet Fernwirkgeräte als Linux-basierte Hosts ab und verknüpft diese mit der Stromnetzsimulation. So wirken sich Stellbefehle direkt auf das Stromnetz aus und alle übermittelten Messwerte entsprechen den realistischen Werten aus der Simulation. WATTSON erlaubt auch die Umsetzung echter Angriffe, sodass die Teilnehmerinnen und Teilnehmer einerseits mit bereits gegen echte Stromnetze durchgeführten Angriffen konfrontiert werden können, andererseits auch realistische Gegenmaßnahmen mit gängigen Programmen und Tools umsetzen können.

2.3 Krisenfallübung: Normalbetrieb, Störungen und Cyberangriff

Während der Krisenfallübung werden die Teilnehmerinnen und Teilnehmer mit diversen Situationen konfrontiert, die entweder zum Normalbetrieb gehören, eine Störung als Ursache haben oder direkte Folge des Cyberangriffs sind. Zu Beginn der Übung überwiegen Aufgaben zum Normalbetrieb, beispielsweise die Bearbeitung von geplanten Wartungsarbeiten an Trafostationen oder Leitungen. Im Verlauf der Übung werden zudem Störungen wie das Ausfallen von OT-Diensten oder ganzen Geräten verursacht, die eine Zusammenarbeit insbesondere der IT/OT-Gruppe und der Leitwarten-Gruppe erfordern und unterstreichen, dass nicht jede Abweichung vom Normalbetrieb das Resultat eines Cyberangriffs sein muss. Bei OT-Störungen sind die Effekte vor allem für die Leitwarten-Gruppe sichtbar. Die Behebung der Störung fällt allerdings in den Kompetenzbereich der IT/OT-Gruppe. Ein konzeptuell wichtiger Aspekt ist die mögliche Kommunikation mit der Management-Gruppe, da aufgrund der durch die Übung hervorgerufenen erhöhten Sensibilität für Zwischenfälle auch Störungen als Angriffe und andersherum identifiziert werden könnten. Mit dem Fortschreiten der Übung beginnt der eigentliche Cyberangriff, der IT- und OT-seitig das Kommunikationsnetzwerk nutzt, um Informationen zu sammeln, das Netzwerk zu stören und schließlich die Stromversorgung zu beeinträchtigen. Die Bewältigung dieser Situation erfordert eine intensive Kommunikation zwischen den verschiedenen Gruppen, um aktuelle Erkenntnisse miteinander zu teilen, die einzelnen Gruppen zu sensibilisieren, Gegenmaßnahmen zu koordinieren und die anderen Gruppen über bereits getroffene Gegenmaßnahmen mitsamt ihren Folgen – beispielsweise der Einschränkung von IT/OT-Diensten – zu informieren. Für die Bewältigung der Ereignisse und Aufgaben während der gesamten Krisenfallübung stehen den Teilnehmerinnen und Teilnehmern verschiedene Möglichkeiten zur Verfügung, die von inhaltlichen Hilfestellungen bis zu technischen Detektions- und Reaktionsmöglichkeiten reichen, die im Folgenden erläutert werden.

2.4 Detektions- und Reaktionsmöglichkeiten

Um den Teilnehmerinnen und Teilnehmern die Möglichkeit zu bieten, Auffälligkeiten, Störungen und Angriffe im Netzwerk zu erkennen, zu untersuchen und zu beheben, stehen ihnen mehrere Detektions- und Reaktionsmöglichkeiten zur Verfügung.

Als Unterstützung bei der Detektion von Angriffen wird der IT/OT-Gruppe auf der Netzwerkebene ein kommerzielles System zur Angriffserkennung zur Verfügung gestellt, das ins Netzwerk eingebunden und konfiguriert werden kann. Richtig platziert und konfiguriert, lassen sich so insbesondere unbekannte Netzwerkgeräte, auffälliger Netzwerkverkehr und neue Kommunikationskanäle entdecken. Für EnerCise II wird der *Industrial Protector* von Rhebo genutzt.

Auch in der virtuellen Leitwarte (VCC) von WATTSON werden dem Leitwarten-Personal Auffälligkeiten, Störungen und Ausfälle gemeldet. Diese Meldungen umfassen sowohl Informationen zum Zustand des Stromnetzes und der Stromversorgung wie beispielsweise Hinweise zu überlasteten Leitungen oder Abweichungen von der Sollspannung an einzelnen Stationen als auch Informationen zum Kommunikationsnetz (vgl. **Abbildung 3**). So wird das Leitwarten-Personal bei Verbindungsabbrüchen gewarnt und auch das Ausbleiben von erwarteten Meldungen wird grafisch in der Leitwarten-Umgebung hervorgehoben.

Dienste und Geräte in WATTSON stellen zudem Log-Dateien bereit, die durch fachkundiges IT/OT-Personal zur näheren Analyse von Auffälligkeiten genutzt werden können. Beispielsweise protokollieren Fernwirkgeräte alle Verbindungsversuche sowie durchgeführte fernwirktechnische Schalthandlungen. Auch gescheiterte oder erfolgreiche Zugriffe über Secure Shell (SSH) werden protokolliert und können unter anderem Hinweise

auf Angriffe liefern. Zusätzlich steht auf allen Geräten ein Tool zum Mitschneiden und zur Analyse von Netzwerkverkehr zur Verfügung.

Auf der Meta-Ebene hat die Management-Gruppe die Möglichkeit, Hinweise auf Angriffe und Störungen sowohl durch interne als auch durch externe Kommunikation zu erhalten. Im Rahmen von EnerCise II werden die Rollen der Kunden, Behörden und Angreifer durch die Übungsorganisatoren übernommen, wodurch eine externe Kommunikation ermöglicht wird.

Auch die Reaktionsmöglichkeiten unterscheiden sich zwischen den einzelnen Ebenen und Gruppen und sollen durch die Teilnehmerinnen und Teilnehmer präventiv kommuniziert und reaktiv koordiniert werden, um Störungen und Angriffe effektiv einzudämmen und aufzuarbeiten.

Die Management-Gruppe hat hier insbesondere organisatorische Maßnahmen für die interne Koordinierung des weiteren Vorgehens zur Verfügung. Das Festlegen von Rollen und Verantwortlichkeiten ist spätestens im Krisenfall unabdingbar. Auch die Kommunikation mit externen Akteuren ist eine reaktive Maßnahme auf der Meta-Ebene und explizit Teil der Angriffsbewältigung.

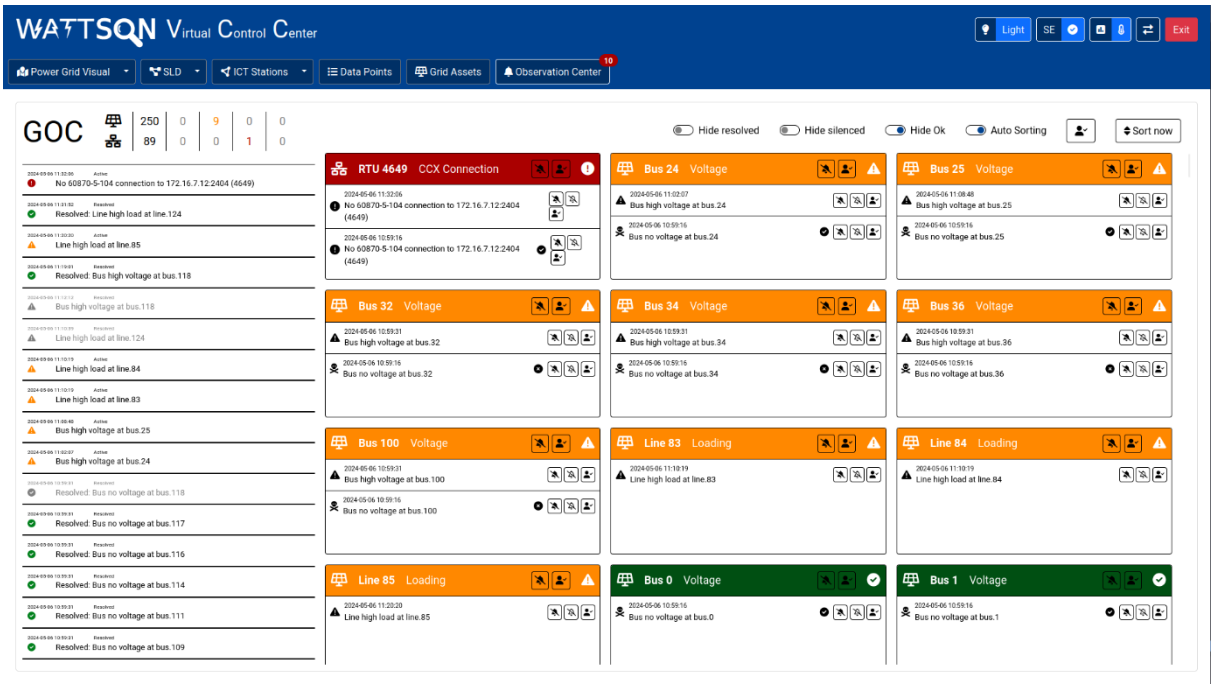

Abbildung 3: Im „Observation Center“ der virtuellen Leitwarte von WATTSON wird das Leitwarten-Personal über relevante Ereignisse sowie über den Zustand von Stromnetz und Kommunikationsnetz informiert.

Auf der Netzwerkebene der IT/OT-Gruppe umfassen die Reaktionsmöglichkeiten unter anderem die Netzwerksegmentierung (beispielsweise eine IT/OT-Trennung), die gezielte Konfiguration von Firewall-Regeln an mehreren Netzwerkknoten, das Starten, Stoppen und Umkonfigurieren diverser Dienste wie der fernwirktechnischen Kommunikation, das Etablieren alternativer Kommunikationspfade sowie die Vor-Ort-Analyse mithilfe virtueller Techniker, deren Rolle die Übungsorganisatoren einnehmen.

Für das Leitwarten-Personal bieten sich einerseits organisatorische Reaktionsmaßnahmen wie das Priorisieren von Aufgaben und andererseits technische Maßnahmen wie aktive Schalthandlungen oder auch der manuelle Vor-Ort-Betrieb einzelner Stationen an. Lasten und Erzeugungsanlagen können abgeworfen werden, um Überlastungen und Spannungsabweichungen entgegenzuwirken. Weiterhin kann die eingespeiste

Leistung durch aktives Einspeisemanagement reguliert werden. Auch ein vermaschter Betrieb des Netzes zu Redundanz- und Überlastschutzzwecken ist möglich. Maßnahmen wie die Umstellung auf einen manuellen Betrieb vor Ort oder das explizite Deaktivieren von fernwirktechnischen Steuerbefehlen müssen mit der IT/OT-Gruppe koordiniert werden.

Insgesamt steht den Teilnehmerinnen und Teilnehmern eine Vielzahl von Möglichkeiten zur Verfügung, um eine Krisensituation zu erkennen und angemessen zu reagieren. Insbesondere die Kombination aus technischen und organisatorischen Maßnahmen und den verschiedenen Möglichkeiten der einzelnen Gruppen erlaubt eine realistische Übung und unterstreicht den Fokus auf die Kommunikation innerhalb der und zwischen den Gruppen.

2.5 Gruppenspezifische Aufgaben und individuelle Lernziele

Besondere Alleinstellungsmerkmale der Cybersicherheitsübung EnerCise II sind die Einbeziehung aller wesentlichen Akteure eines Netzbetreibers sowie der Fokus auf deren Kommunikation und die gruppenübergreifende Koordination und Kooperation. Die Grundlage für diese Kooperation bilden die Kernkompetenzen der jeweiligen Gruppen, die im Konzept in allgemeine Aufgaben und Verantwortlichkeiten, gruppenspezifische Aufgaben zu Beginn der Übung im Normalbetrieb sowie konkrete Handlungsoptionen während des Cyberangriffs unterteilt werden. Im Folgenden werden diese Aspekte für jede der drei Gruppen erläutert.

2.5.1 Management

Die Management-Gruppe umfasst Personen, die sich vorwiegend mit organisatorischen Aspekten und solchen Aspekten befassen, die der Unternehmensführung dienen.

