Future Energy
Lab

ANALYSE

Gemeinsam lernen – Lern- und Austauschformate zu Cybersicherheit in der Energiewirtschaft

Ein Projekt der

dena

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

Autorinnen und Autoren:
Linda Schwarz und Marieke Petersen, Gesellschaft für Informatik e. V.
Stefan Sütterlin, Hochschule Albstadt-Sigmaringen
Marius Dechand und Lukas Huttny, dena

Formate-Design:
Julia Schuetze, Cyber Policy Haus
Linda Schwarz, Gesellschaft für Informatik e. V.

Illustration & Gestaltung:
THANHXTU

Redaktion:
Friederike Wenderoth, dena

Bildnachweis:
Claudius Pflug

Stand:
Mai 2025

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2025): Gemeinsam lernen. Lern- und Austauschformate zu Cybersicherheit in der Energiewirtschaft

Bundesministerium
für Wirtschaft
und Energie

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

Inhalt

Executive Summary

„Wie kann die Energiewirtschaft gemeinsam aus Cyberattacken auf einzelne Unternehmen lernen, um die Resilienz der gesamten Branche zu stärken?“

In der Branchenplattform „Cybersicherheit in der Stromwirtschaft“ wurden auf Grundlage von Theorien aus Psychologie und Pädagogik und im Austausch mit Branchenvertreterinnen und -vertretern die folgenden zentralen Elemente für nachhaltiges Lernen im Bereich Cybersicherheit identifiziert:

- **Verstetigung:** Um eine Verhaltensänderung zu bewirken, müssen drei Faktoren erfüllt werden: Die Person muss motiviert sein, die Lerninhalte müssen an individuelle Fähigkeiten angepasst werden und es braucht regelmäßige Trigger zum Abrufen der Lerninhalte. Ein gutes Verständnis der Zielgruppe ist dafür eine notwendige Voraussetzung.
- **Vertrauen:** Informationen zu einer Cyberattacke auf ein Unternehmen sind sensible Informationen, die missbräuchlich verwendet werden können. Sie zu teilen, setzt Vertrauen in das Gegenüber voraus, das über einen längeren Zeitraum aufgebaut werden muss oder durch klare Regeln wie Non-Disclosure Agreements (NDAs) oder Information Sharing Policies etabliert werden kann.
- **Offene Fehlerkultur:** Eine gesunde Fehlerkultur ist es erforderlich, dass Menschen sich dabei wohlfühlen, ihre eigenen Fehler offenzulegen. Dafür müssen sie darauf vertrauen können, dass ihre Fehler nicht gegen sie verwendet werden. Fehler dürfen daher nicht als persönliches Versagen wahrgenommen werden, sondern als Lernchance. Dafür müssen alle Beteiligten verstehen, welche situativen Bedingungen zu einer Handlung geführt und so einen Fehler verursacht haben.
- **Wissenstransfer und gemeinsame Sprache:** Ein erfolgreicher Austausch über ein bestimmtes Thema setzt voraus, dass beide Seiten im Gespräch das Thema richtig einordnen können, und hängt auch davon ab, wie sich das Gegenüber zum Thema positioniert. Um eine Vergleichbarkeit und einen effektiven Erfahrungsaustausch zwischen Unternehmen zu ermöglichen, müssen sich diese bewusst machen, aus welcher Perspektive sie selbst sprechen, die eigene Perspektive ins Verhältnis zu den Sichtweisen anderer setzen und aus den Erkenntnissen eine gemeinsame Gesprächsgrundlage und übertragbare Einsichten entwickeln, also eine Brücke zwischen den jeweiligen Positionen bauen. Ein großes Unternehmen mit einer eigenen IT-Sicherheitsabteilung kann Cybersicherheitsmaßnahmen anders umsetzen als ein mittelständischer Betrieb mit begrenzten Ressourcen. Damit der Austausch dennoch Mehrwert bietet, müssen Unternehmen nicht nur ihre Lösungen teilen, sondern auch die Bedingungen, unter denen sie funktionieren – etwa regulatorische Anforderungen, interne Strukturen oder verfügbare Budgets.

Auf Basis dieser Anforderungen wurden zwölf Lernformate analysiert, (weiter-)entwickelt und nach ihrer jeweiligen Eignung den vier beschriebenen Elementen zugeordnet. Die Lernformate wurden in übersichtlichen Steckbriefen anhand von Eigenschaften wie Aufwand, Präsenz, Frequenz, Dauer, Ziel und Zielgruppe unterschieden und mit konkreten Umsetzungs- und Moderationstipps greifbar gemacht.

Die Evaluation der Lernformate hat gezeigt, dass durch die Etablierung der vier Kernelemente (Verstetigung, Vertrauen, offene Fehlerkultur sowie Wissenstransfer und gemeinsame Sprache) Inhalte effektiv vermittelt werden können und eine positiv wahrgenommene Veranstaltung durchgeführt werden kann.

Auf Basis der Evaluation können folgende Handlungsempfehlungen gegeben werden:

- **Gemeinsames Lernen stärken:** Wir empfehlen, Lernformate und Weiterbildung zu Cybersicherheit stärker gemeinschaftlich auszurichten. Die Lernenden sollten sich dazu austauschen, Fragen stellen und sich vernetzen können. Das stärkt ihr Autonomie-Empfinden und ihre Motivation. Dies ist damit ein aussichtsreicher Ansatz, um Verhalten nachhaltig zu verändern.
- **Cybersicherheit leben:** Für langfristig wirksame Effekte reicht es nicht, Mitarbeiterinnen und Mitarbeitern Inhalte zu vermitteln. Lernen zu Cybersicherheit umfasst nicht nur Wissen, sondern auch das Leben dieses Wissens und ein vertrauensvolles Miteinander, zum Beispiel eine offene Fehlerkultur. Daran müssen alle Ebenen eines Unternehmens mitarbeiten. Unsere Lernformate nehmen daher auch Prozesse in den Blick.
- **Gemeinschaftliche Lernformate reflektiert auswählen:** Die Entscheidung für ein bestimmtes Lernformat ist immer auch eine Entscheidung für eine bestimmte Art und Weise, wie die Gruppe miteinander in Kontakt tritt (zum Beispiel kooperativ, anonym, in kleinen oder in großen Gruppen). Dies mitzudenken, ist gerade beim Thema Cybersicherheit wichtig, da für einen offenen Austausch unter den Teilnehmerinnen und Teilnehmern erst Vertrauen aufgebaut werden muss.
- **Lernerfolge langfristig messen:** Wir konnten nur die unmittelbare Wirkung der getesteten Lernformate erheben. Um tatsächliche Lernerfolge zu kontrollieren, empfehlen wir, Lernformate langfristig zu evaluieren und nach eigenen Maßstäben und Zielen auszuwerten. Nur so kann beispielsweise herausgefunden werden, ob sich Verhaltensweisen tatsächlich wie gewünscht ändern.
- **Blick über den Tellerrand:** Wie sprechen Menschen aus Unternehmen anderer Länder über Cybersicherheit? Welche Effekte gibt es dort? Cybersicherheit, Transparenz und Fehlerkultur könnten im internationalen Kontext betrachtet werden. Dies könnte weitere wertvolle Erkenntnisse und neue Impulse liefern.

Diese Studie soll dazu anregen, in den Austausch zu treten sowie Erfahrungen und Wissen innerhalb der Branche zu teilen. Wir möchten die Leserinnen und Leser dazu ermutigen, die entwickelten Lernformate an die Bedürfnisse der eigenen Zielgruppe anzupassen, sie auszuprobieren und sie weiterzuentwickeln. Eine detaillierte Beschreibung der Lernformate findet sich im Anhang.

Einleitung

Die Energiewende wird digital – und das ist auch gut so. Neue Erzeugerstrukturen entstehen und erfordern eine stärkere Vernetzung untereinander. Der Einsatz digitaler Technologien bietet neue Möglichkeiten und eröffnet Chancen für einen effizienten und verlässlichen Betrieb des Netzes. Aus der Digitalisierung der Versorgungsnetze folgt jedoch nicht nur mehr Flexibilität für unsere Versorgung, sondern sie bringt auch neue Anforderungen an die bestehenden Sicherheitsstandards mit sich. So wächst mit jedem Ausbau der digitalen Infrastruktur auch die Angriffsfläche für Cyberbedrohungen. Angriffe auf einzelne Systeme oder Anlagen können über die Vernetzungen große Schäden für mehrere Akteure bedeuten.

Cybersicherheit ist daher keine individuelle Herausforderung, sondern eine gemeinsame Aufgabe der gesamten Branche. Neben einzelnen Schutzmaßnahmen von Unternehmen müssen auch kollektive Ansätze zur Bewältigung branchenweit ähnlicher Sicherheitsherausforderungen gefunden werden. Die Zusammenarbeit von verschiedenen Akteuren der Energie- und Digitalwirtschaft ist wesentlich für die Bewältigung dieser Herausforderungen. Zudem bietet eine Zusammenarbeit die Möglichkeit, durch den gezielten Austausch von Erfahrungen zu Risiken, Maßnahmen und Fehlern die Resilienz und Sicherheit der gesamten Branche nachhaltig zu stärken.

Genau hier setzt das Themenmodul „Gemeinsam aus Cyberattacken lernen“ der Branchenplattform „Cybersicherheit in der Stromwirtschaft“ der Deutschen Energie-Agentur (dena) an. Die Branchenplattform bringt Akteure aus der Digital- und Stromwirtschaft zusammen, um die Kommunikation und das Erarbeiten gemeinsamer Lösungen für mehr Sicherheit zu erleichtern. Dazu wurden in einem Stakeholder-Prozess die wesentlichen Herausforderungen identifiziert, priorisiert und in einer Themenroadmap[1] dokumentiert. Das in dieser Publikation behandelte Modul „Gemeinsam aus Cyberattacken lernen“ ist eines davon.

Diese Publikation fasst die Ergebnisse einer Studie zusammen, in der die Herausforderungen eines gemeinsamen Austauschs identifiziert und Lernformate entwickelt wurden, um sie zu überwinden. Sie soll den Leserinnen und Lesern Ideen und Anreize bieten, miteinander zu Cybersicherheit in den Austausch zu treten. Die vorgestellten Lernformate können dazu inspirieren, sie auszuprobieren und weiterzuentwickeln. Insgesamt hoffen wir, damit einen Beitrag zu mehr Transparenz und einer engagierten Umsetzung von Cybersicherheit zu leisten und damit die Cyberresilienz von Unternehmen – nicht nur der Energiewirtschaft – zu stärken.

[1] https://www.dena.de/PUBLIKATION2673

Folgende Lernformate wurden in der Studie entwickelt und teilweise auch erprobt und evaluiert:

	Format	Titel	Inhalt
01 1	Konferenzspiel	**„Entscheidungen unter Strom“**	⇒ Praxisnahe Entscheidungen zu Cybersicherheit als Plenum treffen
01 2	1:1-Gespräche	**„Rotator Live: Compliance vs. Praxis – Wo liegt der Weg zur echten Cyberresilienz?“**	⇒ Interaktiver Austausch zu Cybersicherheit im Speed-Dating-Format
01 3	Workshop	**„Sharing4Resilience – Gemeinsam zur besseren Informationspolitik“**	⇒ Ziele, Hindernisse und Umsetzungswege für eine Sharing Policy entwickeln
02 1	Storytelling	**„Lernabenteuer aus Fehlern“ live**	⇒ „Fuck-ups“ anonym teilen und in der Gruppe Lösungen diskutieren
02 2	Chatgruppen	**Themenbezogene Chatgruppen**	⇒ Geschlossene Chats mit klaren Kommunikationsregeln, um Informationen zu teilen und zu besprechen
02 3	Lerngruppen	**Micro-Learning Circles**	⇒ Regelmäßige, kollaborative Gesprächsrunden zu selbst bestimmten Themen
02 4	Coaching	**Storytelling mit Business Impact**	⇒ Technische Maßnahmen in einem anderen Licht darstellen
02 5	Publikation	**„Butter bei die Fische“**	⇒ Fragen und Antworten zu Cybersicherheitsmaßnahmen anderer Unternehmen in der Branche sammeln
02 6	Jour fixe	**„Problem Roulette – Walking in my Shoes“**	⇒ Lösungsansätze durch Perspektivenwechsel entwickeln
02 7	Fishbowl	**„Cyberangriff, wie war das noch mal?!“**	⇒ Austausch im kleinen Kreis zu Fallbeispielen, während ein größerer Kreis die Diskussion verfolgt
02 8	Kartenspiel	**(Mis-)Match Memory Game**	⇒ Unterschiede zwischen praktischen Empfehlungen und rechtlichen Vorgaben aufdecken
02 9	Warm-up	**Cybersecurity Mapping**	⇒ Eigene Verortung zu Cybersicherheit, Gemeinsamkeiten und Unterschiede visuell feststellen

Die ersten drei dieser Lernformate (hellgrau hinterlegt) wurden am 13. Februar 2025 auf einer Veranstaltung im Future Energy Lab der dena durchgeführt und evaluiert. Dabei wurde sowohl quantitatives Feedback der Teilnehmerinnen und Teilnehmer erhoben als auch qualitative Beobachtungen durch ein dediziertes Beobachterteam angestellt wurden.

1 Gemeinsam lernen: unsere Motivation und unser Vorgehen

Nur wenige Unternehmen sprechen bisher offen über Cyberangriffe, die ihnen Schaden zugefügt haben (Schulte, 2023). Wenn mein Unternehmen einen Cybersicherheitsvorfall öffentlich macht, so die Sorge vieler, zeigt es sich verwundbar. Unternehmen sorgen sich, ihre Reputation zu verlieren (Tagesspiegel Background, 2022), oder sind sich unsicher, ob und was sie aus juristischer Perspektive überhaupt teilen dürfen. Die meisten führen bei Cyberangriffen daher lieber allgemein „technische Probleme“ an und geben so wenig Informationen wie möglich preis.

Dabei kann ein offenerer Austausch über Cybersicherheitsvorfälle das Bewusstsein für Cybersicherheit schärfen und die Wahrnehmung der damit verbundenen Risiken stärken (Kahneman & Tversky, 1979). Die Informationen darüber, was bei einem Cybersicherheitsvorfall passiert und wie eine Organisation damit umgegangen ist, könnten anderen Organisationen dabei helfen, Risiken besser einzuschätzen und eigene Strategien aufzustellen oder anzupassen. Die allgemeine Resilienz würde steigen. Mehr Transparenz könnte schließlich allen helfen.

Transparenz wird jedoch schnell mit zu großer Offenheit und dem leichtfertigen Teilen sensibler Informationen verbunden. Gerade in einem kritischen Sektor wie der Stromwirtschaft können leichtfertig veröffentlichte Details zu neuen Angriffen mit gravierenden Konsequenzen motivieren. Es gibt also gute Gründe, bestimmte Informationen geheim zu halten.

Das Ziel unseres Projekts ist es, die offenkundigen Vorteile aufzuzeigen, die ein transparenterer Austausch zu Cybersicherheit auch im KRITIS-Bereich mit sich bringen kann. Als Branche zusammenzuarbeiten und voneinander zu lernen, bietet viele Möglichkeiten, eigene Schwächen zu erkennen und zu überwinden. Gleichzeitig fehlt es aber an Lernformaten, die einerseits einen sinnvollen Bezug zum Thema haben und andererseits darauf abzielen, Vertrauen aufzubauen und bestehendes Wissen auszutauschen.

Wir wollen diese Lücke schließen. Dafür erdenken wir Formate, die sowohl einen vertrauensvollen Austausch ermöglichen und anregen als auch den Anforderungen der Branche entsprechen. Vor diesem Hintergrund hat sich die zentrale Fragestellung für unser Projekt ergeben:

„Wie kann die Energiewirtschaft gemeinsam aus Cyberattacken auf einzelne Unternehmen lernen, um die Resilienz der gesamten Branche zu stärken?“

Unser Vorgehen

Methodisch haben wir uns an den Forschungsansatz von Design-Based Research (DBR) angelehnt (McKenny & Reeves, 2015). Dafür haben wir im ersten Schritt (Analyse und Erschließung) Einblicke gewonnen, wie offen und worüber sich Stakeholder der Energiewirtschaft bisher zu Cybersicherheit austauschen. Wir haben uns in dieser Phase auch dafür interessiert, welche Lernbedarfe die Stakeholder für sich und in der Energiebranche sehen. Dafür haben wir sieben Interviews mit Stakeholdern der Branchenplattform „Cybersicherheit für die Stromwirtschaft“ geführt.

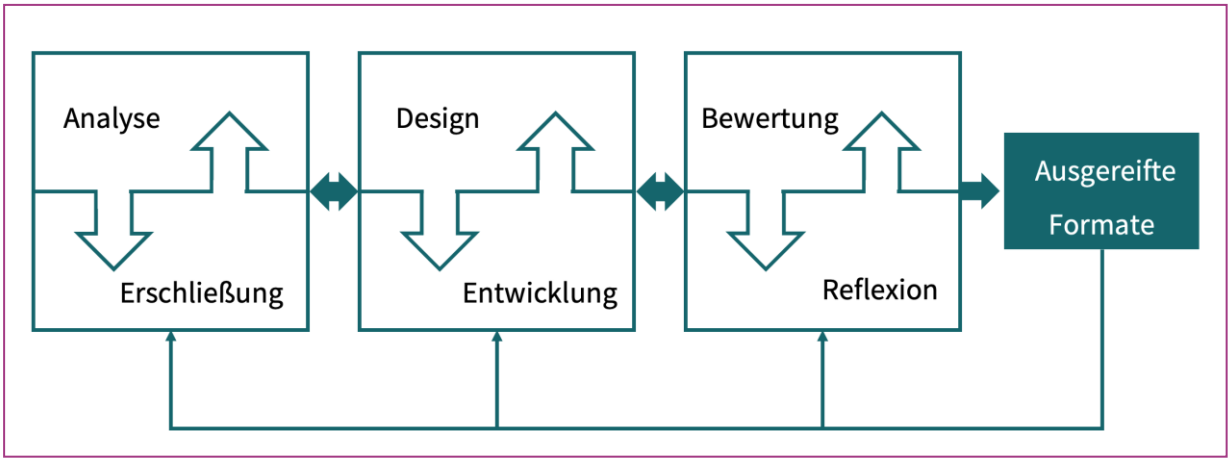


Abbildung 1 Generischer Ablauf der Methode Design-Based Research (nach McKenney & Reeves, 2015)

Parallel zu diesen Interviews haben wir psychologische und pädagogische Theorien zusammengetragen, die Voraussetzungen für gegenseitiges Vertrauen beschreiben und Wege aufzeigen, zu Verhaltensänderungen zu motivieren. Diese Theorien haben auch Ansätze aufgezeigt, um die Interviews auszuwerten. Die Verknüpfung von Interviews und Theorien lieferte uns relevante Faktoren und Themen für mögliche Lernformate.

