Future Energy Lab

dena NIS2-Roadmap für Energie-Start-ups

In 6 Etappen durch die wichtigsten NIS2-Anforderungen. Von der Theorie zur Praxis mit konkreten Beispielen, Übungen und Meilensteinen.

Über die Roadmap >

Dies ist ein interaktives PDF. Sie können zwischen den Etappen springen.

Ein Projekt der dena

int[cube]

CYBER POLICY HAUS

GESELLSCHAFT FÜR INFORMATIK

Impressum Nutzungsbedingungen

Future Energy
Lab

Über die Roadmap

Für die Cybersicherheit in der Stromwirtschaft ist es zentral, dass Compliance in den Unternehmen kein bürokratischer Störfaktor, sondern ein Motor für operative Sicherheit und nachhaltige Resilienz wird.

Die dena NIS2-Roadmap richtet sich an Start-ups und kleine Unternehmen der Energiebranche, die nicht direkt unter die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (Network and Information Security Directive 2, NIS2-Richtlinie) fallen, aber als Dienstleister oder Zulieferer mit regulierten Akteuren zusammenarbeiten. Im Pilot-Mentoring (Q2–Q3 2025) haben wir gemeinsam mit der Zielgruppe einen Prototyp entwickelt, der praxisnahe, verständliche und umsetzbare Handlungsschritte liefert – ohne Überforderung und, mit klarem Fokus auf reale Anforderungen. Durch modulare Bausteine und interaktive Formate sollen kleine Marktteilnehmer Klarheit, Sicherheit und echte Praxiserfahrung gewinnen, um gegenüber größeren Organisationen anschlussfähig zu bleiben.

Die Roadmap basiert auf sechs zentralen NIS2-Themen, die einige wesentliche Maßnahmen der EU-Richtlinie abdecken. Drei davon sind Themen, die die Pilot-Mentees von insgesamt sechs Wahlthemen ausgewählt haben.
In neun Gruppenmentoring-Sitzungen wurden offene Fragen geklärt und es wurde kompaktes Wissen vermittelt und praxisnah geübt. Moderierte Peer-Exchanges und Experten-Q&A-Runden sorgten für vertiefende Impulse. Interaktive Elemente wie Live-Umfragen, Mini-Workshops und Rollenspiele haben den Transfer in den Arbeitsalltag sichergestellt. Daraus haben wir diese Roadmap abgeleitet, die keine rechtliche Beratung darstellt, aber eine strukturierte, praxisnahe Grundlage zur internen Orientierung und externen Kommunikation bietet. Damit schaffen wir eine Brücke zwischen regulatorischen Anforderungen und betrieblicher Realität – für mehr Sicherheit, weniger Komplexität und echte Anschlussfähigkeit.

Zur Roadmap

Ein Projekt der
dena
int[cube]
CYBER POLICY HAUS
GESELLSCHAFT FÜR INFORMATIK

Future Energy Lab

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.

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
David Fuhr, intcube GmbH
Hauke Gierow, intcube GmbH
Kalina Sperber, intcube GmbH
Julia Schuetze, Cyber Policy Haus

Design
Ulf Seißenschmidt, Cyber Policy Haus
Julia Schuetze, Cyber Policy Haus

Wissenschaftliche Begleitung
Marieke Petersen, Gesellschaft für Informatik e.V.
Linda Schwarz, Gesellschaft für Informatik e.V.

Redaktion
Katerina Simou, dena
Friederike Wenderoth, dena

Stand
August 2025

Danksagungen
Die Projektpartner bedanken sich bei den Unternehmen, die durch die Teilnahme am Mentoring diese Roadmap mitgestaltet haben, namentlich EnergieDock, decarbon1ze, Blindleister, Rosenxt und DETOplus.

Urheberrecht
Die Roadmap ist urheberrechtlich geschützt. Die Vervielfältigung oder Weitergabe richtet sich nach der Deed - Attribution 4.0 International - Creative Commons Lizenz, abrufbar unter: https://share.google/cAMhi0z39su9RuCt5.

Der kommerzielle Weiterverkauf des Dokumentes ist nicht gestattet.

Bitte zitieren als:
„dena NIS2-Roadmap für Energie-Start-ups“ © 2025 by dena is licensed under Creative Commons Attribution 4.0 International. https://creativecommons.org/licenses/by/4.0/

Ein Projekt der dena

int[cube]

CYBER POLICY HAUS

GESELLSCHAFT FÜR INFORMATIK

Zur Roadmap

Future Energy
Lab

Nutzungsbedingungen der Roadmap

Die Informationen, Inhalte und Übungen, die in der Roadmap bereitgestellt werden, dienen ausschließlich Bildungs- und Informationszwecken.
Sie stellen keine Rechtsberatung dar und sollten nicht als Ersatz für die Konsultation qualifizierter juristischer Fachleute herangezogen werden.
Obwohl alle Anstrengungen unternommen wurden, die Relevanz und Genauigkeit der präsentierten Informationen sicherzustellen, wird keine Gewähr für ihre Vollständigkeit, Richtigkeit oder Eignung für Ihre spezielle Situation übernommen. Die Inhalte spiegeln eine allgemeine Interpretation der geltenden Cybersicherheitsvorschriften einschließlich der NIS2-Richtlinie wider und sind nicht als verbindliche Rechtsberatung gedacht.

Die Nutzung der Roadmap erfolgt ausschließlich auf eigenes Risiko. Die dena sowie ihre Beschäftigten und Partner übernehmen keine Haftung für direkte oder indirekte Schäden, die sich aus der Nutzung der Roadmap ergeben, es sei denn, diese beruhen auf vorsätzlichem Fehlverhalten oder einer gesetzlich vorgeschriebenen Haftung.

Wir empfehlen dringend, vor Entscheidungen, die auf den über die Roadmap bereitgestellten Informationen basieren, rechtlichen Rat von qualifizierten Rechtsanwältinnen und Rechtsanwälten einzuholen.

Zur Roadmap

Ein Projekt der
dena
int[cube]
CYBER POLICY HAUS
GESELLSCHAFT FÜR INFORMATIK

Etappe

Endgegner Einkauf

Zur Roadmap

Etappe

Endgegner Einkauf

Relevanz: IT-Sicherheit ist ein Kriterium bei der Dienstleisterwahl. Wenn Sie von NIS2 betroffene Kunden haben, werden diese NIS2-Anforderungen weitergeben. Zeigen Sie proaktiv, dass Sie vorbereitet sind!

In dieser Etappe lernen Sie, wie Sie die Erwartungen Ihrer Auftraggeber besser verstehen, Ihren eigenen Geltungsbereich (Scope) definieren und realistische Nachweise vorbereiten.

Wir zeigen Ihnen, welche Kriterien Ihre Kunden anwenden, wie Sie Transparenz schaffen und wie Sie einen zielführenden Dialog auf Augenhöhe führen – statt Stress beim Fragebogen-Marathon.

Etappenabschnitt

Auswahlkriterien auf Kundenseite

Worauf schauen Kunden? Wie viel Security ist ihnen wann wichtig?

- Info: Gesetze und Richtlinien – Blick in die Cyberregulatorik
- Übung: Scoping – Wer ist wer?

Etappenabschnitt

Zielführender Dialog mit Kunden

Wie gelingt ein Austausch auf Augenhöhe?

- Übung: Meldestelle einrichten
- Übung: Perspektivwechsel im Einkauf

Etappen FAQ

Zur Roadmap

Info: Gesetze und Richtlinien – Blick in die Cyberregulatorik

Dieser Abschnitt gibt einen Überblick über die wichtigsten Gesetze und Richtlinien, die im Energie- und KRITIS-Umfeld relevant sind. Zusätzlich gibt es Technische Richtlinien vom BSI, die Security-Anforderungen (z. B. für Smart Meter Gateways) enthalten.

NIS2-Richtlinie (verabschiedet)

EU-Richtlinie zur Mindestharmonisierung von Cybersicherheitsstandards mit Schwerpunkt auf Betreibern Kritischer Infrastrukturen sowie wichtige und besonders wichtige Unternehmen. Fordert konkrete Maßnahmen zum Risikomanagement im IT-Security-Bereich.

NIS2UmsuCG (in Vorbereitung)

NIS2 ist eine EU-Richtlinie und muss daher durch nationale Gesetze von den Mitgliedsstaaten implementiert werden. Das „NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz“ soll genau das tun – in Deutschland voraussichtlich Ende 2025.

NIS2 Implementing Act

Diese Durchführungsverordnung der EU konkretisiert die Cybersecurity-Anforderungen aus NIS2 in über 150 einzelne Kontrollen. Sie ist verbindlich für digitale Infrastrukturen wie Cloud und IT-Dienstleister und für diese Zielgruppe bereits unmittelbar in Kraft.

BSI-Gesetz/BSI-KritisVO

Sobald eine Anlage einen gewissen Versorgungsschwellenwert erreicht und rund 500.000 Menschen versorgt, gilt sie in Deutschland als KRITIS. Kritische Anlagen im Energiesektor werden abweichend davon durch das EnWG reguliert.

EnWG

Das EnWG soll die Sicherheit internetfähiger Produkte steigern. Betroffen sind Produkte für Privatanwender, aber auch kritische Produkte für den geschäftlichen oder industriellen Einsatz. Die Anforderungen aus dem EnWG müssen Ende 2027 umgesetzt sein, eine Meldepflicht für Schwachstellen gilt bereits ab September 2026.

EnWG

Das Energiewirtschaftsgesetz regelt den Netzbetrieb und den Wettbewerb von Energieerzeugern. § 11 Abs. 1a und 1b geben vor, dass die Betreiber von Energieversorgungsnetzen und Energieanlagen einen „angemessenen Schutz“ ihrer Anlagen gewährleisten müssen. Diesen definiert die Bundesnetzagentur (BNetzA) im IT-Sicherheitskatalog (IT-SiKat).

Zur Etappe

Zur Roadmap

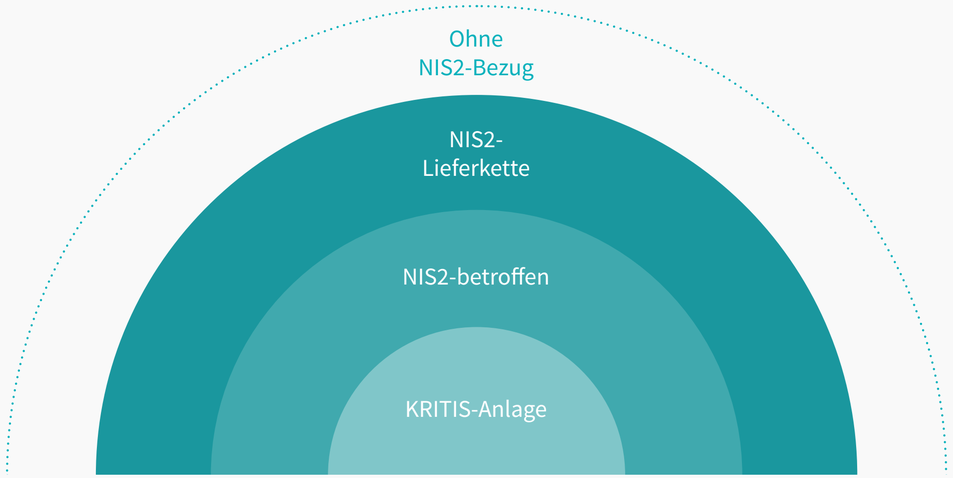
Übung: Scoping – Wer ist wer?

Nachdem Sie die Gesetze grob überblickt haben, können Sie sich und Ihre (potenziellen) Kunden einordnen, um einen Überblick über die regulatorischen und marktlichen Anforderungen in Ihrem Umfeld zu bekommen.

1. Kunden und Partner auflisten

Eigenes Unternehmen	Kunde A	Kunde B	Partner A

2. NIS2-Bezugstypen zuweisen



3. Begründung

Start-up XY ist in der NIS2-Lieferkette, weil es für eine große Erzeugungsanlage Batteriespeicher liefert, aber nur 10 Beschäftigte und weniger als 10 Mio. € Umsatz hat.“

Zur Etappe

Zur Roadmap

Übungsablauf

Verorten Sie sich und Ihr Umfeld. Was betrifft Ihr Unternehmen und Ihre Kunden?

1. Liste erstellen

Erstellen Sie eine Liste Ihrer wichtigsten Kunden und Projektpartner.