Allgemeine Aufgaben und Verantwortlichkeiten

Operativen Betrieb des Verteilnetzes sicherstellen: Es sollen klare Prozesse und Verfahren zur effektiven Koordination und Fehlerbehebung bei Störungen und Cyberangriffen festgelegt werden. Hierzu gehört auch die regelmäßige Überprüfung der Betriebs- und Cybersicherheitskonzepte, um auf potenzielle Bedrohungen vorbereitet zu sein.

Risikomanagement und Investitionsentscheidungen: Das Management soll mit Unterstützung der anderen Gruppen eine spezifische Risikobewertung durchführen, um die Prioritäten für Investitionen in Cybersicherheit festzulegen. Dabei ist es wichtig, klare Kriterien zu entwickeln, um die Entscheidungsfindung bei der Zuweisung von Ressourcen zu unterstützen.

Stakeholder-Kommunikation und Krisenmanagement: Kommunikation ist eine der Hauptaufgaben dieser Gruppe. Zum einen bedeutet dies externe Kommunikation mit Kunden, Behörden und der Presse. Zum anderen schließt es die interne Kommunikation mit ein, insbesondere für eine Krisenfallsituation. Außerdem ist die Management-Gruppe gegenüber der Geschäftsleitung für alle Erfolge und Misserfolge verantwortlich.

Gruppenspezifische Aufgaben bei Beginn der Übung

Die Hauptaufgabe der Management-Gruppe ist die Koordination der anderen Gruppen und der internen und externen Kommunikation. Es ist daher wichtig, dass frühzeitig entsprechende Kommunikationsprozesse für den Normal- und den Notfallbetrieb etabliert werden. Ein essenzieller Schritt dazu ist die Ernennung einer Teamleitung bzw. von Schnittstellenpersonal in den anderen Gruppen, die die Kommunikation mit der

Management-Gruppe übernehmen. Weitere mögliche Maßnahmen sind unter anderem auch die Einrichtung regelmäßiger Meetings sowie die Festlegung der Kommunikationskanäle je nach Dringlichkeit und Situation. Außerdem können Verantwortlichkeiten innerhalb der eigenen Gruppe fest verteilt werden.

Im Übungsszenario ist das existierende Präventionskonzept des Netzbetreibers für die Cybersicherheit in die Jahre gekommen. In den letzten Jahren wurden kaum noch Investitionen in die Erhöhung der Cybersicherheit getätigt. Daher muss das vorhandene Präventionskonzept überarbeitet, verbessert und modernisiert werden. Dies umfasst folgende Arbeitsschritte:

1. *Bestandsaufnahme:* Welche organisatorischen und technischen Maßnahmen werden im Präventionskonzept bereits berücksichtigt? Da die vorliegende Dokumentation unvollständig ist, muss die Management-Gruppe mithilfe der anderen Gruppen die Bestandsaufnahme vervollständigen.
2. *Identifikation von Schwachstellen und Verbesserungsvorschläge:* Basierend auf der Bestandsaufnahme muss überprüft werden, an welchen Stellen im Präventionskonzept noch Nachbesserungsbedarf besteht. Es müssen konkrete organisatorische und technische Maßnahmen für das überarbeitete Präventionskonzept vorgeschlagen werden.
3. *Krisenstab und Verantwortlichkeiten während eines Cyberangriffs:* Für den Fall eines Cyberangriffs muss geplant werden, wer welche Aufgaben übernimmt und wie eine effektive Kommunikation innerhalb der und zwischen den Gruppen sichergestellt wird. Dies kann auch die Bildung eines Krisenstabs beinhalten, der im Krisenfall unter der Führung einer oder mehrerer Personen die Krisensituation bewertet und ihre Aufarbeitung vorantreibt.
4. *Umsetzung des Präventionskonzepts*: Durch ein begrenztes Budget können typischerweise nicht alle neuen Maßnahmen auf einmal umgesetzt werden. Daher muss eine Priorisierung stattfinden. Um die Umsetzung der beschlossenen Maßnahmen zu planen, ist eine Abstimmung mit den anderen Gruppen notwendig.

Handlungsoptionen während des Cyberangriffs

Die Handlungsoptionen der Management-Gruppe unterteilen sich in die folgenden Hauptaspekte:

Meldung des Cybersicherheitsvorfalls an das BSI: Ein Cybersicherheitsvorfall muss umgehend an das BSI gemeldet werden. Dabei müssen folgende Schritte beachtet werden:

1. *Cybersicherheitsvorfall identifizieren und bewerten:* Zuerst muss der Vorfall identifiziert und bewertet werden, um festzustellen, ob es sich um einen meldepflichtigen Vorfall handelt.
2. *Meldung an das BSI:* Bei Vorliegen eines meldepflichtigen Vorfalls muss dieser unverzüglich an das BSI gemeldet werden. Die Meldung erfolgt über ein BSI-Meldeformular. Dabei sollen möglichst alle relevanten Informationen zum Vorfall bereitgestellt werden, einschließlich des Umfangs, der Auswirkungen und der durchgeführten Maßnahmen.
3. *Gegebenenfalls Zusammenarbeit mit dem BSI:* Der Netzbetreiber sollte eng mit dem BSI zusammenarbeiten, um den Vorfall zu untersuchen, weitere Schritte zu seiner Bewältigung zu planen und unter Umständen Empfehlungen des BSI umzusetzen.
4. *Maßnahmen zur Schadensbegrenzung und zur Behebung des Sicherheitsvorfalls:* Parallel zur Meldung an das BSI sollte das betroffene Unternehmen interne Maßnahmen zur Schadensbegrenzung und zur Behebung des Sicherheitsvorfalls einleiten. Dazu gehören die Isolierung des Vorfalls, die Wieder-

herstellung von Systemen und Daten sowie die Implementierung zusätzlicher Sicherheitsmaßnahmen. Hierfür ist die Zusammenarbeit mit den anderen Gruppen unabdingbar.

5. *Dokumentation:* Es ist wichtig, den gesamten Prozess der *Incident Response*, einschließlich der Meldung an das BSI, detailliert zu dokumentieren. Dies hilft bei der Nachverfolgung und Analyse des Vorfalls sowie bei der Vorbereitung auf mögliche zukünftige Sicherheitsvorfälle.

Kommunikation mit der Öffentlichkeit (Kunden und Presse): Das Management muss entscheiden, wann welche Informationen über den Cybersicherheitsvorfall nach außen getragen werden und wie zu bereits bekannt gewordenen Informationen Stellung bezogen werden soll. Dazu gehören beispielsweise Pressemitteilungen und die Kommunikation mit Kunden oder der Politik. Weiterhin muss entschieden werden, welche Informationen aus gutem Grund noch zurückgehalten werden. Die Mitarbeiterinnen und Mitarbeiter müssen entsprechend angewiesen werden.

Organisation und Überwachung der internen Kommunikation: Während des Cyberangriffs muss das Management überwachen, ob die interne Kommunikation gemäß Präventionskonzept umgesetzt wird, und gegebenenfalls nachsteuern. Dies ist insbesondere notwendig, wenn die Kommunikationsinfrastruktur ebenfalls von dem Cyberangriff betroffen ist. In diesem Fall sollte das Management unter Zeitdruck ein Konzept für eine alternative Kommunikation erstellen, bis die vorhandene Kommunikationsinfrastruktur wiederhergestellt ist. Beispielsweise können regelmäßige Meetings oder die Nutzung alternativer Kommunikationskanäle hilfreich sein.

Übersicht und Deeskalation: In der Kommunikation sowohl nach außen als auch nach innen sollte die Management-Gruppe Souveränität bewahren. Investigative oder offen antagonistische Vertreter der Presse könnten versuchen, in (Telefon-)Interviews Informationen zu erhalten, die nicht für die Öffentlichkeit freigegeben sind, odervermeintliche Widersprüche in der präsentierten Storyline zu finden. Hier ist es wichtig, den Überblick zu behalten und die richtige Balance zwischen Schweigen und Transparenz zu finden. Auch intern können aufgeregte Führungskräfte im Kontakt zur Management-Gruppe sogar konfrontativ agieren, da finanzielle oder Reputationsschäden zu erwarten sind, sodass eine Deeskalation hier ebenfalls wichtig ist.

Ressourcen-Management und externe Dienstleistungen: Das Management kann auf Beschäftigte im Außendienst zurückgreifen, um die Gegebenheiten vor Ort überprüfen zu lassen. Es kann externe Dienstleister für Unterstützungsmaßnahmen beauftragen. Allerdings muss das Management bei begrenzten Ressourcen und einem begrenzten Budget entscheiden, wann welche internen oder externen Dienstleistungen beauftragt werden.

Schadensbegrenzung und Wiederherstellung des Normalbetriebs: Um die Auswirkungen eines Cyberangriffs abzumildern, müssen unter Umständen Maßnahmen ergriffen werden, die den laufenden Betrieb des Verteilnetzes beeinflussen, beispielsweise die Abschaltung von Geräten und Komponenten. Hier ist es Aufgabe des Managements, vorhandene Handlungsoptionen mithilfe der anderen Gruppen abzuwägen und zu einer Entscheidung zu gelangen. Gleichermaßen ist es Aufgabe des Managements, in Abstimmung mit den anderen Gruppen zu entscheiden, wann nach einem Cyberangriff der Normalbetrieb wieder aufgenommen werden kann.

Nachbereitung des Cyberangriffs: Abschließend sollten auf Management-Ebene Lehren aus dem Cyberangriff gezogen werden. Dies umfasst eine kritische Analyse des Präventionskonzepts, um mögliche Schwachstellen zu identifizieren, die den Cyberangriff ermöglicht haben. Es muss auch das Verhalten während des Cyberangriffs aufgearbeitet werden, um auf zukünftige Cyberangriffe besser reagieren zu können.

2.5.2 Leitwarten-Personal

Das Leitwarten-Personal ist für den operativen Betrieb des Stromnetzes zuständig. Hierzu zählen die Aufrechterhaltung der Stromversorgung sowie die sichere Durchführung von technischen Arbeiten.

Allgemeine Aufgaben und Verantwortlichkeiten

Überwachung und Steuerung: Das Leitwarten-Personal ist für die Überwachung und Steuerung des Stromnetzes verantwortlich. Dies umfasst die Überprüfung von Lastflüssen und Spannungsniveaus sowie die Sicherstellung eines stabilen Betriebs. Bei Unregelmäßigkeiten oder Ausfällen muss es schnell und effizient reagieren.

Koordination von Wartungsarbeiten: Das Personal ist für die Durchführung und Koordination von geplanten Wartungsmaßnahmen verantwortlich. Hierzu gehören insbesondere die Koordination mit den Technikern vor Ort und die Durchführung der geplanten Freischaltmaßnahmen.

Dokumentation und Berichterstattung: Alle Vorfälle, Störungen und Maßnahmen müssen präzise dokumentiert werden, um sowohl für interne Analysen und Trainings als auch zur Einhaltung gesetzlicher Vorgaben zu dienen. Diese Vorgaben umfassen die genaue Aufzeichnung und Berichterstattung von Ereignissen im Einklang mit gesetzlichen Regelungen.

Gruppenspezifische Aufgaben bei Beginn der Übung

Netzführung: Während der gesamten Übung ist die Netzführung – in Normalsituationen, in Problemsituationen und bei Angriffsauswirkungen – das oberste Ziel für das Leitwarten-Personal. Hierzu zählen insbesondere die Steuerung von Anlagen, die Konzipierung und Umsetzung von Topologie-Veränderungen, die Überwachung des Netzzustands und die Umsetzung angemessener Maßnahmen im Angriffsfall. Zu Beginn der Übung können die Teilnehmerinnen und Teilnehmer die verwendete Leitwarten-Umgebung sowie die Interaktions- und Analysemöglichkeiten genauer kennenlernen. Auch übliche Aufgaben des Leitwarten-Personals – beispielsweise Leitungswartungen – fallen bereits zu Beginn der Übung an. Hierbei besteht die Möglichkeit, „normale“ betriebliche Fehlfunktionen, wie das Nichtreagieren einer dezentralen Erzeugungsanlage auf ein Steuersignal, zu simulieren, um so Reaktionsoptionen auch im Falle eines Cyberangriffs zu erproben.