In der zweiten Phase (Design und Entwicklung) haben wir diese Ergebnisse genutzt, um verschiedene Lernformate zu entwickeln. Drei Lernformate haben wir ausgewählt und in der dritten Phase (Bewertung und Reflexion) bei einem Workshop am 13. Februar 2025 im Future Energy Lab der dena mit Mitgliedern der Branchenplattform und interessierten Teilnehmerinnen und Teilnehmern getestet.

Auf Grundlage der Ergebnisse der Befragungen und der Bewertung der erarbeiteten Lernformate bekommen Stakeholder der Branche Möglichkeiten an die Hand, um einen gemeinsamen Austausch und ein gegenseitiges Lernen zu erleichtern. Damit wird ein erster, wichtiger Schritt in Richtung einer besseren Cyberresilienz gemacht.

Inhalte dieser Veröffentlichung

Diese Publikation fasst unsere Ergebnisse zusammen. Im folgenden Kapitel 2 stellen wir vier relevante Herausforderungen für unsere Lernformate vor, die sich aus der Verknüpfung von Theorien und Interviews ergeben haben. Diese sind:

- Teilnehmerinnen und Teilnehmer motivieren („Bereitschaft zum Lernen und Anwenden steigern“)
- Vertrauen zwischen den Teilnehmerinnen und Teilnehmern aufbauen („Gegenseitiges Vertrauen aufbauen und fördern“)
- Eine offene Fehlerkultur herstellen („Offene Fehlerkultur statt Schuldzuweisungen umsetzen“)
- Die Übertragbarkeit von Erfahrungen einordnen („Erfahrungen teilen und gemeinsam profitieren“)

Kapitel 3 stellt die Lernformate, die auf dieser Grundlage entstanden sind, in einer kurzen Übersicht dar. Die Steckbriefe in voller Länge befinden sich im Anhang. In Kapitel 4 fassen wir schließlich die Erfahrungen und Einschätzungen zusammen, die wir aus dem Praxistest der Lernformate gewinnen konnten.

2 Vier Herausforderungen für gemeinsames Lernen

Im ersten Schritt wollten wir verstehen, welche Bedarfe und Herausforderungen Mitglieder der Strombranche bei der Umsetzung von Cybersicherheit und dem Austausch dazu wahrnehmen. Zwar hatten alle bei den Interviews Befragten eigene Punkte, die für sie wichtig waren, um ihre Arbeit gut umzusetzen und ihr Unternehmen voranzubringen. Im Zusammenspiel mit den theoretischen Ansätzen konnten wir jedoch vier grundlegende Herausforderungen identifizieren. Es handelt sich um die Herausforderungen, zum Thema Cybersicherheit zu lernen und sich dazu weiterzubilden sowie Informationen dazu zu teilen. Im Folgenden stellen wir diese vier Herausforderungen vor. Wir verknüpfen dabei Eindrücke aus den Interviews mit psychologischen und pädagogischen Theorien.

2.1 Bereitschaft zum Lernen und Anwenden steigern

In den Interviews zeigten sich die Befragten unterschiedlich begeistert davon, sich mit Cybersicherheit zu befassen. Auch ihr Umfeld schätzten sie verschieden ein. Einer unserer Interviewpartner[2] betonte gleich zu Beginn des Interviews, wie unbeliebt Cybersicherheit sei: *„Niemand schreit hurra, wenn man mit Cybersicherheit kommt, weil es ja im ersten Augenblick ausschließlich Aufwand ist und die Leute nervt*.*“* Ein anderer verwies auf die jährlichen Pflichtschulungen im Unternehmen: *„Das müssen wir dann einmal pro Jahr durchklickern [sic], [...] das ist dann halt nicht ganz so spannend.“*

Gleichzeitig gab es aber auch Gesprächspartner, die mit Leidenschaft von Lernformaten zu Cybersicherheit erzählten. Ein Interviewter kam ins Schwärmen, als er vom persönlichen Austausch zu Cybersicherheit erzählte, den es in seiner Firma als etabliertes Format auf freiwilliger Basis gibt. Dabei können Kolleginnen und Kollegen zu bestimmten Zeitpunkten jedes Thema vorschlagen. Begeistert erzählte er davon, wie ein Kollege einen Ransomware-Angriff auf einen Landkreis in Ostdeutschland vorstellte und dabei scheinbar geschickt die Hintergründe mit konkreten Tipps zu Cybersicherheitsmaßnahmen verband: *„Da hat [er] das noch mal aufgearbeitet, was da alles passiert ist, wie die Erpresser vorgegangen sind und natürlich auch, welche Fallstricke im Vorhinein dabei gewesen sind und worauf man achten muss. Was man nicht anklickt und so weiter*.“ Er ergänzte: „*Und das sind natürlich Momente, die einem dann im Gedächtnis bleiben.“*

Was ist das Rezept dafür, Menschen für das Thema Cybersicherheit zu begeistern?

Um dies näher zu ergründen, bedienen wir uns des von Fogg (2009) entwickelten Modells „B=MAT“. Es erklärt, dass Verhalten (B wie das englische *Behaviour*) durch drei Einflussfaktoren bestimmt wird:

1. die *Motivation (M)* der Teilnehmerinnen und Teilnehmer, die gewünschten Verhaltensweisen zu zeigen,
2. *Ability (A)*, also das Anknüpfen an individuelle Kompetenzen und Kompetenzerfahrungen, die den gewünschten Verhaltensweisen zugrunde liegen, und
3. *Trigger (T)*, also das Bieten entsprechender Anlässe und Möglichkeiten, um die motivierten Handlungen abzurufen und auch längerfristig die Wahrscheinlichkeit ihres Auftretens zu erhöhen.

Im Folgenden stellen wir die drei Einflussfaktoren genauer vor.

[2] Bei den Interviewten handelte es sich ausschließlich um männliche Personen

Motivation – es geht nicht um Wissen, sondern um Grundbedürfnisse

Unterschiedliche Formate sind unterschiedlich ansprechend – wir sind unterschiedlich motiviert, sie zu besuchen. Das zeigen unsere Beispiele am Beginn des Kapitels. Überraschend mag sein, dass der Inhalt (oder der zu erwartende Wissensgewinn) von Lernformaten gar nicht der entscheidende Faktor für Motivation ist. Die Unterscheidung zwischen „drögen" Pflichtschulungen und vermeintlich „spannenderen" Lernsessions lässt sich stattdessen gut durch die Selbstdeterminationstheorie (SDT) von Ryan und Deci (2000) erklären.

Die SDT unterscheidet zwischen intrinsischer und selbst gewählter extrinsischer Motivation. Jemand ist intrinsisch motiviert, wenn sie oder er aus eigenem Antrieb handelt – etwa aus Spaß oder Neugier. Jemand handelt demgegenüber extrinsisch motiviert, wenn der Antrieb auf eine Konsequenz abzielt, etwa auf einen Vorteil (z. B. Geld, Anerkennung usw.) oder eine Strafe.

Zusätzlich betont die SDT die zentrale Rolle der Befriedigung dreier psychologischer Grundbedürfnisse: **Autonomie**, **Kompetenz** und **soziale Eingebundenheit**. Wenn diese Grundbedürfnisse erfüllt werden, motiviert dies. Konkret: Wenn Menschen sich als **autonom** und **kompetent** wahrnehmen und sich **bei anderen Menschen wohlfühlen**, wird ihre Motivation gefördert – unabhängig davon, ob sie eher intrinsisch oder extrinsisch ist. Die Erfüllung der drei Grundbedürfnisse führt also zu höherem Wohlbefinden, zu einer gesteigerten Leistungsbereitschaft und zu nachhaltigerem Lernen.

Tatsächlich wird dieser Dreiklang bei dem vom Interviewten vorgestellten Format bedient, bei dem ein Kollege anderen Kolleginnen und Kollegen einen Ransomware-Angriff auf einen Landkreis vorstellte: An diesem Format teilzunehmen, ist freiwillig, was die Autonomie fördert. Es ist eine interne Veranstaltung mit einem relativ kleinen Kreis von Kolleginnen und Kollegen, sodass eine gewisse soziale Eingebundenheit vorliegen sollte. Außerdem kann jede und jeder sich hier mit einem Vortrag oder einem Diskussionsbeitrag einbringen, wodurch die Teilnehmerinnen und Teilnehmer ihre wahrgenommene Kompetenz stärken können. Demgegenüber ist die jährliche Schulung zu Cybersicherheit verpflichtend. Alle führen sie allein vor dem eigenen Computer durch. Je nach Gestaltung kann sie auch das Kompetenz-Gefühl einschränken. Einer unserer Interviewpartner erklärte das so: *„Gerade wenn ich an diese Multiple-Choice-Tests denke, da habe ich es häufig, dass ich sage: Das sehe ich anders. Also, ich sehe die Lösung und sage: Ich bin trotzdem anderer Meinung. Auch wenn ich die Lösung jetzt kenne. Und ich habe ja gar keine Möglichkeit, das zu diskutieren*."

Ob die Motivation der Kolleginnen und Kollegen, an einem Format teilzunehmen, primär extrinsisch ist (weil sie dort etwa von ihrem Vorgesetzten gesehen werden wollen) oder intrinsisch (weil das Thema sie tatsächlich sehr interessiert), ist für den Outcome nachrangig. Im besten Fall kann die Ansprache der drei Grundbedürfnisse dazu führen, die Anwesenden zu einer weiteren motivierten Teilnahme am Format oder für das Thema zu begeistern. Somit kann sich langfristig auch extrinsische in intrinsische Motivation umwandeln.

Ability – auf individuelle Lernniveaus eingehen

Um das Verhalten einer Person positiv zu beeinflussen, ist es laut dem „B=MAT"-Modell auch notwendig, auf die Fähigkeiten (*Ability*) der jeweiligen Person einzugehen. Die Frage hierbei ist, wie gut Lernformate an die individuellen Fähigkeiten der Teilnehmerinnen und Teilnehmer anknüpfen.

Die meisten unserer Interviewpartner berichteten von Online-Pflichtschulungen zu Cybersicherheit für alle Beschäftigten. Diese Schulungen sind allgemein, das heißt, alle Mitarbeiterinnen und Mitarbeiter erhalten dieselben Informationen. Spezifische Schulungen, die aufeinander aufbauen und an die jeweiligen Fähigkeiten anknüpfen, erwähnten die Interviewten als Weiterbildungen. Diejenigen, die sie nannten, waren für

sie intrinsisch motiviert: *„Weil es mich halt so sehr interessiert, habe ich bei unserem ersten Anbieter, mit dem wir Pen-Tests[3] zusammen gemacht haben, […] den Junior[-Pen-Tester] dieses Jahr absolviert. Das war ein 8-Tage-Kurs mit einer Prüfung im Anschluss, Theorie und Praxis. Ich würde nächstes Jahr gerne dann den Professional-Pen-Tester machen.“* In diesem Fall begeisterte es unseren Interviewpartner, immer mehr Expertise aufzubauen. Doch auch das Unternehmen profitiert: *„Weil wir es ja auch hier für uns im Unternehmen haben wollen, dann haben wir halt nicht nur die eine Woche im Jahr, wo die Pen-Tester bei uns unterwegs sind. Dann kann ich auch selber mal zwischendurch was machen, gucken, ob das neue Gerät, das wir da jetzt in Betrieb genommen haben, sicher ist etc.“*

Ability umfasst jedoch nicht nur die Notwendigkeit, Formate an das vorhandene Wissen einer Zielgruppe anzupassen. Der Einflussfaktor beinhaltet auch die Notwendigkeit, sich kommunikativ auf das Gegenüber einzustellen und seine Perspektive übernehmen zu können. Ein Interviewter mit Erfahrung in Lernformaten erläuterte: *„Bei einem CIO müssen sich die Sachen anders erklären als bei einem CISO, einem CERT-Leiter, einem Incident Responder oder einem Meldeanalysten.“* Weiterhin erläuterte er am Beispiel des Erstellens von Gruppenregeln: *„[Es braucht] eine Sprache, mit der man diese Regeln allen erklärt und verständlich macht.“*

Wir verstehen einander also besser, wenn wir an unser jeweiliges Wissen und unsere Sprache anknüpfen. Noch ein weiterer Schritt für ein gegenseitiges Verständnis ist es, ein gemeinsames Situationsverständnis zu schaffen. Dabei erarbeiten Personen ein übereinstimmendes Bild einer Situation, um Missverständnissen und falschen Annahmen vorzubeugen. Dieses gemeinsame Situationsverständnis kann als Basis für eine nachhaltige Kommunikationsstruktur dienen und das angestrebte Verhalten selbstständig verstetigen.

Wie kann das konkret aussehen? Ein Interviewter gab hierfür ein Beispiel. Er sprach davon, wie er selbst Menschen für die Dringlichkeit von Cybersicherheit sensibilisiert, die damit wenig zu tun haben. Er schafft ein gemeinsames Situationsverständnis, indem er ihnen Cyberangriffe als Teil einer hybriden Kriegsführung erläutert. Diese Einordnung rufe bei Menschen sehr lebhafte Reaktionen hervor: *„[Es ist] wichtig, im Hintergrund zu wissen, was da passiert und dass das jetzt nicht alles harmlos ist, sondern dass da schon richtig was hintersteht. […] Die Leute sind sehr interessiert daran […]. Und sie hören das häufig in dieser Deutlichkeit dann zum ersten Mal, was dazu führt, dass man mehr Aufmerksamkeit bekommt und dass das dann eher hängenbleibt.“*

Lerninhalte müssten so vermittelt werden, dass die Menschen, die sie adressieren, sie verstehen und annehmen können. Genauso müssen sie die Lerninhalte als relevant für ihr eigenes Handlungsfeld begreifen.

Trigger setzen – Lernen in den Alltag einbinden

Der dritte und letzte Einflussfaktor des „B=MAT“-Modells sind Trigger, also das Schaffen von Auslösern oder Gelegenheiten für das gewünschte Verhalten. Trotz vorhandener Fähigkeiten und bestehender Motivation, so das Modell, bleibt ohne entsprechende Auslöser vielfach die Umsetzung des erlernten Verhaltens aus.

Trigger können durch Regelmäßigkeit gesetzt werden. Ein Interviewpartner erzählte zum Beispiel: *„Jeden Mittwochmorgen haben wir alle in eine Konferenz geholt und darüber gesprochen, was eigentlich die Woche bei wem vorgefallen ist. [...] Und haben dazu dann auch regelmäßig Online-, also nicht nur On-site-Meetings gemacht. Das war schon ziemlich viel Aufwand, auch Organisationsaufwand [...]. Das hat sich aber ausgezahlt.“*

Neben Regelmäßigkeit ist es aber auch wichtig, dass Anlässe niedrigschwellig und anschlussfähig sind. Eine Beobachtung aus unseren Interviews veranschaulicht dies: Viele Interviewte konnten auf unsere Frage, wie

[3] Bei einem Pen-Test (Penetrationstest) wird ein Cyberangriff simuliert, um Schwachstellen in der IT, aber auch im Betrieb festzustellen.

viel Zeit sie wöchentlich zum Lernen hätten, nur schwer antworten. „*Explizite Lernzeit? Null*“, so ein Interviewpartner. *„Bei meiner Arbeit ist nicht so genau zu unterscheiden zwischen Lernen und Arbeiten“*, so ein anderer. Das klassische Verständnis von Lernen als das Ruhenlassen sonstiger Tätigkeiten, um etwa ein Buch aufzuschlagen und zu lesen, ist für viele im Alltag nur schwer umsetzbar. Stattdessen sollten Lernformate an konkrete Aufgaben und Arbeitsinhalte anknüpfen.

Schlussfolgerungen

Für ein erfolgreiches Lernformat muss die Zielperson verstanden werden: Was motiviert sie, was kann und weiß sie schon, bei welchen Gelegenheiten kann sie das Verhalten anwenden? Entsprechend müssen alle drei Punkte des „B=MAT“-Modells berücksichtigt werden, damit die gewünschte Handlung eintritt.

Um die angesprochene Person zu motivieren, ist es darüber hinaus wichtig, zu verstehen, warum sie Interesse an einer Weiterbildung hat: Ist sie von sich aus am Thema interessiert oder motiviert es sie beispielsweise, in Lernformaten mit ihren Kolleginnen und Kollegen gemeinsam zu arbeiten und dabei als kompetent wahrgenommen zu werden? Entsprechend muss der Aufbau eines Lernformats angepasst werden.

Ebenso setzt ein gelungenes Lernformat voraus, dass die Inhalte und die Darstellung zu den tatsächlichen Fähigkeiten der Zielperson passen. Erfolgreiche Lernformate dürfen die Zielperson weder frustrieren noch unterfordern. Wenn eine Person Lerninhalte versteht, kann sie auch einen Bezug zum eigenen Handeln herstellen und Erlerntes sinnvoll einsetzen.

Empfehlungen zu den Lernformaten

Für die Umsetzung der angesprochenen Punkte empfehlen wir die folgenden entwickelten Lernformate. (Eine vollständige Erläuterung der jeweiligen Lernformate findet sich im Anhang.)