2. NIS2-Bezugstypen zuweisen

Weisen Sie jedem, inklusive Ihres eigenen Unternehmens, einen der folgenden Typen zu:

- **Ohne NIS2-Bezug:** Kein erwarteter Einfluss durch NIS2 oder KRITIS-Vorgaben
- **NIS2-Lieferkette:** Das Unternehmen ist nicht direkt NIS2-pflichtig, beliefert aber wiederum andere NIS2-betroffene Unternehmen.
- **NIS2-betroffen:** Die Einrichtungsart des Unternehmens ist in Anhang 1 der NIS2 genannt und es gibt >= 50 Beschäftigte oder >10 Mio. € Jahresumsatz/Bilanzsumme.
- **KRITIS-Anlage:** Zum Beispiel eine Energieerzeugungsanlage mit >= 104 MW Netto-Nennleistung oder ein Stromnetz (hier gilt ab 3.700 GWh die Kritis-VO, der IT-SiKat jedoch bereits unabhängig von der Größe)

3. Begründung schreiben

Schreiben Sie zu jeder Einstufung 1 bis 2 Sätze zur Begründung für die Nachvollziehbarkeit.

Übung: Meldestelle einrichten

NIS2 fordert von regulierten Unternehmen die Einrichtung einer festen Meldestelle, die als Kontaktstelle für Regulierungsbehörden, Zulieferer und Partner bereitsteht.

Neben regulatorischen Anforderungen ist es auch schon seit einiger Zeit gängig, in Dienstleistungsverträgen Ansprechpartner für zeitkritische Security-Informationen festzulegen.

Eine einheitliche Meldestelle im Unternehmen, die eine entsprechende Reaktionszeit bietet und über entsprechende Kompetenzen verfügt, ist also für den Kunden und Lieferantenkontakt wichtig, auch ohne von NIS2 betroffen zu sein.

Zur Etappe

Zur Roadmap

Basisinformationen Meldestelle Security/Informationssicherheit

Name	Rolle/Position
Abteilung	Stellvertretung
Kontaktdaten	Verfügbarkeit und Reaktionszeiten intern/extern (SLA)
Anmerkungen	

Übungsablauf

Als Vorbereitung für mögliche Verhandlungen mit dem Einkauf NIS2-regulierter Unternehmen füllen Sie bitte das nebenstehende Template für die NIS2-Meldestelle aus!

Übung: Perspektivwechsel im Einkauf

Angenommen, Ihr Zielkunde ist nach NIS2 reguliert und muss risikoorientierte Sicherheitsmaßnahmen in seiner Lieferkette umsetzen. Mit einer sorgfältig vorbereiteten Dokumentation und einem klaren Verständnis der regulatorischen Anforderungen verwandeln Sie Ihre Security in einen Wettbewerbsvorteil. Versetzen Sie sich in die Rolle des ausschreibenden Unternehmens und hinterfragen Sie Ihr eigenes Angebot aus Kundensicht: Welche Risiken deckt es ab? Welche Nachweise und Prozesse können Sie vorlegen, um die Compliance- und Audit-Anforderungen lückenlos zu erfüllen?

Wie kritisch ist diese Dienstleistung für den Kunden?	Wie kann die Dienstleistung abgesichert werden?
Welche Daten muss der Kunde an den Dienstleister geben, damit dieser arbeiten kann? Wie schlimm wäre eine Veröffentlichung?	Welche und wie viele Anforderungen müssen durch die erfasste Kritikalität an den Dienstleister weitergeben werden?
Was passiert, wenn der Dienstleister unangekündigt nicht mehr arbeitet? Wie lange kann der Kunde einen Ausfall tolerieren?	Welche und wie viele Anforderungen werden aufgrund der erfassten Kritikalität an den Dienstleister weitergegeben?
Welche Konsequenzen hat es für den Kunden, wenn der Dienstleister mir als Kunde falsche Daten liefert?	Sind diese Anforderungen verhältnismäßig?
Zu welchen Systemen bekommt der Dienstleister Zugang?	Welche Nachweise zu Schutzmaßnahmen sind für den Kunden ausreichend? Reicht eine vertragliche Zusicherung oder braucht es Zertifikate etc.?
Benötigt der Dienstleister Fernzugriff auf IT-Systeme?	Welche Struktur brauchen die Nachweise, damit der Kunde Dienstleister sinnvoll steuern kann?

Übungsablauf

Beantworten Sie die Fragen konsequent aus Kundensicht.

Tipp

Um in der „echten“ Welt diese Fragen zu beantworten, sollten Sie Bieterfragen in Ausschreibungen aktiv nutzen! Wer kluge Rückfragen stellt, zeigt Fachlichkeit und Vorbereitung.
Formulieren Sie Rückfragen präzise, neutral und als **geschlossene Leitfragen**: „Gehen wir richtig in der Annahme, dass …?“ So reduzieren Sie Unklarheiten, ohne Ahnungs- oder Planlosigkeit zu signalisieren.

Zur Etappe

Zur Roadmap

Etappen-FAQ

Wie aufwendig ist eine ISO-27001-Zertifizierung – und hilft eine ISO-9001 dabei?

Planen Sie 6 bis 12 Monate Vorbereitungszeit ein, wenn es sich nicht nur um einen extrem begrenzten Scope handelt und keine umfangreichen Dokumentationen vorliegen. Eine ISO-9001-Zertifizierung hilft beim Aufbau von Prozessen, ersetzt aber keine der spezifischen Anforderungen aus der ISO-27001 – z. B. zum Umgang mit Risiken oder zur technischen Sicherheit.

Ersetzt eine ISO-27001-Zertifizierung den IT-Grundschutz? Wie entscheide ich mich?

Nein – IT-Grundschutz baut auf ISO-27001 auf, geht aber strenger und detaillierter vor. Er eignet sich besonders für Behörden und bestimmte Kritische Infrastrukturen. Die ISO-27001 ist international anerkannt und oft besser geeignet für Unternehmen mit internationalen Kunden. Die Entscheidung hängt von Zielkunden, Branche und Ressourcenrahmen ab.

Normen sind privatwirtschaftlich und nicht verpflichtend. Wie realistisch ist ein Nachweis der Anforderungen auf anderem Wege?

Es ist möglich – aber aufwendiger. Statt einer Norm wie der ISO-27001 können Sie Ihre Sicherheitsmaßnahmen auch mit einem eigenen Konzept und einer eigenen Dokumentation nachweisen. Entscheidend ist, dass Sie die essenziellen Anforderungen aus NIS2 strukturiert, nachvollziehbar und wirksam erfüllen.

Was sind die ersten Schritte, die am meisten bringen im Vergleich zum Aufwand? Was sollte ich zuerst machen – und wie dokumentiere ich es auditfähig?

Starten Sie mit:
Asset-Übersicht – Was betreiben Sie, was nutzten Sie, was wird extern verwaltet?

Risikobewertung light – Identifiziere Sie zentrale Risiken und bestehende Schutzmaßnahmen.

Verantwortlichkeiten klären – Wer ist für IT, Sicherheit und Notfälle zuständig?

Zur Etappe

Zur Roadmap

Tipp

In der IT-Sicherheit sind klassische Projektreferenzen oft nicht genug. Kunden wollen wissen, wie Security konkret umgesetzt ist. Wenn ein Kunde Ihre Lösung bereits auditiert hat, ist das Gold wert – teilen Sie solche Nachweise, wenn möglich. Grundsatz: Je detaillierter die Dokumentationen oder die Prüfberichte, desto glaubwürdiger.

Etappe

Krisenkom-munikation

Zur Roadmap

Etappe

Krisenkommunikation

Diese Etappe beschäftigt sich mit der Frage, wie sich die Reputation eines Unternehmens auch im Krisenfall schützen lässt durch klare, offene Kommunikation und gezieltes Stakeholder-Management.

Relevanz: Wie bringe ich mein Unternehmen ohne Reputationsschaden durch eine Cyberkrise?

Etappenabschnitt

Grundlagen Krisenkommunikation

Was ist Krisenkommunikation, warum ist das Thema NIS2-relevant und welche Standards gibt es dazu?

- Info: Einführung Krisenkommunikation
- Info: Relevante Standards

Etappenabschnitt

Vorbereitung und Durchführung

Welche Fragen stehen vor, während und nach einer Krise im Vordergrund?

- Info: Was kann ich vor der Krise tun?
- Methode: Stakeholder-Map
- Info: Wie komme ich während einer akuten Krise vor die Lage?
- Info: Abschluss der Kommunikation, Lessons Learned

Etappenabschnitt

Übung Krisenkommunikation

Übung zur Erstellung einer Stakeholder-Map und Ableitung einer Strategie

- Übung: Anpassungsfähige Kommunikationsstrategie

Zur Roadmap

Info: Einführung Krisenkommunikation

Ein Cybervorfall im Unternehmen kann maximal disruptiv sein: Übliche Kommunikationswege funktionieren nicht mehr, Kunden, Zulieferer und Regulierer stellen unangenehme Fragen und die eigene Belegschaft ist verunsichert. Gut, wenn Sie in dieser Situation einen Plan haben, wie die Kommunikation nach innen und außen aufrechterhalten werden kann.

Nicht immer hat ein Vorfall so dramatische Auswirkungen, aber schon Schwachstellen in der eigenen Software können besonderen Kommunikationsbedarf auslösen.

Die gute Nachricht: Auf solche Fälle können Sie sich vorbereiten, damit Sie im Ernstfall nicht im „Headless-Chicken-Modus“ durch die Gegend rennen, sondern strategisch und geplant kommunizieren können.

Zur Etappe

Zur Roadmap

Warum beschäftigt sich diese Roadmap im Kontext von NIS2 mit der Krisenkommunikation, auch wenn das Wort nicht explizit in der Regulierung auftaucht?

Die NIS2 legt großen Wert auf eine sichere Lieferkette und eine durchgängige Handlungsfähigkeit regulierter Unternehmen. Dafür ist es enorm wichtig, dass Unternehmen klare, definierte Prozesse haben, wie sie mit herausfordernden Sondersituationen wie einem Sicherheitsvorfall oder einer Schwachstelle im Produkt umgehen. Hier leistet die Krisenkommunikation einen wichtigen Beitrag zur Handlungsfähigkeit und Verhaltenserwartbarkeit.

Tipp

Einen Krisenstab zu konzipieren und einzurichten, lohnt sich für fast jedes Unternehmen – unabhängig von der Größe. Er hilft, im Notfall Handlungsfähigkeit herzustellen.

Info: Relevante Standards

Die Notfall- und Krisenkommunikation (NuK) ist fester Bestandteil von Standards und Handreichungen. Die wichtigsten stellen wir hier vor.

Leitfaden Krisenkommunikation

Der Leitfaden Krisenkommunikation des Bundesministeriums des Innern bietet zahlreiche Anleitungen und Taktiken für die erfolgreiche Durchführung von Krisenkommunikationsmaßnahmen.

Es gibt Tools und Übungen zur Vorbereitung von Kommunikationsmaßnahmen und Planungshilfen, etwa auch für die Social-Media-Arbeit im Krisenfall.

BSI-Standard 200-4 – Business Continuity Management
Der BSI-Standard 200-4 stellt eine umfangreiche Methodik zur Einrichtung eines Business Continuity Management System (BCMS) zur Verfügung. Dabei zielt das Dokument nicht auf eine Zertifizierung ab, sondern bietet verschiedene niedrigschwellige Möglichkeiten an, die Betriebskontinuität im Krisenfall zu stärken.

Die Notfall- und Krisenkommunikation ist ein zentraler Baustein des BCM und wird detailliert beschrieben.

Der Standard ist gut verständlich formuliert und somit auch für Laien zugänglich.

Zur Etappe

Zur Roadmap

Info: Was kann ich vor der Krise tun?

Wenn Sie vorbereitet sind, kommen Sie besser durch eine Krise. Klingt wie eine Binsenweisheit, ist aber trotzdem richtig. Denn auch wenn Sie nicht alle Eventualitäten vorhersehen können, so können Sie doch Szenarien für verschiedene Situationen entwerfen, Strukturen schaffen und Fähigkeiten aufbauen.

Auf welche Szenarien können Sie sich vorbereiten?

Bereiten Sie abgestimmte Statements für Presse und andere Stakeholder vor, die Sie bei Bedarf sofort abrufen können. Dazu gehören:

- Ausfall Ihrer SaaS-Anwendung: schnelle Information zur Ursache, zur betroffenen Nutzerzahl und zu den nächsten Schritten
- Vorwürfe gegen die Geschäftsführung: Faktencheck, veranlasste Untersuchungen und Ihr offizieller Standpunkt
- Reputationsrisiken durch Kundenbeziehungen: Erläuterung von Zusammenarbeit, Compliance-Maßnahmen und Ihrer Haltung

Erarbeiten Sie im Vorfeld eine klare, abgestimmte Haltung, benennen Sie eine Sprecherin oder einen Sprecher und legen Sie Freigabeprozesse fest, damit Sie im Ernstfall schnell, einheitlich und professionell kommunizieren.

Was können Sie für den Notfall regeln?