Präventive Optimierung: Die Teilnehmerinnen und Teilnehmer haben Gelegenheit, das Netz zu studieren und gegebenenfalls präventiv Maßnahmen zu ergreifen, um die Netzstabilität zu optimieren. Dazu gehört auch, die Reaktion auf mögliche Störungen vorzubereiten. Die Identifizierung von Rückfallplänen im Falle eines Ausfalls der Leittechnik ist hierbei ein erster Schritt. Auch die Sicherstellung der Verfügbarkeit des Netzplans im Falle des Ausfalls des Leitsystems ist ein weiterer wichtiger Schritt, um weiterhin koordinierende Aufgaben übernehmen zu können. Hier sollten auch die für den Betrieb neuralgischen Punkte im Netz identifiziert werden, um bei der Koordination und Priorisierung von Maßnahmen unterstützen zu können. Diese Maßnahmen können von Personal vor Ort umgesetzt werden oder es wird nur die Reihenfolge von Wiederanfahrmaßnahmen von Leittechnik vorgegeben. Einige Maßnahmen müssen mit den anderen Gruppen koordiniert werden.

Handlungsoptionen während des Cyberangriffs

Detektion von Cyberangriffen und Problemsituationen: Ein besonderes Lernziel ist die Unterscheidung von allgemeinen Problemsituationen – beispielsweise Engpässen, Störungen und Defekten – und Cyberangriffen. Um angemessene Reaktionen umsetzen zu können, ist diese Unterscheidung sehr wichtig und in gewissen

Situationen sogar Voraussetzung dafür, keine fehlgeleiteten Maßnahmen zu ergreifen. Eine der Herausforderungen für das Leitwarten-Personal ist es, aus der Vielzahl an einlaufenden Meldungen und Informationen die wichtigsten zu identifizieren und korrekt auf sie zu reagieren. Insbesondere in der Situation eines Cyberangriffs wird diese Herausforderung noch größer, da gegebenenfalls falsche und irreführende Meldungen aussortiert werden müssen und relevante Ereignisse sich unter der Flut an Meldungen mit derselben unterlagerten Ursache verstecken können. Somit ist die *Root-Cause-Analyse* für die effiziente Eindämmung der Auswirkungen des Angriffs unabdinglich.

Interne Kommunikation: Eine weitere Aufgabe ist die interne Kommunikation sowohl mit dem IT-Personal als auch mit dem Management. Hierbei sollte darauf geachtet werden, dass die Kommunikation auch proaktiv erfolgt, um auf Auffälligkeiten hinzuweisen. Neben der Wichtigkeit der Kommunikation sollte jedoch auch berücksichtigt werden, dass die operativen Aufgaben in der Regel von höherer Priorität sind. Dennoch sollen gewonnene Erkenntnisse festgehalten und kommuniziert werden, um zukünftige Vorfälle besser zu bewältigen. Genau wie im Normalbetrieb gehört auch während des Angriffs die Dokumentation von Maßnahmen und Ereignissen zu den Aufgaben der Leitwarte. Hierbei müssen Lösungen gefunden werden, diese Maßnahmen im Zweifelsfall auch außerhalb des Leitsystems durchführen zu können.

Eindämmung von Angriffsauswirkungen: Im Angriffsfall soll das Leitwarten-Personal aktiv an der Eindämmung und Aufarbeitung mitarbeiten. Hierzu zählen die Umsetzung von operativen Maßnahmen zur Sicherstellung eines möglichst störungsfreien Netzbetriebs sowie die Koordination und Kommunikation mit dem Management und dem IT-Personal. Mit Letzterem sollten insbesondere forensische Maßnahmen durchgeführt werden, um die Angriffsursache domänenübergreifend zu identifizieren. Eine Handlungsoption des Betriebspersonals ist die Identifikation von neuralgischen Stationen, um diese dann mit Personal vor Ort zu besetzen. Nachdem die akute Angriffssituation bewältigt ist, soll der Normalzustand wiederhergestellt werden.

Koordination des Betriebs: Im Angriffsfall muss weiterhin der Stromnetzbetrieb bestmöglich aufrechterhalten werden. Hierzu muss das Leitwarten-Personal entsprechende Maßnahmen ergreifen. Die Priorisierung von Aufgaben steht hierbei besonders im Fokus. So können beispielsweise routinemäßige Wartungen abgelehnt oder verschoben werden, um den Betrieb sicherzustellen.

2.5.3 IT/OT-Personal

Die IT/OT-Gruppe betreibt und verwaltet die IT- und OT-Infrastruktur. Sie ist für deren Betrieb zuständig und soll Sicherheitsmaßnahmen konzipieren und umsetzen sowie auf Störungen und Angriffe reagieren.

Allgemeine Aufgaben und Verantwortlichkeiten

Ordnungsgemäßen Betrieb der IT/OT-Infrastruktur sicherstellen: Die Hauptaufgabe des IT/OT-Personals ist die Sicherstellung des ordnungsgemäßen Betriebs der gesamten IT- und OT-Infrastruktur. Dies umfasst die kontinuierliche Überwachung der Infrastruktur, regelmäßige Wartungsarbeiten und alle technischen Maßnahmen zur Behebung von Ausfällen und Fehlfunktionen.

Gruppenspezifische Aufgaben bei Beginn der Übung

Überblick und Bestandsaufnahme: Zu Beginn der Übung sollte sich das IT-Personal zunächst einen Überblick über die vorhandene IT/OT-Infrastruktur verschaffen, um einen ordnungsgemäßen Betrieb sicherstellen zu können. Insbesondere sollte das IT/OT-Personal das Management bei der Erstellung des Präventionskon-

zepts unterstützen, indem es alle Fragen zum Ist-Zustand der IT/OT-Infrastruktur beantwortet oder die entsprechenden Informationen einholt. Später sollte das IT/OT-Personal prüfen, wie die neu vorgeschlagenen Maßnahmen des Präventionskonzepts umgesetzt werden können und sie, sofern möglich, unverzüglich durchführen.

Detektion von Cyberangriffen: Das IT/OT-Personal sollte dazu beitragen, dass Cyberangriffe möglichst frühzeitig erkannt werden können. Dazu gehören beispielsweise die Auswertung von Meldungen des Angriffserkennungssystems und Nachforschungen bei ungewöhnlichem Verhalten in der IT/OT-Infrastruktur. Des Weiteren sollte das IT/OT-Personal Meldungen zu ungewöhnlichem Verhalten von anderen Gruppen ernst nehmen, zum Beispiel wenn aus der Leitwarte ein Gerät nicht mehr angesteuert werden kann. Es sollte untersucht werden, ob es sich dabei um eine technische Fehlfunktion oder einen Cyberangriff handelt.

Interne Kommunikation: Alle zuvor benannten Punkte können nur durch eine enge Kommunikation mit dem Leitwarten-Personal und dem Management effizient behandelt werden. Außerdem brauchen diese Gruppen für ihre Aufgaben die Expertise des IT/OT-Personals. Daher sollte das IT/OT-Personal großen Wert auf eine effiziente Kommunikation mit anderen Gruppen legen und insbesondere interne Rollen und Verantwortlichkeiten dafür festlegen.

Handlungsoptionen während des Cyberangriffs

Forensik von Cyberangriffen: Eine Hauptaufgabe des IT/OT-Personals nach der Erkennung eines potenziellen Cyberangriffs ist die umfassende Aufklärung und Untersuchung des Vorfalls. Hierbei geht es, anders als beim Leitwarten-Personal, vor allem darum, zu verstehen, welche Systeme und Komponenten von dem Angriff betroffen sind und welche Sicherheitslücken ausgenutzt wurden. Ziel ist es, durch eine gründliche Analyse von Netzwerkverkehr und Log-Dateien das genaue Ausmaß des Cyberangriffs zu verstehen, um dann gezielte Gegenmaßnahmen einleiten zu können.

Eindämmung des Cyberangriffs: Nachdem der Cyberangriff identifiziert und sein Ausmaß verstanden wurde, müssen die Folgen des Angriffs gezielt eingedämmt werden. Hier ist das IT/OT-Personal für die Identifizierung von sinnvollen Maßnahmen und, nach Rücksprache mit den anderen Gruppen, für ihre Umsetzung zuständig.

Bereinigung der Systeme und Steigerung der Resilienz: Um den Normalbetrieb wieder aufnehmen zu können, müssen alle vom Cyberangriff betroffenen Systeme bereinigt und Maßnahmen ergriffen werden, um Folgeangriffe zu verhindern. Hierzu sollte das IT/OT-Personal eigene Maßnahmen zur Erhöhung der Resilienz vorschlagen, wie beispielsweise die Erweiterung von Firewall-Regeln. Sofern möglich, sollten diese Maßnahmen, nach Rücksprache mit den anderen Gruppen, unmittelbar umgesetzt werden.

3 Ablauf der Krisenfallübung

Im Folgenden wird der tatsächliche Ablauf der Cybersicherheitsübung EnerCise II am 24. April 2024 im Future Energy Lab der dena beschrieben. Hierbei werden neben dem allgemeinen Ablauf auch konkrete Einsichten in die einzelnen Gruppen gegeben. Zur Übung waren ursprünglich 14 Personen angemeldet, es nahmen elf Personen teil.

3.1 Allgemeiner Ablauf

Im Vorlauf zur praktischen Präsenzübung fand ein digitaler Workshop statt, in dem den Teilnehmerinnen und Teilnehmern der angedachte Übungsablauf vorgestellt wurde, theoretische Grundlagen zum Thema Cybersicherheit vermittelt wurden und eine Einführung in die verwendete Übungsumgebung WATTSON gegeben wurde. Der Workshop fand in der Woche vor der praktischen Übung statt.

Der allgemeine Ablauf der praktischen Übung folgte dem im Konzept erstellten Ablaufplan. Die zeitliche Struktur ist in der folgenden Abbildung zusammengefasst und beinhaltet die im Konzept vorgesehenen Aufgaben und Handlungsoptionen.

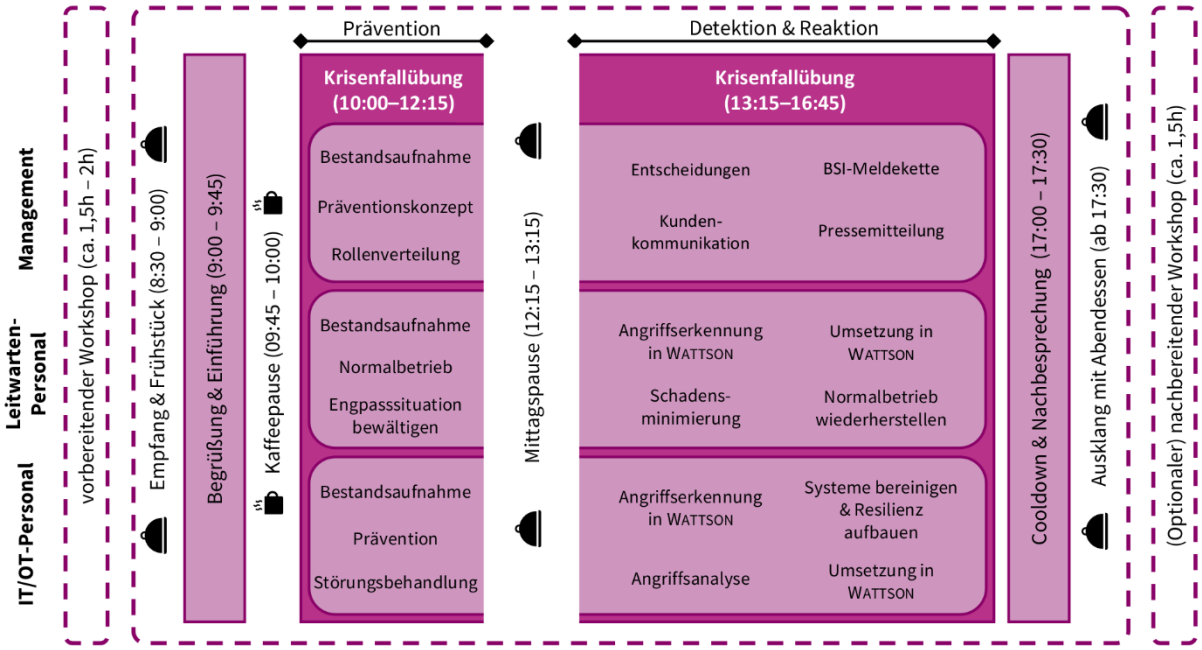

Abbildung 4: Am Übungstag unterteilte sich die praktische Übung in eine Einarbeitungs- und eine Präventionsphase sowie eine Phase, in der sich die Teilnehmerinnen und Teilnehmer mit dem Cyberangriff konfrontiert sahen.