- *„Entscheidungen unter Strom“:* Das Konferenzspiel animiert zu strategischen Entscheidungen im Fall eines Cybersicherheitsvorfalls und verbindet Wissensabfrage und Wissensvermittlung. Der kooperative Aufbau motiviert die Teilnehmerinnen und Teilnehmer, zusammenzuarbeiten. Das schafft soziale Eingebundenheit. „Joker“-Rollen, bei denen alle mit ihrem Wissen das Team unterstützen können, steigern die Kompetenzwahrnehmung. Entscheidungsfreiheiten im Spielverlauf unterstützen die wahrgenommene Autonomie. Zu Beginn ordnen die Teilnehmerinnen und Teilnehmer sich nach ihrer Rolle im Bereich Cybersicherheit ein, sodass die Moderation Erklärungen und Hilfen im Spielverlauf an das Kompetenzniveau der Gruppe anpassen kann. Zuletzt ermöglicht das Spiel, Wissen abzufragen und zu testen, ob Gelerntes richtig angewendet werden kann.
- *(Mis-)Match Memory Game:* Auch dieses Lernformat ist kooperativ. In Anlehnung an das klassische Memory bilden die Spielkarten Standards, praktische Empfehlungen und Best Practices ab, deren Passung gemeinsam reflektiert werden soll. Spielerinnen und Spieler decken etwa Unterschiede zwischen technischen Anforderungen und vorgegebenen Standards auf und diskutieren sie. Die Verknüpfung von Spiel- und Lerninhalt erleichtert es, sich mit Lücken in einer Cybersicherheitsstruktur zu befassen. Das Spiel wendet sich an verschiedene Personen mit unterschiedlichen Lernniveaus. Es ist sowohl für intrinsisch als auch für extrinsisch motivierte Spielerinnen und Spieler geeignet.

2.2 Gegenseitiges Vertrauen aufbauen und fördern

In den Interviews waren wir auch daran interessiert, wie weit unsere Gesprächspartner dazu bereit sind, eigene Learnings zu teilen. Viele Interviewpartner waren dabei vorsichtig. Die Frage, ob er Erfahrungen aus Krisenübungen teilen würde, verneinte ein Gesprächspartner kategorisch: *„Nur wenn du Ermittlungsbehörde oder Polizei wärst."* Auch viele andere Interviewteilnehmer waren vorsichtig, besonders hinsichtlich technischer Details: *„Ich würde die aktuelle Konfiguration unserer Software und Docker-Infrastruktur nicht aufmalen und rausgeben."* Ähnlich ein weiterer Interviewter: *„Ich würde natürlich nie über technische Details von Maßnahmen sprechen, die wir hier im Haus haben."* Letzterer fügte aber hinzu: *„Zumindest nicht so, dass sie öffentlich irgendwo stehen."*

In einem gewissen, vertrauten Rahmen waren einige Interviewte bereit, transparent über unternehmerische Strategien und Vorfälle sowie ihren Umgang mit Cybersicherheit zu sprechen. Schließlich sind es auch solche Details, auf die viele besonders neugierig sind. Über Cybersicherheitsvorfälle und effektive Sicherheitsmaßnahmen zu schweigen, heißt, dass andere nicht davon lernen können. Es unterbindet, sich über reale Gefahren auszutauschen. Oder wie ein Interviewter zusammenfasste: *„Obscurity is no security."*

Wie lässt sich also ein sicherer und vertrauter Rahmen für einen transparenten Austausch zu Cybersicherheit schaffen?

Interpersonales Vertrauen bedeutet, dass man sich in einer sozialen Beziehung verletzlich zeigt und darauf vertraut, nicht ausgenutzt zu werden. Laut dem Modell von Mayer et al. (1995) wird Vertrauen durch die **Wahrnehmung** von **Kompetenz, Wohlwollen** und **Integrität** gefördert. Integrität beschreibt, wie sehr das Verhalten einer Person mit **ihren inneren Werten** und **Überzeugungen** übereinstimmt. Diese Übereinstimmung sorgt dafür, dass ihr Handeln vorhersehbar bleibt – unabhängig von der Situation oder dem Zeitpunkt. **Vorhersehbarkeit** ist also eine grundlegende Voraussetzung für das Entstehen von Vertrauen.

In der Praxis heißt das zum einen: Vertrauen braucht Zeit. Der Interviewpartner, der von den regelmäßigen wöchentlichen Meetings in geschlossener Runde erzählte, bestätigte dies: *„Die Menschen sind immer offener geworden im Laufe der Zeit, haben immer mehr erzählt, haben immer mehr reingegeben und es ging dann auch nicht so darum, dass man über Incidents erzählt, sondern über eigene Erkenntnisse."*

Zum anderen lässt sich Vertrauen durch Regeln fördern. Ein Beispiel aus den Interviews: *„Da haben wir einen Rahmen geschaffen, in dem man offen reden konnte. Und dann kannst du ganz anders miteinander umgehen. Es war ein organisatorischer Rahmen, es war auch ein legaler Rahmen, mit eigenen NDAs und Sharing Policies und so weiter."* Gut recherchierte und miteinander abgestimmte Regeln geben Teilnehmerinnen und Teilnehmern schließlich auch Sicherheit und die Kompetenz zur Differenzierung, welche Informationen sie teilen dürfen und welche nicht.

Schlussfolgerungen

Bei den Befragten besteht ein großes Interesse an Informationen zu Cybersicherheit von anderen Unternehmen. Die Sorge davor, dass andere preisgegebene Informationen ausnutzen oder missbrauchen, verhindert jedoch oft Transparenz. Das Teilen von Informationen setzt daher im ersten Schritt voraus, dass das Gegenüber als vertrauenswürdig eingeschätzt wird.

In den Interviews zeigten die Befragten bereits Wege auf, die ein Teilen von Informationen ermöglichen würden: durch die gegenseitige Zusicherung von Verschwiegenheit mittels NDAs oder Sharing Policies und

durch den Aufbau von Vertrauen zum Gegenüber. Dies setzt wie oben beschrieben voraus, dass man das Gegenüber als integer, wohlwollend und kompetent wahrnimmt. Dies kann man durch wiederkehrende Formate erreichen, in denen Teilnehmerinnen und Teilnehmer sich als Personen kennenlernen. Zusätzlich kann man gemeinsame Regeln und eine Sharing Policy für den Austausch festlegen.

Empfehlungen zu den Lernformaten

Um das gegenseitige Vertrauen zu steigern, empfehlen wir folgende Lernformate, die wir im Anhang mittels Steckbriefen ausführlich erläutern:

- *Fishbowl – „Cyberangriff, wie war das noch mal?!":* In einem kleineren Kreis diskutieren die Teilnehmerinnen und Teilnehmer über ihre Erfahrungen mit Cyberangriffen, während ein größerer Außenkreis zuhört und bei Bedarf eigene Inhalte beiträgt. Der im inneren Kreis stattfindende offene Austausch über Erfahrungen mit Cybersicherheitsvorfällen erzeugt reziproke Beziehungen: Ich teile und erwarte damit, dass auch du teilst. Ein klarer Rahmen (hier die kleinen Kreise des Austauschs) steigert die Vorhersehbarkeit, da abzuschätzen ist, wer alles aktiv zuhören wird. Jede Person kann außerdem selbst flexibel entscheiden, wie und in welcher Tiefe sie auf ihre Erfahrungen eingeht.
- *Micro-Learning Circles:* Teilnehmerinnen und Teilnehmer mit einem ähnlichen fachlichen Hintergrund treffen sich über einen längeren Zeitraum regelmäßig, um zu einem Thema zu arbeiten. Aufgrund ihres ähnlichen Erfahrungshintergrunds können sie davon ausgehen, dass ihr geteiltes Wissen von den anderen leicht verstanden wird und bei diesen damit einen Mehrwert erzeugen kann. Gemeinsam an einem festen Thema zu arbeiten und sich wiederholt zu treffen, fördert die Involviertheit der Teilnehmerinnen und Teilnehmer. Gleichzeitig gibt das Format feste Regeln des Austauschs vor, die innerhalb des Kreises angepasst werden können.
- *Themenbezogene Chatgruppen:* Durch eine klare Übersicht der Teilnehmerinnen und Teilnehmer in geschlossenen Chatgruppen ist Vorhersehbarkeit sowie Reziprozität gegeben, da alle etwas beisteuern können. Mittels einer Sharing Policy werden dem Austausch klare Grenzen gesetzt. Ebenso ermöglicht die Sharing Policy, das gegenseitige Vertrauen durch Formalisierung zu stärken.
- *Sharing4Resilience Policy Guide:* In einem Workshop erarbeiten kleine Gruppen erste Ansätze für eine Sharing Policy. Das Format dient weniger einem unmittelbaren Austausch. Es soll den Austausch verbessern, indem die Teilnehmerinnen und Teilnehmer Regeln und Möglichkeiten dafür erarbeiten. Sie können so selbstständig einbringen, welche Themen für sie wichtig sind, welche Hindernisse sie für einen transparenten Austausch sehen und wie sich diese überwinden lassen. Das Format dient dem Aufbau gegenseitigen Vertrauens, da die Regeln des Austauschs selbst definiert werden.

2.3 Offene Fehlerkultur statt Schuldzuweisungen umsetzen

Vor allem den Interviewten aus kleineren Unternehmen war es wichtig, über Fehlerkultur zu sprechen: *„Wir haben Leute, die fangen bei uns neu an, die haben mega Angst am Anfang, weil sie es aus anderen Bereichen oder aus dem Studium so kennen: Wenn ein Fehler passiert, dann kriegst du eine schlechte Note, dann wirst du abgestraft, dann wirst du halt abgesetzt.“* Stattdessen setzt dieser Interviewte, ein Geschäftsführer, auf Offenheit: *„Ich finde, das ist ein ganz essenzieller Part des Lernens, dass man halt sagt: Okay, es können Fehler passieren und Fehler können auch dreimal passieren, das gehört einfach dazu.“* Für ihn sei eine fehlende offene Fehlerkultur der größte Inhibitor für Fortschritt und für Lernen. Er ergänzte*: „Cybersecurity funktioniert nur, wenn jemand Verantwortung dafür übernimmt, was da steht. Und dass man auch anerkennt, dass das auch schiefgehen kann.“*

Auch weitere Interviewte sprachen das Thema Fehlerkultur von sich aus an. Ein zweiter Gesprächspartner sah eine fehlende offene Fehlerkultur insbesondere als Problem mittelständischer Konzerne: *„Gerade im Mittelstand hast du halt häufig noch einen alten, also einen autoritären und Top-down-Führungsstil.“* Dieser sei auch nach außen hin bemerkbar und verhindere den Austausch und einen gemeinsamen Fortschritt. Der Interviewte fragte entsprechend: *„Wie kriegen wir einen Kulturwandel hin, wie können wir anders mit Security umgehen? Wie kommen wir dahin, dass wir die Opfer von Angriffen wirklich auch als Opfer begreifen und nicht in so ein doofes Blame Game gehen: ‚Ihr seid ja selber schuld. Kein Backup, kein Mitleid.‘?“*

Wenn Fehler als persönliche oder organisatorische Inkompetenz angesehen werden, spricht man in der Psychologie vom **Fundamentalen Attributionsfehler** (FAI) (Ross, 1977). Diese Theorie beschreibt eine **kognitive Verzerrung**, bei der Handlungen anderer Menschen primär auf ihre Dispositionen – also auf internale Persönlichkeitseigenschaften – zurückgeführt werden. **Situative Einflüsse werden unterschätzt.** Passiert einem Menschen also ein Fehler, nimmt seine Umgebung häufig an, dass er auf willentlichen Entscheidungen beruht, anstatt die Sachzwänge dieses Menschen zu reflektieren.

Fällt ein Mitarbeiter beispielsweise auf einen Phishing-Versuch herein, wird aufgrund des FAI angenommen, er sei zu inkompetent, um Phishing-Mails zu identifizieren. Dabei wird außer Acht gelassen, dass Phishing inzwischen ein hohes Niveau erreicht hat und nur durch sorgfältige Prüfung entlarvt werden kann. Ebenso wird nicht berücksichtigt, ob der Mitarbeiter in dem Moment unter Stress stand, weil er eine Frist einhalten musste und seine Stelle personell unterbesetzt ist. Situative Probleme wie Zeitdruck, fehlendes Personal oder auch schlechte Spam-Filter werden nicht beachtet, obwohl sie entscheidende Rollen im Fall einnehmen.

Der FAI führt so dazu, dass **Fehler eher in der Inkompetenz von Beschäftigten gesehen** werden als in den systemischen Voraussetzungen, mit denen sie bei der Arbeit konfrontiert sind. Fehlinterpretationen dieser Art sind nachweislich in der Lage, Missverständnisse und fehlgeleitete Schlussfolgerungen zu fördern. Insbesondere im Bereich der Cybersicherheit kann dies zu **ineffektiven Entscheidungen** führen (Reeves et al., 2021).

Beschäftigte oder Unternehmen dazu zu motivieren, eigene Fehler offenzulegen, kann also als Stärke und als der erste Schritt interpretiert werden, strukturelle Verbesserungen anzugehen. Denn durch eine transparente Kommunikation können vorhandene Sachzwänge aufgedeckt und im nächsten Schritt verändert werden. Damit könnten alle Seiten von strukturellen Verbesserungen profitieren.

Einen Ansatz für ein solches Umdenken, das schließlich zu mehr Transparenz führen kann, äußerte ein Interviewter, dessen Unternehmen bereits Opfer eines Cybersicherheitsvorfalls geworden war: *„Es ist nicht eine*

Frage der Zeit, ob man angegriffen wird, das passiert ja ständig auf allen Kanälen, überall. Es ist eigentlich nur die Frage, wann mal einer mit so einem Angriff Erfolg hat.“ Kein System sei so sicher, dass es nie zu einem Vorfall kommen könnte. Man müsse vielmehr begreifen, dass Cybervorfälle ein systemisches Problem sind, dem sich alle stellen müssten.

Schlussfolgerungen

Eine gesunde Fehlerkultur setzt eine Atmosphäre voraus, in der Menschen Fehltritte angstfrei zugeben und teilen können. Menschen müssen darauf vertrauen können, dass ihre Fehler nicht gegen sie verwendet werden. Dies ist auch Voraussetzung dafür, dass sie sich ausprobieren und motiviert neue Dinge angehen.

Um eine offene Fehlerkultur zu schaffen, ist es hilfreich, wenn die Beteiligten verstehen, wie situative Bedingungen zu einer Handlung führen und einen Fehler hervorbringen können. So können etwa strukturelle Probleme einer Organisation entdeckt und angegangen werden.

Empfehlungen zu Lernformaten

Um nachhaltig aus Fehlern lernen zu können, braucht es auf der einen Seite die Bereitschaft, eigene Fehler transparent zu machen, und auf der anderen Seite die Fähigkeit, Fehler richtig einzuordnen. Hierfür empfehlen wir folgende Lernformate:

- *Joure fixe – „Problem Roulette – Walking in my Shoes“:* Die Teilnehmerinnen und Teilnehmer teilen aktuelle Herausforderungen in ihren Unternehmen und diskutieren sie mit der Gruppe. Die unterschiedlichen Hintergründe und Erfahrungen der Teilnehmerinnen und Teilnehmer ermöglichen eine interdisziplinäre Betrachtung des Themas. Es können neue Lösungsansätze entwickelt werden, indem das Problem herausgelöst aus dem üblichen Kontext betrachtet wird. So können sich neue Möglichkeiten ergeben, die bisher durch Sachzwänge oder eine eindimensionale Betrachtung nicht sichtbar waren.
- *Storytelling mit Business Impact:* Mit narrativen Techniken werden komplexe technische Themen für fachfremde Beschäftigte aufbereitet, sodass die Notwendigkeit und die Herausforderungen besser verstanden werden können. Ausgehend von der Position der Teilnehmerinnen und Teilnehmer (beispielsweise technisch versus strategisch) kann durch die neue Erzählung des Themas eine bessere Brücke geschlagen und mehr Verständnis erreicht werden.
- *„Lernabenteuer aus Fehlern“ live:* Durch anonymes Teilen von Fehlern und Lösungen kann einem Schamgefühl entgegengewirkt werden. Es ermöglicht mehr Transparenz im Wiedergeben von eigenen „Fuck-ups“. Da die Absender nicht bekannt werden, entsteht auch kein personenbezogener Bias. Das heißt, dass keine Informationen über die Rolle oder Person verfügbar sind und damit der Inhalt nicht mit ihnen in Beziehung gesetzt werden kann.

2.4 Erfahrungen teilen und gemeinsam profitieren

Was interessiert die Stakeholder inhaltlich aneinander, was möchten sie voneinander lernen? Mehrere Interviewte wünschten sich konkrete Benchmarks und Einschätzungen aus anderen Unternehmen ihrer Branche, zum Beispiel: *„Ich würde gerne wissen, was aus Sicht der anderen Unternehmen die fünf wichtigsten Maßnahmen sind, um die Cybersicherheit mit überschaubarem Aufwand zu verbessern.“* Oder *„Wenn [das andere Unternehmen] nur eine Cybersache ändern, abschaffen oder einführen könnte, was wäre das?“*

Die Befragten interessierten sich für die Ausgaben für und den Einsatz von konkreten Cybersicherheitsmaßnahmen, um etwa das Budget für Cybersicherheit im eigenen Betrieb einordnen zu können. Ebenso war für sie interessant, welche Angriffsvektoren die anderen Unternehmen als relevant identifiziert haben. Dabei versprachen sich die Interviewten ein objektiveres Bild von der Lage. Ziel war es, die eigene Cybersicherheit effizient zu gestalten und so unnötige Kosten einzusparen.

Doch inwiefern können Aussagen anderer tatsächlich weiterhelfen, wenn die Antworten aus unterschiedlichen Unternehmenskontexten stammen?

Um eine Vergleichbarkeit und einen effektiven Erfahrungsaustausch zwischen Unternehmen zu ermöglichen, bietet sich das Modell **Orient, Locate, Bridge** (OLB) (Knox et al., 2018) an. Das OLB-Modell ist ein kommunikationswissenschaftlicher Ansatz, der sich mit den Herausforderungen einer interdisziplinären Kommunikation in soziotechnischen Systemen, also dem Zusammenspiel von Menschen und Technik im Betrieb, befasst.