Ein Notfallplan für die Kommunikation definiert Entscheidungs- und Eskalationswege sowie Vertretungsregelungen im Krisenfall. Zudem verankert er die zentralen Unternehmenswerte, die Sie gegenüber der Öffentlichkeit, Kunden, Partnern und Beschäftigten jederzeit verteidigen, zum Beispiel Transparenz. Das bedeutet die zeitnahe und nachvollziehbare Offenlegung relevanter Informationen, um Vertrauen zu stärken.

Wer sitzt in meinem Krisenstab – und was darf er entscheiden?

Ein Krisenstab bündelt alle Aktivitäten in Sondersituationen. Hier sitzen alle wichtigen Funktionen des Unternehmens an einem Tisch und können schnell Entscheidungen treffen. Ein Krisenstab sollte in der Lage sein, schnell und unbürokratisch Ressourcen zu mobilisieren, um „vor die Lage“ zu kommen.
Übliche Beteiligte eines Krisenstabs sind die Geschäftsführung, die Kommunikationsabteilung, die technische Entwicklung (so vorhanden) und die Vertriebsleitung. Funktionen wie ein Rechtsbeistand, die HR-Abteilung und andere können bei Bedarf hinzugezogen werden.

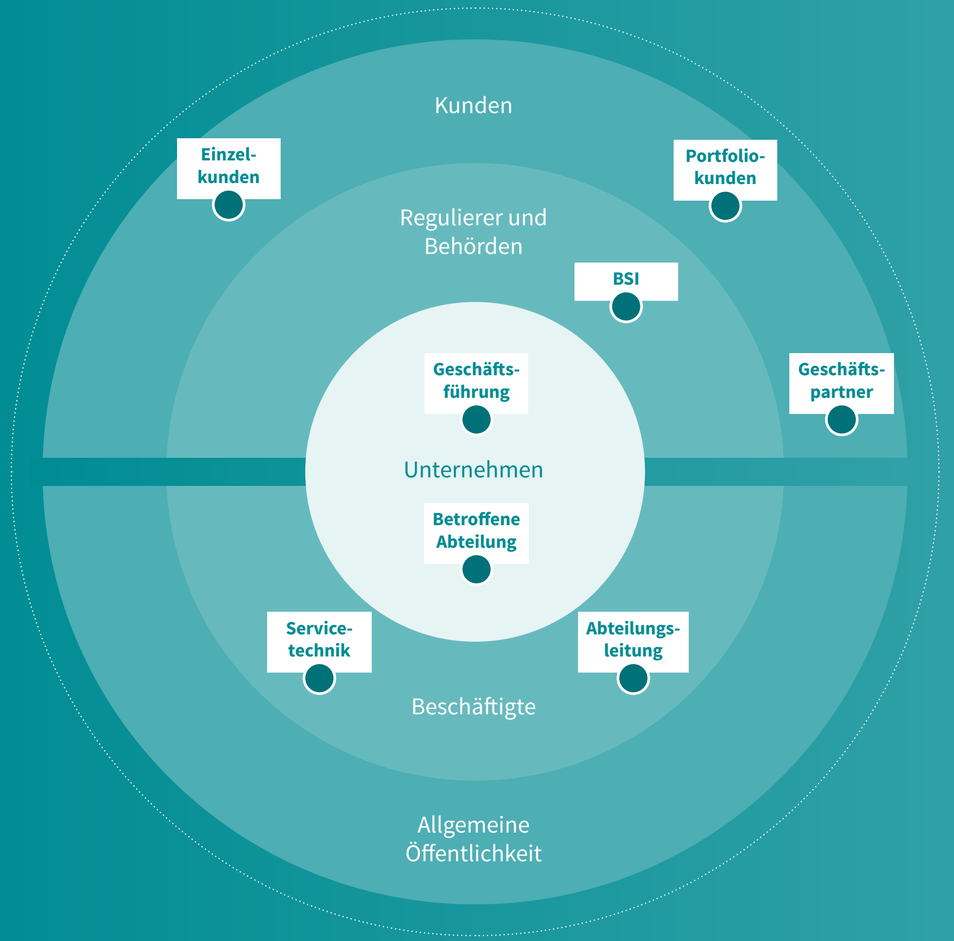
Zur Etappe

Zur Roadmap

Methode: Stakeholder-Map

Eine Stakeholder-Map hilft Ihnen, alle relevanten Akteure im NIS2-Kontext auf einen Blick zu erfassen: Anpassungsfähige Kunden und Dienstleistern über Regulierungs- und Aufsichtsbehörden bis hin zu Banken und Investor:innen. Durch die Visualisierung Ihrer Erwartungen, Rollen und Einflussmöglichkeiten können Sie Kommunikationsstrategien gezielt abstimmen, Risiken minimieren und Compliance-Anforderungen effizient erfüllen.

Zielgruppen definieren mit einer Stakeholder-Map



Zielgruppen definieren

Nutzen Sie Ihre Stakeholder-Map, um die wichtigsten Adressaten zu identifizieren.

Diese Adressaten können Sie in der Übung „Anpassungsfähige Kommunikationsstrategie“ als Grundlage für die Frage „Bei welcher Krise müssen Sie wen wie informieren?“ nutzen.

Zur Etappe

Zur Roadmap

Info: Wie komme ich während einer akuten Krise vor die Lage?

Es ist eingetreten: ein Cyberangriff, eine Sicherheitslücke im Produkt oder ein Ausfall Ihrer Infrastruktur. Nun zählt jeder Schritt, um den drohenden Reputationsschaden einzudämmen und das Vertrauen wiederherzustellen. In diesem Abschnitt zeigen wir Ihnen, wie Sie durch sorgfältige Vorbereitung im akuten Notfall schnell handeln, klare Kommunikationswege nutzen und mit abgestimmten Entscheidungen eine Krise beherrschen können, bevor sie zur Katastrophe wird.

Wer darf kommunizieren?

In der Krise gilt: Kommunikation strikt zentralisieren. Nur klar benannte Ansprechpersonen – etwa Vorstand, Pressesprecher oder Vertriebsleitung gegenüber Kunden – geben offizielle Statements ab. Unabgestimmte Statusberichte, persönliche Einschätzungen oder Spekulationen zum Wiederanlauf der Produktion sind tabu.

Welche Message möchten Sie senden?

Definieren Sie frühzeitig Ihre Leitbotschaft im Krisenfall, an der sich alle Presse- und Kundenaussagen orientieren. Bei Cybervorfällen geht es meist darum, Ihre Handlungsfähigkeit zu demonstrieren und klar darzulegen, welche Schritte Sie einleiten, um schnellstmöglich den Normalbetrieb wiederherzustellen.

Wann sollten Sie die Kommunikation starten?

Im Krisenfall gilt: schnell informieren, aber erst wenn die Fakten stimmen. Vermeiden Sie voreilige Meldungen, die später revidiet werden müssen – das unterminiert das Vertrauen. Ein kurzes Holding-Statement reicht zunächst aus, zum Beispiel:

„Wir sind uns der Situation bewusst und klären den Vorfall mit Hochdruck. Wir tun alles, um den Normalbetrieb so rasch wie möglich wiederherzustellen, und halten Sie auf dem Laufenden.“

Alle externen Statements sollten auf verifizierten Informationen basieren und vorab von den relevanten Entscheidungsträgerinnen und -trägern freigegeben werden.

Wie sollte die Kommunikation mit Kunden während einer akuten Krise konkret aussehen – tägliche Updates, direkte Ansprechpartner oder dedizierte Informationskanäle?

Die Anforderungen an die Krisenkommunikation mit Kunden hängen stark vom eigenen Produkt und seiner Kritikalität beim Kunden ab. Eine gute Krisenkommunikationsstrategie berücksichtigt diese individuellen Anforderungen. Wichtig ist eine proaktive Kommunikation, die Vertrauen schafft. Zudem sollte wenn möglich der Dialog mit Kunden gesucht werden, um Verständnis für ihr Kommunikationsbedürfnis zu demonstrieren.

Tipp

Krisenmanager sprechen bei Notfällen oft von der „Lage“, die sich entwickelt. Ziel der Maßnahmen des Krisenstabs und somit auch der Krisenkommunikation ist es, „vor die Lage“ zu kommen, also Handlungsfähigkeit und Souveränität zurückzugewinnen.

Zur Etappe

Zur Roadmap

Info: Abschluss der Kommunikation, Lessons Learned

Auch nach der Akutphase ist der Einsatz noch nicht vorbei: Jede Krise benötigt ein formelles Schluss-Statement und gezielte Maßnahmen, um verlorenes Vertrauen wieder aufzubauen. Nehmen Sie sich außerdem Zeit, den Vorfall und Ihren Umgang damit kritisch zu analysieren, um aus den Erfahrungen zu lernen und künftige Reaktionen zu optimieren.

Never waste a good crisis.

Wie geht es nach der akuten Phase weiter?

Sobald die Krisen-Hotphase beendet ist, informieren Sie alle Stakeholder sichtbar über diesen Meilenstein. Beenden Sie beispielsweise einen Liveblog auf der Website mit einem kurzen Abschluss-Posting. Schicken Sie außerdem eine knappe Nachricht an die Presse, Investoren, Behörden und weitere Beteiligte, um zu signalisieren, dass die intensive Kommunikationsphase nun abgeschlossen ist.

Welche Schwachstellen wurden ausgenutzt und welche Fehler wurden begangen?

Im Cybersicherheitsbereich hat sich das Format „post mortem“ bewährt. Nach einem Sicherheitsvorfall wird in einem solchen Blogpost beschrieben, was falsch gelaufen ist und welche Gegenmaßnahmen das Unternehmen ergriffen hat, um künftige Vorfälle zu verhindern.
So kann Vertrauen wieder aufgebaut werden.

Wie groß ist der Reputationsschaden?

Nach großen Krisen kann es sinnvoll sein, den Status quo des Vertrauens in die Marke zu erheben. Das kann durch strukturierte Stakeholder-Befragungen oder Marktforschung geschehen. Ein Abgleich der Ergebnisse mit Vor-Krisen-Benchmarks zeigt Ihnen, wie stark das Vertrauen tatsächlich gelitten hat.

Tipp

Nach der Krise versammelt sich der Krisenstab zur Analyse:

- Wie haben wir als Team zusammengearbeitet?
- Waren die Notfallpläne adäquat?
- Hat das Messaging funktioniert?
- Welche neuen Szenarien müssen wir für unsere Notfallplanung berücksichtigen?

So verbessern Sie Ihre Reaktionsfähigkeit kontinuierlich.

Zur Etappe

Zur Roadmap

Übung: Anpassungsfähige Kommunikationsstrategie

In einer Krise ändert sich die Lage oft im Minutentakt. Ihre Kommunikationsstrategie muss daher flexibel angepasst werden können – ohne dabei wichtige Konstanten wie klar benannte Sprecherinnen und Sprecher, eine zentrale Leitbotschaft und verbindliche Freigabeprozesse aus den Augen zu verlieren.

1. Unternehmenskrise

„Ransomware-Befall“
Die Produktion und Logistik des Unternehmens stehen still

2. Kommunikationsstrategie

Akteure

Wer muss informiert werden?
(z. B. Geschäftsführung, Beschäftigte, Kunden, Medien, Behörden)

- Geschäftsführung
- Kommunikationsabteilung

Adressaten

- Kunden
- Beschäftigte
- Investoren

Inhaltsarten

Welche Botschaften benötigen Sie?
(z. B. Holding-Statement, Status-Update, FAQ, Abschlusskommunikation)

- Welche Unternehmensbereiche sind betroffen?
- Wie lange wird der Ausfall etwa dauern?

Kanäle

Über welche Medien kommunizieren Sie?
(z. B. Pressemitteilung, E-Mail, Intranet, Social Media)

- Wiki
- Erklärvideo

Übungsablauf

1. Szenario entwerfen

Suchen Sie nach einer fiktiven, aber realistischen Unternehmenskrise (z. B. Datenleck, Produktionsausfall) und notieren Sie Auslöser und Auswirkungen.

2. Kommunikationsstrategie vorbereiten

Erarbeiten Sie einen kompakten Plan und halten Sie fest:

- Akteure
- Adressaten
- Inhaltsarten
- Kanäle

3. Abschluss

Präsentieren Sie Ihre Strategie im Team. Diskutieren Sie, welche Elemente Sie je nach Krise anpassen würden und welche stets unverändert bleiben sollten.

Zur Etappe

Zur Roadmap

Etappe

Asset Management

Zur Roadmap

Etappe

Asset Management

Relevanz: Ein aktuelles Asset-Inventar ist Grundlage jeder Sicherheitsmaßnahme und schafft Vertrauen bei Partnern und Prüfern.