Die Krisenfallübung unterteilte sich konzeptionell in zwei Hauptaspekte: die Einarbeitungs- und Normalbetriebsphase sowie die Cyberangriffsphase. Um die Teilnehmerinnen und Teilnehmer auf die praktische Aufgabe vorzubereiten, fand einige Tage vor der Übung ein vorbereitender Online-Workshop statt, in dem Ablauf, Grundszenario und einige Inhalte zur Cybersicherheit in Stromnetzen vorgestellt wurden. Diese Inhalte wurden am Übungstag im Zuge der Einführung zusammengefasst.

Während der ersten praktischen Phase hatten die Teilnehmerinnen und Teilnehmer die Möglichkeit, sich mit der Übungsumgebung vertraut zu machen, erste präventive Maßnahmen (z. B. das Konfigurieren von Firewalls und die Erarbeitung von Krisenplänen) zu ergreifen und Aufgaben zu erfüllen, die im Normalbetrieb anfallen (z. B. das Freischalten von Leitungen zu Wartungszwecken). Die Teilnehmerinnen und Teilnehmer sahen sich auch mit gezielt herbeigeführten Störungen von OT-Geräten und zugehörigen Diensten konfrontiert. Die konkreten Maßnahmen und Aufgaben sind in Abschnitt 3.2 im Detail erläutert.

In der zweiten Phase wurden die Teilnehmerinnen und Teilnehmer mit einem Cyberangriffsszenario konfrontiert, das auf zwei im OT-Netzwerk eingebrachten Fremdgeräten basierte. Es bestand im Wesentlichen aus vier Stufen:

1. **Reconnaissance:** Scan aller gefundenen Subnetze auf aktive Hosts sowie potenzielle Dienste.
2. **Lateral Movement:** Hosts, auf denen ein SSH-Dienst erkannt wurde, werden mithilfe eines Brute-Force-Angriffs attackiert. So können Zugangsdaten erbeutet werden.
3. **Blackmailing:** Die gesammelten Informationen werden genutzt, um Forderungen an die Unternehmensführung zu stellen. Im Zuge der Übung wird die Zahlung von Bitcoins im Wert von ca. 1 Million Euro gefordert. Für den Fall eines Zahlungsversäumnisses wird mit weiteren Angriffen gedroht.
4. **Command and Control / Impact:** Als Reaktion auf ausbleibende Zahlungen werden kritische Dienste im OT-Netz gestört, manipuliert und abgeschaltet. Diese Aktionen haben direkten Einfluss auf den Betrieb des Stromnetzes.

Der genaue zeitliche Ablauf, die Reihenfolge der einzelnen Angriffsaspekte sowie die konkrete Ausprägung des Cyberangriffs wurden hierbei während der Übung an den Fortschritt der einzelnen Gruppen angepasst, um den Übungsablauf herausfordernd, aber nicht überfordernd zu gestalten. So wurde beispielsweise eine Erpresser-E-Mail an das Management verschickt, nachdem erste Angriffsaktivitäten im OT-Netz unerkannt blieben. Die Management-Gruppe kommunizierte den Eingang der E-Mail an die IT/OT-Gruppe, die somit über den bereits gestarteten Angriff informiert wurde. Die Leitwarten-Gruppe erhielt diese Information vorerst nicht.

Die letzte Phase des Angriffs steuerte nach Ausbleiben der geforderten Erpresserzahlung gezielt Fernwirkgeräte an, um einen Stromausfall herbeizuführen. Zusätzlich wurden Ablenkungsmaßnahmen ergriffen, um die Identifizierung der Angriffsquelle zu erschweren und weitere Dienste im Netzwerk zu stören. Aufgrund der fehlenden Information über einen Cyberangriff wurden die Angriffsauswirkungen in der Leitwarte zuerst als mögliche Störung identifiziert, die man vorerst ohne die Hilfe der IT/OT-Gruppe zu beheben versuchte. Hier wurde ein virtueller Techniker vor Ort eingesetzt, um die Ursache des Stromausfalls näher zu untersuchen. Dieser konnte der Leitwarten-Gruppe telefonisch den Hinweis geben, dass offenbar Steuerbefehle gesendet wurden. Daraufhin wurde die IT/OT-Gruppe in die Ursachenforschung einbezogen und die Angriffsquelle zeitnah identifiziert und durch Einrichten von Firewall-Regeln blockiert. Der sporadische Ausfall weiterer Fernwirkgeräte, der ebenfalls Folge des Angriffs war, blieb einige Zeit unbeachtet. Gegen Ende der Übung konnten die Teilnehmerinnen und Teilnehmer mithilfe eines Hinweises durch die Übungsorganisatoren jedoch auch dieses Problem identifizieren.

3.2 Gruppenspezifische Abläufe

Im Folgenden werden nähere Details zu den gruppenspezifischen Abläufen diskutiert. Die folgende Tabelle fasst die zeitlichen Abläufe und Aufgaben innerhalb der einzelnen Gruppen zusammen.

	MANAGEMENT	IT/OT-PERSONAL	LEITWARTEN-PERSONAL
Prävention und Normalbetrieb 10:00 – 12:15	▪ Erarbeitung eines IT-Sicherheitskonzepts • Benennung eines Krisenstabs • Krisenreaktionsplan	▪ Bestandsaufnahme ▪ Präventive Sicherheitsmaßnahmen ▪ Detektionsmöglichkeiten ▪ Störungsbearbeitung	▪ Einführung Leitsystem ▪ Normalbetrieb • Netzüberwachung • Wartungsanfragen ▪ Störungsbearbeitung
Eintritt der Krisensituation 13:30 – 14:20	▪ Sicherheitskonzept verfeinern	▪ Netzwerkanalyse • Anomalien erkennen ▪ Störungsbearbeitung	▪ Normalbetrieb ▪ Störungsbearbeitung
Erpresserschreiben 14:20	▪ Krisenfallkoordination ▪ Einberufung des Krisenstabs ▪ Fachabteilungen kontaktieren und koordinieren ▪ Externe Kommunikation ▪ Interne Kommunikation	▪ Geräte- und Netzwerkanalyse ▪ Störungsbearbeitung ▪ Forensische Maßnahmen ▪ Reaktive Sicherheitsmaßnahmen ▪ Interne Kommunikation	▪ Normalbetrieb sicherstellen ▪ Störungen forensisch hinterfragen und melden ▪ Wartungen priorisieren ▪ Interne Kommunikation
Großflächiger Stromausfall 15:00 – 16:00	▪ Krisenfallkoordination ▪ Externe Kommunikation ▪ Interne Kommunikation	▪ Cyberangriff lokalisieren ▪ Auswirkungen eindämmen ▪ Forensische Maßnahmen ▪ Reaktive Sicherheitsmaßnahmen	▪ Stromversorgung wiederherstellen ▪ Sicheren Betrieb ermöglichen ▪ Resilienzsteigernde Maßnahmen ergreifen ▪ Interne Kommunikation
Kurzfristige Nachbereitung 16:00 – 16:45	▪ Krisenfallkoordination ▪ Aufarbeitung koordinieren ▪ Sicherheitskonzept überarbeiten ▪ Externe Kommunikation	▪ Schwachstelle identifizieren ▪ Systeme bereinigen ▪ Präventionsmaßnahmen durchführen	▪ Normalbetrieb wiederaufnehmen ▪ Auswirkungen analysieren

Tabelle 1: Im Verlauf der Übung und mit Fortschreiten des Cybersicherheitsvorfalls veränderten sich die primären Aufgaben und Tätigkeiten innerhalb der jeweiligen Gruppen.

3.2.1 Management

Zu Beginn der Übung hat die Management-Gruppe mit der Erarbeitung eines IT-Sicherheitskonzepts begonnen. Bestandteil dieses Konzepts war die Erarbeitung eines Krisenreaktionsplans. Hierbei wurden die Erfahrungen aus den eigenen Unternehmen eingebracht. Als Erstes wurden offene Fragen an die Fachabteilungen identifiziert und dann mit den jeweiligen Fachabteilungen geklärt. Die ersten hieraus abgeleiteten Maßnahmen waren die IT/OT-Trennung durch die IT/OT-Gruppe und die Einrichtung eines von der restlichen IT-Infrastruktur unabhängigen Kommunikationskanals. Hier wurde der ohnehin schon eingerichtete Cloud-Mailprovider ausgewählt und die entsprechenden Accounts für die Fachabteilungen wurden eingerichtet. Dies war insbesondere durch die Erfahrungen der Teilnehmerinnen und Teilnehmer motiviert. Anschließend wurde der Notfallplan erstellt, in dem insbesondere eine klare Rollenverteilung innerhalb des Krisenstabs definiert wurde und Mitglieder aus den Fachabteilungen festgelegt wurden. Dieses Sicherheitskonzept wurde dann mit den Fachabteilungen geteilt, hierbei wurde jedoch versäumt, noch einmal ein gemeinsames Verständnis – zum Beispiel durch ein Meeting – sicherzustellen.

Anstoß für den Übergang zu einer Krisensituation war das Eingehen der Erpressermail von einer Ransomware-Gruppe. Hier wurde, sobald die Authentizität des Erpressungsversuchs sichergestellt worden war, der Notfallplan aktiviert und es wurden entsprechend regelmäßige Sitzungen des Krisenstabs durchgeführt. Neben der internen Koordination wurde durch die Management-Gruppe insbesondere die Kommunikation mit externen Stakeholdern übernommen. So wurde eine Meldung an das BSI abgegeben und regelmäßig durch entsprechende Folgemeldungen aktualisiert. Weitere Stakeholder waren unter anderem überlagerte Netzbetreiber, Strafverfolgungsbehörden und die Presse. Die jeweiligen Statusberichte und Entscheidungen des Krisenstabs wurden protokoliert.

Insgesamt konnte die Gruppe praxisrelevante Erfahrungen aus den jeweiligen Unternehmen – insbesondere in der Vorbereitung – sehr gut austauschen und in die Übung einfließen lassen. Im Verlauf der Übung wurde vor allem der Umgang mit externen Stakeholdern immer strukturierter. Die interne Kommunikation hat jedoch zunehmend unter einer unklaren Erfassung der Situation der Fachabteilungen gelitten, wodurch kein klares Lagebild erfasst und somit auch nicht der volle Handlungsspielraum ausgenutzt werden konnte. So waren insbesondere die Arbeitsbelastung und die jeweiligen Aufwände der Fachabteilungen nicht immer klar und der Krisenstab wurde häufig nicht in ausreichendem Maße eingebunden.