Das OLB-Modell bietet eine Struktur, um Erfahrungen aus unterschiedlichen Unternehmenskontexten vergleichbar und für den eigenen Betrieb nutzbar zu machen. Durch die drei Schritte *Orient*, *Locate* und *Bridge* soll ein Austausch ermöglicht werden, der über allgemeine Einschätzungen hinausgeht und konkrete Handlungsoptionen aufzeigt.

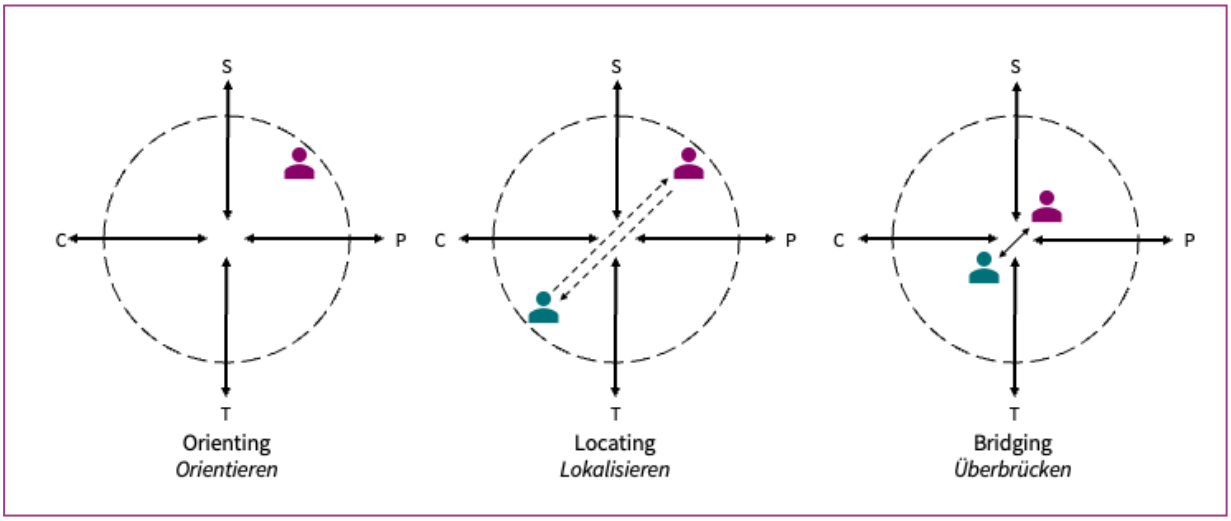


Abbildung 2 Knox et al. (2018). Eine verbildlichte Darstellung der drei Schritte des OLB-Modells: a) *Orienting* (Verorten der eigenen Perspektive im Raum), b) *Locating* (Wahrnehmen und Einordnen der Perspektiven anderer), c) *Bridging* (Überbrücken der unterschiedlichen Positionen durch angepasste Kommunikation)

Orienting bedeutet, sich bewusst zu machen, aus welcher Perspektive man selbst spricht: Welche Annahmen, Rahmenbedingungen und Zielsetzungen habe ich bzw. hat mein Unternehmen? Welche Position habe

ich auf den Achsen „strategisch“ (S), „physischer Raum“ (P), „taktisch/organisatorisch“ (T) und „Cyber-/digitaler Raum“ (C)?

Locating beschreibt den nachfolgenden Schritt, nämlich die eigene Position ins Verhältnis zu der anderer zu setzen. Wo steht mein Gegenüber? Die Frage, welche Schutzmaßnahmen andere ergreifen, erweitert sich also auf die Frage, warum sie sich genau dafür entschieden haben. (Etwa: Welchen regulatorischen, finanziellen oder technischen Hintergrund hat dieses Unternehmen im Vergleich zu meinem?) Dadurch entsteht ein differenzierteres Bild des Gegenübers.

Bridging schließlich beschreibt den letzten Schritt, aus Erkenntnissen eine gemeinsame Gesprächsgrundlage und übertragbare Einsichten zu entwickeln, also eine Brücke zwischen den jeweiligen Positionen zu bauen. In der Kommunikation zwischen Unternehmen bedeutet das, Erfahrungen so aufzubereiten, dass sie auch in anderen Kontexten anwendbar sind. Ein großes Unternehmen mit einer eigenen IT-Sicherheitsabteilung kann Cybersicherheitsmaßnahmen anders umsetzen als ein mittelständischer Betrieb mit begrenzten Ressourcen. Damit der Austausch dennoch Mehrwert bietet, müssen Unternehmen nicht nur ihre Lösungen teilen, sondern auch die Bedingungen, unter denen sie funktionieren – etwa regulatorische Anforderungen, interne Strukturen oder verfügbare Budgets. So entstehen praxisnahe Erkenntnisse, die an verschiedene Unternehmensrealitäten angepasst werden können.

Als Resultat können Gesprächspartnerinnen und -partner gezielter einordnen, was sie von anderen Kontexten lernen oder was sie nur mit Anpassungen adaptieren können.

Schlussfolgerungen

Ein erfolgreicher Austausch über ein bestimmtes Thema setzt voraus, dass beide Seiten im Gespräch das Thema sowie die eigene Positionierung und die des Gegenübers zu diesem Thema richtig einordnen können. Das OLB-Modell beschreibt, wie diese Einordnung stattfinden kann: Zuerst stellt man die eigene Position bzw. Perspektive fest, dann die des Gegenübers. Eine Distanz zwischen beiden Positionen können beide Seiten überbrücken, indem sie über ihre jeweiligen Kontexte sprechen.

Empfehlungen zu Lernformaten

Folgende Lernformate erachten wir als geeignet, um gegenseitige Positionen zu erkennen und Differenzen zu überwinden:

- *„Rotator Live: Compliance vs. Praxis“:* Im schnellen Austauschformat treffen die Teilnehmerinnen und Teilnehmer immer wieder auf neue Personen mit unterschiedlichen Hintergründen. Probleme, die diskutiert werden sollen, müssen knapp zusammenfassbar sein und so, dass die Gegenseite sie versteht. Damit wird die Verständnisbrücke gebaut.
- *Sheets – „Butter bei die Fische“:* Das Teilen von konkreten und faktenbasierten Erkenntnissen in Unternehmen ermöglicht es den Teilnehmerinnen und Teilnehmern, eigene Erfahrungen einzuordnen. Damit können sie die eigene Position mit der in anderen Unternehmen leichter vergleichen und damit Lücken aufdecken.
- *Cybersecurity Mapping:* Die Teilnehmerinnen und Teilnehmer sortieren sich räumlich nach Cybersicherheitskategorien. Die Einordnung visualisiert einen eigenen Standpunkt in Relation zu den anderen und ermöglicht so eine Orientierung und Lokalisierung. Als Warm-up-Übung bereitet das Format auf weitere Lernformate vor, die ein Bridging erreichen wollen.

3 Entwicklung der Lernformate

Angepasst an die Ergebnisse unserer Befragungen konnten wir Lernformate entwickeln, die sich an den Anforderungen von Branchenmitgliedern orientieren. Die Lernformate sprechen so zielgenau die Punkte an, die die Interviewten als Herausforderungen ansahen.

Ein Teil der Interviews war neben den Herausforderungen beim Lernen innerhalb der Branche auch darauf ausgerichtet, bevorzugte Lernmethoden und -räume der Interviewteilnehmer zu erfahren. So konnten wir nicht nur gewünschte Lerninhalte ermitteln, sondern auch nachvollziehen, wie sie am besten umsetzbar wären, um zu einer Teilnahme zu motivieren.

Mit diesem Wissen konnten wir zwölf verschiedene Lernformate entwickeln, die auf gegenseitigen Austausch, Vertrauensaufbau, Wissensvermittlung und -abfrage sowie Zusammenarbeit ausgelegt sind. Dabei können manche Formate vollständig online umgesetzt werden, andere wiederum setzen ein Treffen in Präsenz voraus. Ebenso sind die Formate unterschiedlich intensiv im Vorbereitungsaufwand. Sie können also bei Bedarf teilweise auch schnell umgesetzt werden und dienen damit als mögliche Ergänzung zu herkömmlichen Weiterbildungen oder als Warm-up vor Workshops.

Eine eindeutige Erkenntnis aus den Interviews ist, dass Vertrauensaufbau Zeit und soziale Strukturen benötigt. Daher zielen die Lernformate nicht alle vollständig auf den reinen Wissensaustausch ab, sondern bieten in einigen Formen eine „Hilfe zur Selbsthilfe“, indem sie Rahmenbedingungen vorgeben, in denen Regeln eines Austauschs erarbeitet und umgesetzt werden können.

In der unten stehenden Tabelle listen wir alle zwölf Lernformate auf und schildern kurz ihren Inhalt. Folgende Erläuterungen helfen, sie zu verstehen:

In der Tabelle sind die Lernformate, die wir im Rahmen des Workshops im Future Energy Lab der dena am 13. Februar 2025 durchführen und damit testen konnten, hellgrau hinterlegt (01-1 bis 01-3). Diese Lernformate wurden als Prototypen ausgewählt, um durchgeführt und dabei getestet zu werden. Die Testerinnen und Tester (Mitglieder der Branchenplattform und andere interessierte Personen) besprachen im Anschluss die verbliebenen neun Lernformate (02-1 bis 02-9) und diskutierten die Umsetzbarkeit aus ihrer Perspektive. Ihr Feedback haben wir im Anschluss verwendet, um die Steckbriefe zu überarbeiten.

Im Anhang haben wir die vollständige Liste der Lernformate eingefügt und visuell aufbereitet. Dort sind sie nach Aufwand, Veranstaltungsort (präsent/digital) und Frequenz aufgeschlüsselt sowie mit Hinweisen zu Lernziel und Zielgruppe versehen. Eine zusätzliche Hilfestellung für eine zukünftige Durchführung der Lernformate bieten eine Ablaufbeschreibung, eine Anleitung und Tipps zur Umsetzung.

	Format	Titel	Inhalt
01 1	Konferenzspiel	**„Entscheidungen unter Strom“**	⇒ Praxisnahe Entscheidungen zu Cybersicherheit als Plenum treffen
01 2	1:1-Gespräche	**„Rotator Live: Compliance vs. Praxis – Wo liegt der Weg zur echten Cyberresilienz?“**	⇒ Interaktiver Austausch zu Cyber-sicherheit im Speed-Dating-Format
01 3	Workshop	**„Sharing4Resilience – Gemeinsam zur besseren Informationspolitik“**	⇒ Ziele, Hindernisse und Umsetzungswege für eine Sharing Policy entwickeln
02 1	Storytelling	**„Lernabenteuer aus Fehlern“ live**	⇒ „Fuck-ups“ anonym teilen und in der Gruppe Lösungen diskutieren
02 2	Chatgruppen	**Themenbezogene Chatgruppen**	⇒ Geschlossene Chats mit klaren Kommunikationsregeln, um Informationen zu teilen und zu besprechen
02 3	Lerngruppen	**Micro-Learning Circles**	⇒ Regelmäßige, kollaborative Gesprächsrunden zu selbst bestimmten Themen
02 4	Coaching	**Storytelling mit Business Impact**	⇒ Technische Maßnahmen in einem anderen Licht darstellen
02 5	Publikation	**„Butter bei die Fische“**	⇒ Fragen und Antworten zu Cyber-sicherheitsmaßnahmen anderer Unternehmen in der Branche sammeln
02 6	Jour fixe	**„Problem Roulette – Walking in my Shoes“**	⇒ Lösungsansätze durch Perspek-tivenwechsel entwickeln
02 7	Fishbowl	**„Cyberangriff, wie war das noch mal?!“**	⇒ Austausch im kleinen Kreis zu Fallbeispielen, während ein größerer Kreis die Diskussion verfolgt
02 8	Kartenspiel	**(Mis-)Match Memory Game**	⇒ Unterschiede zwischen praktischen Empfehlungen und rechtlichen Vorgaben aufdecken
02 9	Warm-up	**Cybersecurity Mapping**	⇒ Eigene Verortung zu Cybersicherheit, Gemeinsamkeiten und Unterschiede visuell feststellen

Tabelle 1 Kurzsteckbriefe der Lernformate

4 Ergebnisse umsetzen: Welche Formate helfen beim Lernen?

Der letzte Schritt des Design-Based Research besteht in der Bewertung und der Reflexion. Hier war das Ziel, die oben erwähnten Lernformate zu testen und damit Feedback zu ihrer Umsetzbarkeit und Akzeptanz zu erhalten. Um diese Punkte nachvollziehen zu können, haben wir das Verhalten der Teilnehmerinnen und Teilnehmer während der Durchführung der Lernformate beobachtet. Im Anschluss an die Formate haben wir zudem jeweils eine kurze Umfrage durchgeführt. Damit haben wir geprüft, ob die Lernziele des jeweiligen Formats erreicht wurden.

Für die Bewertung der Lernformate haben wir uns am Learning-Transfer Evaluation Model (LTEM) (Thalheimer, 2024) orientiert. Es ermöglicht Rückschlüsse auf die Motivation und die Interessen der Teilnehmerinnen und Teilnehmer sowie auf die Qualität des Lernprogramms. Der Lernprozess wird dabei in acht Phasen unterteilt, die die Umsetzung des Lernformats, die Möglichkeiten zur Partizipation und die Umsetzung des Gelernten bewerten (siehe Abbildung 3). Wir haben uns in der Bewertung auf die ersten vier Schritte konzentriert, da sie zeitlich vor und während eines Lernformats erhoben werden und daher im Rahmen der Veranstaltung umsetzbar waren.

Der erste Schritt besteht darin, zu evaluieren, wer und wie viele Menschen an den Lernformaten teilnehmen. Im zweiten Schritt beobachteten wir, wie aktiv die Anwesenden in den Lernformaten waren. Für den dritten und vierten Schritt führten wir nach jedem Lernformat eine kurze Umfrage unter den Teilnehmerinnen und Teilnehmern durch. Damit holten wir uns Feedback dazu ein, wie sie die Lernformate empfanden und inwiefern sie Neues gelernt haben.

Die verbleibenden vier Schritte des LTEM-Modells erfordern eine Befragung der Teilnehmerinnen und Teilnehmer längere Zeit nach der Veranstaltung und können bei sich wiederholenden Lernformaten eingesetzt werden. Wir empfehlen daher, die verbleibenden vier Schritte bei einer eigenen Umsetzung der vorgestellten Lernformate selbst zu erfassen.

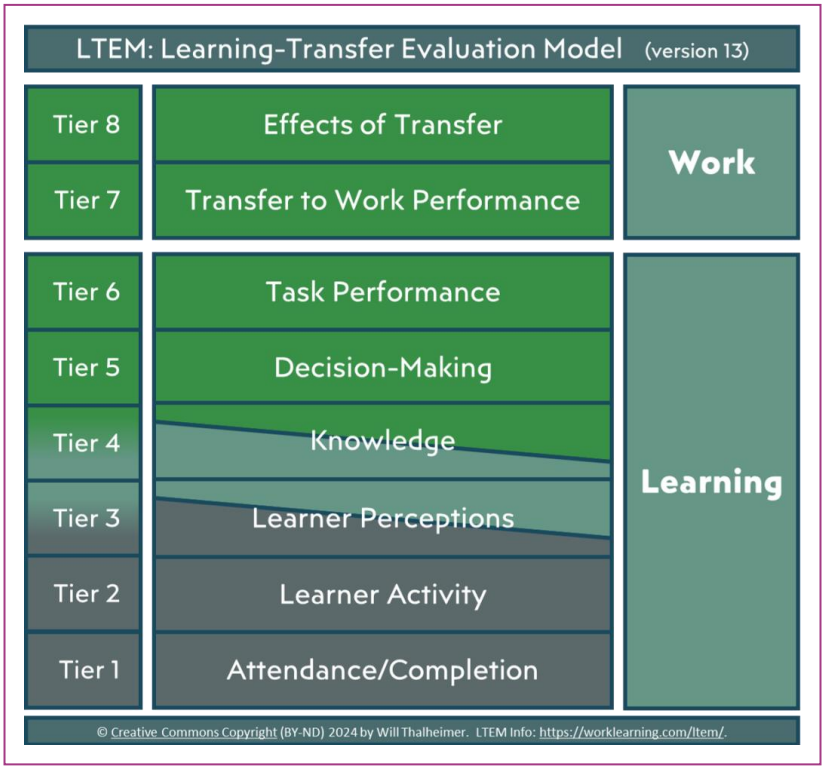


Abbildung 3 Learning-Transfer Evaluation Model nach Thalheimer (2024)

4.1 Erkenntnisse aus der Erprobung der Lernformate

Am Workshop nahmen 13 Personen teil, die sich als Mitglieder der Branchenplattform angemeldet hatten oder von uns aufgrund ihres Arbeitsschwerpunkts gezielt eingeladen wurden. Dabei waren die Teilnehmerinnen und Teilnehmer regional und organisatorisch divers verteilt. Während eine Person beispielsweise aus der Forschung kam, beriet eine andere Stromunternehmen bei der Umsetzung ihrer Cybersicherheitsmaßnahmen. Andere waren wiederum direkt für die Cybersicherheit ihres Unternehmens zuständig. Durch die Durchmischung innerhalb der Gruppe konnten verschiedene Perspektiven und Erfahrungen der Teilnehmerinnen und Teilnehmer die Gruppe bereichern.

Konferenzspiel „Entscheidungen unter Strom“

Das Konferenzspiel wurde im Plenum durchgeführt. Die Teilnehmerinnen und Teilnehmer mussten gemeinsam einen Cybersicherheitsvorfall in einem fiktiven Unternehmen bewältigen, indem sie als Team ihr Wissen zu Cybersicherheit bündelten. Dabei gab es eine Moderation sowie einen externen Experten für inhaltliche Expertise.