Asset Management schafft Transparenz hinsichtlich der IT- und Informationswerte eines Unternehmens und bildet die Grundlage für wirkungsvolle Schutzmaßnahmen.

Ein strukturiertes Asset Management erleichtert nicht nur interne Sicherheitsentscheidungen, sondern zeigt auch gegenüber Kunden und Prüfern, dass Ihre Organisation die eigene Systemlandschaft kennt und kontrolliert steuert – eine zentrale Anforderung der NIS2-Richtlinie.

Etappen FAQ >

Zur Roadmap

Etappenabschnitt

Vorbereitung

Was Sie vor dem Start wissen müssen

- Info: Relevante Dokumente und Standards >
- Info: NIS2-Anforderungen >

Etappenabschnitt

Inventar

Erfassung und Dokumentation aller Assets als Basis für Risikoanalysen

- Methode: Geschäftsprozesse, Orte und Personen erfassen >
- Methode: Anwendungen und Systeme erfassen >
- Methode: Organisatorische Aspekte >
- Übung: Assets strukturiert selbst erfassen >

Etappenabschnitt

Asset-Beziehungen

Beziehungen zwischen Assets modellieren, um bei Zwischenfällen Auswirkungen schnell abzuleiten

- Info: Herausforderungen und Ablauf von Asset-Modellierung >
- Übung: Beziehungen zwischen den Assets durchdenken >
- Methode: Asset-Modellierung >

Info: Relevante Dokumente und Standards

In diesem Abschnitt finden Sie eine Übersicht über relevante Dokumente und Standards zum Asset Management. Die meisten Informationssicherheits-Rahmenwerke verlangen zwar ein Inventar, liefern aber kaum Hinweise zur praktischen Umsetzung. Der IT-Grundschutz des BSI bildet hier eine Ausnahme und bietet eine konkrete Anleitung. Ergänzend stellen wir weitere Richtlinien und Normen vor, die Ihnen helfen, Ihr Asset Management systematisch aufzubauen.

DIN SPEC 27076

Das BSI empfiehlt in diesem CyberRisiko-Check für kleine und Kleinstunternehmen, eine Übersicht über alle werthaltigen Ressourcen anzulegen – etwa unter Kategorien wie „IT-Geräte“ (z. B. Smartphones) –, auch wenn keine konkreten Vorgaben zur Modellierung von Asset-Beziehungen bestehen. Eine vollständige Bestandsaufnahme ist jedoch Voraussetzung, um Maßnahmen wie zum Beispiel durchgängigen Passwortschutz umzusetzen. Ebenso müssen Backups so gestaltet sein, dass der Fortbestand des Betriebs gesichert bleibt. Um dafür zu planen, welche Assets in welchen Geschäftsprozessen benötigt werden, ist es notwendig, zu verstehen, welche Prozesse auf welche Ressourcen zugreifen.

IT-Grundschutz (200-2 Kapitel 8.1)

Die detaillierte Vorgehensweise zur Inventarisierung und Modellierung der Abhängigkeiten ist im Kapitel zur „Strukturanalyse“ beschrieben. Grob gliedert sie sich in folgende Schritte:

1. Geschäftsprozesse erheben
2. Pro Geschäftsprozess die Anwendungen erheben
3. Netzplan erheben
4. IT-Systeme (IT-, IoT- und OT-Geräte, aktive Netzkomponenten, Netzdrucker, TK-Anlagen, Smartphones, virtuelle IT-Systeme) erheben
5. Beziehungen von Anwendungen zu IT-Systemen modellieren
6. Räume erheben
7. Beziehungen von IT-Systemen zu Räumen modellieren

ISO 27002 (Kapitel 5.9)

Nach ISO 27001/27002 die Organisation identifiziert alle Informationen und zugehörigen Vermögenswerte und bewertet ihre Bedeutung für die Informationssicherheit. Sie führt eine dynamische Inventarliste, die Hardware, Software, virtuelle Maschinen, Einrichtungen, Personal, Kompetenzen und Aufzeichnungen umfasst. Für jeden Eintrag bestimmt sie einen Asset Owner, der den Vermögenswert über den gesamten Lebenszyklus verwaltet und sicherstellt, dass unterstützende Technologiekomponenten (Datenbanken, Speicher, Software) im Inventar verknüpft sind.

Zur Etappe

Zur Roadmap

Info: NIS2-Anforderungen

Der Ausdruck „Network and Information Security“ (NIS) bezieht sich auf die Sicherheit von Netz- und Informationssystemen. In der zweiten Ausführung der EU-Richtlinie (NIS2) erweitern sich die Anforderungen auf alle informationsrelevanten Unternehmensressourcen. Voraussetzung für die Umsetzung ist eine vollständige Inventur aller vorhandenen Werte mit Informations- und IT-Bezug (Assets).

Was sind Netz- und Informationssysteme?

Laut NIS2 (§ 6 Nr. 1 Richtlinie (EU) 2022/2555) gehören dazu:

- Systeme zum Aufbau von Netzwerken (z. B. Switches oder Satelliten)
- Systeme zum Ausführen von Programmen, allein oder in Kombination (klassische Computer), die von diesen Systemen verarbeiteten Daten

Eine vollständige Inventur dieser Komponenten bildet die Grundlage für alle weiteren Maßnahmen.

Welche Vorgaben gibt es in NIS2 zum Thema Asset Management?

Gefahrenübergreifender Ansatz

„…die [...] genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen […]“ (§ 21 Abs. 2 S. 1 Richtlinie (EU) 2022/2555).

Inventarpflicht

Um die genannten Systeme zielführend zu schützen, muss man zunächst wissen, welche es gibt. Die Richtlinie schreibt deshalb vor:
„[…] Konzepte für die Zugriffskontrolle und Management von Anlagen […]“
(§ 21 Abs. 2 i Richtlinie (EU) 2022/2555).

Detailvorgaben im Implementing Act und Best-Practice-Standards

NIS2 Implementing Act: Enthält konkrete Vorgaben, wie ein Sicherheitsinventar aufgebaut und dokumentiert werden sollte.
ISO 27001, IT-Grundschutz, CIS Controls: Beschreiben Mindestanforderungen für Inhalt, Struktur und Pflege eines Inventars aus Sicht der Informationssicherheit.

Diese Regelungen stellen sicher, dass Organisationen
a) ihre Assets systematisch identifizieren,
b) Zugriffsmodelle und Verantwortlichkeiten festlegen und
c) das Inventar laufend aktuell halten, um Netz- und Informationssysteme wirksam gegen Risiken abzusichern.

Zur Etappe

Zur Roadmap

Methode: Geschäftsprozesse, Orte und Personen erfassen

Der NIS2 Implementing Act (EU 2024/2690) fordert ein „kohärentes Vorgehen“ für das Asset Management, das nur durch eine nachvollziehbare Dokumentation der Methodik sichergestellt werden kann. Er spezifiziert außerdem:

„Ein umfassendes Anlagen- und Werteinventar könnte für jede Anlage bzw. jeden Wert mindestens eine eindeutige Kennung, den jeweiligen Eigentümer, eine Beschreibung, den Standort, die Art der Anlage bzw. des Wertes, die Art und Klassifizierung der damit verarbeiteten Informationen, das Datum der letzten Aktualisierung oder des letzten Patches, die bei der Risikobewertung vergebene Klassifizierung und das Ende der Lebensdauer enthalten“ (Anm. 26 (EU) 2024/2690).

Zur Etappe

Zur Roadmap

Diese Anleitung beschreibt die erforderliche Methodik zur Inventarerstellung, dient als anpassbare Vorlage für Ihr Unternehmen und präsentiert Kategorien und Attribute als Vorschlag zur Erfassung nach diesem Mindeststandard.

Geschäftsprozesse erfassen

1. Bestimmen Sie Ihre geschäftsrelevanten Kernprozesse.
2. Erfassen Sie anschließend die wichtigen Unterstützungsprozesse.
3. Achten Sie dabei auf den Kontext Ihres Unternehmens: In einem Softwareentwicklungs-Unternehmen gilt Softwareentwicklung als Kernprozess, Personalverwaltung als Unterstützungsprozess. In anderen Unternehmen kann Softwareentwicklung hingegen ein Unterstützungsprozess sein.

Orte erfassen

1. Listen Sie alle physischen Räume und Orte auf.
2. Jeder Büroraum oder Serverschrank erhält einen Eintrag.
3. Erfassen Sie auch Remote-Arbeitsplätze, um Verknüpfungen zu Hardware-Assets später zu erleichtern.
4. Ähnliche Einträge können hier wie in den anderen Kategorien gruppiert zusammengefasst werden.

Personen und Accounts erfassen

1. Führen Sie eine Liste aller Personen mit regelmäßigem Zugriff auf Informationssysteme.
2. Ergänzen Sie vorhandene Mitarbeiter-Listen um Dienstleister- und Freelancer-Daten.
3. Vermerken Sie zu jeder Person die zugewiesenen Rechte und Freigaben.

Tipp

Im NIS2 IA wird spezifiziert: „Ein umfassendes Anlagen- und Werteinventar könnte für jede Anlage bzw. jeden Wert mindestens eine eindeutige Kennung, den jeweiligen Eigentümer, eine Beschreibung, den Standort, die Art der Anlage bzw. des Wertes, die Art und Klassifizierung der damit verarbeiteten Informationen, das Datum der letzten Aktualisierung oder des letzten Patches, die bei der Risikobewertung vergebene Klassifizierung und das Ende der Lebensdauer enthalten.“

Die hier vorgeschlagenen Kategorien und Attribute sind ein Vorschlag zur Erfassung nach diesem Mindeststandard.

Methode: Anwendungen und Systeme erfassen

Ziel ist die aktive Verwaltung (Inventarisierung, Verfolgung und Korrektur) aller genutzten IT-Assets – von Infrastruktur (IaaS) über Plattform-as-a-Service bis zu Anwendungen. Dabei steht ein übersichtlicher Bestand im Vordergrund, nicht maximale Detailtiefe.

Passen Sie die vorgeschlagenen Kategorien an Ihren Tech-Stack an.

Der Automatisierungsgrad Ihres Asset-Inventars sollte dem Ihrer IT-Infrastruktur entsprechen:
- Traditionelle Umgebungen (z. B. „Turnschuh-Admin“): manuelle Pflege aufwendig, aber möglich
- Cloud-native Umgebungen: umfassende Automatisierung möglich und erforderlich, um Inventar effizient und aktuell zu halten

Zur Etappe

Zur Roadmap

SaaS erfassen

1. Führen Sie alle eingesetzten Software-as-a-Service-Anwendungen auf.
2. Dokumentieren Sie die Lizenztypen und -umfänge.
3. Verwalten Sie die zugehörigen Zugangsdaten und Berechtigungen.

Hardware erfassen

Listen Sie alle physischen Assets auf, die sich regelmäßig mit dem Firmennetz verbinden.

Beziehen Sie ein:
1. (Mobile) Endnutzergeräte
2. Netzwerkkomponenten (Switches, Router)
3. IoT-Geräte (z. B. Kaffeemaschine, Drucker)
4. Server (physisch und virtuell)
5. Nehmen Sie auch Geräte auf, die extern oder außerhalb der direkten Kontrolle betrieben werden, aber eine Verbindung herstellen.
6. Verwenden Sie diese Liste als Basis, um unbekannte oder nicht autorisierte Geräte im Netzwerk zu identifizieren.

Administrierte Software erfassen

Erfassen Sie alle Assets mit Administrationsaufwand.

Unterscheiden Sie nach „Software-Art“:
1. PaaS/FaaS/Serverless: Verwaltung der Anwendung, nicht des OS
2. IaaS/VPS/Root-Server: zusätzliches Tracking der Betriebssystem-Verwaltung
3. On-Premise/Rack-Space: inklusive Hardwareverwaltung
4. Dokumentieren Sie zu jedem Eintrag die jeweilige Software-Art als Attribut.

Tipp

Der Automatisierungsgrad der IT sollte zum Automatisierungsgrad des Unternehmens passen. Veränderungen, die durch verstärkte Nutzung der Cloud entstehen, sind manuell kaum zu erfassen. Es ist wichtig, dass der Automatisierungsgrad der IT-Infrastruktur dem des Inventars entspricht. In traditionellen Umgebungen, die von einem „Turnschuh-Admin“ betreut werden, ist eine manuelle Pflege des Inventars möglich. Im Gegensatz dazu erfordert (und ermöglicht) eine Cloud-native Umgebung eine umfassende Automatisierung, um effizient und aktuell zu bleiben.

Methode: Organisatorische Aspekte

Asset Management umfasst nicht nur das Sammeln technischer Daten, sondern auch klare organisatorische Strukturen. Nur wenn Verantwortlichkeiten, Ablagestrukturen und Versionskontrolle der Inventarlisten intern abgestimmt und zentral dokumentiert sind, entsteht eine belastbare Grundlage für Risikoanalyse, Compliance und effektive Incident Response.