3.2.2 IT/OT

Die Einführung in das Kommunikationsnetz war – basierend auf Aufgabenkärtchen – so konzipiert, dass die Teilnehmerinnen und Teilnehmer an die Aktions- und Reaktionsmöglichkeiten während des Übungsablaufs herangeführt wurden. Damit alle Teilnehmerinnen und Teilnehmer aktiv in die Übung eingebunden wurden und da sie auch eigenständig einige zusätzliche Aufgabenstellungen identifiziert haben, waren während der ersten Phase mehrere Aufgaben parallel zu bearbeiten. Dabei haben die Teilnehmerinnen und Teilnehmer selbstständig kleinere Gruppen gebildet, die sich einzelner Aufgaben angenommen haben. Diese dynamische Identifizierung von Aufgaben war explizit Teil des Konzepts von EnerCise II und wurde in der IT/OT-Gruppe besonders schnell und eigenständig angenommen. Zwischen den Teilgruppen wurde anfangs wenig kommuniziert, sodass sich keine gemeinsame Übersicht über das System ergeben hat. Auch wurden die ausgegebenen Aufgabenkärtchen nicht immer im Detail gelesen, sodass den Teilnehmerinnen und Teilnehmern beispielsweise anfänglich nicht bewusst war, dass die Möglichkeit bestand, einen Techniker vor Ort zu kontaktieren.

Im Laufe der Übung hat sich die gruppeninterne Kommunikation sukzessive verbessert. Die Kommunikation mit anderen Gruppen fand allerdings weiterhin nur sehr begrenzt statt. So wurde die IT/OT-Gruppe zum Beispiel nicht über einen laufenden Angriff informiert, der bereits einige Zeit vorher in der Leitwarte identifiziert worden war. Nachdem diese Information nach einem Hinweis durch die Übungsleitung übermittelt wurde, konnte der Angriff auch schnell identifiziert und die Fehlerquelle behoben werden. In die andere Richtung lief die Kommunikation ebenfalls suboptimal. So wurden beispielsweise zwei suspekte Geräte präventiv von der IT/OT-Gruppe geblockt, weil sie auffällig viel Netzwerkverkehr verursachten. Diese Geräte stellten sich allerdings als Bedienung der Leitwarte heraus, die somit für einen kurzen Zeitraum vom Netzwerk abgekoppelt und daher außer Funktion war.

Insgesamt hat die IT/OT-Gruppe jedoch zielgerichtet gearbeitet, sobald klare Aufträge vorlagen. Insbesondere konnten klar identifizierte Störungen und Angriffsauswirkungen schnell und effektiv durch die IT/OT-Gruppe behoben werden. Allerdings war der Gruppe teilweise ihr eigener Handlungsspielraum nicht bewusst, wie beispielsweise der Einsatz von Technikern vor Ort. Im Nachgang zur Übung wurde außerdem angemerkt, dass die Leitwarte Zugang zum IT-Netzwerk hätte gebrauchen können. Dies hätte jederzeit von der IT/OT-Gruppe umgesetzt werden können, da zusätzliche Geräte bereitstanden, die drahtlos an das IT-Netzwerk angeschlossen werden konnten. Alles in allem nutzte die IT/OT-Gruppe den ihr bekannten Handlungsspielraum jedoch effektiv und zielgerichtet aus.

3.2.3 Leitwarte

Der Ablauf in der Leitwarten-Gruppe begann mit einer Einführung in das verwendete Netz sowie in das Leitsystem (WATTSON VCC), seine Funktionalität und seine Beobachtungs- und Steuerungsmöglichkeiten. Nach einer kurzen Eingewöhnungsphase startete der Normalbetrieb. Hierbei waren diverse Wartungsaufgaben über einen bereitgestellten Wartungsplan bekannt. Die verschiedenen Wartungsaufgaben erforderten unterschiedlich viele Eingriffe durch das Personal, von keinem Aufwand bis hin zu komplexeren Schaltmaßnahmen. Die Arbeiten wurden wie erwartet mit dem Plan abgeglichen, durchgeführt und protokolliert.

Zu den geplanten Ereignissen kamen im weiteren Verlauf zusätzliche ungeplante hinzu, wie zum Beispiel ein Kommunikationsausfall von Fernwirkgeräten aufgrund einer Fehlfunktion. Informationen darüber wurden an die IT/OT-Gruppe gemeldet und die Probleme wurden von dieser gelöst. Erste Cyberangriffe, die sich primär auf Netzwerkscans beschränkten, hatten keinen Einfluss auf den Leitwarten-Betrieb und wurden daher auch nicht in der Gruppe bemerkt. Erst als tatsächliche Angriffe zum Ausfall von Kommunikationsstrecken oder -geräten führten, wurde dies registriert. Der Unterschied zu (zufälligen) Fehlfunktionen und Ausfällen ist jedoch in der Leitwarte nicht erkennbar und die Informationen wurden an die IT/OT-Gruppe weitergeleitet. Diese Informationsweitergabe erfolgte teilweise jedoch verzögert oder unvollständig.

Durch die regelmäßige Zusammenkunft des Krisenstabs als Reaktion auf das Erpresserschreiben der Angreifer war das Leitwarten-Personal stark eingeschränkt, da nur zwei Personen die Leitwarte besetzten, von denen eine regelmäßig abwesend sein musste. Der Normalbetrieb wurde weitergeführt, während ein Cyberangriff vermutet wurde und später auch bestätigt war. Hier gab es keine Vorgabe oder eigenmächtige Entscheidung, den Normalbetrieb einzustellen oder beispielsweise Zu- oder Umschaltungen in der aktuellen Situation nicht mehr durchzuführen. Außerdem litt die wenige vorhandene Kommunikation mit anderen Gruppen stark unter der geringen Personalkapazität. Aspekte unterschiedlicher Angriffsvektoren, wie beispielsweise blockierte Kommunikationseinheiten, wurden nicht bemerkt oder vernachlässigt, da sie in einer Flut von Meldungen untergingen. Diese Meldungen wurden teilweise als wichtiger eingeordnet, da zum Bei-

spiel Teile des Netzgebiets abgeschaltet wurden, die alternativ wieder versorgt werden mussten.

Die gestellte Umgebung mit Leitwarte, Netz und Regelbetrieb bildete eine gute und realitätsnahe Grundlage. Eine reduzierte Netzkomplexität hätte die Einarbeitung erleichtern können, um den Fokus mehr auf die Kommunikationsaspekte zu legen. Die zunehmende Überforderung durch eine Meldungsflut zum Ende des Szenarios ist ebenfalls als realistisch einzuordnen, jedoch kann auch hier die Reduktion der Komplexität helfen, einen größeren Lerneffekt zu erzielen. Alternativ oder zusätzlich kann auch eine weitere Person in dieser Gruppe helfen, aufgekommene Probleme zu reduzieren. Außerdem hätte im Verlauf der Übung die Leitwarten-Gruppe die Management-Gruppe auf die personelle Unterbesetzung der Leitwarte hinweisen können, um zeitweise Unterstützung aus einer anderen Gruppe zu erhalten.

3.3 Beobachtungen zum Ablauf und zur Herangehensweise des Teilnehmerkreises

Im Allgemeinen entsprach der Ablauf der Übung dem ausgearbeiteten Konzept. Die technische Umsetzung war bis auf einige Probleme mit den bereitgestellten Headsets problemlos und alle Teilnehmerinnen und Teilnehmer waren für das Übungsszenario offen. Sie waren bereit, sich in das unbekannte und vergleichsweise komplexe Übungsszenario einzuarbeiten, und haben sich umfassend auf die fiktive Übungssituation eingelassen. Im Verlauf der Übung wurden auch die gruppenübergreifende Kommunikation und Zusammenarbeit gestärkt, nachdem die Gruppen zu Beginn der Übung vorwiegend intern arbeiteten.

Die interne Kommunikation innerhalb der Gruppen funktionierte von Anfang an sehr gut, was sich vor allem durch eine klare Rollenverteilung und Aufgabenzuweisung zeigte. Wenn es zu Schwierigkeiten kam, wurden sie in der Regel rasch mit den anderen Gruppenmitgliedern besprochen und es wurde gemeinsam an Lösungen gearbeitet. Im Gegensatz dazu gestaltete sich der Informationsfluss zwischen den Gruppen eher mühsam, wodurch wichtige Informationen über Ausfälle und Vorfälle teilweise gar nicht oder erst mit erheblicher Verzögerung weitergegeben wurden. Sobald relevante Informationen jedoch die entsprechenden Akteure erreichten, konnten die Störungen schnell und effektiv behoben werden. Insgesamt hätten die einzelnen Gruppen ihre Handlungsspielräume teilweise besser nutzen können, um die verschiedenen Herausforderungen pragmatisch und kreativ zu bewältigen.

4 Erkenntnisse und Analyse

Im Folgenden werden das Verhalten und die gewonnenen Erkenntnisse der Teilnehmerinnen und Teilnehmer diskutiert und das Übungskonzept als Ganzes wird bewertet. Hierbei fließen sowohl die Beobachtungen und Analysen der Übungsorganisatoren ein (Kapitel 4.1 und 4.2.2), als auch das direkte Feedback der Teilnehmerinnen und Teilnehmer in mündlicher und schriftlicher Form (Kapitel 4.2.1).

4.1 Evaluation der Lernziele und entwickelten Fähigkeiten

EnerCise II verfolgte drei wesentliche Lernziele für die Teilnehmerinnen und Teilnehmer (vgl. Kapitel 2.1):

1. Sensibilisierung für Cybersicherheit und die Auswirkungen von Cyberangriffen
2. Praktische Anwendung von IT-Sicherheitsmaßnahmen
3. Stärkung der Kommunikation und Vernetzung der relevanten Akteure

Allgemein lässt sich feststellen, dass die Übung alle drei Lernziele adressierte und dies auch von den Teilnehmerinnen und Teilnehmern so empfunden wurde (vgl. Kapitel 4.2.1).

Sensibilisierung für Cybersicherheit und die Auswirkungen von Cyberangriffen: Die Übung hat mögliche Abläufe von Cyberangriffen auf mehreren Ebenen sowie mögliche Fallstricke beim Umgang mit Reaktionsplänen aufgezeigt. So wurde den Teilnehmerinnen und Teilnehmern durch EnerCise II die Bedeutung eines jederzeit einheitlichen und aktuellen Lagebilds deutlich. Die hierfür notwendige Kommunikation und klare Zuweisung von Verantwortlichkeiten wurden hier als besonders wichtig identifiziert – auch aufgrund der während der Übung teilweise aufgekommenen Kommunikationsschwierigkeiten. Neben einer Sensibilisierung für den Einfluss veralteter und unvollständiger Informationen über die fachliche Lage innerhalb der und zwischen den Gruppen wurde auch eine Sensibilisierung für die Wichtigkeit von Informationen über die aktuelle Belastung und notwendige Priorisierung innerhalb der Fachabteilungen erreicht. So lässt sich festhalten, dass alle Teilnehmerinnen und Teilnehmer für die Grundthematik und Relevanz von Cybersicherheitsaspekten bereits sensibilisiert waren, die Übung diese Sensibilität jedoch stärken konnte und insbesondere Details aufgezeigt hat, die nur durch praktische Erfahrungen erkannt werden können.

Praktische Anwendung von IT-Sicherheitsmaßnahmen: Die konkreten Übungsaspekte von EnerCise II haben zu weiteren Lernfortschritten geführt: Die Teilnehmerinnen und Teilnehmer konnten den Umgang mit einer einzigartigen Verkettung von Ereignissen und Herausforderungen üben und sowohl konkrete Gegenmaßnahmen anwenden als auch wichtige allgemeine Handlungsoptionen und -empfehlungen mitnehmen. Hier sind insbesondere die IT/OT-Gruppe und die Leitwarten-Gruppe zu nennen, da deren Personal für die konkrete Umsetzung technischer Gegenmaßnahmen zuständig ist. Für die Management-Gruppe war hingegen die Erstellung eines Notfallplans eine besonders wertvolle Erfahrung, da dieser im Verlauf der Übung auch unmittelbar in die Praxis umgesetzt werden musste. Außerdem zeigte für alle Gruppen der Umgang mit einem IT-basierten Angriff, der direkte Auswirkungen auf den Stromnetzbetrieb hatte, die Notwendigkeit einer interdisziplinären forensischen Herangehensweise auf, die von den Teilnehmerinnen und Teilnehmern auch entsprechend angenommen und umgesetzt wurde. Die Aspekte der praktischen Anwendung können auch mit vorbereitenden und nachbereitenden Schulungen verbunden werden, um so eine noch stärkere Verbindung von Theorie und Praxis zu erreichen.