Der externe Experte war ein wichtiger Faktor für das Spiel. Er stand dem Publikum für Fragen und Erläuterungen zur Verfügung. Am Tag des Workshops nahm diese Rolle ein Vertreter vom Bundesamt für Sicherheit in der Informationstechnik (BSI) ein, dessen Erläuterungen umfassend, aber leicht verständlich waren. Die Einbettung seiner Person als „Joker“ im Spiel gab diesem Experten eine weniger belehrende als vielmehr unterstützende und nahbare Rolle.

Die Befragung zeigte (siehe Abbildung 4): Entgegen der Sorge, dass das verwendete Beispiel eines Smart Meter vertreibenden Unternehmens zu spezifisch sein könnte, gaben die Teilnehmerinnen und Teilnehmer

an, dass sie einen Mehrwert aus den Inhalten des Spiels ziehen konnten. Dies ist erfreulich, besonders weil die Teilnehmerinnen und Teilnehmer ein durchmischtes Bild zeichneten, ob sie einen Cybersicherheits-aspekt entdecken konnten, den ihr Unternehmen noch verbessern kann.

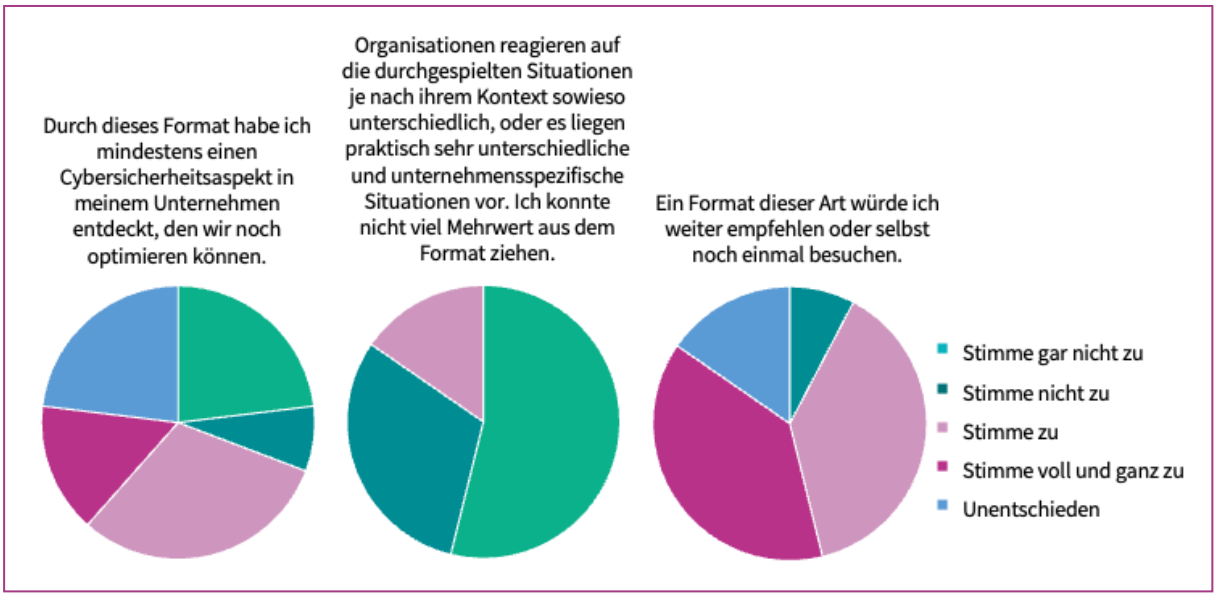


Abbildung 4 Bewertung des Konferenzspiels durch die Teilnehmerinnen und Teilnehmer; abgegebene Bewertungen: 13

Wir hatten dieses Lernformat an den Anfang unseres Workshops gesetzt. Das erwies sich als gute Entscheidung: Die Teilnehmerinnen und Teilnehmer, die sich zum großen Teil noch nicht kannten, konnten sich in dem kooperativen und moderierten Spiel ungezwungen kennenlernen. Sie konnten sich als „Joker“ mit ihrem Wissen zwanglos in die Diskussion einbringen. Um die Redebeiträge zu verteilen, sah das ursprüngliche Format vor, dass diese Rolle nur einmalig eingenommen werden darf. Es zeigte sich aber, dass diese Regel in der kleineren Runde nicht eingehalten werden musste. Stattdessen war der Raum durchgehend offen für Diskussionen, in die sich fast alle Anwesenden mit ihren unterschiedlichen Hintergründen einbrachten.

Rotator Live

Das „Rotator Live“-Spiel war vorrangig auf einen sozialen Austausch und einen Vertrauensaufbau zwischen den Teilnehmerinnen und Teilnehmern ausgerichtet. Hier nahmen sie an Zweiergesprächen teil, wobei die Zusammensetzung in regelmäßigen Abständen rotiert wurde. In jeder Runde wurde eine Einstiegsfrage gestellt.

Die Teilnehmerinnen und Teilnehmer gaben an, dass sie in den kurzen, aber anscheinend intensiven Gesprächen tatsächlich gegenseitiges Vertrauen aufbauen konnten (siehe Abbildung 5). Ebenso konnte eine Mehrheit eine andere Perspektive zu Cybersicherheit beim Gegenüber erkennen. Die Ziele des Formats wurden damit erreicht.

In der Beobachtung des Lernformats sowie durch anekdotische Berichte nach dem Format zeigte sich, dass die Einstiegsfragen oft nur als Stütze verwendet wurden und im Gespräch selbst wenig Beachtung fanden.

Hier zeigt sich: Oft ist es sinnvoll, Formate nicht zu stark zu durchdenken und stattdessen den Teilnehmerinnen und Teilnehmern eigenen Gestaltungsraum zu gewähren.

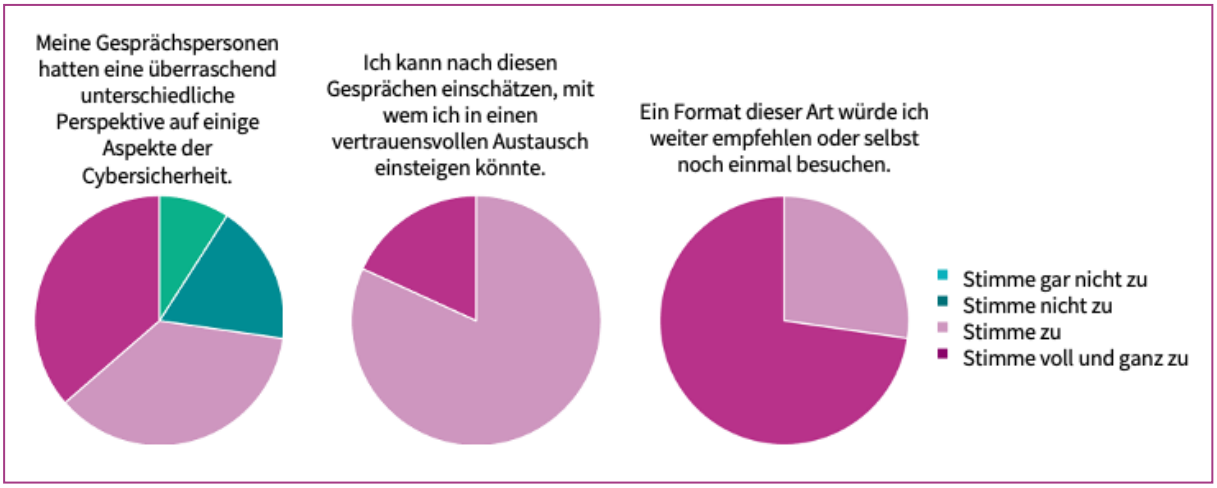


Abbildung 5 Bewertung des „Rotator Live"-Spiels durch die Teilnehmerinnen und Teilnehmer; abgegebene Bewertungen: 11

Sharing4Resilience

Das zuletzt erprobte Format „Sharing4Resilience" diente einem organisatorischen Wissensaustausch: Das Format soll Teilnehmerinnen und Teilnehmern helfen, Best Practices für einen Wissens- und Informationsaustausch zu identifizieren. In kleineren Gruppen mit bis zu sechs Personen besprachen die Teilnehmerinnen und Teilnehmer, welche Inhalte für eine gemeinsame Sharing Policy relevant wären und welche Hindernisse und Lösungen es dafür in der Praxis geben könnte. Die Ergebnisse wurden auf Flipcharts dokumentiert und im Plenum vorgestellt.

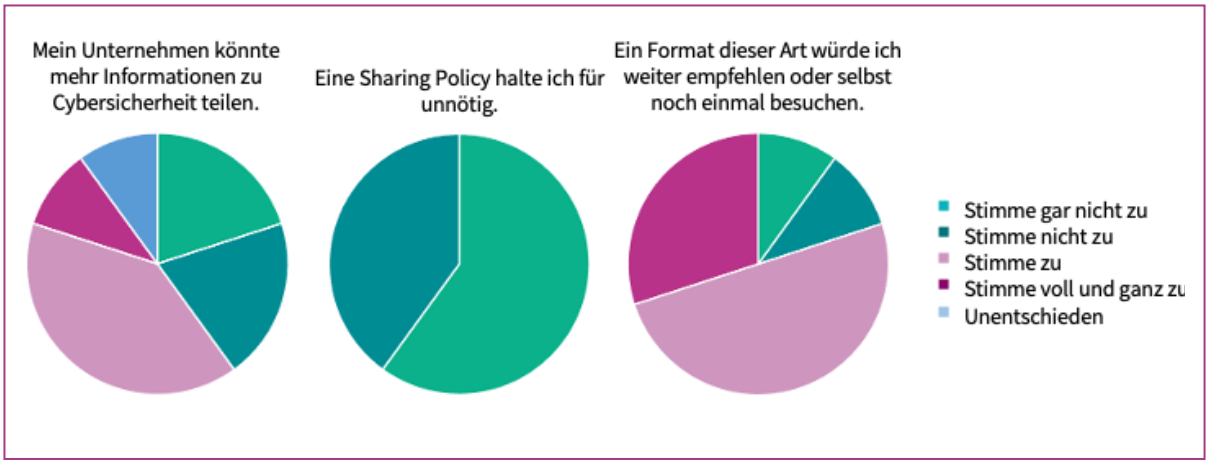


Abbildung 6 Bewertung des „Sharing4Resilience"-Spiels durch die Teilnehmerinnen und Teilnehmer; abgegebene Bewertungen: 10

In der Auswertung zeigt sich ein durchmischtes Bild: Alle Teilnehmerinnen und Teilnehmer hielten eine Sharing Policy für sinnvoll. Nur knapp die Hälfte stimmte zu, dass ihr Unternehmen mehr Informationen zu Cybersicherheit teilen könnte.

Die Gruppenergebnisse zeigen, dass die Gruppen die Frage nach einer Sharing Policy unterschiedlich reflektierten: Während sich eine Gruppe auf der Meta-Ebene fragte, was und warum geteilt werden sollte, wurde eine andere bei den Inhalten, die eine Policy umfassen könnte, deutlich konkreter. Die Ergebnisse wurden anschließend von der Moderation gesammelt. Den Teilnehmerinnen und Teilnehmern war es wichtig, das Ziel einer Sharing Policy von vornherein festzulegen und auch zu klären, welche Inhalte überhaupt geteilt werden sollten: Learnings oder konkrete Assets? Wäre es sinnvoll, konkrete Angaben zu Dienstleistern zu machen? Hier gab es den Vorschlag, über eine Taxonomie Informationen sinnvoll zu bündeln und auszutauschen. Dazu stellte sich die Frage, wer aus dem eigenen Unternehmen teilnehmen sollte und mit wem diese Person in einen Austausch treten könnte.

Zustimmung zu den Lernformaten

Bei allen Lernformaten stimmten die Teilnehmerinnen und Teilnehmer mit überwiegender Mehrheit zu, dass sie diese Formate weiterempfehlen würden. Wir gehen daher davon aus, dass die Formate nicht nur eine angenehme Abwechslung zu bekannten Lernformaten waren. Stattdessen können sie den Teilnehmerinnen und Teilnehmern weiterhelfen, ihre Fähigkeiten zu erweitern und neue Einblicke zu gewinnen. Auch der Gemeinschaftsaspekt nimmt eine wichtige Rolle ein: Die Wege der Zusammenarbeit haben den Aufbau einer Gruppendynamik ermöglicht, die zum Lernen hilfreich sein kann.

Fazit und Bewertung der Evaluationsergebnisse

Den Teilnehmerinnen und Teilnehmern gefielen die Umsetzung von Lerninhalten in Games und anderen Lernformaten. Ebenfalls ist positiv anzumerken, dass sie, den Evaluationen nach, einen inhaltlichen Mehrwert aus den Lernformaten ziehen konnten. Dies zeigt, dass auch der Faktor des eigenen Wissensniveaus angemessen integriert wurde. Die Gäste unterstützten sich zudem gegenseitig, wenn es Rückfragen gab oder technischer Support notwendig war. Diese spontanen Interaktionen förderten ebenso wie die strukturierten Formate zum Austausch ein gegenseitiges Vertrauen, das sich in weiter geführten Diskussionen zwischen und nach den Formaten widerspiegelte. Auch in den Lernübungen zeigten sich die Teilnehmerinnen und Teilnehmer offen, ihre eigenen Erfahrungen zu teilen, um das Ziel des jeweiligen Formats gut umzusetzen.

In der Umsetzung konnten wir feststellen, dass bei den erprobten Lernformaten nicht alle Regeln strikt eingehalten werden mussten. Vielmehr erscheint es sinnvoll, die Lernformate als Rahmenbedingungen zu verwenden und bei Bedarf von vorgeschlagenen Inhalten oder Regeln abzuweichen oder sie an die Gruppe anzupassen.

4.2 Empfehlungen für die weitere Umsetzung

Aufbauend auf unseren Beobachtungen und Bewertungen halten wir folgende Handlungsempfehlungen fest:

- *Gemeinsames Lernen stärken:* Wir empfehlen, Lernformate und Weiterbildung zu Cybersicherheit stärker gemeinschaftlich auszurichten. Die Lernenden sollten sich dazu austauschen, Fragen stellen und sich vernetzen können. Das stärkt ihr Autonomie-Empfinden und ihre Motivation. Dies ist damit ein aussichtsreicher Ansatz, um Verhalten nachhaltig zu verändern.
- *Cybersicherheit leben:* Für langfristig wirksame Effekte reicht es nicht, Mitarbeiterinnen und Mitarbeitern Inhalte zu vermitteln. Lernen zu Cybersicherheit umfasst nicht nur Wissen, sondern auch das Leben dieses Wissens und ein vertrauensvolles Miteinander, zum Beispiel eine offene Fehlerkultur. Daran müssen alle Ebenen eines Unternehmens mitarbeiten. Unsere Lernformate nehmen daher auch Prozesse in den Blick.
- *Gemeinschaftliche Lernformate reflektiert auswählen:* Die Entscheidung für ein bestimmtes Lernformat ist immer auch eine Entscheidung für eine bestimmte Art und Weise, wie die Gruppe miteinander in Kontakt tritt (zum Beispiel kooperativ, anonym, in kleinen oder in großen Gruppen). Dies mitzudenken, ist gerade beim Thema Cybersicherheit wichtig, da für einen offenen Austausch unter den Teilnehmerinnen und Teilnehmern erst Vertrauen aufgebaut werden muss.
- *Lernerfolge langfristig messen:* Wir konnten nur die unmittelbare Wirkung der getesteten Lernformate erheben. Um tatsächliche Lernerfolge zu kontrollieren, empfehlen wir, Lernformate langfristig zu evaluieren und nach eigenen Maßstäben und Zielen auszuwerten. Nur so kann beispielsweise herausgefunden werden, ob sich Verhaltensweisen tatsächlich wie gewünscht ändern.
- *Blick über den Tellerrand:* Wie sprechen Menschen aus Unternehmen anderer Länder über Cybersicherheit? Welche Effekte gibt es dort? Cybersicherheit, Transparenz und Fehlerkultur könnten im internationalen Kontext betrachtet werden. Dies könnte weitere wertvolle Erkenntnisse und neue Impulse ermöglichen.

5 Abschluss

Sich zu Cybersicherheit auszutauschen, so gab ein Interviewpartner an, sei *„so ein bisschen wie ein Kasten Pralinen: Man weiß vorher nicht, was man bekommt."* Ziel unseres Projekts war es, die positive Seite eines transparenteren Austauschs zu Cybersicherheit im KRITIS-Bereich durch passende Austausch- und Lernformate besser aufzuzeigen.

Die Forschungsfrage dieses Projekts lautete: *„Wie kann die Energiewirtschaft gemeinsam aus Cyberattacken auf einzelne Unternehmen lernen, um die Resilienz der gesamten Branche zu stärken?"* Es zeigt sich, dass die Vermittlung reiner Lerninhalte wie ein Vergleichen von Anschaffungen oder ein Teilen von Best Practices nicht zielführend sind. Viel entscheidender ist es, Grundlagen für einen offenen Austausch zu schaffen. In unseren Interviews konnten wir mehrere Punkte identifizieren, die die Grundlage für unsere Lernformate bildeten: Menschen können und müssen für das Thema Cybersicherheit motiviert werden. Es gilt, ein gegenseitiges Vertrauen für einen Austausch zu schaffen. Und es braucht eine offene Fehlerkultur, in der die Mitarbeiterinnen und Mitarbeiter eigene Fehler angstfrei transparent machen und dabei auf Unterstützung ihrer Umgebung zählen können. Je weiter diese vier Punkte angegangen und umgesetzt werden, umso mehr profitieren alle davon – und umso resilienter wird die Branche.

Die Branchenplattform ist ein passendes Format, um das erforderliche Miteinander aufzubauen, zu erhalten und weiterzuentwickeln. Wie sich in den Interviews gezeigt hat, erfordern ein Wissensaufbau und ein Wandel, dass Cybersicherheit von allen Seiten eines Unternehmens verstanden und umgesetzt wird, um erfolgreich zu sein. Daher bietet es sich an, auf organisatorischer Ebene mit dem angesammelten Wissen weitere Akteure anzusprechen und sie zum Mitmachen und zum Austausch zu motivieren. Dabei könnte weitergehend evaluiert werden, welche Wege der Branchenplattform dabei besonders erfolgreich sind und welche neuen Möglichkeiten es hierfür gibt. Dies ermöglicht es, den gegenseitigen Wissensaustausch weiter zu vertiefen und in die Breite zu bringen.

