dena
Deutsche Energie-Agentur

Future Energy Lab

ABSCHLUSSBERICHT

EnerCise

Eine Cybersicherheitsübung für das sichere Verteilnetz

Impressum

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

Autorinnen und Autoren:
Jasmin Wagner, dena
Stephanie Carstensen, Ernst & Young GmbH
Ulrike van Venrooy, Ernst & Young GmbH
Vinzenz Weidner, Ernst & Young GmbH

Stand:

4/2023

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2023): „EnerCise – Eine Cybersicherheitsübung für das sichere Verteilnetz“

Bundesministerium für Wirtschaft und Klimaschutz

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

Inhalt

Vorwort

Von der Theorie in die Praxis! Das ist das Motto des vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) beauftragten Projekts „EnerCise – Cybersicherheitsübung für ein sicheres Verteilnetz“, denn das Thema Cybersicherheit gewinnt durch die Digitalisierung des Energiesystems in der Branche immer weiter an Bedeutung. Auf Fachveranstaltungen wird häufig über mögliche Angriffsvektoren und Schutzmechanismen informiert. Neben diesen wichtigen Maßnahmen muss aber auch die Resilienz des Systems, sprich die Wiederherstellungsfähigkeit nach einem erfolgreichen Angriff, stärker in den Fokus rücken.

Genau an diesem Punkt setzt das Projekt EnerCise an. In einer realitätsnahen Krisensimulation werden Routinen und Response-Mechanismen nach einem Sicherheitsvorfall zusammen mit den Teilnehmerinnen und Teilnehmern entwickelt und erprobt. Dabei soll zum einen ein Verständnis für Rollen und die damit verbundenen Funktionen sowie für das Zusammenspiel dieser Rollen geschaffen werden. Bei diesem Aspekt liegt der Fokus auf der Förderung von Kompetenzen wie der Kommunikation innerhalb und außerhalb eines angegriffenen Unternehmens und der Umsetzungsorientiertheit, auch bei einer gegebenenfalls unvollständigen oder unsichereren Informationslage. Zum anderen wird durch die Übung Fachwissen zum Erkennen und Eindämmen von Angriffen vermittelt. Hierbei stehen vor allem Kompetenzen wie analytische Fähigkeiten im Fokus, um beispielsweise Handlungsoptionen und die daraus folgenden Konsequenzen strukturiert identifizieren zu können. Ein weiteres Ziel der Übung ist die Vernetzung wesentlicher Akteure. Daher richtet sich die Übung hauptsächlich an Verteilnetzbetreiber, darüber hinaus allerdings auch an Behörden sowie IT-Sicherheitsexpertinnen und -experten.

Die steigende Bedeutung einer solchen Übung wird durch die jüngsten Ereignisse in der Energiebranche deutlich. Allein im letzten Jahr meldeten mehrere Stadtwerke, Netzbetreiber und weitere für die Energiewirtschaft relevante Unternehmen, dass sie Opfer erfolgreicher Cyberattacken wurden. Aktuell handelt es sich dabei meist um wirtschaftlich motivierte Angriffe, die nicht das primäre Ziel verfolgen, die Systemstabilität zu gefährden. Nichtsdestotrotz wird dadurch die Angreifbarkeit der Branche deutlich, zu der zumindest auch zum Teil kritische Infrastrukturen gehören. Daher widmet sich die Deutsche Energie-Agentur (dena) im Auftrag des BMWK neben EnerCise auch in weiteren Projekten dem Thema Cybersicherheit. Hierzu zählen das Innovationsgutachten EnerCrypt, der Aufbau der Branchenplattform Cybersicherheit in der Stromwirtschaft sowie die Betreuung der deutsch-israelischen Partnerschaft, in der Cybersicherheit ein Schwerpunktthema darstellt.

Die Ergebnisse dieser Projekte, wie der hier ausgeführte Bericht zur Cybersicherheitsübung EnerCise, sollen das Bewusstsein für das Thema in der Branche stärken und zugleich Impulse und Orientierung für eine effiziente Strategie zur Cybersicherheit in der Energiewirtschaft bieten.

Andreas Kuhlmann
Vorsitzender der Geschäftsführung
der Deutschen Energie-Agentur (dena)

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

1 Einleitung

Ein einziger Sicherheitsvorfall bei einem Netzbetreiber kann größere Kreise bis in das gesamte Stromnetz ziehen und spiegelt in der gegenwärtigen Lage ein realistisches Bedrohungsszenario für Industrie und Bevölkerung wider. Energienetze sind attraktive Angriffsziele und durch Attacken aus dem Cyberraum erhöhten Bedrohungen ausgesetzt. Cyberangriffe zu verhindern, frühzeitig zu erkennen und ihren Schaden zu minimieren, ist mittlerweile eine Grundlage für die Versorgungssicherheit.

Im August 2022 veröffentlichte die dena eine vorab durchgeführte Netzbetreiber-Umfrage zum Thema Cybersicherheit im Verteilnetz. Daraus ging hervor, dass der aktuelle Schwerpunkt vieler Netzbetreiber auf dem Verhindern von Angriffen liegt. Resilienzmaßnahmen, die im Fall eines erfolgreichen Angriffs greifen, werden wenig bis gar nicht berücksichtigt. Für eine gute Abwehr sollten jedoch sowohl der Schutz als auch die Resilienz des Systems gestärkt werden. Übungen basierend auf Cyberangriffssimulationen sind ein Instrument, um die Resilienz zu erhöhen.

Vor diesem Hintergrund lud die dena im Auftrag des BMWK 23 Organisationen in das Future Energy Lab zu einer Cybersicherheitsübung ein.

Die in Form einer Table-Top-Übung durchgeführte Cybersicherheitsübung diente dazu, den Teilnehmerinnen und Teilnehmern Kenntnisse über die möglichen und wahrscheinlichen Einfallstore für Angriffe (Angriffsvektoren) zu vermitteln und sie damit in die Lage zu versetzen, typische Schwachstellen in ihrem Unternehmen zu identifizieren. Insbesondere sollte die Übung die Kommunikationsfähigkeit für den Krisenfall stärken und entsprechende Rollenbilder und Funktionen vermitteln. Zudem wurden sinnvolle Maßnahmen zur Prävention und Reaktion erörtert. Hierzu zählte vor allem das Verständnis für die zur Angriffserkennung und -abwehr sowie zur Schadensbegrenzung erforderlichen Rollen zu schärfen, die konkreten Funktionen dieser Rollen und die zur Funktionserfüllung benötigten Informationen, Kenntnisse und Werkzeuge zu verdeutlichen sowie die Zusammenarbeit zwischen diesen Rollen zu fördern. Ein besonderer Schwerpunkt wurde auf die Fähigkeiten zur angemessenen Kommunikation innerhalb und außerhalb der Organisation gelegt.

Die Veranstaltung richtete sich primär an verschiedene Netzbetreiber sowie Bundes- und Landesbehörden. Zusätzlich wurden zur technischen Unterstützung Sicherheitsexpertinnen und -experten von Hochschulen, Stromerzeugern und IT-Dienstleistern eingeladen. Dies förderte auch die Vernetzung wesentlicher Akteure im Themenbereich Cybersicherheit.

Ziel der Cybersicherheitsübung war und ist die Vorbereitung der Teilnehmerinnen und Teilnehmer auf das richtige Verhalten vor, während und nach einem Cybervorfall. Die Ergebnisse der Übung sowie darauf aufbauende Handlungsempfehlungen sind in dieser Publikation zusammengefasst und sollen der Branche als Orientierung und Hilfestellung dienen. Hierfür verschafft das erste Kapitel einen Überblick über den Aufbau und Ablauf der Cybersicherheitsübung. Danach folgt eine Analyse der während der gesamten Übung durchgeführten Beobachtungen, die sich auf einzelne Kompetenzbereiche, wie unter anderem Fachkompetenz, Kooperation oder Umsetzungsorientierung, bezieht. Dabei werden die Kompetenzbereiche anhand eines Punktesystems bewertet und um ausgewählte Empfehlungen ergänzt.