Automatisierung und Speicherort festlegen

1. Automatisieren, wo möglich: Starten Sie mit manuellen Tabellen, aber streben Sie an, Assets automatisiert zu erfassen.
2. Speicherorte dokumentieren: Legen Sie fest, wo jede Asset-Kategorie abgelegt wird (z. B. Tool A, Tabellenblatt B).
3. Zentralen Referenzpunkt einrichten
4. Erstellen Sie eine zentrale Übersicht (z. B. Intranet-Seite), die zu jedem Asset-Typ den aktuellen Speicherort angibt.

Asset Owner und technische Verwaltung festlegen

1. Asset Owner zuweisen: Bestimmen Sie für jedes Asset eine verantwortliche Person (Asset Owner).
2. Rollen definieren: Asset Owner legen Klassifizierung und Nutzungsregeln fest und tragen aus Business-Sicht die Gesamtverantwortung.
3. Technische Verwalter betreuen Systeme (z. B. Computer, Datenbanken) und setzen die Nutzungsregeln um.
4. Dokumentation: Erfassen Sie für jedes Asset den Asset Owner und den technischen Verwalter.
5. Verantwortung auf Management-Ebene: Ordnen Sie bei prozesskritischen Assets die Ownership idealerweise einer Management-Position zu.

Inventar aktualisieren und Änderungen managen

1. Regelmäßige Reviews einplanen: Legen Sie feste Intervalle (z. B. monatlich, quartalsweise) fest, um das Inventar systematisch zu prüfen.
2. Änderungen erfassen: Dokumentieren Sie jeden Patch-Stand und End-of-Life-Termin sowie sonstige Lifecycle-Informationen direkt im Inventar.
3. Aktualisierungsmechanismus festlegen: Beschreiben Sie das Verfahren und die zuständigen Rollen oder Tools, die im Unternehmen für die Pflege und Freigabe von Inventaränderungen verantwortlich sind.

Assets nach Schutzbedarf klassifizieren

1. Schutzbedarfskategorien festlegen: Vertraulichkeit, Integrität und Verfügbarkeit
2. Schutzbedarf einstufen: Für jede Kategorie vergeben Sie eine Stufe: normal, hoch, sehr hoch
3. Dokumentation: Tragen Sie die Einstufungen direkt im Inventar ein, idealerweise als eigene Spalten.
4. Verweis auf Risikomanagement: Detaillierte Kriterien und Bewertungsmethoden finden Sie in der Etappe Risikomanagement.

Assets gruppieren

1. Definieren Sie sinnvolle Gruppen, zum Beispiel alle Büroräume eines Standorts, als ein Asset.
2. Wählen Sie eine Granularität, die den Anforderungen Ihrer Einrichtung entspricht.
3. Dokumentieren Sie zentral Ihre Kriterien für Gruppen und Granularität.

Zur Etappe

Zur Roadmap

Übung: Assets strukturiert selbst erfassen

Diese Übung dient als Orientierung, wie ein ausgereiftes Inventar aufgebaut sein könnte. Es muss im ersten Schritt nicht vollständig und extrem detailliert gefüllt werden – der Fokus liegt auf Übersicht und Struktur.

Asset-Tabellen

Tabellenspalten für Geschäftsprozesse

ID | Name | Beschreibung | Prozessart (Kern/Unterstützung) | Asset Owner | Klassifizierung | Risikobewertung

Tabellenspalten für Orte

ID | Name | Beschreibung | Typ (Raum/Gebäude) | Anzahl | Asset Owner | Risikobewertung

Tabellenspalten für Personen und Accounts

Vor- und Nachname | Rolle | Admin (ja + wo/nein) | Haben die Personen die Rolle Asset Owner?(ja + wo/ nein) | Status (aktiv/ langfristige Abwesenheit/inaktiv)

Tabellenspalten für Administrierte Software

ID | Name | Beschreibung | Asset Owner | Anzahl der Lizenzen Software-Art | Herausgeber | Erstnutzung Datum | URL | App Store | Version | Letzter Patch Datum | Deployment-Mechanismus Status (aktiv/ungepatcht + aktiv / dekommissioniert) | Außerbetriebnahme Datum | Risikobewertung

Tabellenspalten für SaaS

ID | Name | Beschreibung | Asset Owner | Anzahl der Lizenzen | Software-Art | Herausgeber URL | Erstnutzung | Datum | Außerbetriebnahme Datum | Status | Risikobewertung

Tabellenspalten für Hardware

ID | Name | Beschreibung | Asset Owner | Art (Endnutzer Geräte/ Netzwerkgeräte | IoT (Kaffeemaschine/Drucker/Server) | Standort | Risikobewertung | Status (aktiv/dekommissioniert) | Außerbetriebnahme Datum | Risikobewertung | Kontrolliert von der Firma (ja/nein) | Netzwerk-Adresse (statisch) | Hardware-Adresse

Übungsablauf

Listen Sie Ihre Asset-Kategorien auf:

- Geschäftsprozesse
- Orte
- Personen und Accounts
- Administrierte Software
- SaaS
- Hardware

Für jede Kategorie stellen Sie einen Timer auf 5 Minuten. Während dieser 5 Minuten notieren Sie im Brain-Dump so viele Assets wie möglich in der aktuellen Kategorie – ganz ohne Details oder Klassifizierungen.

Wenn der Timer abläuft, wechseln Sie zur nächsten Kategorie, bis alle Kategorien durchlaufen sind.

Im Anschluss wählen Sie einzelne Assets aus und ergänzen erste Details (z. B. Eigentümer, Standort, Klassifizierung).

Hinweis:
Dieses Vorgehen liefert Ihnen schnell eine strukturierte Übersicht. Tiefergehende Details können Sie in einem zweiten Durchgang ergänzen.

Zur Etappe

Zur Roadmap

Info: Herausforderungen und Ablauf von Asset-Modellierung

Assets stehen nie isoliert, sondern immer in Abhängigkeit zu anderen Assets und Geschäftsprozessen. Ein Ausfall oder eine Beeinträchtigung kann Kaskadeneffekte auslösen und so weitreichende Folgen haben. Die zentrale Herausforderung besteht darin, diese Beziehungen vollständig zu erfassen und transparent darzustellen, um fundierte strategische Entscheidungen treffen zu können (z. B. gezielte Investitionen in den Schutz der kritischsten Assets).

Was ist die größte Herausforderung bei der Asset-Modellierung?

Die transparente Abbildung der Abhängigkeiten zwischen Assets und Geschäftsprozessen, um Risiken ganzheitlich zu bewerten und Schutzmaßnahmen dort zu priorisieren, wo sie den größten Einfluss haben.

Was ist der Kernpunkt bei der Asset-Modellierung?

Nicht das Inventarisieren selbst, sondern

- die Beziehungen zwischen Assets transparent zu machen (z. B. Abhängigkeiten, Wirkungsketten).
- diese Beziehungen so zu modellieren, dass sich die Kritikalität ableiten lässt (z. B. Folgen eines Ausfalls von Asset A für Asset B).

Warum empfiehlt sich ein pragmatischer Modellierungsansatz für kleine Firmen, und wie sieht dieser Ablauf aus?

Die Darstellung von Asset-Beziehungen kann schnell unübersichtlich werden. Für kleinere Unternehmen mit überschaubarer Infrastruktur ist deshalb folgender dreistufiger Ansatz sinnvoll:

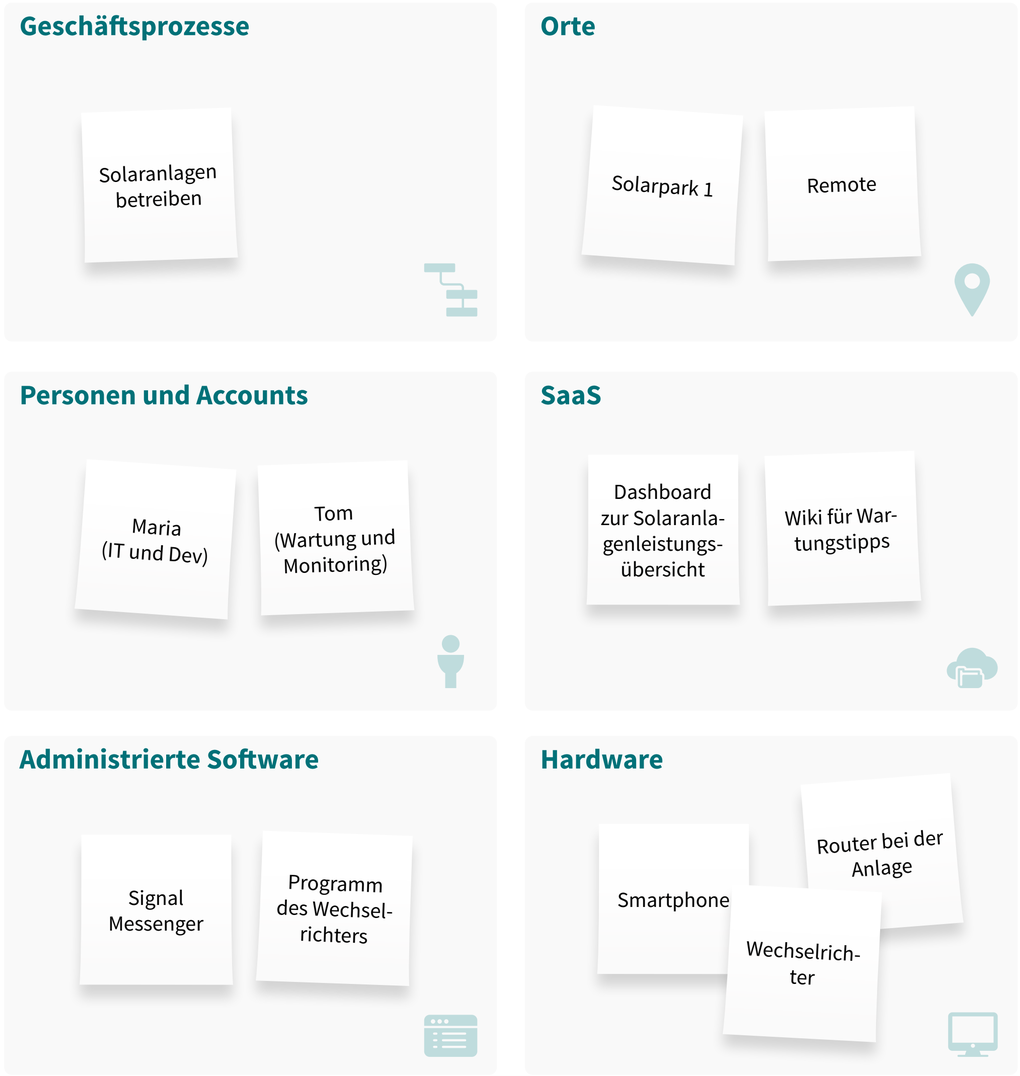
- Reihenfolge der Beziehungsmodellierung kennenlernen
- Eigenen Lösungsvorschlag modellieren
- Modellierungs-Challenge selbst durchdenken

Zur Etappe

Zur Roadmap

Übung: Beziehungen zwischen den Assets durchdenken

In dieser Übung visualisieren Sie die Abhängigkeiten zwischen den Assets eines Geschäftsprozesses. Wählen Sie einen beliebigen Prozess, abstrahieren Sie die zugehörigen Assets als Knoten und zeichnen Sie die Verbindungen (z. B. „Asset A liefert Input für Asset B“). Nutzen Sie dafür ein Whiteboard, Papier oder ein digitales Tool – der Fokus liegt auf den Beziehungen, nicht auf Detaildaten.



Übungsablauf

1. Beziehungen modellieren – 5 Minuten

Wählen Sie einen Geschäftsprozess und seine Assets (z. B. aus vorheriger Inventar-Übung). Zeichnen Sie die Abhängigkeiten zwischen den Assets (z. B. Pfeile von Quelle zu Ziel).

2. Assets ergänzen – 3 Minuten

Brainstormen Sie pro Kategorie weitere Assets, die im Beziehungsdiagramm fehlen.
Notieren Sie diese auf Post-its und fügen Sie sie in Ihre Darstellung ein.