Dieser sehr menschenzentrierte Aspekt der Cybersicherheit ist von wesentlicher Bedeutung für die Resilienz einzelner Unternehmen und der gesamten Branche. Im Zeitalter von generativer KI, Deepfakes und Social Bots[4] ist es umso wichtiger, sich der Imperfektion des Menschen bewusst zu machen und Räume zu schaffen, in denen Menschlichkeit nicht nur akzeptiert, sondern bestärkt wird. Ähnliche Botschaften finden sich in diversen Cybersicherheits-Frameworks, -Missionen und -Strategien einschlägiger Institutionen wieder. Die Forschung dazu und ihre Umsetzung sind somit Pflicht einer digital kompetenten Gesellschaft.

[4] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/Exkurs-bots/social-bots.html

6 Abkürzungen

B=MAT	Behaviour = Motivation + Ability + Trigger
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
FAI	Fundamentaler Attributionsfehler
KI	Künstliche Intelligenz
KRITIS	Kritische Infrastruktur
LTEM	Learning-Transfer Evaluation Model
NDA	Non-Disclosure Agreement
OLB-Modell	Orient, Locate, Bridge
SDT	Self Determination Theory

7 Abbildungs- und Tabellenverzeichnis

8 Literaturverzeichnis

Fogg, Brian Jeffrey (2009, April): A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology (S. 40). Association for Computing Machinery.

Kahneman, Daniel, & Tversky, Amos (1979): Prospect Theory. An Analysis of Decision under Risk. Econometrica, 47(2), 263–291.

Knox, Benjamin J., Jøsok, Øyvind, Helkala, Kirsi, Khooshabeh, Peter, Ødegaard, Terje, Lugo, Ric G., & Sütterlin, Stefan (2018): Socio-technical communication: the hybrid space and the OLB model for science-based cyber education. Military Psychology, 30(4), 350-359.

Mayer, Roger C. & Schoorman, David F. (1995): An Integrative Model of Organizational Trust. The Academy of Management Review, Vol. 20, No. 3 (Jul., 1995), pp. 709-734

McKenney, Susan, & Reeves, Thomas (2015): Design-Based Research. In: The SAGE Encyclopedia of Educational Technology, herausgegeben von J. M. Spector, 189–91. 2455 Teller Road, Thousand Oaks, California 91320: SAGE Publications, Inc.

Reeves, Andrew, Calic, Dragana, & Delfabbro, Paul (2021): "Get a red-hot poker and open up my eyes, it's so boring": Employee perceptions of cybersecurity training. Computers & Security, 106, 102281.

Ross, Lee (1977): The intuitive psychologist and his shortcomings: Distortions in the attribution process. In: L. Berkowitz (Hrsg.): Advances in Experimental Social Psychology (10), S. 173–220). New York: Academic Press.

Ryan, Richard M., & Deci, Edward. L. (2000): Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist, 55(1), S. 68–78.

Schulte, Andreas (2023): Schweigen ist Gold?. Tagesspiegel Background, 28.03.2023. https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/schweigen-ist-gold, zuletzt besucht am 23.10.2023.

Tagesspiegel Background (2022): Unternehmen scheuen Zusammenarbeit nach Cyberangriff. Tagesspiegel Background, 20.12.2022. https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/unternehmen-scheuen-zusammenarbeit-nach-cyberangriff, zuletzt besucht am 23.10.2023.

Thalheimer, Will (2024): LTEM. The Learning-Transfer Evaluation Model. Work-Learn-Research. https://www.worklearning.com/ltem/, zuletzt besucht am 17.02.2025.

9 Steckbriefe Lernformate

„Gemeinsam Lernen” Formate

GESELLSCHAFT FÜR INFORMATIK
dena
Future Energy Lab
CYBER POLICY HAUS

Übersicht aller Formate

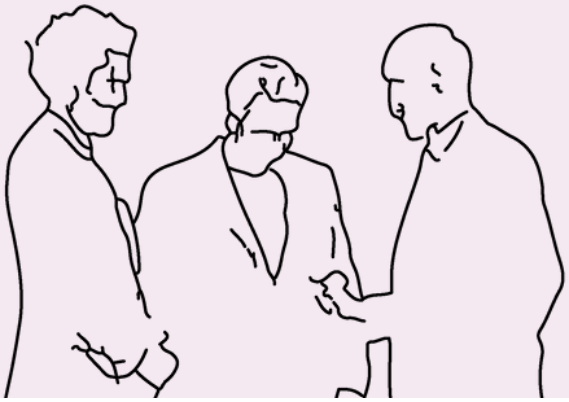
Getestete Formate

	01—1	01—2	01—3
FORMAT	**Konferenzspiel**	**1:1 Gespräche**	**Workshop**
TITEL	“Entscheidungen unter Strom”	“Rotator Live: Compliance vs. Praxis – Wo liegt der Weg zur echten Cyber-Resilienz?"	"Sharing4Resilience – Gemeinsam zur besseren Informationspolitik"
MITMACHEN	→ Live im Podium → Per Abstimmung auf dem Handy	→ Live 1:1 Gespräch im Speed Dating Format	→ Ideen teilen, Beispiele mitbringen, Meinung sagen

Formatideen

	02—1	02—2	02—3	02—4	02—5	02—6	02—7	02—8	02—9
FORMAT	**Storytelling**	**Chatgruppen**	**Lerngruppen**	**Coaching**	**Publikation**	**JourFixe**	**Fishbowl**	**Kartenspiel**	**Warm-Up**
TITEL	„Lernabenteuer aus Fehlern“ live	Themenbezogene Chatgruppen	Micro-Learning Circles	Storytelling mit Business-Impact	Butter bei Die Fische	Probleme Roulette – Walking in my Shoes	Cyberangriff, wie war das nochmal?!	(Mis-)Match Memory Game	Cybersecurity Mapping
MITMACHEN	→ Schreiben Sie (anonym) Ihren Fehlerbericht und Lösungs-ansatz auf.	→ Kommunika-tionsregeln einhalten und über den vorge-sehenen Kanal Informationen teilen	→ Themen einreichen (z.B. ihre To Dos), anmelden und sich zur regelmäßigen Teilnahme verpflichten.	→ Bringen Sie Ihre Bereitschaft mit, aktiv an der gemeinsamen Storyentwicklun g teilzunehmen.	→ Reichen Sie Fragen ein, nehmen Sie anonym teil.	→ Um teilzuneh-men, melden Sie sich über den vorgesehenen Anmeldeprozess an und bringen Sie Probleme und Offenheit mit.	→ Bringen Sie Ihre Erfahrungen oder Fragen mit.	→ Bringen Sie sich ins Game Design ein.	→ Bringen Sie Ihre Einschätzungen aktiv in die Übung ein.

01—1
Entscheidungen unter Strom – Ein Konferenzspiel



KURZBESCHREIBUNG

„Entscheidungen unter Strom“ ist ein Cybersecurity-Konferenzspiel, welches in dem Projekt "Gemeinsam lernen” entstand. Es versetzt die Teilnehmenden in praxisnahe Entscheidungsszenarien. Im Spiel schlüpfen sie in die Rolle eines Entscheidungsträgers eines deutschen Unternehmens und müssen unter Zeitdruck strategische Entscheidungen treffen – etwa zur Produktzertifizierung, zum Umgang mit der NIS-2-Richtlinie oder zum Management von Cybervorfällen.

Aufwand	●●●●●
Präsenz	in persona
Frequenz	einmalig

Ziele

- → Maßnahmen und Empfehlungen zur Informationssicherheit praxisnah kennenlernen und diskutieren.
- → Den Einsatz von Hilfe-zur-Selbsthilfe-Produkten im Cybersecurity-Bereich fördern.
- → Gegenseitiges Lernen und den Austausch in realitätsnahen, regulatorischen Herausforderungen anregen.

Zielgruppe

- → Erfahrene KRITIS-Betreiber und zukünftige kritische Infrastrukturen
- → CISOs, ISB, Compliance Officer und weitere Fachkräfte aus der Energiewirtschaft mit unterschiedlichem Fähigkeitslevel

ABLAUF & ANLEITUNG FÜR DEN FACILITATOR:

Hinweis: Dieses Format wurde im Rahmen des Projekts gestaltet und umgesetzt. Ähnliche Spiele müssen den Designprozess – in dem konkrete Szenarien definiert werden – als ersten Schritt durchlaufen. Das Spiel kann bei den Projektverantwortlichen angefragt werden.

Technik & Gamification:

- Technik: Beamer, Mikrofon, Entscheidungstool
- Gamification-Elemente: Punktevergabe, Feedbackmechanismen, Rollenzuweisung und zeitgesteuerte Entscheidungen

Einleitung
(ca. 5–10 Min.)

1. Begrüßung und Vorstellung des Spiels, der Ziele und der Rollen
2. Erklärung der Spielregeln, der Punktevergabe und des zeitlichen Ablaufs.

Rundenphase
(ca. 40–45 Min.)

1. Runde 1 – NIS-2 & Zertifizierung:
   - Präsentation des Szenarios (SmartGrid Solutions GmbH, neue gesetzliche Anforderungen).
   - Darstellung der Entscheidungsmöglichkeiten (z. B. Produktzertifizierung zuerst, NIS-2 zuerst, oder beides gleichzeitig mit Plan).
   - Absprache, Individuelle Abstimmung, Live-Punktevergabe und kurzes Feedback.
2. Runde 2 – Schutzbedarfsanalyse:
   - Vorstellung der Herausforderung zur Sicherheit von Zählerdaten.
   - Auswahl der wichtigsten Sicherheitsaspekte (z. B. Integrität, Authentizität, etc.) unter Zeitdruck.
   - Diskussion, Abstimmung und Punktevergabe.
3. Weitere Runden mit zusätzlichen Szenarien, die ähnliche Abläufe haben.

Abschluss
(ca. 5–10 Min.)

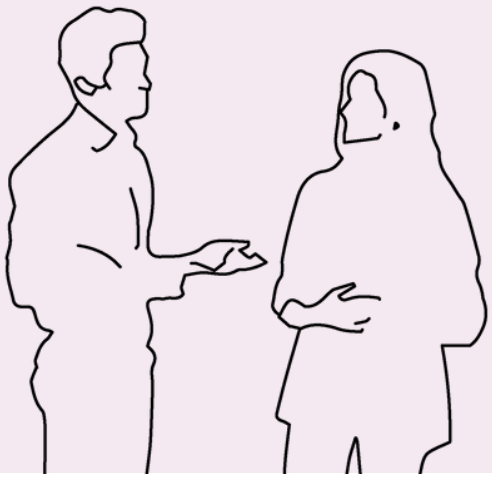
1. Zusammenfassung der wichtigsten Erkenntnisse und Feedbackrunde.
2. Bekanntgabe der Gesamtpunktzahl und Ausblick auf nächste Schritte bzw. weiterführende Diskussionen.

Tipps

→ Setzen Sie einen engagierten Facilitator und eine fachkundige Person ein, um den Ablauf zu moderieren und fundierte Rückmeldungen zu geben.
→ Sorgen Sie für eine einfach umzusetzende technische Infrastruktur sowohl beim Design als auch bei der Durchführung, sodass alle Teilnehmenden den Ablauf problemlos verfolgen können.
→ Erklären Sie die Spielregeln klar und präzise, damit jeder die Punktevergabe und die Entscheidungsfindung nachvollziehen kann.
→ Ordnen Sie die gefundenen Lösungen systematisch ein, um im Anschluss Best Practices und Verbesserungsmöglichkeiten herauszuarbeiten.
→ Achten Sie auf ein straffes Zeitmanagement und ermutigen Sie die Teilnehmenden, ihre Entscheidungsprozesse zu erläutern, um den Austausch zu vertiefen.

01—2
„Rotator Live: Compliance vs. Praxis

„Wo liegt der Weg zur echten Cyber-Resilienz?“ im Speed-Dating-Format



KURZBESCHREIBUNG

Interaktives schnelles Austausch-Format, bei dem Teilnehmer in rotierenden Gesprächen zu spezifischen Themen oder Problemstellungen interdisziplinär Probleme und Lösungen diskutieren können.

Aufwand ●●○○○

Präsenz in persona

Frequenz seriell

Format Speed-Dating-Gespräche in Zweiergruppen

Ablauf

1. Sich an Tischen gegenüber sitzen
2. Brainstorming-Frage einwerfen
3. Signal zum Wechsel
4. Rotationen (z.B. 4 Runden): Alle 7 Minuten

Ziele

→ Perspektivwechsel
→ Vertrauen aufbauen

Zielgruppe

→ Erfahrene KRITIS Betreiber und zukünftige bwE CISOs, ISB, Compliance Officer
→ Unterschiedliches Fähigkeitslevel
→ Energiewirtschaft

BEISPIEL-ABLAUF

1. Begrüßung & Einführung
(5 Min.)

Erklären Sie, was die Teilnehmenden erwartet und worauf sie achten sollen. Gehen Sie insbesondere auf folgende Punkte ein:

- Die Teilnehmenden sprechen jeweils 7 Minuten mit einer anderen Person.
- Nach dem Signal (Gong) wechseln die Teilnehmenden zum nächsten Tisch bzw. Gesprächspartner. Entscheiden Sie wer in welche Richtung wechselt und wer stehen bleibt.
- Ziel des Formats ist es, neue Perspektiven zu gewinnen und Best Practices auszutauschen.
- Ermutigen Sie die Teilnehmenden, wichtige Erkenntnisse zu notieren, da diese am Ende gesammelt werden.
- Weisen Sie darauf hin, an wen sie sich bei Fragen wenden können.

2. Gesprächsrunden
(5 x 7 Min.)

(Gong nach jeder Runde + kurzer Reminder durch den Moderator)

Themen für die Gespräche:
Runde 1: Was bedeutet für Sie Cyber-Resilienz? (Praxis vs. Theorie)
Runde 2: Wo hilft Compliance wirklich – und wo wird sie zur Hürde?
Runde 3: Welche Maßnahmen funktionieren aus Ihrer Erfahrung am besten?
Runde 4: Wie kann interdisziplinäre Zusammenarbeit die Sicherheit verbessern?
Runde 5: Ihr persönlicher Best-Practice-Tipp für Cyber-Resilienz

3. Abschluss & Reflexion
(5 Min.)

Moderator: „Fantastisch! Sie haben nun fünf verschiedene Perspektiven kennengelernt. Bevor wir abschließen, eine kurze Reflexion:

→ Was war Ihre wichtigste Erkenntnis? Gab es eine
→ überraschende Perspektive? Was nehmen Sie aus
→ diesem Austausch mit?“

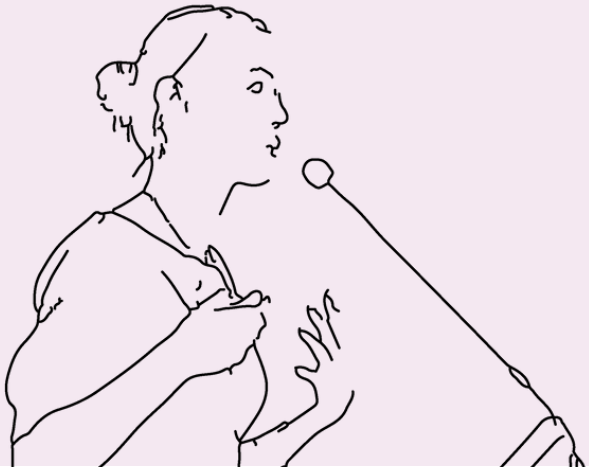
(Lasse 2-3 Teilnehmende kurz antworten.) „Danke für Ihre Teilnahme! Nutzen Sie die Gelegenheit, sich weiter auszutauschen und vernetzen Sie sich mit Ihren Gesprächspartner:innen. Viel Erfolg bei der Umsetzung Ihrer neuen Erkenntnisse!“

Tipps für eine dynamische Moderation:

→ Sei enthusiastisch und halte die Energie hoch.
→ Vermeide lange Erklärungen, halte die Regeln einfach.
→ Falls eine Runde ins Stocken gerät, ermutige zu neuen Blickwinkeln.
→ Falls nötig, kürze oder verlängere eine Runde leicht.
→ Motiviere dazu, Kontakte zu knüpfen und Gespräche fortzusetzen.

01—3
Sharing4Resilience

Gemeinsam zur besseren Informationspolitik



KURZBESCHREIBUNG

In diesem interaktiven Workshop erarbeiten Sie gemeinsam mit anderen Teilnehmenden erste Ansätze für eine unternehmensinterne Sharing Policy. Ziel ist es, Good Practices für den sicheren und schnellen Informationsaustausch zu identifizieren und konkrete Templates zu entwickeln – und dabei Hindernisse sowie Lösungsansätze in den Phasen eines Cybervorfalls (Prävention, Detektion, Reaktion, Lernen) zu beleuchten.

Aufwand ●●●○○

Präsenz in persona

Frequenz einmalig

Ziele

→ Erkennen, welche Ansätze für den sicheren und schnellen Informationsaustausch funktionieren.
→ Herausforderungen im Informationsaustausch bei Cybervorfällen (Prävention, Detektion, Reaktion, Lernen) identifizieren und praxisnahe Lösungsansätze diskutieren.
→ Die Must-Haves einer Sharing Policy herausarbeiten, die später weiter ausdefiniert werden kann.
→ Die Bereitschaft zur weiteren Zusammenarbeit und Umsetzung der erarbeiteten Ansätze sichern.

Zielgruppe

→ Führungskräfte, IT-Sicherheitsverantwortliche und Entscheidungsträger:innen, die daran interessiert sind, interne Informationsflüsse zu optimieren und die Cyber-Resilienz ihres Unternehmens zu stärken.