Nachfolgend werden die Ergebnisse der Umfragebögen detailliert aufgezeigt, um die Meinung und Einschätzung der Teilnehmerinnen und Teilnehmer in der Auswertung der Übung zu berücksichtigen.

2 Aufbau und Ablauf der Cybersicherheitsübung

EY hat in Zusammenarbeit mit der dena eine Übung entworfen, welche die Möglichkeit geboten hat, die realistische Simulation eines Cybervorfalls zu erleben und in einer sicheren Umgebung die einzigartigen Herausforderungen bei der Entscheidungsfindung zu bewältigen, die durch Cyberbedrohungen entstehen.

Das Szenario basiert auf einem fiktiven Unternehmen, das durch einen Phishing-Angriff infiltriert wurde und nun mit den daraus resultierenden Problemen wie Datenschutz sowohl hinsichtlich der Mitarbeiterinnen und Mitarbeiter als auch der Kunden, aber auch mit der Aufrechterhaltung und Fortführung des Geschäfts umgehen muss. Dafür wurden vorab wesentliche Angriffsereignisse (Injects) definiert, um die verschiedenen Lernziele und Informationsinteressen zu bedienen.

Die Übung zur Simulation eines Cybervorfalls wurde auf Führungs- und Techniker-Ebene entwickelt und moderiert. Hierfür wurden die Teilnehmerinnen und Teilnehmer in zwei Gruppen unterteilt:

- In der **Management-Gruppe** ging es vor allem darum, die spezifischen Rollen, ihre Fähigkeiten und ihren Kommunikationsbedarf untereinander kennenzulernen.
- In der **Techniker-Gruppe** zielten die Inhalte vor allem darauf ab, spezifische Angriffsmethoden kennenzulernen und Prozesse zur Identifikation und zum Umgang mit ihnen zu verdeutlichen.

Die wichtigsten Merkmale der Simulation waren:

- Motivation und Angriffsvektoren von Cyberbedrohungsakteuren
- Interne und externe Kommunikationsstrategien
- Entscheidungsfindung unter hohem Druck und bei unvollständigen Informationen

Organisationsteam

Um den optimalen Ablauf der Veranstaltung zu gewährleisten, begleitete das Organisationsteam die Cybersicherheitsübung. Es unterteilte sich dabei in vier unterstützende Bereiche:

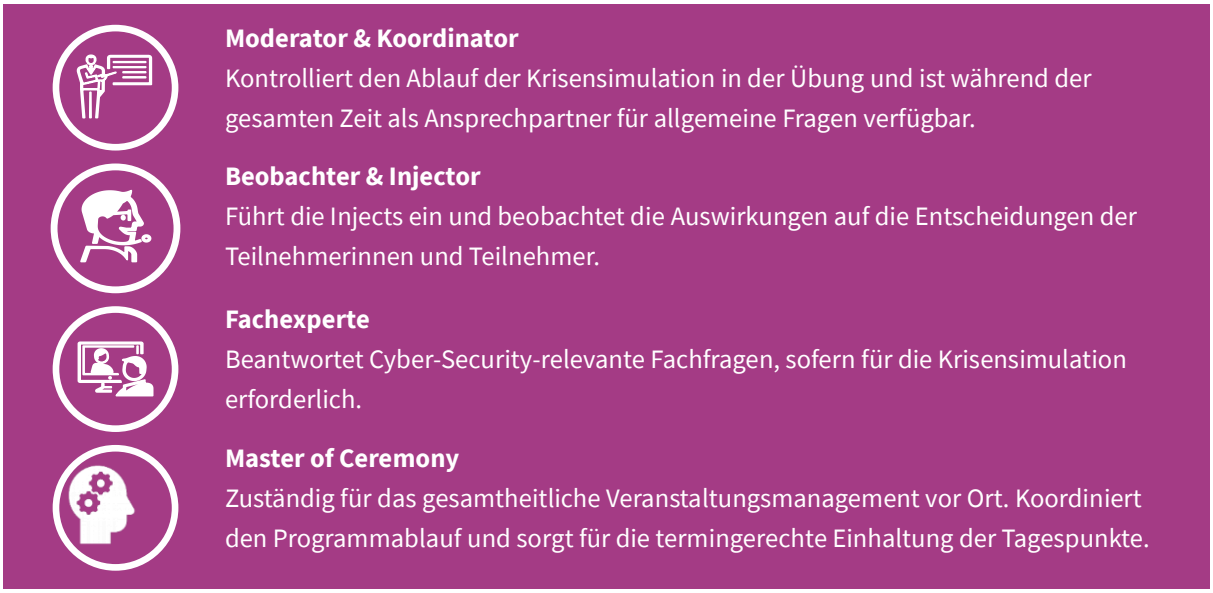

Abbildung 1: Organisationsteam

3 Detaillierte Beobachtungen und Empfehlungen

Während der Cybersicherheitsübung wurden von den Beobachterinnen und Beobachtern sowie den Injectorinnen und Injectoren Beobachtungen angestellt, um die Kompetenzen der Teilnehmerinnen und Teilnehmer in vorab definiteren Kompetenzfeldern vergleichend bewerten zu können. Die Bewertung unterliegt keiner streng wissenschaftlichen Vorgehensweise, sondern ist durch den Abgleich der Verhaltensweise relativ zu der Musterlösung und im Vergleich der Gruppen untereinander erstellt worden.

Skala
Nicht ausgeprägt
Gering ausgeprägt
Mäßig ausgeprägt
Gut ausgeprägt
Sehr gut ausgeprägt

Anhand der Bewertungen konnten spezifische Empfehlungen hinsichtlich der Wissens- und Kompetenzlücken entworfen werden.

Folgende Kompetenzen wurden dabei untersucht:

- Fachkompetenz
- Kooperation & Zusammenarbeit
- Umsetzungsorientierung
- Kommunikation
- Analytische Kompetenz & Urteilsvermögen

3.1 Fachkompetenz

Innerhalb dieses Kompetenzbereichs wurde bei den Teilnehmerinnen und Teilnehmern überprüft, wie sie fachbezogenes Wissen einsetzen, gegebenenfalls kritisch überprüfen und daraus je nach Situation erforderliche Handlungen ableiten.

Eine ausgeprägte Kompetenz äußert sich in diesem Bereich folgendermaßen:

Die Gruppe nutzt ihr Fachwissen in der Übung und fördert den fachlichen Austausch untereinander. Aufgrund des Zusammenwirkens verschiedenster individueller Erfahrungshintergründe kann die Priorisierung der relevanten Aufgaben und Prozesse während der Cybersicherheitsübung sachgerecht vorgenommen werden.

Beobachtungen

Obwohl nur wenige Teilnehmerinnen und Teilnehmer zuvor bereits an einer Simulation auf Basis eines Cyber-Incident-Szenarios teilgenommen haben, wurden fachliche Zusammenhänge schnell erkannt und struktu-

riert wiedergegeben. Die Gruppenmitglieder verfügten über eine hohe Fachkompetenz und nutzten ihr individuelles Know-how zur Bewältigung der Übung. Auch das Verständnis zum Zusammenspiel technischer Komponenten und das Bewusstsein für die jeweiligen Konsequenzen bei der Abschaltung oder Entkopplung einzelner Bereiche wurden über die gesamte Übungszeit zielführend eingesetzt. Es herrschte ein gutes Grundverständnis zum Aufbau der eigenen Organisation und zu den relevanten Kommunikationsschnittstellen.