3. Vorgehensweise dokumentieren – 2 Minuten

Halten Sie fest, in welcher Reihenfolge Sie die Beziehungen modelliert haben, z. B.:

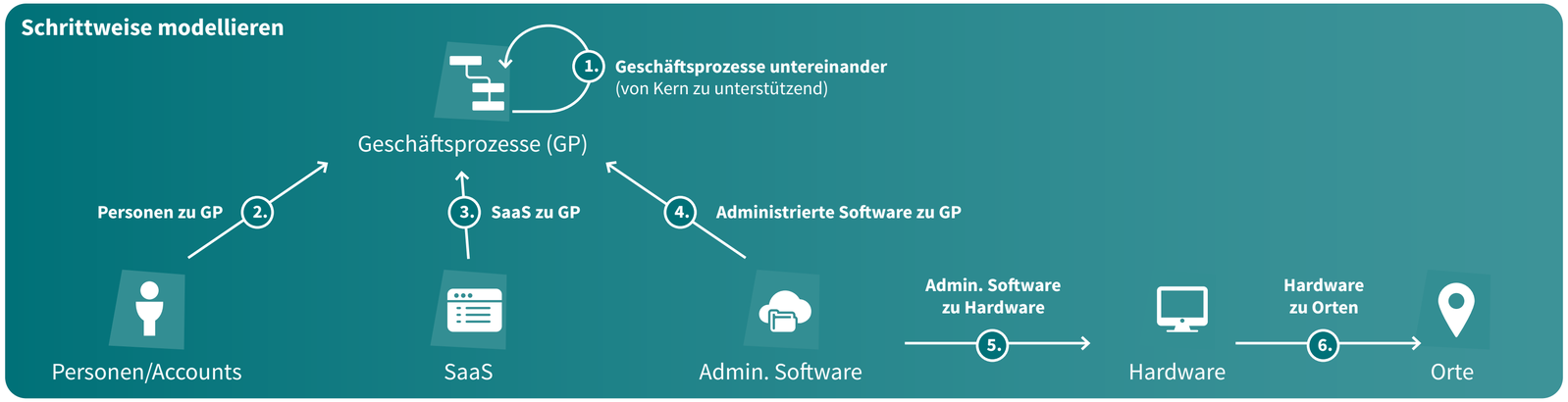
- von Kategorie A zu Kategorie B
- von Asset X zu Asset Y

Zur Etappe

Zur Roadmap

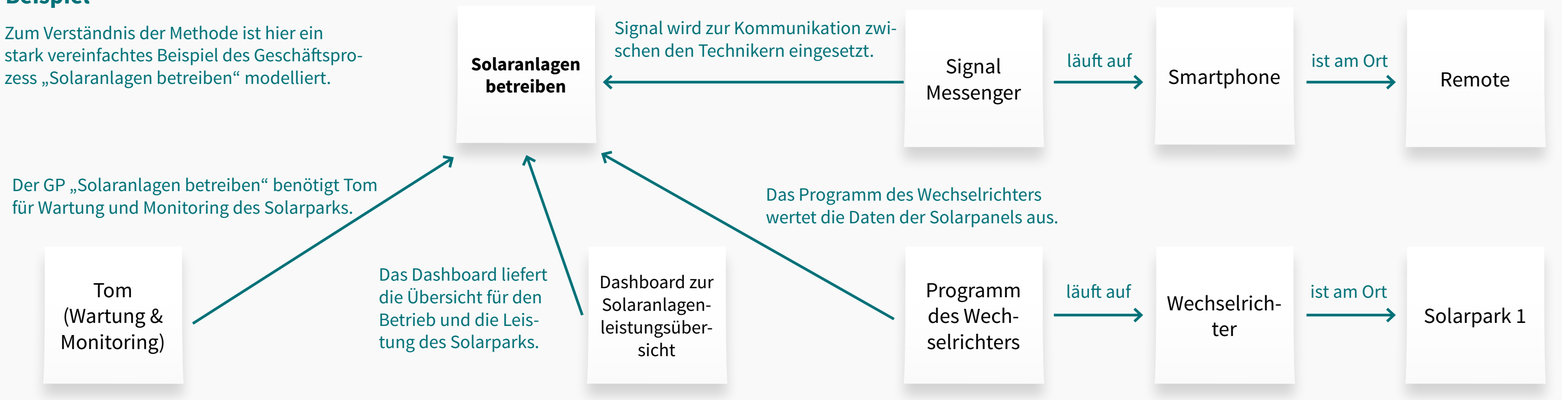
Methode: Asset-Modellierung

Komplexe Abhängigkeiten zu modellieren, ist gerade in der Energiewirtschaft eine wiederkehrende Herausforderung. Selbst mit etablierten Konventionen entstehen schnell unübersichtliche „Wimmelbilder“. Im Assetmanagement liegen Beziehungen zwischen Kategorien oft in zu vielen Konstellationen vor und sind nicht trivial zu erfassen. Rechts finden Sie daher eine methodische Reihenfolge, die Ihnen Schritt für Schritt hilft, diese Abhängigkeiten klar und strukturiert abzubilden.



Beispiel

Zum Verständnis der Methode ist hier ein stark vereinfachtes Beispiel des Geschäftsprozess „Solaranlagen betreiben“ modelliert.



Achtung Abhängigkeit

Ja, es stimmt natürlich, dass das Dashboard nur Daten anzeigen kann, wenn der Wechselrichter Daten liefert. Und diese Daten kommen auch erst im SaaS-Tool an, wenn der Router an der Anlage läuft und die Software darauf funktioniert. Es gibt viele Abhängigkeiten zwischen den technischen Systemen. Je nachdem, wie komplex die Systeme sind, können diese Beziehungen zwischen den technischen Assets modelliert werden. In dieser abstrakten Betrachtung reicht es, wenn die Beziehung zu den Geschäftsprozessen deutlich wird.
Wer an dieser Stelle lieber konkreter werden will, kann die Anleitung zu einer genaueren Modellierung aus dem IT-Grundschutz (Stichwort „Strukturanalyse“) nutzen.

Zur Etappe

Zur Roadmap

Etappen-FAQ

Wie erfolgreich ist heterogenes Asset Management in der Praxis?

Asset Management ist komplex. Ein 100-prozentiges Inventar oder ein völlig wartungsfreier Asset-Management-Prozess werden in der Praxis selten erreicht. Und doch kann nur eine regelmäßig aktualisierte Asset-Datenbank Transparenz hinsichtlich der Informationswerte schaffen und so als Entscheidungs- und Umsetzungsgrundlage der Schutzmaßnahmen dienen.

Welche Geschäftsprozesse sind in Bezug auf Asset Management relevant?

Alle Geschäftsprozesse sind relevant für das Asset Management. Allerdings kann zu Beginn ein verstärktes Augenmerk auf die kritischen Geschäftsprozesse gelegt werden.

Wie sollen nicht technische Assets wie Bankkonto, Handelsregister oder Marktstammdatenregister eingeordnet werden?

Diese Assets werden typischerweise nicht gelistet. Es könnte aber beispielsweise der Zugang zum Online-Banking als SaaS-Tool gelistet werden.

Wie wird selbst entwickelte Software als Asset erfasst?

Selbst entwickelte Software wird typischerweise über den Prozess des Entwickelns erfasst. Ein Stück Software kann aber auch als „selbs administrierte Software“ erfasst werden.

Einige SaaS-Dienste laufen über private statt Firmenaccounts. Sollten diese SaaS-Lösungen auch aufgelistet werden?

Ja, unbedingt! Und im zweiten Schritt sollten diese Accounts von zentral verwalteten Accounts abgelöst werden. Sonst besteht das Risiko, dass diese Accounts auch mit Dritten geteilt werden – abgesehen von lizenzrechtlichen Problemen.

Zur Etappe

Zur Roadmap

Etappe

Sichere Software

Zur Roadmap

Etappe

Sichere Software

Relevanz: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Management von Software schützen vor Angriffen, sichern den Betrieb und erhalten so das Vertrauen in das Produkt.

In dieser Etappe erfahren Sie, welche Anforderungen die NIS2-Richtlinie für sichere Software formuliert und wie sich das für den Softwareeinkauf und die Softwareentwicklung auswirkt.

Außerdem wird das Thema Schwachstellenmanagement aus dem Blick der Softwareentwicklung erklärt und mit Mythen in diesem Bereich aufgeräumt.

Etappenabschnitt

Einkauf und Entwicklung

Erfahren Sie, welche Themen und Schritte relevant sind, um Sicherheit in der Software zu etablieren.

- Info: Anforderungen an Softwareentwicklung und -beschaffung
- Info: Softwareeinkauf
- Methode: Softwareentwicklung

Etappenabschnitt

Schwachstellenmanagement

Lernen Sie, welche Regeln relevant sind, um das Fundament für effektives Schwachstellenmanagement aufzubauen.

- Methode: Schwachstellenmanagement
- Übung: Vorbereitung Schwachstellenmanagement

Etappen FAQ

Zur Roadmap

Info: Anforderungen an Softwareentwicklung und -beschaffung

Ein paar Klicks und in den Warenkorb, noch ein paar Klicks und Daten freigeben – so sorglos geht es im Unternehmenskontext nicht. Risikoorientiert müssen Sie Maßnahmen umsetzen, um die Sicherheit entlang der Softwarelieferkette zu gewährleisten.
Der NIS2 Implementing Act konkretisiert in Abschnitt 6.1 Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten die Anforderungen für den Softwareeinkauf. Auf dieser Grundlage haben wir die wichtigsten Themen und Fragen im Beschaffungsprozess zusammengestellt.
Besprechen Sie diese Punkte vorrangig mit zentralen Dienstleistern und lassen Sie sich die Erfüllung der Anforderungen vertraglich zusichern. Bei weniger kritischen Anbietern genügt meist eine gröbere Absprache entlang der genannten Themen.
Hinweis: Weitere Anforderungen, etwa zur Netzsegmentierung des Dienstleisters, sind nicht spezifisch für Software und daher hier nicht aufgeführt.

Zur Etappe

Zur Roadmap

Wie detailliert muss man sich mit sicherer Software befassen?

Die NIS2-Richtlinie legt fest, dass „Sicherheitsmaßnahmen in Erwerb, Entwicklung und Wartung von [...] Systemen“ (§ 21 (2) c) Richtlinie (EU) 2022/2555) ergriffen werden sollen. In den Anmerkungen wird spezifiziert, dass Unternehmen auf sichere Entwicklungsprozesse (Anm. (85) EU NIS2) bei ihren Dienstleistern achten sollen. Deswegen muss man sich, ob man entwickelt oder nicht, mit den Basissicherheitsmaßnahmen auseinandersetzen oder sie in Verträgen einfordern.

Wo bekommt man konkrete Maßnahmen her?

Wie für die NIS2 üblich, sollen risikoorientiert Sichermaßnahmen gewählt werden. Dafür braucht es etwas Übung und einen Katalog an Maßnahmen (z. B. ISO-27002), an dem man sich orientieren kann. Etwas kompakter sind zum Start die Empfehlungen, die sich aus dem NIS2 Implementing Act (2024/2690) ergeben. Hier sollten insbesondere Abschnitt 6.1 „Sicherheitsmaßnahmen beim Erwerb von IKT-Diensten oder IKT-Produkten“ und 6.2.1 2Sicherer Entwicklungszyklus“ beachtet werden.

ISO-27002

Etabliert als Referenzwerk in der Informationssicherheit, stellt die ISO-27002 sehr umfangreiche Anforderungen auch im Bereich sicherer Softwareentwicklung.
Ein Vorteil ist, dass die meisten anderen Standards und Gesetze ein Mapping zu ihr bieten.

IEC 62443

Diese Standardfamilie adressiert spezifisch Security in industriellen Automatisierungssystemen. Sie definiert technische und prozessuale Sicherheitsanforderungen für die Entwicklung von Komponenten, Maschinen und Anlagen sowie Anforderungen an einen sicheren Entwicklungsprozess.

Info: Softwareeinkauf

Ob Sie Anwendungen einkaufen oder selbst entwickeln – heute kommt kein Unternehmen mehr ohne Software aus. Im Energiebereich ist sichere Software besonders wichtig, da sie direkt oder indirekt in kritische Prozesse wie Stromhandel, Lastmanagement und Anlagenwartung eingreifen kann. Die NIS2-Richtlinie fordert daher, dass Sie Sicherheitsmaßnahmen entlang des gesamten Software-Lebenszyklus umsetzen, um Betriebssicherheit und Compliance zu gewährleisten.

Zur Etappe

Zur Roadmap

Thema: Updates

Fragen bie der Beschaffung:
1. Wie (schnell) werden Patches und Upgrades ausgespielt?
2. Wie lange gibt es Sicherheitsaktualisierungen?
3. Was passiert am EOL (End of Life) der Software?

Hinweise:
Durch den ebenfalls neuen Cyber Resilience Act (CRA) müssen ersteller von Produkten mit digitalen Elementen mindestens 5 Jahre Support garantieren (Ausnahmen möglich). Darunter sollte das Angebot der Dienstleister also nicht liegen.
Gerade bei Bekanntwerden von verbreiteten und kritischen Sicherheitslücken (z. B. Log4j) ist es nützlich, wenn vorab festgelegt wurde, wie schnell Sicherheitsaktualisierungen erfolgen.