Stärkung der Kommunikation und Vernetzung der relevanten Akteure: Ein weiterer zentraler Aspekt von EnerCise II war das Ziel, die Relevanz von Kommunikation zu unterstreichen. Sie sollte sowohl während der Übung forciert als auch über die Übung hinaus in Form von Vernetzung zwischen verschiedenen Akteuren gefördert werden. Dieser Aspekt wurde von allen Teilnehmerinnen und Teilnehmern als Lernfortschritt identifiziert, der insbesondere bei der Management-Gruppe auch bereits während der Übung beobachtet werden konnte. Die Teilnehmerinnen und Teilnehmer dieser Gruppe tauschten sich zu Beginn der Übung unternehmensübergreifend aus, sodass Erfahrungen auch andere relevante Akteure erreichten und Anreize geschaffen wurden, Risikobewertungen, Präventionspläne und Krisenkonzepte auch im Austausch mit anderen Netzbetreibern weiterzuentwickeln. Die Besetzung der Gruppen mit Akteuren verschiedener Netzbetreiber in EnerCise II ermöglichte diese Kommunikation und Vernetzung. Eine mehrtägige Umsetzung der Übung könnte diesen Aspekt noch weiter stärken.

Der Großteil der Teilnehmerinnen und Teilnehmer war bereits zu Beginn der Übung überzeugt, dass für angemessene Reaktionen in Krisensituationen regelmäßige praktische Übungen ein wichtiges bis unabdingbares Mittel sind. EnerCise II hat diese Überzeugung weiter gestärkt und zudem zu weiterführender Sensibilität für konkrete Zwischenfälle geführt. Neben der Sensibilisierung war auch der konkrete Umgang mit und das Üben von praktischen Gegenmaßnahmen ein Lernziel von EnerCise II. Durch die mitgebrachte Expertise der Teilnehmerinnen und Teilnehmer war auch hier bereits vor der Übung ein großes Maß an allgemeiner Erfahrung vorhanden.

4.2 Rückblickende Bewertung des Konzepts und der Durchführung der Übung

Insgesamt lässt sich feststellen, dass das Konzept und die Durchführung von EnerCise II alle Lernziele adressieren und erfolgreich vermitteln konnten. Dies ergaben sowohl das Feedback der Teilnehmerinnen und Teilnehmer als auch die Beobachtungen durch die Übungsorganisatoren. Für zukünftige Cybersicherheitsübungen lassen sich dennoch Optimierungen sowohl im Bereich der Konzeption als auch bei der Durchführung selbst ableiten. Hierzu wurde das Feedback der Teilnehmerinnen und Teilnehmer und der dena als Übungsbeobachterin eingeholt und durch die Erkenntnisse der Übungsorganisatoren ergänzt.

4.2.1 Auswertung des Feedbacks der Teilnehmerinnen und Teilnehmer

Im direkten Nachgang zur praktischen Übung wurde diese mit den Teilnehmerinnen und Teilnehmern in einer offenen Diskussion nachbereitet. Dies bot dem Teilnehmerkreis die Möglichkeit, direktes Feedback abzugeben sowie offene Fragen zum Übungskonzept, zum Ablauf und zur in der Übung behandelten Krisensituation zu klären. Auch erfolgte ein direkter gruppenübergreifender Austausch mit den anderen Teilnehmerinnen und Teilnehmern.

Szenario-Komplexität: Insbesondere in der Leitwarten- und in der IT/OT-Gruppe wurde die in der Übung verwendete Strom- und Kommunikationsnetz-Infrastruktur als zu unübersichtlich empfunden, um sie in der begrenzten Zeit der Übung vollständig überblicken zu können. Dies führte beispielsweise dazu, dass auf Störungs- und Angriffssituationen nicht direkt in dem Umfang reagiert werden konnte, wie es in einem kleineren Szenario möglich gewesen wäre. Der Fokus auf ein realitätsnahes Szenario sollte somit – in Abhängigkeit von der Übungsdauer und Zielgruppe – auf eine geringere Komplexität verschoben werden. Eine angemessene Balance zwischen Realitätsnähe, Komplexität und verfügbaren Handlungsoptionen muss vor jeder Übung individuell gefunden werden.

Fehlerhafte Dokumentation: Die im Konzept gezielt eingestreuten Mängel an der vorhandenen Dokumentation konfrontierten die Teilnehmerinnen und Teilnehmer mit zu vielen „Unbekannten“ für die effektive Bearbeitung von Problemen. Während nicht aktuelle Netzwerkpläne der Realität entsprechen, sind die aktuellen Netze zumindest im Kopf der Mitarbeiterinnen und Mitarbeiter bekannt, was für das fiktive Übungsnetz nicht der Fall ist.

Gruppenübergreifende Kommunikation: Die Kommunikation und der Austausch innerhalb der einzelnen Gruppen haben gut funktioniert. Die gruppenübergreifende Kommunikation und Koordination wurden von mehreren Teilnehmerinnen und Teilnehmern jedoch als Probleme erkannt, die die Bewältigung der Krisensituation verzögerten.

Vorbereitungszeit und Übungsdauer: Insgesamt hätten sich die Teilnehmerinnen und Teilnehmer mehr Zeit für die Vorbereitung und die Übung gewünscht. So hätte man mehr Angriffsszenarien durchspielen bzw. die subtileren Angriffe in Form von Netzwerkscans hätten auch als solche erkannt und bearbeitet werden können.

Minimale Gruppengröße: Die Leitwarte sollte mit mehr als zwei Personen besetzt werden. Da eine Person der Leitwarten-Gruppe meist im Austausch mit dem Krisenstab stand, war die andere Person in der Leitwarte somit oft trotz hoher Aufgabenlast allein.

Neben der Möglichkeit zu offenem Feedback und Diskussionen wurde den Teilnehmerinnen und Teilnehmern ebenfalls eine anonyme, jedoch nach Gruppen unterteilte digitale Umfrage angeboten, die die Übung selbst, die gewonnenen Erkenntnisse und erzielten Lernerfolge sowie Wünsche nach weiteren Übungen abdeckte. Diese Umfrage bestand aus zwölf Fragen. Es nahmen zehn Personen teil.

Das Feedback zum Konzept, zur technischen Umsetzung und zur Betreuung während der Übung fiel durchweg positiv aus. Alle Teilnehmerinnen und Teilnehmer gaben hier die Antworten „Eher gut“ oder „Sehr gut“. Die genaue gruppenspezifische Feedback-Verteilung ist **Abbildung 5** zu entnehmen. Die Komplexität des Szenarios sowie technische Probleme mit den bereitgestellten Headsets sind hier anhand des mündlichen Feedbacks der Teilnehmerinnen und Teilnehmer die wesentlichen negativen Aspekte, die für eine Weiterführung der Übung optimiert werden sollten.

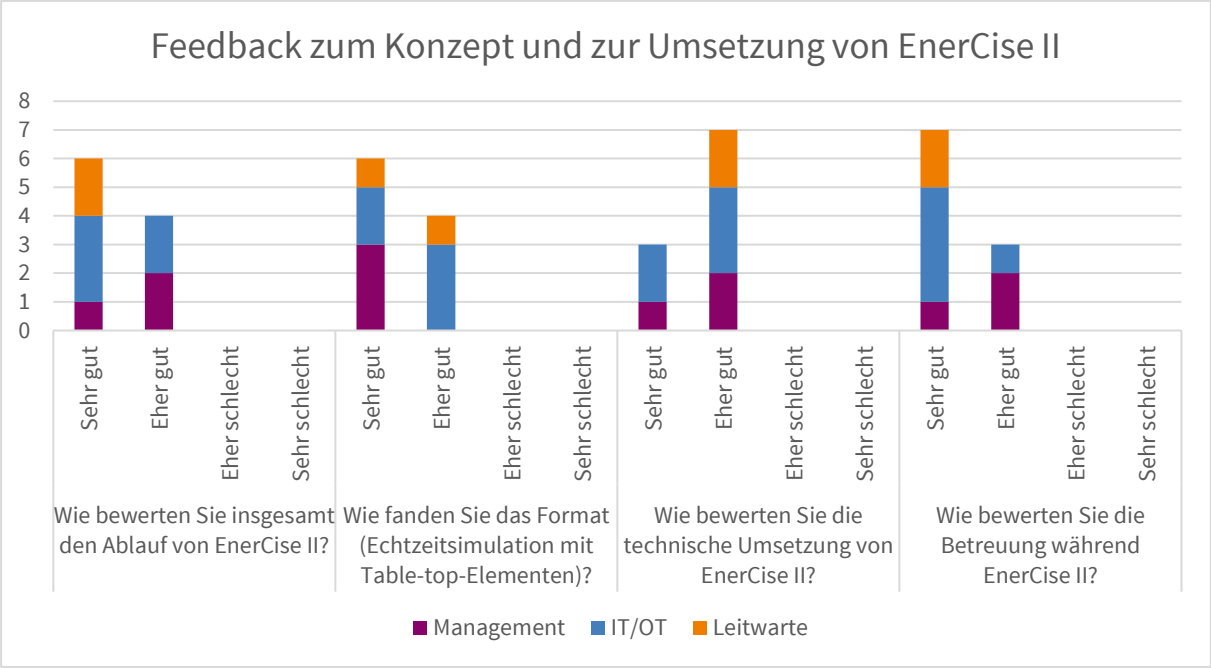

Abbildung 5: Das Feedback zu den Fragen hinsichtlich des Konzepts, der technischen Umsetzung und der Betreuung während der Übung fiel durchweg positiv aus.

Der zweite Teil der Feedback-Umfrage deckte die Bewertung der Kommunikation zwischen den Teilnehmerinnen und Teilnehmern während der Übung ab. Die Ergebnisse entsprechen den Kommentaren aus der offenen Feedback-Runde und unterstreichen, dass insbesondere die gruppenübergreifende Kommunikation ein Problem bei der Aufarbeitung des Cyberangriffs darstellte (vgl. **Abbildung 6**). Allgemein ist zu beobachten, dass die technisch orientierten Gruppen die Kommunikation besser bewerten als die Management-Gruppe. Die Antworten auf eine weitere Frage nach dem empfundenen Lernfortschritt zeigen, dass insbesondere die Mitglieder der Management-Gruppe Lernfortschritte bei der Kommunikation an erster Stelle sehen, während die Leitwarten-Gruppe vorwiegend „Sensibilisierung für Cybersicherheit“ und die praktische Anwendung von Gegenmaßnahmen angegeben hat.