Jedoch war der Wissensstand bezüglich einzubindender Akteure lückenhaft. Dies galt sowohl für Akteure, die im Fall eines Cyberangriffs eingebunden werden müssen, wie zum Beispiel Großkunden, Beschäftigte, Politik und Bundesämter, als auch für solche, die eingebunden werden können (wie unter anderem das Landeskriminalamt und das Bundesamt für Sicherheit in der Informationstechnik).

Die Fachkompetenz erreichte eine Bewertung von „gut“ bis „sehr gut“.

Empfehlungen

Bezüglich der Fachkompetenz lassen sich für die Organisationen folgende Empfehlungen ableiten:

- Intensivierung von Schulungen für Mitarbeiterinnen und Mitarbeiter und Etablierung von Support-Leveln für Mitarbeiterinnen und Mitarbeiter im Unternehmen zur Adressierung von Cyberangriffen
- Sicherstellung des Wissenstransfers, um im Falle eines Cyberangriffs adäquat reagieren zu können:
    - Stellen Sie sicher, dass alle Beschäftigten wissen, wie sie einen Cyberangriff identifizieren und effektiv darauf reagieren können.
    - Richten Sie Notfallwiederherstellungsprozesse für langfristige Cybervorfälle ein.
    - Führen Sie regelmäßig Wiederherstellungstests unter Berücksichtigung realistischer Szenarien durch, um eine ordnungsgemäße Wiederherstellung und Orchestrierung zwischen Abteilungen und etwaigen externen Dienstleistern sicherzustellen.
    - Identifizieren Sie weitere Optionen zur Wiederherstellung als zusätzliche Alternative zu Backups oder einzelnen Stammdaten.
    - Fertigen Sie als Vorbereitung auf Krisen Listen an, die nicht nur die zu kontaktierenden externen Organisationen und Behörden aufführen, sondern auch die zu ergreifenden Maßnahmen mit den daraus jeweils entstehenden Konsequenzen aufzeigen (z. B. visualisiert als Entscheidungsbaum).

3.2 Kooperation & Zusammenarbeit

Bei der Kooperation & Zusammenarbeit steht die zweckorientierte gemeinsame Arbeit einer Gruppe im Vordergrund.

Eine ausgeprägte Kompetenz äußert sich in diesem Bereich folgendermaßen:

In der Gruppe herrscht eine angenehme Arbeitsatmosphäre, die Teilnehmerinnen und Teilnehmer begegnen sich respektvoll und wertschätzend, unterstützen sich gegenseitig im Bedarfsfall und tragen dafür Sorge, dass Vorgehensweisen untereinander abgestimmt sind. Dies äußert sich auch darin, dass sie einander aktiv zuhören und Handlungsvorschläge diskutieren.

Beobachtungen

Alle Teilnehmerinnen und Teilnehmer beteiligten sich aktiv und arbeiteten eng zusammen, obwohl sie aus verschiedensten Unternehmen in den Gruppen zusammenkamen. Außerdem entstanden effiziente Strukturen im Verlauf der Übung, in denen jeder eine wichtige Rolle übernahm und wertvollen Input mit der Gruppe teilte. Stets wurde eine respektvolle Gesprächskultur gewahrt und die getroffenen Entscheidungen wurden vom Team respektiert.

Das Verhalten der Teilnehmerinnen und Teilnehmer innerhalb dieser Betrachtungsperspektive wurde mit „sehr gut ausgeprägt“ bewertet. Trotzdem lassen sich einige allgemeine Empfehlungen aussprechen, die sich im Unternehmenskontext als hilfreich erweisen könnten.

Empfehlungen

- Verbessern Sie die interdisziplinäre Zusammenarbeit zwischen den Mitarbeiterinnen und Mitarbeitern und der IT-Sicherheit, um bei Cyberangriffen den Wissenstransfer zur Identifikation zu gewährleisten.
- Stellen Sie den Informationsfluss zwischen verschiedenen Arbeitsteams durch regelmäßige Meetings und Alignments sicher.
- Stellen Sie sicher, dass die Teams des Krisenstabs im virtuellen Setup zusammenarbeiten können, wie sie es im analogen Setup gewohnt sind (Tools usw. erforderlich).
- Erstellen Sie einen Leitfaden mit den wichtigsten Fakten, die für die Arbeit in der virtuellen Krisenreaktion von Bedeutung sind.

3.3 Umsetzungsorientierung

Eine weitere wesentliche Kompetenz ist die Umsetzungsorientierung, mit der die Fähigkeit bezeichnet wird, Strategien, Ideen und/oder Ziele in konkrete Maßnahmen und Ergebnisse umzusetzen.

Eine ausgeprägte Kompetenz äußert sich in diesem Bereich folgendermaßen:

Die Gruppe nutzt ihren Handlungsspielraum angemessen und trifft auch bei unvollständiger Informationslage notwendige Entscheidungen. Sie findet für Probleme pragmatische Lösungen, sorgt für die Umsetzung von getroffenen Vereinbarungen und übernimmt Verantwortung für die Ergebnisse.

Beobachtungen

Die Entscheidungsprozesse waren geprägt von den verschiedenen Entscheidungshintergründen der Teilnehmerinnen und Teilnehmer. Aufgrund dessen entstanden ausführliche Diskussionen, um alle auf den gleichen Erfahrungsstand zu bringen. Endgültige Entscheidungen als Reaktion auf Injects blieben daher vereinzelt aus oder erfolgten erst nach Aufforderung. Besonders im Kontext von Presseanfragen, bei denen ein Statement oder eine Pressemitteilung erforderlich war, zeigte sich hier ein deutliches Verbesserungspotenzial.

Auch bei der Entscheidungsfindung auf Basis unzureichender Informationen taten sich viele Gruppen schwer. Handlungsoptionen wurden diskutiert, gingen dann aber unter, sodass eine Entscheidung am Ende ausblieb. Hier fehlte in einigen Gruppen eine strukturierte Vorgehensweise, bei der Optionen und Konsequenzen diskutiert und in einheitlicher, übersichtlicher Form dokumentiert werden, um dann entschieden zu werden.

In einzelnen Gruppen wurde eine strukturierte Vorgehensweise von Beginn an festgelegt und umgesetzt. Hier wurden fest getaktete Lagebesprechungen durchgeführt und getroffene Entscheidungen sowie der Verlauf der Übung übersichtlich dokumentiert.

In allen Gruppen verbesserten sich die Strukturierung und das damit verbundene konsequentere Vorgehen in der Krisensimulation. Dies verdeutlicht das Verbesserungspotenzial dieser Kompetenz durch eine Krisensimulation. Die Übung wurde zudem genutzt, um Erfahrungen und Umsetzungsstrategien der einzelnen Unternehmen untereinander auszutauschen. Die Verbesserungen sind nicht zuletzt auch darauf zurückzuführen, dass sich die verschiedenen Gruppenmitglieder im Verlaufe der Übungszeit mehr aufeinander eingespielt haben. Dies lässt sich auch auf die individuelle Situation der Unternehmen übertragen.