Thema: Dokumentation und Konfiguration

Fragen bei der Beschaffung:
1. Wo und wie wird die Dokumentation zur Verfügung gestellt?
2. Gibt es die Möglichkeit, Fragen zu stellen?
3. Wird die Dokumentation aktualisiert?
4. Gibt es Informationen zu den umgesetzten Sicherheitsfunktionen?
5. Welche Default Dettings sollten aus der Sicherheitsperspektive verändert werden?

Hinweise:
Eine moderne Softwaredokumentation enthält meist eine sog. „Software Bill of Materials“ (SBOM), die gerade bei neu gefundenen Schwachstellen den Kunden hilft einzuschätzen, ob sie die Software entspannt weiter nutzen können oder beim Dienstleister Alarm schlagen sollten.
Ein weiterer Startpunkt für diese Anforderung bietet der OWASP ASVS (Application Security Verification Standard) mit einer umfassenden Liste von Sicherheitsanforderungen für die Entwicklung und Prüfung von (Web-)Anwendungen.

Thema: Tests und Audits

Fragen bei der Beschaffung:
1. Wie wurde die Einhaltung der Anforderungen geprüft?
2. Darf die Kundenseite Einsicht in Berichte der Prüfung erhalten?
3. Gibt es ein Recht darauf, die Einhaltung der Sicherheitsmaßnahmen selbst zu prüfen?

Hinweise:
Software und Softwareentwicklung sollten in ihrem Lebenszyklus immer wieder überprüft werden. Üblicherweise unterscheidet man hier zwischen der technischen Prüfung (z. B. einem Penetrationstest) und der Compliance-Prüfung (meist „Audit“).
Gerade für kritische Betreiber ist es üblich, neben der vertraglichen Zusicherung auch Lieferantenaudits durchzuführen, in denen sie die Zusicherung in den Räumlichkeiten der Lieferanten selbst überprüfen.
Solche aufwendigen und schwer zu verhandelnden Maßnahmen sollten jedoch nur nach gewissenhafter Abwägung der Verhältnismäßigkeit gewählt werden.

Thema: Melden und Schwachstellen

Fragen bei der Beschaffung:
1. Wer meldet an wen was?
2. Wie schnell müssen Vorfälle gemeldet werden?
3. Wie werden Schwachstellen kommuniziert?

Hinweise:
Die Meldefristen nach NIS2 (24 Stunden bei „erheblichen Sicherheitsvorfällen“) sollten innerhalb der Lieferkette weitergegeben werden.
Außerdem sollten hier nicht nur Vorfälle, sondern auch Schwachstellen inkludiert werden, die ein Risiko für das Unternehmen darstellen könnten.

Methode: Softwareentwicklung

Das Thema, wie man Software sicher macht, ist ein gewaltiges, über das Bücher und Standards geschrieben werden. NIS2 grenzt hier nicht ein, welche Bereiche der sicheren Softwareentwicklung in den Vordergrund rücken sollen.

Daher finden Sie statt einer Checkliste eine Anleitung, wie Sie von all den Themen rund um sichere Softwareentwicklung nachvollziehbare Eingrenzungen treffen können, um so die vage formulierten Anforderungen mit Leben zu füllen.

Eingrenzende Anleitung für sichere Softwareentwicklung

1. Auswahl des Referenzwerks

Die in der Roadmap viel zitierte Durchführungsverordnung für IKT-Dienste konkretisiert die NIS2-Richtlinie in Anhang 6.2 „Sicherer Entwicklungszyklus“. Da diese Überschrift immer noch sehr vage ist, sollte ein detaillierter Standard zur Orientierung genutzt werden. Konsultieren Sie einen für Ihre Organisation passenden Standard, an dem Sie Ihr Vorgehen und die Struktur der Dokumentation ausrichten.

2. Dokumentation des Ist-Zustandes

Nutzen Sie die Kapitel- und Überschriftenstruktur aus dem gewählten Standard und schreiben Sie pro Thema alle bereits getroffenen Sicherheitsmaßnahmen mit dem Entwicklungsteam auf. Solche Dokumentationen sind gerade in der Kommunikation mit Kunden als Nachweis oder bei neuen Beschäftigten als Onboarding sehr hilfreich.
Jedes Mal, wenn Sie in den Workshops auf Lücken stoßen, notieren Sie sich das separat fürs Risikomanagement.
Das Stichwort in der Informationssicherheit für diese Methodik ist „Gap-Analyse“.

3. Etablierung eines Risikomanagements

Orientieren Sie sich an der Etappe Risikomanagement, um Lücken zwischen Isi-Stand und Referenzwerk zu erfassen und strukturiert zu beheben. Die erfassten Lücken zum Standard können im Risikomanagement als „Gefährdungen“ gelistet, bewertet und behandelt werden. Eine weitere Quelle für Gefährdungen für (Web-) Anwendungen bietet die OWASP TOP 10 mit einer regelmäßig aktualisierten Liste der zehn kritischsten Sicherheitsrisiken.
Falls Ihnen das Vorgehen bisher nicht vertraut ist, können Sie auch mit einer To-do-Liste beginnen und zu einem späteren Zeitpunkt den Entwicklungsprozess über den Risikomanagementprozess erfassen.

4. Schulen und Durchsetzen der Vorgaben

Die dokumentierten Vorgaben müssen allen betroffenen Personen kommuniziert werden. Sie sind in ihrer Einhaltung verpflichtend und sollten, wo möglich, technisch forciert werden. Ein Beispiel: Zugriff auf das Code Repository dürfen nur Personen mit aktivierter MFA haben.

Zur Etappe

Zur Roadmap

Methode: Schwachstellenmanagement

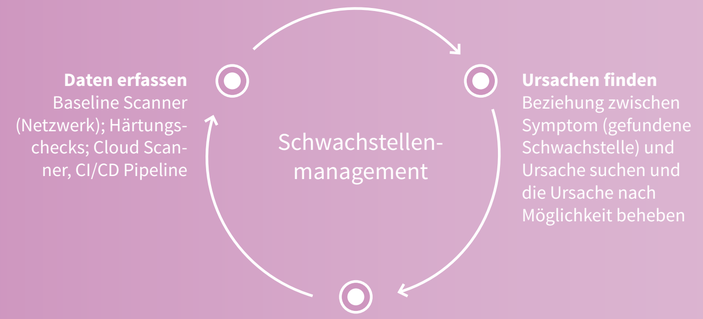
Schwachstellenmanagement ist verpflichtend für NIS2-regulierte Unternehmen (vgl. § 21 (2) (e) Richtlinie (EU) 2022/2555) und eine Vorgabe mindestens im Bereich Softwareentwicklung, sofern diese nicht komplett outgesourct ist.

Daneben ist ein zentraler Teil der NIS2-Richtlinie auch die koordinierte Offenlegung von Schwachstellen auf nationaler wie europäischer Ebene. So sollen innerhalb von noch zu definierenden Plattformen Informationen über Schwachstellen vertrauensvoll ausgetauscht werden können, um zum Beispiel Frühwarnsysteme zu ermöglichen.

Was ist Schwachstellenmanagement?

Schwachstellenmanagement ist ein zentraler Bestandteil Ihrer Informationssicherheit. Unternehmen nutzen verschiedene Scanning-Tools, um Infrastrukturen – von Servern über Netzwerke bis hin zu Anwendungen – auf bekannte Schwachstellen wie veraltete Patch-Stände oder falsche Konfigurationen zu untersuchen. Ziel ist nicht nur, die oft langen Listen gefundener Lücken systematisch zu beheben, sondern auch die zugrunde liegenden Ursachen zu erkennen und nachhaltig zu beseitigen. Häufig besteht jedoch das Missverständnis, nach der Behebung sei die Aufgabe erledigt – während etwa der Prozess zum Härten einer Komponente oder die Dokumentation weiterhin fehlerhaft bleiben.

Prozess des Schwachstellenmanagements



Zur Etappe

Zur Roadmap

Übung: Vorbereitung Schwachstellenmanagement

Ein effektives Schwachstellenmanagement fußt auf vier zentralen Prinzipien: Agilität, um schnell auf neue Bedrohungen zu reagieren, hohe Datenqualität, um verlässliche Erkenntnisse zu gewinnen, Reduktion, um den Fokus auf kritische Risiken zu legen, und geplante Reaktion, um gezielt und strukturiert Gegenmaßnahmen umzusetzen.

Zur Etappe

Zur Roadmap

Die vier Säulen des effektiven Schwachstellenmanagements

So sicher wie es geht
Belastbar sichere Software, die sicher bleibt, sicherer wird und zuverlässig ist.

Agilität	**Datenqualität**	**Reduktion**	**Reaktion**
Vorbedingung für eine effiziente Behebung von Schwachstellen ist ein schneller Patch- und Testprozess.	Um nicht in vielen False Positive Findings unterzugehen, müssen Schwachstellen-Scanner richtig konfiguriert sein.	Geringere Menge an unsicherem eigenen Code und weniger Abhängigkeit erreichen. Reduktion Technischer Schulden macht Ressourcen für Produktives frei.	Vorbereitet mit transparenter Kommunikation nach außen, klaren Verantwortlichkeiten und festem Zeitrahmen.

Praxisprobleme

Downtime, da fehlerhafter Patch Daten zerstört	Große Menge an False Positive Findings in jedem Assessment; ihre aufwendige Priorisierung und Evaluation	Viele Findings (True Positive) in jedem Assessment	Auf „Beg Bounty“ hereingefallen („Sicherheits-forscher“ fordern Belohnung) oder unkoordinierter Disclosure-Prozess
Dev/Stage/Prod-Umgebungen aufsetzen	Automatische Scanner mit maschinenlesbaren Informationen (bspw. SBOMs) nutzen	Secure-Coding-Standards etablieren	security.txt erstellen (s. RFC 9116)

Konkrete Vorbereitungsmaßnahme

Updates nicht eingespielt aus Sorge um Inkompatibilitäten	Unklare Kritikalität des betroffenen Systems	Andauernd CVEs (bekannte Schwachstellen) in Abhängigkeiten	Schwachstellenmeldung an beurlaubten Mitarbeiter gegangen; Verschleppung des Fixes über mehrere Sprints
Ein Tool wie Dependabot & Co. einsetzen	Kritikalität eingesetzter Komponenten im Asset-/Risikomanagement festlegen	Nicht vertrauenswürdige Abhängigkeiten reduzieren	Interne Verantwortlichkeiten personell festlegen und ausdefinieren

Übungsablauf

1. Festlegung von Bereich und Strategie

Definieren Sie vor dem ersten Schwachstellenscan den Scanbereich und die Reaktionsstrategie. Anleitung: Ordnen Sie alle Vorbereitungsmaßnahmen typischen Praxisproblemen zu.

2. Erstellung von Listen

Erstellen Sie eine Liste typischer Praxisprobleme und eine Liste möglicher Vorbereitungsmaßnahmen.

3. Zuordnung von Maßnahmen

Legen Sie eine Tabelle an mit einer Spalte für Praxisprobleme und einer Spalte für Maßnahmen. Ordnen Sie jeder Maßnahme das jeweils passende Praxisproblem zu. Prüfen Sie die Vollständigkeit und diskutieren Sie Abhängigkeiten. Dokumentieren Sie die finalen Zuordnungen kurz und prägnant.

Etappen-FAQ

Muss ich an alle Software-Beschaffungen den gleichen Maßstab anlegen, was die Sicherheit angeht?

Nein, Software kann in verschiedenen Bereichen des Unternehmens eingesetzt werden und hat dort auch jeweils individuelle Sicherheitsanforderungen. Die Entscheidungen sollten aber begründet und dokumentiert werden, falls es Nachfragen gibt.

Ich habe keinen Einblick in meine Software, sollte ich mit einem „Pentest“ anfangen?

Nein, Penetrationstests werden von qualifizierten „ethischen“ Hackern durchgeführt mit dem Ziel, zu evaluieren, ob bereits implementierte Sicherheitsmaßnahmen wirklich greifen. Beginnen sollte man mit dem Aufbau einer sicheren Build-Infrastruktur: Dev/Staging/Prod-Systeme sowie Bereitstellung von Kapazitäten zum Beheben von Schwachstellen.

Wie integriere ich Security Reviews effektiv in den Entwicklungsprozess?

Bauen Sie Sicherheit von Anfang an in Ihren Entwicklungsprozess ein – nicht als nachträglichen Check. Im Threat Modeling (strukturierte Analyse potenzieller Angriffswege) identifizieren Sie Risiken schon vor dem ersten Code. Bei Code Reviews (systematische Prüfung auf Fehler und Schwachstellen) wirkt stets mindestens ein Teammitglied mit Security-Know-how mit.