Der letzte Teil der Umfrage befasste sich mit Verbesserungsvorschlägen, alternativen Übungsideen und Fragen zum Interesse an weiteren Übungen. Die Fragen „Würden Sie die Übung weiterempfehlen?“, „Wünschen Sie sich weitere Übungen zu diesem Thema?“ und „Würden Sie wieder an einer solchen Übung teilnehmen?“ wurden durchgehend positiv beantwortet, sodass hier deutlich ein Interesse an weiteren Übungen im Format von EnerCise II zu erkennen ist. Die Frage nach Verbesserungsvorschlägen brachte keine neuen Aspekte, die über das mündliche Feedback hinausgingen. Die Frage, ob andere Übungsformate gewünscht seien, wurde weitestgehend mit „Nein“ beantwortet. Als Ergänzung für weitere Übungen oder auch als eigenständige Module wurde Interesse an Schulungen geäußert, die allgemeine IT-Themen, beispielsweise eine Zusammenstellung aktueller Cybersicherheitsvorfälle oder auch Informationen zu neuen Gegenmaßnahmen, behandeln könnten. Der Vorschlag, Übungen wie EnerCise II mit vorbereitenden gruppenspezifischen Workshops und Schulungen zu erweitern sowie die Hauptübung um weitere konkrete Cyberangriffe zu ergänzen, wurde ebenfalls von den Teilnehmerinnen und Teilnehmern in die Diskussion eingebracht

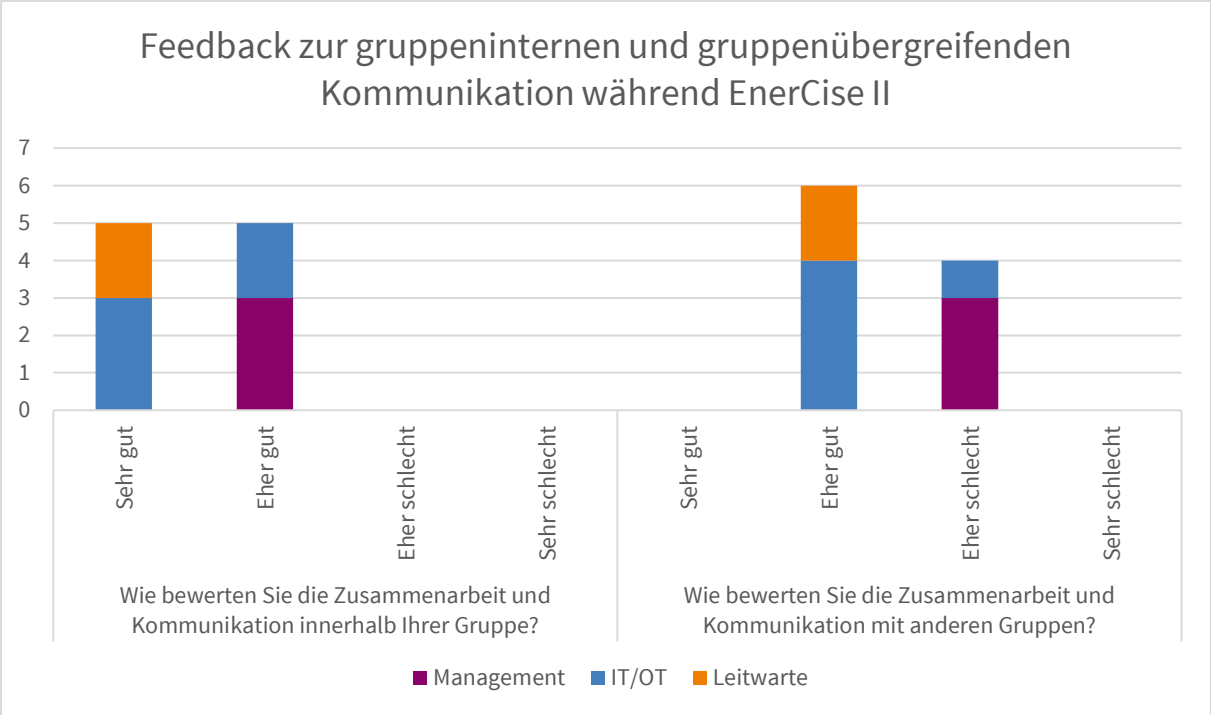

Abbildung 6: Die Teilnehmerinnen und Teilnehmer, insbesondere aus der Management-Gruppe, identifizierten Probleme in der gruppenübergreifenden Kommunikation als Ursache für Schwierigkeiten bei der Aufarbeitung des Cyberangriffs.

4.2.2 Gewonnene Erkenntnisse hinsichtlich Konzeption und Durchführung

Die Beobachtungen durch die Übungsorganisatoren während der Übung sowie das Feedback der Teilnehmerinnen und Teilnehmer brachten einerseits wertvolle Erkenntnisse, wie das Konzept für weitere Übungen angepasst werden kann, andererseits auch Einsichten, welche bereits vorhandenen Aspekte besonders wertvoll für die Übung waren.

Insgesamt hat sich das Grundkonzept der Übung – die Kombination aus einer realistischen Simulationsumgebung mit WATTSON und Table-top-Elementen in Form von Aufgaben- und Hinweiskarten sowie extern verursachten Ereignissen – als ein geeignetes Format erwiesen, um praktische Erfahrungen zu vermitteln, die Relevanz von Kommunikation, Priorisierung und Koordination zu unterstreichen und zusätzlich theoretisches Wissen zu vermitteln. Auch die generelle Teilnehmerzahl von ca. 15 Personen ist für eine solche Übung geeignet und bietet eine Balance zwischen ausreichend Personalkapazitäten in jeder Gruppe und Arbeitsbelastung der einzelnen Teilnehmerinnen und Teilnehmer. Eine Mindestgröße von drei Personen pro Gruppe sollte jedoch eingehalten werden, sodass beispielsweise mindestens drei Personen der Leitwarten-Gruppe zugewiesen sein sollten. Während gruppenspezifische Expertise unabdingbar ist, können koordinierende und gruppenübergreifende Aufgaben auch von Personen übernommen werden, deren normale Tätigkeit nicht vorwiegend im Bereich der zugewiesenen Gruppe liegt. So ergeben sich erstrebenswerte Gruppengrößen von drei bis vier Personen in der Leitwarten-Gruppe, fünf bis sechs Personen in der IT/OT-Gruppe und ebenfalls fünf bis sechs Personen in der Management-Gruppe.

Während der Übung und im darauffolgenden Feedback-Gespräch stellte sich heraus, dass das erstellte Stromnetz-Szenario in Bezug auf seinen Umfang komplexer war als notwendig. Die Teilnehmerinnen und

Teilnehmer hatten daher Schwierigkeiten, sich innerhalb der vorgesehenen Zeit vollständig in das Szenario einzuarbeiten. Bei zukünftigen Durchführungen der Übung könnte die Größe des Szenarios durchaus reduziert werden, ohne dass dies zu einem Qualitätsverlust führt. Darüber hinaus könnte die vorhandene Dokumentation des Szenarios deutlich erweitert werden, um eine schnellere Einarbeitung zu ermöglichen. Auch eine umfassendere Einführung durch die jeweiligen Gruppenbetreuer kann die Einarbeitung und das Verständnis erleichtern. Ein herausforderndes Szenario ist jedoch auch Voraussetzung dafür, die Teilnehmerinnen und Teilnehmer ausreichend zu fordern und den notwendigen Druck zu erzeugen, um Schwierigkeiten zu provozieren. Insgesamt sollte daher die Größe des Szenarios an die Übungsdauer angepasst werden.

Insbesondere in der Management-Gruppe wurde das breite Spektrum an möglichen Handlungsoptionen nur teilweise genutzt. Für zukünftige Übungen wäre es daher ratsam, bereits in der Einführungsphase intensiver auf die verschiedenen Handlungsmöglichkeiten und potenziellen Aktionen einzugehen. Gleichzeitig ist ein offener Ablauf und das damit verbundene Risiko von Fehlern ein entscheidendes Merkmal praktischer Cybersicherheitsübungen, das einen individuellen Lerngewinn für die Teilnehmerinnen und Teilnehmer gewährleistet. Daher sollte weiterhin darauf geachtet werden, den Verlauf der Übung nicht zu sehr durch starre, vorgegebene Abläufe einzuschränken, sondern stattdessen kreative Lösungsansätze zu fördern.

5 Konzept- und Handlungsempfehlungen

Die Konzeption und Durchführung der Übung EnerCise II, die dabei gemachten Beobachtungen, das gewonnene Feedback sowie die im Bereich der Cybersicherheit vorhandene Expertise der Übungsorganisatoren erlauben es, Empfehlungen für die Konzeption und Durchführung weiterer Cybersicherheitsübungen für Verteilnetzbetreiber zu formulieren und zusätzlich allgemeine Handlungsempfehlungen für die Vorbereitung auf und den Umgang mit Cybersicherheitsvorfällen für Verteilnetzbetreiber abzuleiten.

5.1 Empfehlungen für die Durchführung von Cybersicherheitsübungen für Verteilnetzbetreiber

Aus der Durchführung der Übung sowie ihrer Evaluation und Analyse ergeben sich konkrete Empfehlungen für die Durchführung weiterer Übungen sowie für Anpassungen des Konzepts. Dieser Abschnitt fasst die Erkenntnisse und abgeleiteten Empfehlungen aus Kapitel 4 zusammen.

Übungsszenario: Das für die Übung gewählte Szenario sollte sowohl die notwendige Komplexität aufweisen, um eine anspruchsvolle Krisenbewältigung zu ermöglichen, als auch so weit zu überblicken sein, dass die Teilnehmerinnen und Teilnehmer sich in der Kürze der Zeit angemessen in die Struktur und Funktionalität des Verteilnetzes einarbeiten können. Hierbei muss weiterhin auf die Realitätsnähe des Szenarios geachtet werden. Auf einige realistische Aspekte, wie beispielsweise fehlerhafte oder unvollständige Dokumentationen, sollte dennoch aus Zeitgründen verzichtet werden. Somit ergeben sich die folgenden vier Kernaspekte bezüglich des Szenarios:

- Die Komplexität des Szenarios muss an die Dauer der Übung und die verfügbare Einarbeitungszeit angepasst werden.
- Das Szenario muss komplex genug sein, um realistische Angriffe umzusetzen.
- Das Szenario sollte realistisch sein. Dies erlaubt eine schnellere Einarbeitung und erleichtert die Übertragung des Gelernten auf die unternehmenseigene Infrastruktur.
- Das Szenario kann hinsichtlich Topologie, Komplexität und der Cyberangriffe auch im Vorfeld mit den Teilnehmerinnen und Teilnehmern oder ihren Organisationen abgestimmt werden, um so sehr gezielte Situationen üben zu können.

Übungsdurchführung: Im Hinblick auf die konkrete Durchführung der Übung lassen sich fünf wesentliche Empfehlungen ableiten, die direkten Einfluss auf den Übungsablauf und das erfolgreiche Erreichen der Lernziele haben. So müssen die Teilnehmerinnen und Teilnehmer angemessen auf den zu erwartenden Übungsablauf und ihre Handlungsoptionen vorbereitet werden. Neben der Anleitung vor und während der Übung durch die Übungsorganisatoren können auch losgelöste Theorieschulungen und -übungen vor der eigentlichen Übung dabei helfen, die Übung zu optimieren.

- Es kann hilfreich sein, im Vorfeld zur Übung theoretisches Wissen zu Cybersicherheit in Form einer Schulung oder eines Workshops zu vermitteln.
- Es sollte darauf geachtet werden, eine minimale Gruppengröße nicht zu unterschreiten. So sollten jeder Gruppe mindestens drei Personen zugeordnet sein, um eine angemessene Aufgabenverteilung innerhalb der Gruppe zu ermöglichen.

- Die Übungsleitung sollte die Teilnehmerinnen und Teilnehmer zu Beginn umfassend über das Szenario und die ihnen zur Verfügung stehenden Handlungsmöglichkeiten informieren.
- Die Einarbeitungszeit sollte dynamisch verlängert oder verkürzt werden, damit die Teilnehmerinnen und Teilnehmer ein ausreichendes Verständnis des Szenarios und ihrer Handlungsoptionen haben. Eine umfangreichere Information während des vorbereitenden Workshops bietet die Möglichkeit, das zeitliche Ausmaß während der eigentlichen Übung zu reduzieren.
- Die Übungsleitung sollte die Teilnehmerinnen und Teilnehmer während der Übung in angemessener Weise über potenzielle Fehler, Probleme oder versäumte Handlungsmöglichkeiten informieren. Hierbei ist darauf zu achten, dass dies erst geschieht, wenn die Teilnehmerinnen und Teilnehmer genügend Zeit hatten, diese Aspekte selbst zu erkennen und zu adressieren. Zudem sollte die Übungsleitung nicht alle Schritte vorgeben, um die Dynamik der Übung nicht einzuschränken.

Übungsnachbereitung: Um die Übung sowohl für die Teilnehmerinnen und Teilnehmer als auch für die Übungsorganisatoren zufriedenstellend abzuschließen, ist eine entsprechende Nachbereitung wichtig. Sie sollte klar in inhaltliche und konzeptuelle Aspekte unterteilt werden. Für die Teilnehmerinnen und Teilnehmer ist wichtig, dass die erlebte Situation verständlich und vollständig aufgeklärt wird. So können sie einordnen und verstehen, welche Handlungsweisen zur Bewältigung der Situation angemessen oder auch weniger zielführend waren. Dies hilft den Teilnehmerinnen und Teilnehmern direkt, aber auch für die Konzipierung weiterer Übungen. Direktes Feedback der Teilnehmerinnen und Teilnehmer hinsichtlich der Übungsdurchführung und -inhalte ermöglicht ebenfalls eine bessere inhaltliche Aufarbeitung und Konzipierung weiterer Übungen.