Die Umsetzungsorientierung der Teilnehmerinnen und Teilnehmer wurde mit „mäßig ausgeprägt“ bewertet. Daher lassen sich folgende Empfehlungen ableiten:

Empfehlungen

- Stellen Sie sicher, dass bestimmten Ereignissen vordefinierte Prozesse zugeordnet sind, die für alle Beschäftigten, zumindest aber für ein ausgewähltes Krisenteam zugänglich sind.
- Binden Sie die IT-Sicherheit stärker in den BCM-Prozess (Business Continuity Management) ein, um Cyberangriffe zu identifizieren.
- Dokumentieren Sie Links zu wichtigen Stakeholdern.
- Definieren und richten Sie ein Online-Tool ein, das als „Arbeitsraum“ verwendet wird, um alle relevanten Informationen zu sammeln und mit allen Beteiligten zu teilen. Nutzen Sie dieses Tool, um in Aufgabenlisten arbeiten zu können.
- Identifizieren Sie Abhängigkeiten von Websites und richten Sie Workaround-Prozesse bei einer Nichtverfügbarkeit dieser Websites ein.
- Stellen Sie sicher, dass die Beschäftigten in Phishing-Angriffsübungen geschult sind und darin, wie sie cyberbezogene Vorfälle erkennen können. Stellen Sie sicher, dass ein lokaler Notfallreaktionsplan (einschließlich lokaler Kontaktdaten) für alle Beschäftigten verfügbar ist, falls ein verdächtiges Ereignis gemeldet wird.
- Abhängigkeiten von zu treffenden Entscheidungen sollten in einer Liste hervorgehoben werden. Für den Fall, dass etwas entschieden werden muss, gibt diese Liste einen klaren Überblick, welcher Stakeholder für die Entscheidung informiert bzw. einbezogen werden sollte.

3.4 Kommunikation

Auch die Kommunikation der Teilnehmerinnen und Teilnehmer mit den fiktiven Kontakten während der Übung sowie untereinander wurde genauer untersucht, da der Austausch von Informationen mit internen und externen Kontakten eine ausschlaggebende Rolle spielt.

Eine ausgeprägte Kompetenz äußert sich in diesem Bereich folgendermaßen:

Die Gruppe reagiert auf Mitarbeiteranfragen, Meldungen der Kunden oder der Presse etc. bedacht und professionell. Man bemüht sich darum, eine optimale Lösung für den Kunden zu finden, jedoch ohne dabei die Organisationsinteressen aus dem Blick zu verlieren. Auch die Meldungen an externe Institutionen werden sachgemäß erwogen und bei Notwendigkeit präzise und informativ vollzogen.

Beobachtungen

Die Teilnehmerinnen und Teilnehmer bemühten sich um Rollenverteilungen und eine Krisenkommunikationsstruktur mit einer klaren Vorgehensweise, um mit externen und internen Meldungen umzugehen. Zu Beginn der Übung erfolgten Reaktionen hinsichtlich der Kommunikation mit den Stakeholdern oft nur oberflächlich und verzögert. Auch im Umgang mit der Presse oder den Kunden wäre eine intensivere Auseinandersetzung angebracht gewesen. Beide Beobachtungen weisen darauf hin, dass die Krisenkommunikation ein eigenes Tätigkeitsfeld und einen eigenen Kompetenzbereich darstellt, wofür die Teilnehmerinnen und Teilnehmer während der Übung sensibilisiert wurden. Im weiteren Verlauf der Übung verbesserten sich die Kommunikationsstrukturen entsprechend deutlich.

Für den Kompetenzbereich Kommunikation wurden als „gut ausgeprägt“ bewertet.

Empfehlungen

Für die Kommunikation von Organisationen im Krisenfall lassen sich folgende Empfehlungen ableiten:

- Lassen Sie den Krisenkommunikationsplan und die vorbereiteten Nachrichten für Kunden, Beschäftigte, Regulierungsbehörden, Presse, Interessengruppen und soziale Medien regelmäßig überprüfen, um sicherzustellen, dass sie in einer Reihe von verschiedenen Szenarien eingesetzt werden können.
- Goldene Regel: Achten Sie auf präzise, konkrete Botschaften bei einem Sicherheitsvorfall.
- Wenn die Kommunikation während eines Cybervorfalls vorbereitet wird, stellen Sie Folgendes sicher:
    - Kommunizieren Sie positiv, um sich gegen Kritik in der Presse zu schützen. Es ist „keine Sünde, angegriffen zu werden“. Adressieren Sie Kritik nicht (nur) mit Rechtfertigungen, sondern blicken Sie nach vorne und stellen Sie dar, welche Maßnahmen Sie bereits ergriffen haben und noch ergreifen werden.
    - Antizipieren Sie „Shitstorms“ und negative digitale Diskurse in sozialen Medien und Blogs und entwickeln Sie für bestimmte Narrative mögliche Reaktionsmuster.
    - Klären Sie, welche Abteilung die obligatorische Kommunikation mit den Behörden übernimmt.
    - Verstärken Sie die Kommunikation mit der IT-Sicherheit, um besser zu verstehen, wie Sie Cyberbedrohungen verhindern können und welche Prozesse im Falle eines Vorfalls eingeleitet werden müssen.
    - Stellen Sie sicher, dass die Zusammenarbeit zwischen lokalen und globalen Teams verstanden wird: Überprüfen Sie, ob die Stakeholder für cyberbezogene Vorfälle im Incident-Response-Plan berücksichtigt werden.
    - Stellen Sie in Ihrer Organisation eine Liste mit einer vollständigen Übersicht aller etwaigen einzubindenden Akteure bereit.

3.5 Analytische Kompetenz & Urteilsvermögen

Analytische Kompetenz ist die Fähigkeit, ein komplexes System sowohl physisch als auch gedanklich in seine Elemente zu trennen und zu klassifizieren und daraus die kausalen Zusammenhänge zu erkennen. Neben der analytischen Kompetenz spielt auch das Urteilsvermögen der Teilnehmerinnen und Teilnehmer eine wichtige Rolle. Sie sollten in der Lage sein, einen Sachverhalt korrekt einzuordnen.

Eine ausgeprägte Kompetenz äußert sich in diesem Bereich folgendermaßen:

Die Gruppe strukturiert komplexe Sachverhalte logisch und zielgerichtet, zeigt Ursache-Wirkungs-Zusammenhänge auf, erweitert ihre Urteilsbasis zielgerichtet und nutzt vorhandene Informationen für die Entscheidungsfindung.

Beobachtungen

Die Mehrheit der Teilnehmerinnen und Teilnehmer verfügte über eine ausgeprägte analytische Kompetenz. In den Teams wurden der Zusammenhang von Ursache und Wirkung sowie Konsequenzen der Entscheidungen ausführlich beleuchtet. Erschwert wurde das Vorgehen dadurch, dass die Rollenverteilung in der Gruppe zu Beginn teils nicht detailliert genug vordefiniert worden war. Daher fehlte vereinzelt eine Leiterin oder ein Leiter in der Gruppe, der Vorfälle nach verschiedenen Zuständigkeiten sortiert und Informationen sammelt.

Die Notwendigkeit dieser Rolle wurde im Verlauf der Übung deutlich und die Struktur entsprechend angepasst. Insgesamt wurde auch die Struktur der Lagebesprechungen und der Dokumentation durch die adaptiven Fähigkeiten der Teilnehmerinnen und Teilnehmer im Verlauf der Übung besser.

Die Fachkompetenz und die Identifikation von Zusammenhängen möglicher Ursachen und Wirkungen waren in fast allen Gruppen äußerst ausgeprägt, was für umfängliche, mehrdimensionale Analysen sorgte.

Trotz der richtigen Zuordnung der Verantwortlichkeiten taten sich einige Gruppenmitglieder aufgrund unzureichender Informationen schwer, Entscheidungen zu treffen. Daher waren die Diskussionen teilweise nicht zielführend, jedoch lernten die Gruppen mit der Zeit, besser mit den Gegebenheiten umzugehen.

Die analytische Kompetenz und das Urteilsvermögen erreichten eine Bewertung von „mäßig ausgeprägt“.