BEISPIEL-ABLAUF

1. Begrüßung & Einführung
(10 Min.)

1. Begrüßen Sie die Teilnehmenden und erläutern Sie den Workshop „Sharing4Resilience – Gemeinsam zur besseren Informationspolitik".
2. Stellen Sie den Hintergrund vor: Unternehmen haben häufig Schwierigkeiten, sicherheitsrelevante Informationen strukturiert zu teilen – sei es aufgrund rechtlicher Bedenken, Unsicherheiten oder fehlender Prozesse.
3. Erklären Sie den Ablauf des Workshops und betonen Sie, dass es darum geht, in Gruppen praxisnahe Ansätze für eine unternehmensübergreifende Sharing Policy zu entwickeln.

Tipp: Idealerweise stellt der Facilitator zudem einen Aufschlag und einen Draft einer Sharing Policy bereit, um als Ausgangspunkt für die Diskussion zu dienen.

Gruppenarbeitsphase
(25 Min.)

1. Teilen Sie die Teilnehmenden in Gruppen von ca. fünf Personen ein.
2. Jede Gruppe erarbeitet Ideen und Lösungen für die Frage: Welche sicherheitsrelevanten Informationen sollten in den Phasen Prävention, Detektion, Reaktion und Lernen geteilt werden?
3. Leiten Sie gezielt Impulse:
   - Welche Informationen sind für Ihre Rolle besonders relevant?
   - Welche Hindernisse verhindern aktuell einen effektiven Austausch?
   - Welche Good Practices und organisatorischen Rahmenbedingungen könnten helfen, diese Hürden zu überwinden?

3. Ergebnispräsentation & Good Practices
(15 Min.)

1. Bitten Sie jede Gruppe, ihre wichtigsten Erkenntnisse (jeweils ca. 3 Minuten) im Plenum vorzustellen.
2. Sammeln Sie die Ergebnisse an einer Pinnwand oder einem digitalen Board und moderieren Sie eine Diskussion, in der Sie gemeinsam die erarbeiteten Good Practices und Templates reflektieren.

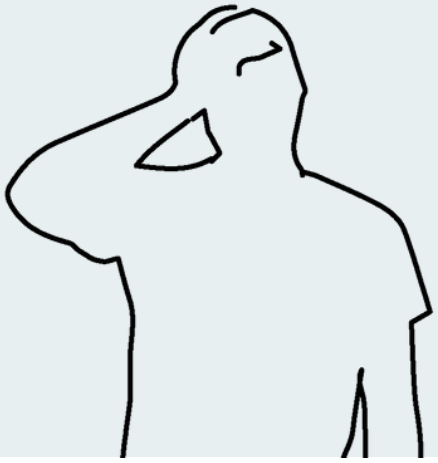
4. Commitment & Nächste Schritte
(5 Min.)

1. Fragen Sie, wer bereit ist, an einer weiterführenden Arbeitsgruppe mitzuwirken, um die Sharing Policy weiter zu entwickeln.
2. Diskutieren Sie mögliche nächste Schritte, wie die Erstellung eines konkreten Templates oder die Planung eines Folgetreffens, um die Ergebnisse zu vertiefen.

Tipps

→ Nutzen Sie praxisnahe Beispiele und stellen Sie sicher, dass alle Teilnehmenden aktiv eingebunden werden.
→ Halten Sie den Ablauf klar und moderieren Sie die Diskussion, sodass auch leise Stimmen Gehör finden.
→ Dokumentieren Sie zentrale Erkenntnisse und stellen Sie sicher, dass die nächsten Schritte klar kommuniziert werden.

02—1
„Lernabenteuer aus Fehlern“ live



KURZBESCHREIBUNG

(Anonym) eingereichte „Fuck-ups“ werden mittels eines Templates festgehalten, vorgelesen und diskutiert – für einen offenen, praxisnahen Lerneffekt.

Aufwand ●●●○○

Präsenz in persona

Frequenz seriell

Ziele

→ Fehler transparent machen und daraus lernen
→ Praxisnahe Lösungsansätze teilen
→ Eine Kultur der kontinuierlichen Verbesserung fördern

Zielgruppe

→ IT- und Sicherheitsexpert:innen
→ Verantwortliche im Risiko-, Compliance- und Krisenmanagement
→ Fachleute, die praxisorientierte Erfahrungen einbringen möchten

BEISPIEL-ABLAUF

1. Begrüßung & Einführung
(ca. 5 Min.)

1. Begrüßen Sie die Teilnehmenden und stellen Sie das Format vor.
2. Erklären Sie, dass in dieser Session (anonym) „Fuck-ups“ geteilt werden, um voneinander zu lernen und die Resilienz zu stärken.
3. Gehen Sie insbesondere auf folgende Punkte ein:
   - Die Teilnehmenden notieren ihre eigenen Fehler mithilfe des bereitgestellten Templates.
   - Jeder Fehlerbericht soll auch eine Lösung oder einen Ansatz zur Fehlerbehebung enthalten.
   - Die Beiträge können anonym eingereicht werden; es dürfen keine identifizierbaren oder sensiblen Informationen enthalten sein.
   - Weisen Sie darauf hin, dass alle Berichte später zufällig vorgelesen und gemeinsam besprochen werden.

Fehlerbericht-Erstellung & Einreichung
(ca. 10–20 Min.)

1. Fordern Sie die Teilnehmenden auf, ihre „Fuck-ups“ in dem vorgegebenen Format aufzuschreiben.
2. Erinnern Sie sich daran, unbedingt auch den dazugehörigen Lösungsansatz zu ergänzen.
3. Bitten Sie die Teilnehmenden, ihre Berichte – anonym, wenn gewünscht – einzureichen.

Vorleserunde & Diskussion
(ca. 10–20 Min.)

1. Wählen Sie nach einem definierten Verfahren (z. B. zufällige Auswahl oder feste Reihenfolge) einen Fehlerbericht aus, der vorgelesen wird.
2. Nach jedem vorgelesenen Bericht:
   - Geben Sie der Gruppe die Möglichkeit, kurz die wesentlichen Lernpunkte zu diskutieren.
   - Achten Sie darauf, dass keine sensiblen Details preisgegeben werden.

Abschluss & Reflexion
(ca. 5–10 Min.)

1. Fassen Sie die wichtigsten Erkenntnisse der Session zusammen.
2. Bitten Sie die Teilnehmenden, kurz zu reflektieren, was sie aus den vorgestellten „Fuck-ups“ mitnehmen.
3. Weisen Sie darauf hin, dass die gesammelten Berichte die Basis für ein jährliches Lernabenteuerbuch bilden können – ein Anreiz, offen über Fehler zu sprechen und daraus zu lernen.
4. Bedanken Sie sich für die Teilnahme und die Bereitschaft, Erfahrungen zu teilen.

Tipps

→ Das Format ist auf eine Dauer von ca. 30–60 Minuten ausgelegt.
→ Die Teilnehmerzahl sind mindestens 15 Personen, um einen intensiven Austausch zu ermöglichen, aber gleichzeitig Anonymität zu gewährleisten, falls die Gruppe anonym teilen möchte.
→ Halten Sie das Template klar und strukturiert, um den Teilnehmenden eine einfache und fokussierte Darstellung ihres "Fuck-ups" zu ermöglichen. Ein mögliches Template könnte folgende Felder enthalten: Titel/Kurzbeschreibung, Fehlerbeschreibung, Ursachen/Auslöser, Maßnahmen & Lösungsansatz.

02—2
Themenbezogene Chatgruppen

KURZBESCHREIBUNG

Geschlossene Chatgruppen bieten IT- und Cybersecurity-Expert:innen einen sicheren, verschlüsselten Raum, um akute Informationen, News und praxisrelevante Learnings auszutauschen.

Aufwand ●●●●○

Präsenz digital

Frequenz seriell

Ziele

→ Aktuelle und relevante Informationen sowie Erfahrungen teilen.
→ Fortlaufender fachlicher Austausch zur Weiterbildung und Verbesserung der Praxis.
→ Schaffung eines sicheren und regelkonformen Diskussionsraums, in dem sich alle auf Augenhöhe begegnen.

Zielgruppe

→ IT- und Cybersecurity-Expert:innen, Instant Responder und Fachkräfte aus Risiko-, Compliance- und Krisenmanagement.
→ Personen mit gleich hohem Fachniveau, die an einem intensiven, kontinuierlichen Austausch zu einem Thema interessiert sind.

BEISPIEL-ABLAUF

1. Begrüßung & Einführung

1. Begrüßen Sie die Teilnehmenden in der digitalen Chatgruppe.
2. Erklären Sie die Teilnahmebedingungen, etwa Verpflichtung zur Einhaltung der festgelegten Kommunikationsregeln.
3. Stellen Sie das Konzept kurz vor und erläutern Sie, dass es sich um eine geschlossene, themenspezifische Gruppe handelt, in der ausschließlich aktuelle, relevante Informationen geteilt werden.
4. Weisen Sie darauf hin, dass der Austausch über einen verschlüsselten Messenger erfolgt und ein festgelegtes Regelwerk eingehalten werden muss.

2. Aktive Moderation & Austausch (laufend während der Chatphase)

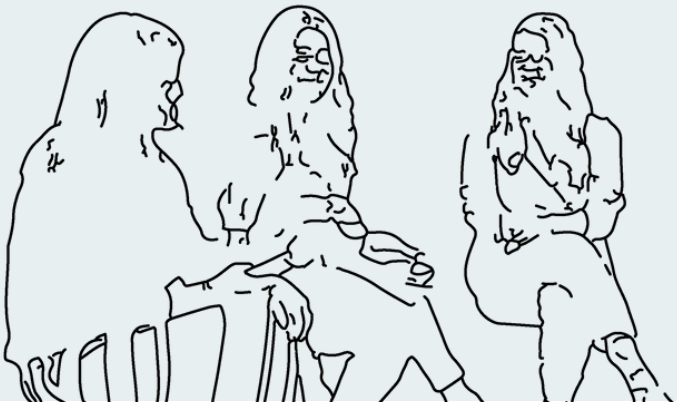
- Fassen Sie nach einem definierten Zeitraum (z. B. am Ende eines Arbeitstages oder einer festgelegten Austauschphase) die wichtigsten Erkenntnisse zusammen.
- Bitten Sie die Teilnehmenden um Feedback und Vorschläge zur Optimierung des Formats.

Tipps

→ Kommunizieren Sie klar und freundlich, um die Teilnehmenden zur aktiven Beteiligung zu motivieren.

→ Achten Sie darauf, dass alle Beiträge den festgelegten Regeln entsprechen. Seien Sie geduldig und reagieren Sie zeitnah auf Fragen oder Unsicherheiten.

02—3
Micro-Learning Circles



KURZBESCHREIBUNG

Micro-Learning Circles sind regelmäßige, themenspezifische Lerngruppen, in denen sich Teilnehmende über einen definierten Zeitraum (z. B. drei Monate) alle zwei Wochen für 90 Minuten online (oder in persona) treffen, um kollaborativ an einem spezifischen Thema zu arbeiten.

Aufwand ●●●●●

Präsenz digital (auch in in persona möglich)

Frequenz seriell

Ziele

→ Kontinuierliches, kollaboratives Lernen und praxisnahe Umsetzung von Präventions-, Detektions- und Reaktionsmaßnahmen fördern
→ Effiziente, zielgruppengerechte Weiterbildung ermöglichen
→ Austausch von Best Practices und Erfahrungen intensivieren

Zielgruppe

→ Fachkräfte, die wenig Zeit haben und nicht gerne alleine arbeiten
→ Fachkräfte von KMUs, die sich gezielt mit einem bestimmten Thema (z. B. Schwachstellenmanagement) auseinandersetzen möchten
→ Teilnehmende, die von einem regelmäßigen Austausch auf gleichem Fachniveau profitieren möchten

BEISPIEL-ABLAUF

1. Begrüßung & Einführung

1. Begrüßen Sie die Interessierte und stellen Sie das Konzept der Micro-Learning Circles vor.
2. Erläutern Sie den strukturierten Ablauf über den definierten Zeitraum und betonen Sie den Fokus auf kollaboratives Lernen.

2. Themenfindung & Interessenabfrage

1. Leiten Sie eine kurze Umfrage oder Diskussionsrunde ein, um relevante Themen und Interessen der Teilnehmenden zu identifizieren.
2. Erklären Sie, dass es darum geht, ein Thema abzuarbeiten und parallel To-Dos anzugehen – jeder bearbeitet seine eigenen Aufgaben, aber man lernt voneinander und klärt gemeinsam Fragen.
3. Binden Sie externe Expert:innen ein, um zusätzliche Impulse zu geben.

3. Regelmäßige Sessions
(jeweils 90 Minuten, alle zwei Wochen)

1. Moderieren Sie die Online-Sessions, fördern Sie den aktiven Austausch und strukturieren Sie die Diskussionen.
2. Dokumentieren Sie die wichtigsten Erkenntnisse und halten Sie Fortschritte fest, um die kontinuierliche Entwicklung der Gruppe zu unterstützen.

4. Abschluss und Reflexion

1. Fassen Sie am Ende jeder Session die zentralen Lernergebnisse zusammen und ermutigen Sie die Teilnehmenden, Feedback zu geben und zukünftige Themenwünsche einzubringen.
2. Weisen Sie darauf hin, dass das Ende der Session zeitlich definiert ist und den Austausch markiert – es muss nicht bedeuten, dass alle To-Dos vollständig abgearbeitet sind.

Tipps

→ Setzen Sie gezielte Impulse, um den Lernprozess aktiv anzuregen.
→ Sorgen Sie für eine offene, vertrauensvolle Atmosphäre, in der sich alle wohlfühlen und ihre individuellen Lernziele verfolgen können.
→ Achten Sie auf einen reibungslosen technischen Ablauf (z. B. zuverlässige Video-Plattform) und unterstützen Sie bei Bedarf mit Fachexpertise.

02—4
Storytelling mit Business-Impact

KURZBESCHREIBUNG

Storytelling mit Business-Impact ist eine interaktive Coaching-Session, in der narrative Techniken genutzt werden, um technische Sicherheitsmaßnahmen in einen geschäftlichen Kontext zu stellen. In 90-minütigen Sessions lernen Sie, wie komplexe Cybersecurity-Themen in verständliche Geschichten verwandelt werden, die finanzielle, rechtliche und rufbezogene Risiken beleuchten.

Aufwand ●●●●○

Präsenz in persona

Frequenz einmalig

Ziele

→ Vermittlung von Cybersicherheitsinhalten in zielgruppenspezifischer Narration, um den Business-Impact von Sicherheitsmaßnahmen deutlich zu machen.
→ Aufbau von fachlicher Kompetenz und Aktivierung weiterer Kolleg:innen durch gemeinsame Storyentwicklung.
→ Verdeutlichung, wie Sicherheitsmaßnahmen technische Probleme lösen und gleichzeitig geschäftliche Risiken minimieren könne.

Zielgruppe

→ Hauptsächlich CISOs, aber auch weitere Entscheidungsträger:innen und Fachkräfte, die im Bereich Cybersicherheit tätig sind und von narrativen Kommunikationsansätzen profitieren möchten.

BEISPIEL-ABLAUF

1. Begrüßung & Einführung

1. Begrüßen Sie die Teilnehmenden und stellen Sie das Konzept des Storytellings im Kontext der Cybersicherheit vor.
2. Erklären Sie, wie narrative Techniken helfen, den geschäftlichen Impact von Sicherheitsmaßnahmen nachvollziehbar zu machen.

2. Story-Entwicklung & Übungen
(ca. 60 Min.)

1. Führen Sie gezielte Übungen wie „Erklär mal für …“ durch, um die Teilnehmenden dazu anzuregen, komplexe Themen in verständliche Storys zu übertragen.
2. Moderieren Sie den Austausch, sodass jede:r seine/ihre Perspektive einbringt und voneinander gelernt wird.
3. Sammeln Sie die erarbeiteten Storys, die später veröffentlicht werden können.

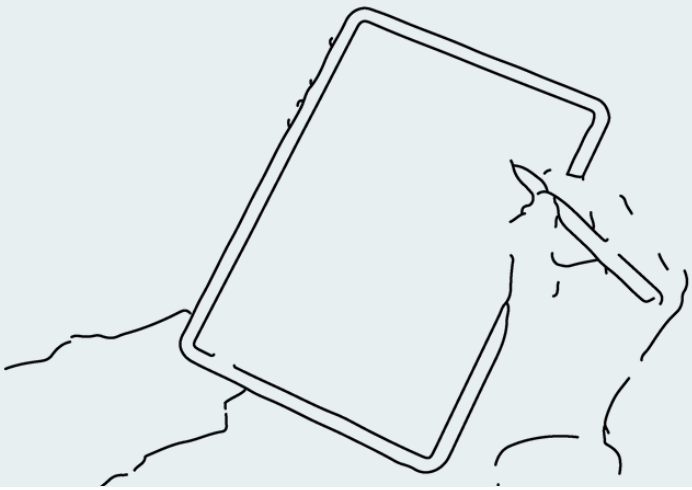
3. Abschluss & Reflexion
(ca. 20 Min.)

1. Fassen Sie die wichtigsten Erkenntnisse zusammen und diskutieren Sie, wie die erarbeiteten Geschichten den Business-Impact von Sicherheitsmaßnahmen verdeutlichen.
2. Ermutigen Sie die Teilnehmenden, die entwickelten Storys als Grundlage für weitere Diskussionen im Unternehmen zu nutzen.

Tipps

- → Arbeiten Sie mit erfahrenen Coaches und Storytellern zusammen, um den Teilnehmenden professionelle Impulse und Best Practices zu bieten.
- → Schaffen Sie eine offene und kreative Atmosphäre, in der auch unkonventionelle Ideen willkommen sind.
- → Nutzen Sie visuelle Hilfsmittel und praxisnahe Beispiele, um den Zusammenhang zwischen technischen Maßnahmen und deren geschäftlichen Auswirkungen zu verdeutlichen.
- → Achten Sie darauf, dass die Übungen stets zielgruppenspezifisch und praxisnah gestaltet sind, um maximalen Mehrwert zu erzielen.