- Eine Nachbereitung im direkten Anschluss an die Übung sollte fest eingeplant werden.
- Eine inhaltliche Reflexion der Übung sollte explizit durchgeführt werden. Hierbei können die Teilnehmerinnen und Teilnehmer selbst ihre Eindrücke und Erkenntnisse schildern, die anschließend durch die Übungsorganisatoren ergänzt werden. Das Ziel sollte sein, dass alle Teilnehmerinnen und Teilnehmer den Ablauf des Cyberangriffs sowie die durchgeführten Maßnahmen und ihre Wirkung verstehen.
- Die Teilnehmerinnen und Teilnehmer sollten Feedback zu ihrer Herangehensweise bekommen. Hierbei ist darauf zu achten, eventuelle Kritik konstruktiv zu vermitteln. Auch hier sollten die Teilnehmerinnen und Teilnehmer zuerst selbst die Möglichkeit haben, das Geschehene einzuordnen, bevor externe Eindrücke durch die Übungsorganisatoren ergänzt werden.
- Eine konzeptuelle Nachbereitung hilft, weitere Übungsbedarfe zu identifizieren und die durchgeführte Übung zu verbessern. Hier kann eine offene Feedback-Runde mit einem anonymisierten Fragenkatalog kombiniert werden. Dabei muss berücksichtigt werden, dass die Teilnehmerinnen und Teilnehmer eine eventuelle Überforderung während der Übung unter Umständen auf Schwächen des Konzepts zurückführen, auch wenn sie explizit Teil des Konzepts ist.

Bei allen Empfehlungen für die Konzeption und Durchführung einer Cybersicherheitsübung für Verteilnetzbetreiber muss die konkrete Übungssituation dynamisch bewertet werden. Ein wesentlicher Aspekt ist die Dauer der Übung selbst, die die Komplexität des Szenarios sowie die Notwendigkeit von Hilfestellungen wesentlich beeinflusst. Auch die konkrete Zusammensetzung der Teilnehmerinnen und Teilnehmer ist relevant. So können individuelle Lernziele berücksichtigt oder unternehmensnahe Szenarien kreiert werden, sollten die Teilnehmerinnen und Teilnehmer alle vom selben Netzbetreiber kommen.

5.2 Abgeleitete Handlungsempfehlungen zum generellen Umgang mit Cybersicherheitsvorfällen

Basierend auf dem ausgearbeiteten Konzept, den Beobachtungen durch die Übungsorganisatoren während der Durchführung, dem Feedback durch die Teilnehmerinnen und Teilnehmer und vorhandener Expertise im Bereich der Cybersicherheit der Autoren sind im Folgenden allgemeine Handlungsempfehlungen für Netzbetreiber zur Vorbereitung auf und zum Umgang mit Cybersicherheitsvorfällen zusammengestellt.

Stärkung der interdisziplinären Kommunikation: Die Durchführung von EnerCise II hat gezeigt, dass während einer Krisensituation insbesondere die Kommunikation zwischen den eingebundenen Gruppen gestärkt werden muss, um einen effektiven Informationsfluss sicherzustellen. Dabei ist es entscheidend, zu erkennen, dass die Bewältigung der Krise nur durch die Bündelung von Kompetenzen möglich ist. Hierfür ist Fachexpertise in verschiedenen Bereichen erforderlich, die gezielt und bedarfsgerecht eingesetzt werden muss. Eine wesentliche Voraussetzung dafür ist ein regelmäßiger und auf die Ereignisse abgestimmter Informationsaustausch, der durch entsprechende organisatorische Maßnahmen gewährleistet sein muss. Darüber hinaus ist ein reibungslos funktionierendes Kommunikationssystem für den Informationsfluss von entscheidender Bedeutung. Dieses sollte unter anderem durch redundante Kommunikationswege zu jeder Zeit sichergestellt sein. Konkret bedeutet dies, dass Verantwortlichkeiten und Ansprechpersonen präventiv festgelegt werden und diese Ansprechpersonen und Verantwortlichkeiten dem gesamten Personal bekannt sein müssen. Zudem müssen Ansprechpersonen dazu geschult werden, relevante Informationen zu erfragen, zusammenzutragen und strukturiert weiterzugeben.

Kollaboratives Lagebild: Die Unverzichtbarkeit der interdisziplinären Kommunikation liegt auch in der Notwendigkeit eines gemeinsamen, aktuellen und konsistenten Lagebilds begründet. Für den Krisenfall sollten alle involvierten Personen dazu angehalten sein, Informationen zum aktuellen Lagebild proaktiv mitzuteilen und zu versuchen, ein möglichst vollständiges Lagebild zu erhalten. Entsprechende Hinweise sollten im Präventionskonzept festgehalten und durch den Krisenstab zudem als konkrete Handlungsanweisung ausgesprochen werden. Durch regelmäßige Übungen kann das Personal geschult werden, die Relevanz von Informationen für das Lagebild einzuschätzen.

Regelmäßige Durchführung von Cybersicherheitsübungen: Eine wesentliche Erkenntnis aus EnerCise II ist, dass zwischen Theorie und Praxis im Bereich Incident Response und Krisenmanagement erhebliche Diskrepanzen bestehen: Selbst wenn umfassende IT-Sicherheitskonzepte und Notfallpläne erstellt wurden, ist deren korrekte und vollständige Umsetzung im Krisenfall nicht gewährleistet. Es ist daher unerlässlich, die praktische Umsetzung regelmäßig mit den relevanten Akteuren zu trainieren, um eine erfolgreiche Übertragung der theoretischen Konzepte in die Praxis sicherzustellen. Auf diese Weise können zudem weitere vorhandene Schwachstellen identifiziert und zeitnah behoben werden.

Priorisierung von Aufgaben: Während der Durchführung von EnerCise II wurde deutlich, dass die Priorisierung von Aufgaben eine immense Bedeutung für die erfolgreiche Bewältigung von Krisensituationen hat. Hierzu zählt einerseits die allgemeine Priorisierung von Tätigkeiten wie Betrieb, Kommunikation und detaillierter Analyse und Forensik, andererseits aber auch die Priorisierung von Aufgaben innerhalb dieser Bereiche. Am Beispiel der Leitwarten-Gruppe lassen sich hier die konkreten Empfehlungen besonders deutlich ableiten. Allgemein entstand durch die reduzierte Besetzung mit nur zwei Personen die besondere Notwendigkeit, Aufgaben zu priorisieren. Durch die regelmäßigen Meetings des Krisenstabs war eine der Personen größtenteils dort gebunden, sodass der operative Betrieb sowie jegliche Aktivitäten im Bereich der Analyse von Anzeichen und Auswirkungen des Cybersicherheitsvorfalls durch eine Person durchgeführt werden

mussten. Es kann hier hilfreich sein, den operativen Betrieb vor die Kommunikation zu stellen, indem Informationen für den Krisenstab beispielsweise telefonisch durchgegeben werden oder die persönliche Teilnahme zeitlich stark eingeschränkt wird. Zudem sollten optionale Tätigkeiten, zum Beispiel die Abschaltung von Transformatoren zu Wartungszwecken, verschoben werden, um Kapazitäten für andere Aufgaben zu schaffen. Die Festlegung entsprechender Handlungsspielräume und Prioritäten sollte somit ein essenzieller Bestandteil eines Präventionskonzepts bzw. Krisenplans sein und auch während eines Vorfalls immer kommunikativ aktualisiert und hinterfragt werden. So sind Personalauslastung und das aktuelle Lagebild wichtige Faktoren für die notwendige Priorisierung, die sich dynamisch verändern.

Vorbereitung von Reaktionsmöglichkeiten: In allen Bereichen lassen sich mögliche Reaktionen vorbereiten, um sie im Krisenfall effizient und zeitnah einsetzen zu können. Dies umfasst organisatorische Maßnahmen wie Reaktionen auf Erpresserbotschaften, aber auch technische Gegenmaßnahmen. Eine einfach durchzuführende IT/OT-Trennung bzw. die Isolierung einzelner Netzbereiche durch vordefinierte Firewall-Regeln sowie Pläne und Handlungsabläufe für den lokalen Betrieb einzelner Stationen sind hier Beispiele für wichtige und gut vorzubereitende Reaktionsmöglichkeiten. Um die Effektivität dieser Maßnahmen sicherzustellen, sollten sie regelmäßig geübt und aktualisiert werden.

Die Durchführung von EnerCise II hat den dringenden Bedarf an Cybersicherheitsübungen im Energiesektor verdeutlicht. Sie sollten sich nicht nur auf technische Schulungen zu präventiven Cybersicherheitsmaßnahmen beschränken, sondern vielmehr die praktische Umsetzung von Notfallplänen, Krisenkommunikation und reaktiven Maßnahmen in den Fokus rücken. Dabei ist eine interdisziplinäre Kommunikation und Vernetzung zwischen den jeweiligen Fachabteilungen von entscheidender Bedeutung, um Cybersicherheitsvorfälle schnell und effektiv zu erkennen und zu bewältigen. Das Management und der Krisenstab spielen hierbei eine zentrale Rolle, indem sie durch proaktives Handeln ein umfassendes Lagebild schaffen und die geordnete Bewältigung der Krise sicherstellen. Es ist daher unerlässlich, diese Aspekte regelmäßig mit den relevanten Akteuren zu trainieren, um mögliche Schwachstellen in den IT-Sicherheitskonzepten und in der Kommunikation zu identifizieren und gezielt anzugehen. Einen besonderen Vorteil bieten unternehmensübergreifende Cybersicherheitstrainings, da sie zusätzliche Vernetzungsmöglichkeiten schaffen und den Erfahrungsaustausch fördern. Insgesamt bilden das ausgearbeitete Konzept und die pilotierte Durchführung von EnerCise II eine solide Grundlage für die regelmäßige Umsetzung solcher praktischen Cybersicherheitsübungen, die je nach Bedarf weiter ausgebaut und angepasst werden können.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bader, Lennart; Serror, Martin; Lamberts, Olav; Sen, Ömer; van der Velde, Dennis; Hacker, Immanuel; Filter, Julian; Padilla, Elmar; Henze, Martin (2023): Comprehensively Analyzing the Impact of Cyberattacks on Power Grids. In 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P) (pp. 1065-1081). IEEE.

Bader, Lennart (2024): PowerOwl – A Deterministic Heuristical Approach for Power Grid Modeling. Website. Letzter Zugriff am 27.05.2024. https://powerowl.org

Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.) (2023): Die Lage der IT-Sicherheit in Deutschland 2023.

Deutsche Energie-Agentur (dena) (Hrsg.) und Gesellschaft für Informatik e.V. (2023): Themenroadmap der Branchenplattform Cybersicherheit in der Stromwirtschaft.

Deutsche Energie-Agentur (dena) (Hrsg.) (2022): EnerCise – Eine Cybersicherheitsübung für das sichere Verteilnetz.

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

Meinecke, Steffen; Sarajlić, Džanan; Drauz, Simon Ruben; Klettke, Annika; Lauven, Lars-Peter; Rehtanz, Christian; Moser, Albert; Braun, Martin (2020): SimBench – A Benchmark Dataset of Electric Power Systems to Compare Innovative Solutions Based on Power Flow Analysis. Energies 13, no. 12: 3290. https://doi.org/10.3390/en13123290

Abkürzungen

BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
HIL	Hardware in the Loop
ISO/OSI	International Organization for Standardization / Open Systems Interconnection
IT/OT	Informationstechnologie und operative Technologie
KRITIS	Kritische Infrastrukturen
kWp	Kilowatt-Peak
MWp	Megawatt-Peak
NIS2	EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union
ONS	Ortsnetzstation
PV	Photovoltaik
RTU	Remote Terminal Unit
SSH	Secure Shell

www.dena.de

dena
Deutsche Energie-Agentur