Empfehlungen

Es lassen sich folgende Empfehlungen ableiten:

- Im Falle eines realen Vorfalls sollten Regeln und Methoden für eine klare analytische Entscheidungsfindung eingerichtet und Verständnis, Urteilsfindung und Vorgehen für die Zusammenarbeit und die Lösung des Vorfalls einstudiert werden. Dazu zählen beispielsweise feste Abläufe in regelmäßigen Krisenmeetings.
- Verlassen Sie sich nicht auf einzelne Personen, sondern identifizieren Sie Rollen und legen Sie stellvertretende Verantwortliche fest, die im Ernstfall den Ablauf koordinieren können und das erforderliche Wissen besitzen.
- Lassen Sie BCM-Material wie BCM-Pläne und Handbücher erstellen. Diese müssen für alle Mitglieder des BCM-Führungsteams und ihre Stellvertretungen online verfügbar sein, falls eine virtuelle Zusammenarbeit erforderlich ist.
- Es sollte eine Überprüfung des gesamten Krisenmanagementrahmens und -plans innerhalb der Unternehmen durchgeführt werden.

3.6 Zusammenfassung

In dieser Visualisierung werden die Kompetenzen Fachkompetenz, Kooperation & Zusammenarbeit, Umsetzungsorientierung, Kommunikation sowie Analytische Kompetenz & Urteilsvermögen gegenübergestellt und so grafisch in Bezug gesetzt. Die Skala reicht von 1 für „gar nicht ausgeprägt“ bis 5 für „sehr gut ausgeprägt“.

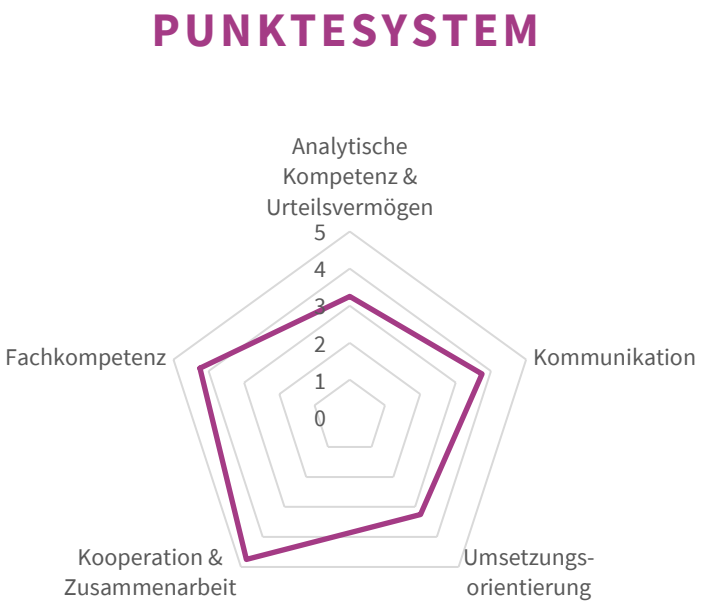

Abbildung 2: Netzdiagramm Kompetenzbereiche der Teilnehmerinnen und Teilnehmer

Die Auswertung über alle Kompetenzen hinweg zeigt eine ausgewogene Verteilung der Fähigkeiten mit einer deutlich positiven Ausprägung, die zur erfolgreichen Bewältigung der Übung durch die Teilnehmerinnen und Teilnehmer führte.

Vor allem die Kompetenz **Kooperation & Zusammenarbeit** war besonders stark ausgeprägt und der Erfolgsfaktor, wenn andere Fähigkeiten weniger stark ausgeprägt waren, und führte zu einer signifikanten Verbesserung im Verlauf der Übung.

Auch die **fachliche Kompetenz** sowie die interne und externe **Kommunikation** wurden in die Übung sehr gut eingebracht und umgesetzt. Lediglich einzelne Aspekte können in zukünftigen Übungen gestärkt werden.

Im Kompetenzbereich **Analytische Kompetenz & Urteilsvermögen** sowie in der **Umsetzungsorientierung** zeigte sich Verbesserungspotenzial. Zukünftige Übungen sollten daher den Fokus auf die Anleitung zum strukturierten Vorgehen im Rahmen einer Krisensituation und die entsprechend effizientere Entscheidungsableitung legen.

Über den Übungsverlauf hinweg wurden die oben dargestellten Kompetenzbereiche gezielt verbessert. Daneben wurde auch das Aufeinandereinspielen der Krisenstabsmitarbeiterinnen und -mitarbeiter untereinander gefördert. Eine Sicherheitsübung entfaltet demnach ihr ganzes Potenzial, wenn sie im eigenen Unternehmen mit den im Krisenfall einzubindenden Beschäftigten durchgeführt wird.

4 Evaluation der Übung durch die Teilnehmerinnen und Teilnehmer

Die Teilnehmerinnen und Teilnehmer erhielten die Möglichkeit, mittels Umfragebögen Feedback zur Übung zu geben. Diese wurden zusammengefasst, ausgewertet und grafisch veranschaulicht. Die Auswertung unterscheidet dabei zwischen den beiden Szenarien der Management-Gruppen und der Techniker-Gruppen.

4.1 Umfrageergebnisse der Management-Gruppe

Die Erwartungen der Management-Gruppe wurden größtenteils erfüllt oder sogar übertroffen.

Nach Angabe der Teilnehmerinnen und Teilnehmer war die dargelegte Storyline nachvollziehbar und die ihnen gestellten Aufgaben waren verständlich erklärt. Die Rückmeldungen belegen den nachhaltigen Effekt der Cybersicherheitsübung. Viele Gruppenmitglieder erkannten Verbesserungspotenzial im eigenen Unternehmen und können sich nun für die Implementierung weiterer Cyber-Security-Maßnahmen einsetzen. Nur 5 Prozent der Teilnehmerinnen und Teilnehmer empfanden die Story als zu starr festgelegt und hätten sich mehr Situationsweichen gewünscht. Bezüglich der Anschaulichkeit herrschte große Zufriedenheit, jedoch wurde angemerkt, dass eine Darstellung der Simulationszeit anhand eines Zeitstrahls wünschenswert wäre.