02—5
Butter bei die Fische



KURZBESCHREIBUNG

Butter bei Die Fische ist ein faktenbasiertes Format, das durch anonymisierte Benchmarking-Umfragen, konkrete Fragen und Prioritäten-Ranking-Übungen praxisnahe Erkenntnisse liefert. Es werden zentrale Fragen gestellt, wie z. B. „Wenn Sie nur eine Cybersicherheitsmaßnahme einführen, ändern oder abschaffen könnten, welche wäre das und warum?“ sowie Fragen zu IT-Sicherheitsausgaben und eingesetzten Tools. Die aggregierten Antworten helfen CISOs, Muster zu erkennen und die effektivsten Resilienzmaßnahmen zu identifizieren – alles auf sicheren, digitalen Kanälen.

Aufwand	●●●●●
Präsenz	digital
Frequenz	seriell

Ziele	→ Anhand konkreter Daten lernen und sich als Unternehmen einordnen können. → Die besten Resilienzmaßnahmen identifizieren und priorisieren. → Direkt anwendbare, faktenbasierte Handlungsempfehlungen aus der Praxis ableiten.
Zielgruppe	→ CISOs und Entscheidungsträger:innen im Bereich Cybersicherheit, die an einem datenbasierten Benchmarking interessiert sind.

BEISPIEL-ABLAUF

1. Einführung & Ankündigung

1. Begrüßen Sie die Teilnehmenden und erklären Sie den Ablauf der anonymisierten Benchmarking-Umfrage, die über einen Monat läuft.
2. Erläutern Sie die zentralen Fragen, beispielsweise:
   a. „Wenn Sie nur eine Cybersicherheitsmaßnahme einführen, ändern oder abschaffen könnten, welche wäre das und warum?“
   b. Fragen zu IT-Sicherheitsausgaben in Relation zum Umsatz und zum teuersten eingesetzten Tool.
3. Weisen Sie darauf hin, dass alle Ergebnisse ausschließlich einem ausgewählten Teilnehmerkreis zugänglich gemacht werden und technisch gesichert sind, sodass ein Download der Daten nicht möglich ist.

2. Durchführung der Umfrage (laufend)

1. Stellen Sie sicher, dass die Umfrage über ein sicheres Tool erfolgt, das eine anonyme Teilnahme gewährleistet.
2. Stellen Sie sicher, dass genügend Unternehmen mitmachen.
3. Unterstützen Sie die Teilnehmenden bei technischen Fragen und sorgen Sie für einen reibungslosen Ablauf.

3. Auswertung & Ranking-Übung (nach Abschluss der Umfrage)

1. Aggregieren Sie die Umfrageergebnisse, um Muster und Trends zu identifizieren.
2. Moderieren Sie eine Prioritäten-Ranking-Übung, in der die Teilnehmenden die ermittelten Daten diskutieren und die effektivsten Resilienzmaßnahmen priorisieren.
3. Erinnern Sie die Gruppe daran, dass die aggregierten Ergebnisse ausschließlich einem ausgewählten Kreis zugänglich sind und technisch nicht herunterladbar sind, um die Vertraulichkeit zu sichern.

Tipps

- → Betonen Sie den Mehrwert anonymisierter, faktenbasierter Daten und wie diese zu praxisnahen Erkenntnissen führen.
- → Arbeiten Sie konsequent mit sicheren Tools, um den Schutz sensibler Informationen zu gewährleisten.
- → Ermutigen Sie die Teilnehmenden, offen und ehrlich ihre Erfahrungen zu teilen, um fundierte, vergleichbare Daten zu generieren.
- → Nutzen Sie die aggregierten Ergebnisse, um konkrete Handlungsempfehlungen und Best Practices abzuleiten.

02—6
Probleme Roulette – Walking in my Shoes

KURZBESCHREIBUNG

Probleme Roulette – Walking in my Shoes ist ein interaktives, digitales Lernformat, in dem Teilnehmende aktuelle Herausforderungen aus ihrem Unternehmen einreichen. In den Online-Sessions werden diese Probleme gemeinsam analysiert, diskutiert und kreative Lösungsansätze entwickelt.

Aufwand	●●●○○
Präsenz	digital
Frequenz	seriell

Ziele

→ Stärkung der Problemlösungskompetenz durch innovative, praxisnahe Lösungsansätze.
→ Förderung von Empathie und Perspektivenvielfalt, um die Herausforderungen anderer besser zu verstehen.
→ Ermöglichung von Wissenstransfer durch den Austausch bewährter Strategien aus verschiedenen Unternehmen.

Zielgruppe

→ Fach- und Führungskräfte, die praxisorientierte, interaktive Schulungen schätzen und von einem offenen Erfahrungsaustausch profitieren möchten.

BEISPIEL-ABLAUF

1. Einführung & Themenvorstellung
(ca. 5 Min.)

1. Begrüßen Sie die Teilnehmenden und erläutern Sie das Konzept von Probleme Roulette – Walking in my Shoes.
2. Erklären Sie den Ablauf und weisen Sie darauf hin, dass vorab aktuelle Herausforderungen aus den Unternehmen eingereicht werden.
3. Verdeutlichen Sie, dass Themen wie „eine Kiste Pralinen" präsentiert werden – man weiß nie, welches Problem als Nächstes kommt.

2. Analyse & Diskussion
(ca. 40 Min.)

1. Wählen Sie ein oder mehrere eingereichte Probleme aus und leiten Sie eine offene Diskussion ein.
2. Binden Sie die Teilnehmenden aktiv ein, indem Sie sie ermutigen, ihre eigenen Erfahrungen, Ideen und Lösungsansätze zu teilen.
3. Moderieren Sie den Austausch so, dass ein interaktiver Dialog entsteht und alle Stimmen Gehör finden.

3. Abschluss & Reflexion
(ca. 15 Min.)

1. Fassen Sie die wichtigsten Erkenntnisse der Session zusammen.
2. Diskutieren Sie, wie die erarbeiteten Lösungsansätze zu einem besseren Umgang mit den Herausforderungen beitragen können – das Ende markiert den Austausch, muss aber nicht alle To-Dos vollständig abarbeiten.
3. Ermutigen Sie die Teilnehmenden, auch zukünftig eigene Beispiele einzubringen und voneinander zu lernen.

Tipps

- → Vermeiden Sie lange Vorträge und setzen Sie stattdessen auf interaktive Diskussionen und Fragen.
- → Schaffen Sie niederschwellige Anlässe, um kontinuierliche Perspektivübernahme und den Austausch im Alltag zu fördern.
- → Nutzen Sie gezielte Impulse und Trigger, um den Dialog anzuregen und den Wissenstransfer zu unterstützen.

02—7
Fishbowl – Cyberangriff, wie war das nochmal?!

KURZBESCHREIBUNG

In diesem interaktiven Fishbowl-Format teilen Teilnehmende ihre Erfahrungen mit Cyberangriffen. Ein kleiner innerer Kreis (ca. 5–9 Personen) berichtet aktiv, während der größere Außenkreis (bis zu ca. 50 Personen) zuhört und bei Bedarf in die Diskussion einsteigt. Dabei werden reale Fallbeispiele und Lessons Learned besprochen, um erfolgreiche Strategien sowie Verbesserungspotenziale zu identifizieren.

Aufwand	●○○○○
Präsenz	in persona
Frequenz	seriell

Ziele	→ Erfahrungen und Erkenntnisse zu Cyberangriffen austauschen. → Erfolgreiche Strategien und unterschiedliche Herangehensweisen kennenlernen. → Risiken sensibilisieren und den Handlungsbedarf bei Cyberangriffen verdeutlichen.
Zielgruppe	→ Personen, die bereits einen Cyberangriff erlebt haben, sowie jene, die sich auf einen möglichen Angriff vorbereiten möchten.

BEISPIEL-ABLAUF

1. Einführung

1. Erklären Sie das Fishbowl-Prinzip: Der innere Kreis (5–9 aktive Sprecher:innen) teilt seine Erfahrungen, während der äußere Kreis zuhört und bei Bedarf einsteigt.
2. Weisen Sie auf die Chatham House Rules hin und betonen Sie, dass keine sensiblen Daten geteilt werden sollen.

2. Moderation

1. Moderieren Sie den Austausch, um sicherzustellen, dass alle Beiträge wertgeschätzt werden und einzelne Personen nicht dominieren.
2. Sorgen Sie für einen strukturierten, lebendigen Dialog und lenken Sie den Fokus auf konkrete Fallbeispiele und Lessons Learned.

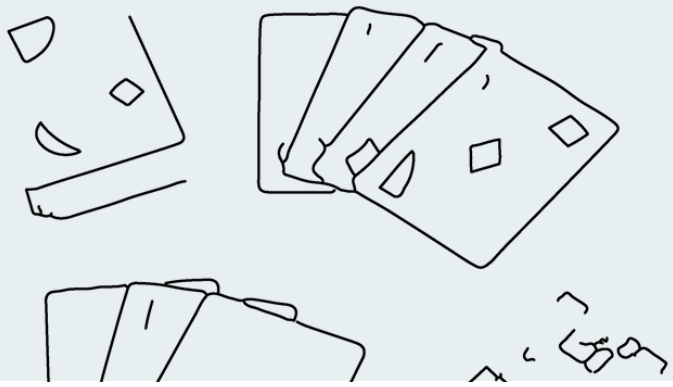
3. Zeitmanagement

Halten Sie die Session auf 60–90 Minuten begrenzt, wobei das Ende als markierter Austauschzeitraum verstanden wird – es muss nicht bedeuten, dass alle Themen vollständig abgearbeitet sind.

Tipps

- → Achten Sie darauf, dass die Räumlichkeiten die notwendige Fishbowl-Sitzordnung (konzentrische Stuhlkreise) ermöglichen.
- → Motivieren Sie die Teilnehmenden, ihre Erfahrungen konkret und praxisnah zu schildern, und setzen Sie gezielte Impulse, um einen kontinuierlichen Austausch zu fördern.
- → Dokumentieren Sie wesentliche Erkenntnisse, ohne sensible Informationen preiszugeben.
- → Nutzen Sie gezielte Impulse und Trigger, um den Dialog anzuregen und den Wissenstransfer zu unterstützen.

02—8
(Mis-)Match Memory



KURZBESCHREIBUNG

(Mis-)Match Memory ist ein interaktives Lernformat, das Sie für die Herausforderungen im Umgang mit Standards sensibilisiert. Mithilfe von Karten, auf denen sowohl Standards als auch praktische Empfehlungen abgebildet sind, suchen Sie nach passenden Matches – oder erkennen bewusst Deltas zwischen den Anforderungen und Best Practices. Am Ende der Matching-Phase werden die gefundenen Matches und Mis-Matches in einer moderierten Diskussion erörtert, um Umsetzungskontexte und Best Practices gemeinsam zu beleuchten.

Aufwand ●●●●●

Präsenz digital / in persona

Frequenz seriell

Ziele

→ Sensibilisierung für Diskrepanzen zwischen Standardanforderungen und technischen Empfehlungen.
→ Förderung von mehr Commitment statt reiner Compliance sowie Steigerung der Effizienz von Cybersicherheitsmaßnahmen.
→ Austausch von Best Practices und Entwicklung praxisnaher Lösungsansätze

Zielgruppe

→ Fach- und Führungskräfte aus den Bereichen IT, operative Sicherheit, Policy und Management, die an innovativen Ansätzen zur Optimierung von Sicherheitsstandards interessiert sind.

BEISPIEL-ABLAUF

Hinweis: Das Spiel muss noch designt werden. Das bedeutet, dass die konkreten Matches und Mis-Matches im Vorfeld noch definiert werden müssen, um einen reibungslosen Ablauf zu gewährleisten.

1. Einführung

Begrüßen Sie die Teilnehmenden und erläutern Sie das Ziel des Formats sowie die Funktionsweise der Karten, die sowohl Standards als auch technische Empfehlungen abbilden.

2. Matching-Phase

Lassen Sie die Teilnehmenden in kleinen Gruppen oder einzeln die passenden Matches finden. Weisen Sie darauf hin, dass es auch zu Mehrfach-Matches (z. B. 3er- oder 4er-Gruppen) kommen kann oder einzelne Karten übrig bleiben..

Beispiel für einen Mismatch:
Ein potenzieller Mismatch könnte bestehen zwischen einer Karte, die den Standard „Regelmäßige Passwortwechsel unter Berücksichtigung von Groß-/Kleinschreibung und Sonderzeichen“ zeigt, und einer Karte, die die technische Empfehlung „Verwendung langer, komplexer Passwörter ohne häufige Änderungen“ präsentiert.

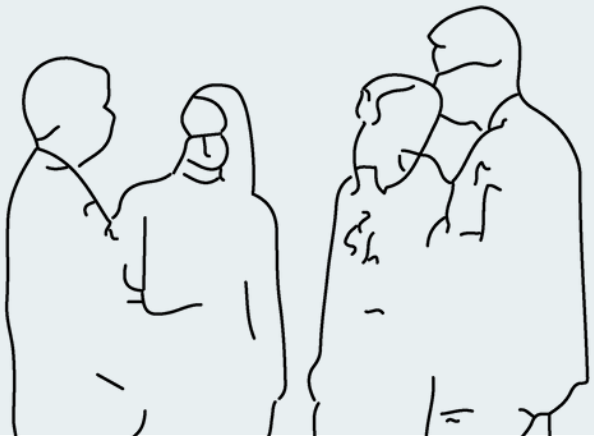
3. Diskussion

Moderieren Sie eine gemeinsame Diskussion, in der die gefundenen Matches und Mis-Matches besprochen werden. Gehen Sie dabei insbesondere auf die unterschiedlichen Umsetzungsmöglichkeiten und identifizierten Deltas ein.

Tipps

- → Fördern Sie den interdisziplinären Austausch, indem Sie die unterschiedlichen Perspektiven der Teilnehmenden einbeziehen.
- → Setzen Sie gezielte Impulse, um die Diskussion anzuregen und den Transfer in den Unternehmenskontext zu erleichtern.
- → Achten Sie darauf, dass alle Teilnehmer aktiv eingebunden werden und ihre Ansichten respektvoll diskutiert werden.
- → Planen Sie ausreichend Zeit ein, um das noch zu designende Spielkonzept (Matches/Mis-Matches) mit den Teilnehmenden zu erproben und anzupassen.

02—9
Warm-Up - Cybersecurity Mapping



KURZBESCHREIBUNG

Dieses Format hilft Ihnen dabei, sich und Ihr Unternehmen im Kontext der Cybersicherheit zu verorten. Anhand vorgegebener Aussagen wie „Hat Ihr Unternehmen eine Cyberversicherung?“, „Führt Ihr Unternehmen Cybersicherheitsschulungen vor Ort durch?“ oder „Gibt es mindestens einmal jährlich Phishing-Kampagnen?“ können Sie ihr Unternehmen in Relation mit einem anderen sehen.

Aufwand ●○○○○

Präsenz in persona (alternativ digital via Miroboard)

Frequenz seriell

Ziele

→ Faktoren identifizieren und reflektieren, die Cybersicherheitsentscheidungen beeinflussen.
→ Benchmarking-Möglichkeiten schaffen und relevante Netzwerkpartner erkennen.
→ Effiziente, kontextbezogene Kommunikation über Sicherheitsstrategien fördern.

Zielgruppe

→ Führungskräfte und Fachverantwortliche aus den Bereichen Management, Technik, operatives Geschäft, Policy und Kommunikation, die ihre Positionierung und die Entscheidungen im Bereich Cybersicherheit reflektieren möchten.

ABLAUF & ANLEITUNG FÜR DEN FACILITATOR:

1. Einführung

1. Begrüßen Sie die Teilnehmenden und erläutern Sie das Ziel des Formats: sich selbst und das eigene Unternehmen im Kontext der Cybersicherheit zu verorten.
2. Erklären Sie das Konzept des Mapping: Es werden verschiedene Fragen bzw. Aussagen präsentiert, zu denen sich die Teilnehmenden farblich codiert positionieren.
3. Stellen Sie das Koordinatensystem vor, z. B. mit den Achsen „Unternehmensgröße“ (x-Achse) und „Cybermaturity“ (y-Achse).

2. Positionierungsphase

1. Präsentieren Sie als erstes Beispiel die Frage: „Wird in Ihrem Unternehmen mindestens einmal jährlich eine Phishing-Kampagne durchgeführt?“
2. Bitten Sie die Teilnehmenden, entsprechend ihrer Antwort eine grüne Karte (bei „ja“) oder eine rote Karte (bei „nein“) mit ihrem Namen oder Firmennamen zu versehen.
3. Lassen Sie die Teilnehmenden ihre Karten im passenden Bereich des Koordinatensystems platzieren.
4. Erklären Sie, wie die Platzierung interpretiert werden kann – beispielsweise können Unternehmen, die groß und hoch „cybermature“ sind, in einem bestimmten Quadranten erscheinen.

3. Weitere Fragen & Mapping

1. Führen Sie weitere, vorab definierte Fragen/Aussagen ein (z. B. „Führt Ihr Unternehmen Cybersicherheitsschulungen vor Ort durch?“).
2. Wiederholen Sie den Vorgang: Die Teilnehmenden wählen für jede Aussage die entsprechende farbige Karte und platzieren diese im Koordinatensystem.

4. Diskussion & Reflexion

1. Moderieren Sie eine gemeinsame Diskussion, in der Sie die Ergebnisse des Mappings betrachten.
2. Diskutieren Sie, welche Faktoren zu den jeweiligen Positionierungen geführt haben und welche Unterschiede in den Umsetzungsstrategien erkennbar sind.
3. Nutzen Sie die Ergebnisse, um Best Practices zu identifizieren und Benchmarks zu setzen.

Tipps

→ Stellen Sie sicher, dass die Technik (Poster, Flipcharts oder Miroboard) reibungslos funktioniert.
→ Motivieren Sie alle Teilnehmenden, sich aktiv einzubringen, und fördern Sie einen respektvollen, offenen Austausch.
→ Verwenden Sie die Ergebnisse, um relevante Faktoren und Netzwerkpartner für zukünftige Cybersicherheitsstrategien zu identifizieren.

Ein Projekt der

dena

www.dena.de

future-energy-lab.de