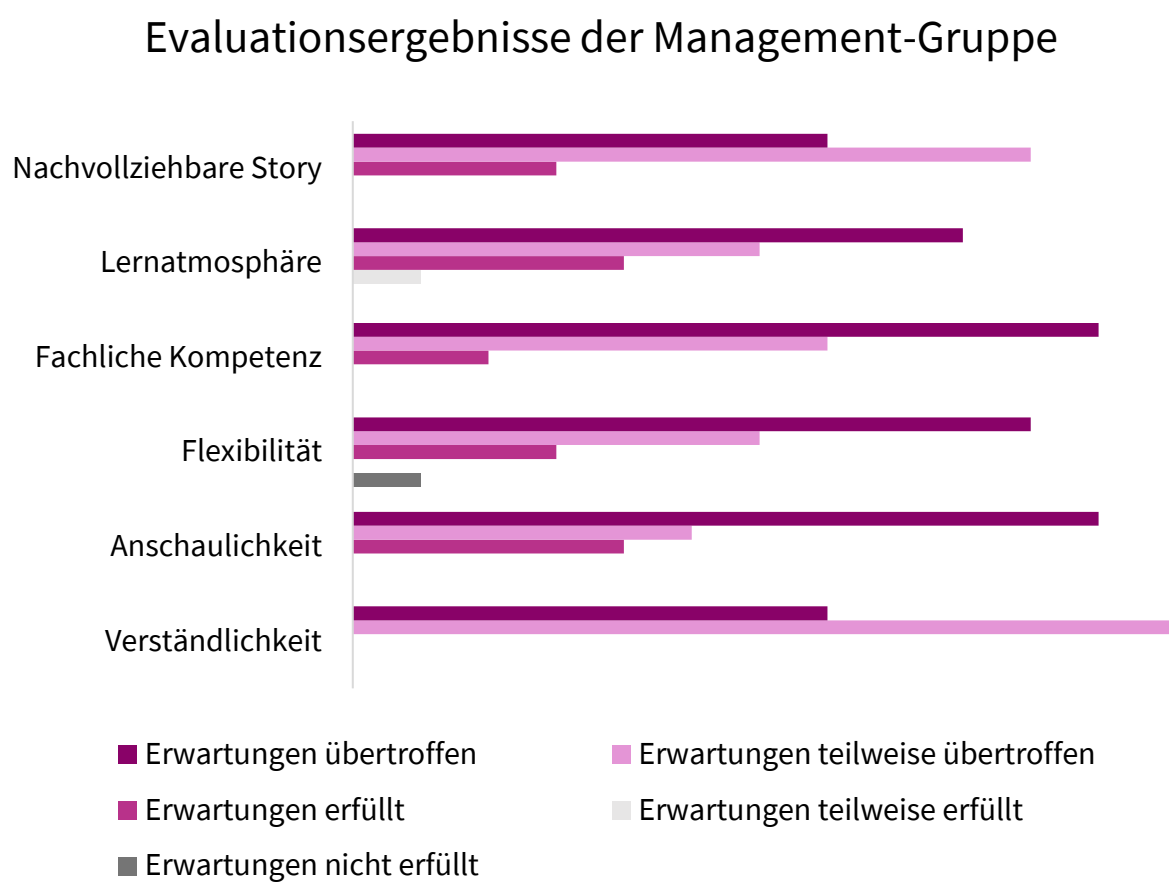

Abbildung 3: Umfrageergebnisse Management-Gruppe – Erwartungen

Im Zusammenhang mit den gelegentlich ausgebliebenen Entscheidungen wäre es sinnvoll, zukünftig zeitliche Fristen festzulegen, nach denen eine endgültige Entscheidung getroffen und mitgeteilt werden muss. Zudem sollte ein Feedback zu den getroffenen Entscheidungen durch die Moderation erfolgen, um so die Konsequenzen der Reaktion zu verdeutlichen.

Im Großen und Ganzen wurde von den Teilnehmerinnen und Teilnehmern betont, dass das Setting der Cybersicherheitsübung zu unkonkret beschrieben worden war. Dazu wurden deutlichere Vorgaben bezüglich einer benötigten Rollenverteilung, des Eigenanteils der Gruppenmitglieder an der Spielgestaltung und der Quellen bzw. erforderlichen Ansprechpartner gewünscht.

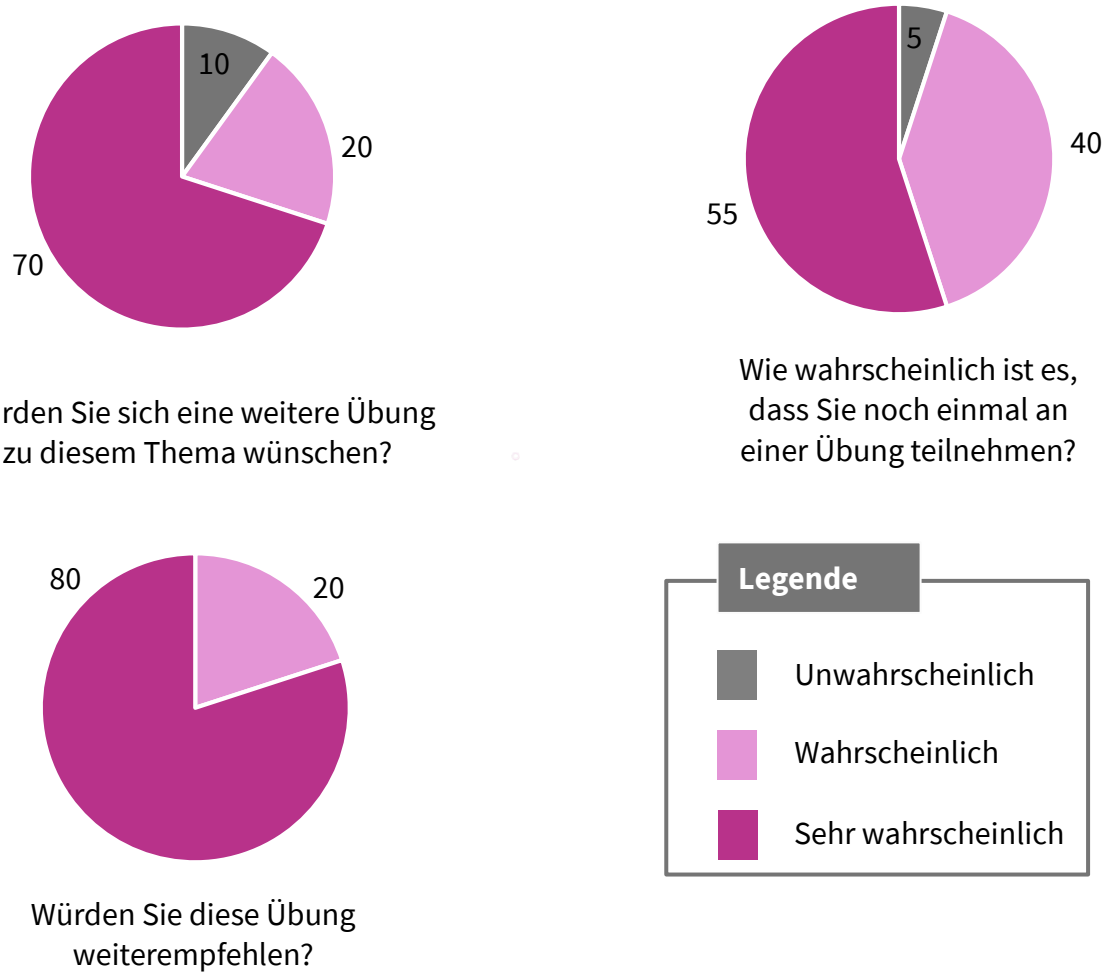

Abbildung 4: Umfrageergebnisse Management-Gruppe – erneute Teilnahme

95 Prozent der Teilnehmerinnen und Teilnehmer des Management-Szenarios würden noch einmal an einer Cybersicherheitsübung wie dieser teilnehmen. Der Großteil, nämlich 90 Prozent, wünscht sich weitere Übungen zu diesem Thema.

Insofern wird ausdrücklich empfohlen, weitere Cybersicherheitsübungen durchzuführen, um das Interesse der Teilnehmerinnen und Teilnehmer zu bedienen.

4.2 Umfrageergebnisse der Techniker-Gruppe

Die Cybersicherheitsübung hat der Mehrheit, nämlich über 80 Prozent der Techniker-Gruppe, gefallen bzw. sogar ihre Erwartungen übertroffen.

Besonders hervorzuheben sind dabei die fachliche Kompetenz (95 Prozent), die Flexibilität der Storyline hinsichtlich der Entscheidungen der Teilnehmerinnen und Teilnehmer (90 Prozent) und die Lernatmosphäre (90 Prozent). Mit der Verständlichkeit der Story waren sogar ausnahmslos alle zufrieden.

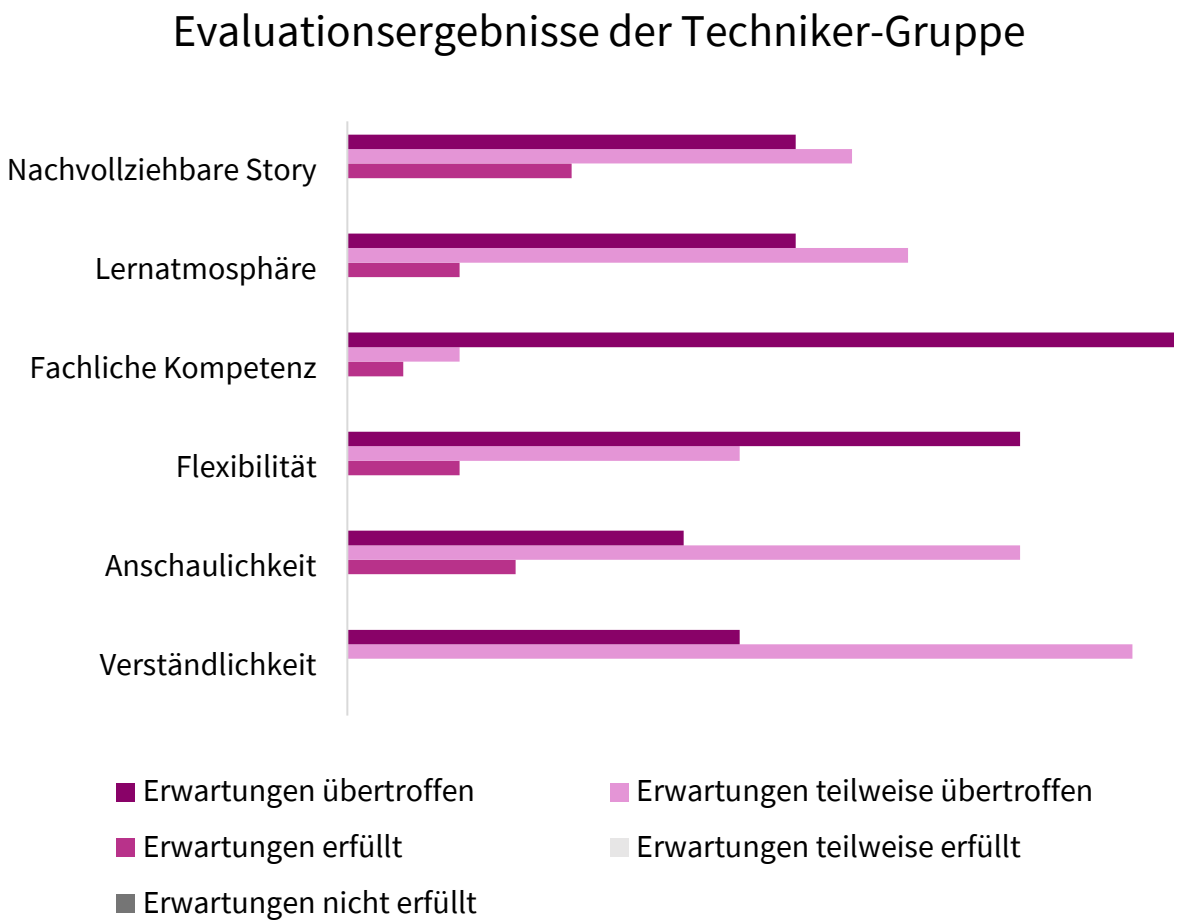

Abbildung 5: Umfrageergebnisse Techniker-Gruppe – Erwartungen

Als Wunsch für zukünftige Übungen wurde ein gruppenübergreifender Austausch genannt, bei dem auch die Entscheidungen der anderen Gruppen berücksichtigt werden können. Außerdem wäre es möglich, im Vorfeld der Übung Listen zu entwerfen, die sich auf die Vorgehensweise innerhalb einer Cyberkrise fokussieren und im Verlauf der Übung gemeinsam mit den Teilnehmerinnen und Teilnehmern ausgefüllt werden. Dadurch kann das erforderliche strukturierte Vorgehen direkt während der Übung trainiert und verinnerlicht werden.

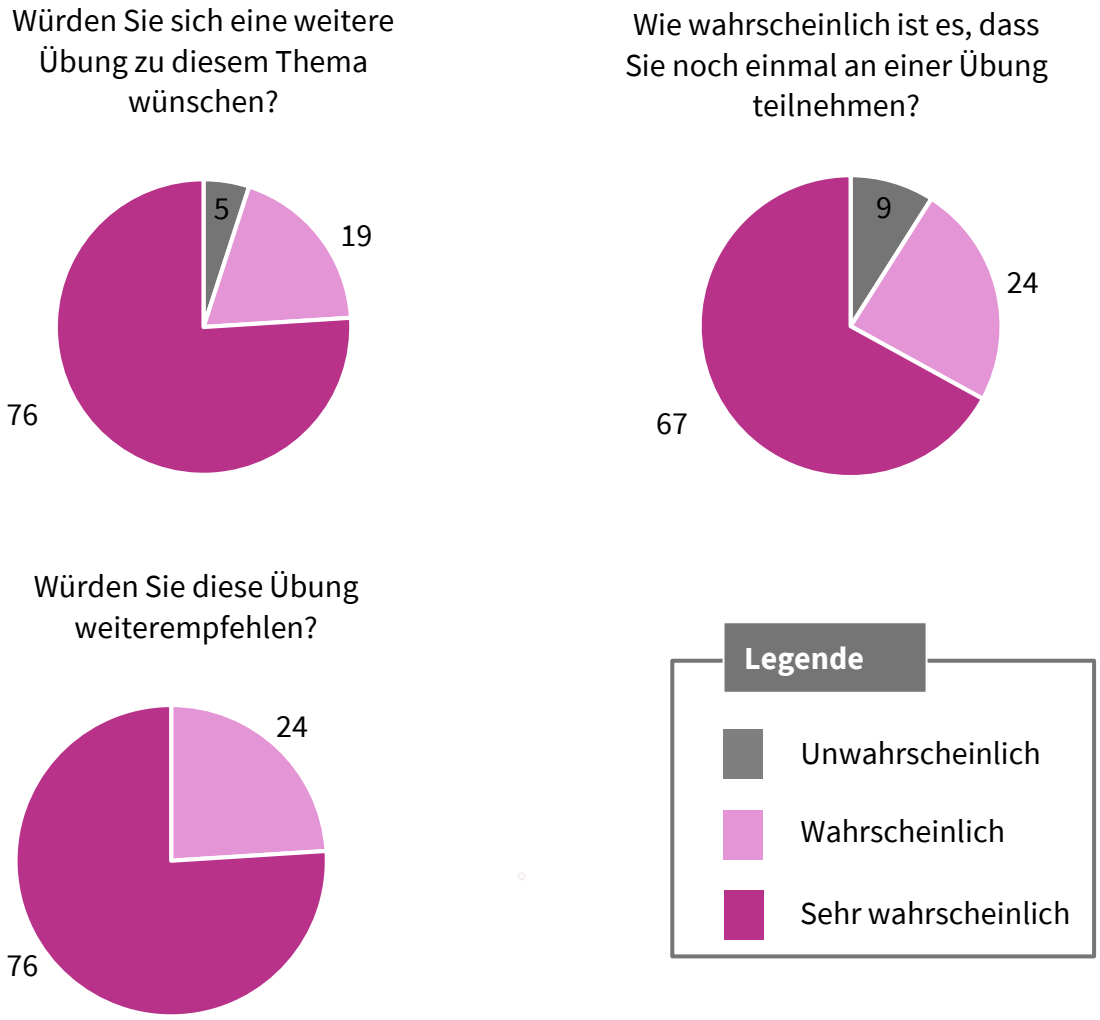

Abbildung 6: Umfrageergebnisse Techniker-Gruppe – erneute Teilnahme

100 Prozent der Techniker-Gruppe würden diese Übung weiterempfehlen. 95 Prozent wünschen sich eine weitere Übung zu diesem Thema und 91 Prozent würden auch noch einmal an einer Übung teilnehmen.

Insofern wird auch hier ausdrücklich empfohlen, weitere Cybersicherheitsübungen auf Techniker-Ebene durchzuführen.

4.3 Positive Aspekte und Verbesserungsvorschläge der Teilnehmerinnen und Teilnehmer

In der folgenden Abbildung sind Begriffe dargestellt, die in der positiven Bewertung der Cybersicherheits-übung durch die Teilnehmerinnen und Teilnehmer besonders häufig gefallen sind. Große Begriffe wurden häufig genannt, kleine hingegen weniger.

Besonders deutlich zeigt sich, dass die Teilnehmerinnen und Teilnehmer mit der Struktur und der klaren Darstellung während der Übung insgesamt zufrieden waren. Auch die Vorgehensweise und der Fokus auf Informationstechnologie (IT) und Operative Technologien (OT) sowie die Vorbereitung auf eine Krise stellten sich als gelungene Aspekte der Cybersicherheitsübung heraus.

Abbildung 7: Wordcloud zu gelungenen Aspekten der Cybersicherheitsübung

In der folgenden Abbildung sind Begriffe für Aspekte dargestellt, die im Rahmen der Cybersicherheitsübung als verbesserungswürdig erachtet wurden. Auch hier gibt die Größe der Begriffe ihre Häufigkeit in den Umfragebögen wieder. Große Begriffe wurden häufig genannt, kleine hingegen weniger.

Deutlich zeigte sich in den Umfragebögen, dass sich die Teilnehmerinnen und Teilnehmer bei einer Folgeübung die Möglichkeit für mehr Austausch zwischen den Gruppen wünschen. Zudem wurde angemerkt, dass auf optimale Bedingungen für eine Sicherheitsübung wie eine gute Raumakustik, die Möglichkeit einer strukturierten Sitzordnung und Arbeitsmaterialien zum strukturierten Arbeiten geachtet werden sollten und die Simulationszeit für einen besseren Überblick anhand eines Zeitstrahls abgebildet werden sollte. Teilweise wünschte man sich auch seitens der Gruppenmitglieder eine stärkere Feedbackkultur zwischen der Moderation und den Gruppen.

Abbildung 8: Wordcloud zu Verbesserungsvorschlägen hinsichtlich der Cybersicherheitsübung

5 Fazit

Gerade Energienetze sind besonders gefährdet und Cyberangriffe auf sie können einen großflächigen Dominoeffekt und überregionale Konsequenzen nach sich ziehen. Damit ist die Sicherheit von Stromnetzbetreibern auch kritisch für die Bevölkerung.

Vor dem Hintergrund dieser Bedrohung ist neben technischen Aspekten zur präventiven Abwehr vor allem auch die interne Vorgehensweise bei einem Cybersicherheitsvorfall erfolgskritisch für die Bewältigung einer Krise. Verantwortliche Akteure, Aufgaben und Prozesse müssen für alle Beteiligten in der Organisation klar sein. Dazu gehören insbesondere auch die Anforderungen an die Kommunikation mit Dritten – seien es Partnerorganisationen oder Behörden.

Cybersicherheitsübungen sollen genau diese Voraussetzungen schaffen und dienen als wichtiges Instrument zur Erhöhung der Resilienz sowie zur Vorbereitung auf einen Sicherheitsvorfall.

Schwerpunkt dieser Übung war es, das Verständnis für Angriffsvektoren sowie für die verschiedenen Rollen einschließlich ihrer Funktionen, der Zusammenarbeit und der Kommunikation zu festigen. Des Weiteren wurden zu berücksichtigende Vorgehensweisen zur Abwehr bei Angriffen definiert sowie notwendiges Know-how vermittelt und erhärtet, um einen Angriff zu erkennen, einzudämmen und abzuwehren und ein sicheres System wiederherzustellen.

Ziel der Cybersicherheitsübung war die Verbesserung der folgenden Kompetenzen:

- **Fachkompetenz:** Fachliche Zusammenhänge wurden schnell erfasst und Wissen über das erforderliche Schnittstellenmanagement war vorhanden.
- **Kooperation & Zusammenarbeit:** Alle Teilnehmerinnen und Teilnehmer waren aktiv an der Bewältigung der Krise beteiligt. Es fand ein reger Gedankenaustausch statt und es herrschte ein respektvoller Umgang miteinander.
- **Umsetzungsorientierung:** Getroffene Entscheidungen sind geprägt von vielseitigen Erfahrungshintergründen und umfangreichen Diskussionen.
- **Kommunikation:** Man bemühte sich um eine klare Krisenkommunikationsstruktur. Die Reaktionen auf Vorfälle/Injects wurden im Verlauf der Übung deutlich präziser und ausführlicher.
- **Analytische Kompetenz & Urteilsvermögen:** Die Teilnehmerinnen und Teilnehmer entwickelten eine strukturierte Vorgehensweise, bei der die Personen mit den einzelnen Zuständigkeiten während der Lagebesprechungen ihr Wissen beisteuern konnten.

Schließlich lassen sich einige positive Aspekte der Cybersicherheitsübung hervorheben. Mithilfe dieser Cybersicherheitsübung konnte nachhaltige Awareness für Cyberattacken geschaffen und es konnten relevante Bewältigungsstrukturen einstudiert werden. Das erlangte Wissen können die Teilnehmerinnen und Teilnehmer nun in ihren Unternehmen weitergeben und eine Umsetzung erforderlicher Sicherheitsmaßnahmen anstreben. Zudem wurde die Relevanz der Zusammenarbeit von Personen mit verschiedenen Verantwortlichkeiten verdeutlicht und die notwendigen Kommunikationswege wurden trainiert.

In der Analyse wurde jedoch an einigen Stellen auch ein gewisses Verbesserungspotenzial von den Teilnehmenden gewünscht:

1. Relevanz von Rollenverteilungen durch die Moderation verdeutlichen, sollten diese nicht vorgenommen werden
2. Klare Kommunikation, inwiefern ein Rollenspielcharakter bei der Simulation gewünscht ist
3. Diskussionen lenken, wenn sie nicht zielführend scheinen und ggf. unterbrechen
4. Gruppengröße auf fünf bis zehn Teilnehmerinnen und Teilnehmer beschränken
5. Meilensteine vordefinieren und Konsequenzen der getroffenen Entscheidungen aufzeigen
6. Zu strukturierten Dokumentationen anregen, da sonst Zwischenergebnisse verloren gehen
7. Bessere Übersicht der Simulationszeit (z. B. Zeitstrahl)
8. Optimale Rahmenbedingungen und Räumlichkeiten für Sicherheitsübung schaffen, vor allem in Bezug auf die Akustik und etwaige Störungen

Es wird empfohlen und von den Teilnehmerinnen und Teilnehmern gewünscht, gezielt und in regelmäßigen Abständen weitere Cybersicherheitsübungen durchzuführen, um die Awareness im Energiesektor als Teil der kritischen Infrastruktur Deutschlands weiter zu fördern. Vor dem Hintergrund der aktuellen politischen Situation ist darauf hinzuweisen, dass die Einübung des Umgangs mit Cyberattacken und die Entwicklung entsprechender Prozesse nicht erst bei einem Vorfall, sondern bereits im Vorfeld im Rahmen von entsprechenden Vorbereitungen auf potenzielle Cybersicherheitsvorfälle wie der Durchführung einer solchen Übung erfolgen müssen. Um unternehmensspezifische Prozesse in derartigen Übungen besser berücksichtigen zu können, ist es von Vorteil, Krisensimulationsübungen explizit im eigenen Unternehmen durchzuführen. Dabei spielen sich die Akteure aufeinander ein und lernen die Abläufe in der Praxis kennen.

Abbildungsverzeichnis

www.dena.de

dena
Deutsche Energie-Agentur