Was ist eine Software Bill of Materials (SBOM) und wofür ist das gut?

Eine Software Bill of Materials (SBOM) ist eine detaillierte Liste aller Komponenten, Bibliotheken und Abhängigkeiten, die in einer Software enthalten sind. Sie dient dazu, Transparenz hinsichtlich der verwendeten Bausteine zu schaffen, und hilft, Sicherheitsrisiken zu identifizieren und zu managen. Für die Erstellung einer SBOM in einem der zwei gängigen Formate (SPDX oder CycloneDX) braucht es nicht notwendigerweise ein spezialisiertes und meist teures Tool.

Reicht es, wenn Security-Tickets nur für das IT-Sicherheitsteam verständlich sind?

Nein! In vielen Organisationen gibt es Konflikte zwischen den IT-Sicherheitsspezialistinnen -und spezialisten und der Entwicklungsabteilung. Um hier gegenzuwirken, sollten Tickets für die Entwicklung so geschrieben sein, dass diese selbstständig die Korrektheit eines Fixes überprüfen kann, am besten sogar automatisiert („Security Unit Test“). Das führt auch zum Aufbau eigener Security-Kompetenzen in der Entwicklung und entlastet alle Seiten.

Warum ist kontinuierliche Weiterbildung im Bereich IT-Sicherheit so entscheidend?

Die Bedrohungslandschaft verändert sich ständig – neue Angriffsvektoren, Schwachstellen und Sicherheitsstandards entstehen laufend. Investieren Sie regelmäßig in Schulungen für das Entwicklungsteam, damit alle über aktuelle Bedrohungen wie die OWASP Top 10 informiert sind. Organisieren Sie interne Security-Workshops und teilen Sie relevante Sicherheitsvorfälle aus der Branche und ihre Lösungsansätze im Team. Ermutigen Sie zur Teilnahme an Security-Konferenzen und schaffen Sie eine Kultur, in der Sicherheitsbewusstsein als gemeinsame Verantwortung verstanden wird.

Zur Etappe

Zur Roadmap

Etappe

Risiko-management

Zur Roadmap

Etappe

Risiko-management

Relevanz: Stringentes Risikomanagement im Kontext der Informationssicherheit schafft Vertrauen für alle Seiten.

Ein strukturiertes Risikomanagement sorgt dafür, dass technische und organisatorische Maßnahmen verhältnismäßig zu den identifizierten Risiken sind. Verfolgen Sie einen „Allgefahrenansatz“, indem Sie Gefahren systematisch identifizieren, bewerten (Vertraulichkeit, Integrität, Verfügbarkeit) und priorisieren. So können Sie gegenüber Ihren Kunden und Investoren und Aufsichtsbehörden nachweisen, dass Sie Risiken konsequent steuern und die Versorgungssicherheit entlang der gesamten Wertschöpfungskette unterstützen.

Etappen FAQ >

Zur Roadmap

Etappenabschnitt

Identifikation von Risiken

Ordnen Sie Ihre Geschäftsprozesse nach Kritikalität und bewerten Sie die zugehörigen Gefährdungen hinsichtlich ihrer Auswirkungen.

- Info: Relevante Dokumente und Standards >
- Übung: Einstufung schutzwürdiger Geschäftsprozesse >
- Übung: Elementare Gefährdungen einstufen >

Etappenabschnitt

Umgang mit Risiken

Implementieren Sie passende technische und organisatorische Maßnahmen, um identifizierte Risiken effektiv zu steuern und zu minimieren.

- Übung: Dimensionen der Risikoeinschätzung >
- Methode: Risiko bewerten >
- Info: Strategien zur Risikobehandlung >

Info: Relevante Dokumente und Standards

Die NIS2-Richtlinie verlangt von betroffenen Unternehmen ein systematisches Risikomanagement. Die genaue Methodik bleibt frei wählbar, muss jedoch „geeignet“ sein, die definierten Ziele zu erreichen. Artikel 21 nennt darüber hinaus eine Reihe konkreter Risikomanagement-Maßnahmen, von denen viele in dieser Roadmap im Detail erläutert werden.

NIS2

NIS2 fordert von betroffenen Unternehmen ein systematisches Risikomanagement ein. Die konkrete Methodik wird offengelassen, sie muss jedoch „geeignet“ zur Erreichung der Ziele sein.

Neben der Methodik zum Risikomanagement und den Methoden zur Überprüfung der Wirksamkeit der Maßnahmen definiert die NIS2-Richtlinie in Artikel 21 eine Reihe konkreter Maßnahmen zum Risikomanagement, von denen viele im Kontext dieser Roadmap genauer betrachtet werden.

ISO-27001 / ISO-31000

Die ISO-27001 ist eine weltweit anerkannte Norm in der Informationssicherheit. Sie fordert eine strukturierte Auseinandersetzung mit Risiken der eigenen Organisation.

Die ISO-31000 definiert Anforderungen an ein Risikomanagement. Hier wird auch eine konkrete Methodik beschrieben. Im Rahmen der ISO-27001 steht es Unternehmen jedoch frei, auch eigene Methoden zum Risikomanagement zu nutzen oder selbst zu entwickeln.

BSI-Standard 200-3

Der BSI-Standard 200-3 bietet eine eigenständige Methodik für das Risikomanagement. Er ist Teil der IT-Grundschutz-Methodik, kann jedoch auch unabhängig davon angewendet werden. Wie der IT-Grundschutz insgesamt ist der Standard 200-3 grundsätzlich kompatibel mit der ISO-27001. Aufgrund seiner umfangreichen Hilfsmittel und präzisen Vorgaben nutzen wir ihn in dieser Roadmap zum Teil als beispielhaften Leitfaden.

Zur Etappe

Zur Roadmap

Übung: Einstufung schutzwürdiger Geschäftsprozesse

Bei dieser Übung klassifizieren Sie alle Geschäftsprozesse nach ihrem Schutzbedarf. Dafür wird zwischen wertschöpfenden Kernprozessen (z. B. Vertrieb, Beratung) und unterstützenden Prozessen (z. B. Recruiting) unterschieden. Anschließend bewerten Sie jeden Prozess anhand der NIS2-Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Das in NIS2 zusätzlich genannte Ziel Authentizität (Nachweis von Urheberschaft/Quelle) wird in der deutschen Umsetzung unter Integrität subsumiert und daher nicht separat betrachtet.

1. Wahl Geschäftsprozess

„Anlagen-Monitoring“
Ein Wartungsprozess von beim Kunden installierten Solaranlagen

2. Einstufung Schutzziele

	normal	hoch	sehr hoch
Schutzziel Vertraulichkeit Nur befugte Personen dürfen die Informationen sehen oder bearbeiten.	**normal**	hoch	sehr hoch
Schutzziel Integrität Informationen müssen vollständig und unverändert bleiben.	normal	**hoch**	sehr hoch
Schutzziel Verfügbarkeit Wichtige Abläufe und Informationen müssen da sein, wenn sie gebraucht werden.	normal	**hoch**	sehr hoch

3. Begründung zur Einstufung

Vertraulichkeit:
Die Daten haben keinen Personenbezug und sind für sich genommen nicht vertraulich.

Integrität:
Die Daten müssen korrekt sein, sonst kann auf ihrer Basis keine Entscheidung getroffen werden; es drohen teure Ausfälle.

Verfügbarkeit:
Bei eingeschränkter Verfügbarkeit kann der Zustand der Anlagen nicht korrekt bewertet werden; es drohen teure Ausfälle.

Übungsablauf

1. Wahl des Geschäftsprozesses

Wählen Sie einen Prozess aus (z. B. „Anlagen-Monitoring“ – Wartung installierter Solaranlagen).

2. Einstufung nach Schutzzielen

Bewerten Sie den gewählten Prozess hinsichtlich:

- Vertraulichkeit: Müssen die Informationen oder Systeme vor unberechtigtem Zugriff geschützt sein?
- Integrität: Müssen die Informationen besonders vor Manipulation geschützt sein?
- Verfügbarkeit: Wie schädlich wäre eine Nichtverfügbarkeit der Informationen oder Systeme?

3. Begründung

Erläutern Sie für jedes Schutzziel kurz, warum Sie diese Einstufung gewählt haben (z. B. „Bei eingeschränkter Verfügbarkeit kann der Anlagenzustand nicht bewertet werden, was zu teuren Ausfällen führt.“).

Zur Etappe

Zur Roadmap

Übung: Elementare Gefährdungen einstufen

Die NIS 2 fordert, für das Risikomanagement den Allgefahrensansatz zu nutzen, also zum Beispiel auch Gefährdungen durch Natureinflüsse, technische Probleme und Angriffe sowie organisatorische Mängel zu berücksichtigen.

Die 47 Gefährdungen im Katalog „Elementare Gefährdungen“ des BSI sind ein guter Ausgangspunkt für die eigene Risikoanalyse. Die Verwendung eines Gefährdungskatalogs entbindet jedoch nicht davon, auch individuelle Gefährdungen zu betrachten, die für das eigene Unternehmen oder die eigene Branche relevant sind.

Zur Etappe

Zur Roadmap

Beispielhafter Geschäftsprozess

„Anlagen-Monitoring“
Ein Wartungsprozess von beim Kunden installierten Solaranlagen

Vorsätzliche Handlungen

Höhere Gewalt

Blitzeinschlag an einem Sensor --> Es gibt keine Messwerte mehr und die Anlage läuft im Blindflug

Technisches Versagen

Menschliche Fehlhandlungen

Organisatorische Mängel

Urlaub der Beschäftigten nicht kohärent geplant -> Niemand ist verfügbar, um Schaden zu beheben

Übungsablauf

1. Bedrohungen einstufen

Überlegen Sie, welche Bedrohungen Ihren gewählten Geschäftsprozess stören, lahmlegen oder anderweitig schädigen könnten. Das kann sowohl technisch als auch menschlich sein – vom Stromausfall bis zur Weitergabe sensibler Daten.

Übung: Dimensionen der Risikoeinschätzung

Nachdem die Risiken identifiziert und analysiert wurden, geht es darum, die Notwendigkeit einer Behandlung einzuschätzen. Dies geschieht anhand der Dimensionen Schadenshöhe bzw. Auswirkung und Eintrittshäufigkeit.

Jedes Unternehmen muss hier für sich passende Metriken finden. Ein etabliertes Industrieunternehmen mit 50 Jahren Geschichte wird andere Zeithorizonte und Schadenssummen haben als ein drei Jahre altes Start-up. Als Beispiel haben wir in dieser Roadmap jeweils drei Stufen definiert.

Zur Etappe

Zur Roadmap

Beispielhafter Geschäftsprozess

„Anlagen-Monitoring“
Ein Wartungsprozess von beim Kunden installierten Solaranlagen

Risiko 1

	Schadenshöhe	Eintrittshäufigkeit
Blitzeinschlag an einem Sensor -> Es gibt keine Messwerte mehr und die Anlage läuft im Blindflug	begrenzt	**selten**
	beträchtlich	häufig
	existenzbedrohend	sehr häufig

Risiko 2

	Schadenshöhe	Eintrittshäufigkeit
Urlaub der Beschäftigten nicht kohärent geplant -> Niemand ist verfügbar, um Schaden zu beheben	begrenzt	selten
	beträchtlich	häufig
	existenzbedrohend	**sehr häufig**

Übungsablauf

1. Auswahl der Gefährdungen

Wählen Sie aus Ihrer Liste zwei Gefährdungen aus, die Sie bereits in der Übung „Elementare Gefährdungen einstufen“ ermittelt haben.

2. Schadensauswirkung bewerten

Beantworten Sie für jede Gefährdung:

- Wie groß wäre der Schaden für Ihr Unternehmen, wenn diese Gefährdung eintritt?
- Wie wahrscheinlich ist es, dass diese Gefährdung tatsächlich eintritt?

Hinweis zu Einstufungen

Die **Schadenshöhe** bezieht sich auf das Unternehmen und kann zum Beispiel finanzielle, juristische oder Umweltauswirkungen beinhalten.

Die **Eintrittshäufigkeit** gliedert sich auf in „sehr häufig“ (könnte 1 x im Monat auftreten), „häufig“ (könnte 1 x pro Jahr auftreten) und „selten“ (könnte 1 x in 5 Jahren auftreten).

Methode: Risiko bewerten

Im nächsten Schritt wird das Risiko anhand der festgelegten Kriterien auf einer Matrix eingeordnet. Jede Farbe in der Matrix beschreibt eine eigene Risikoklasse, der jeweils konkrete Behandlungsoptionen zugeordnet sind. Hellrosa Risiken können in der Regel ohne weitere Behandlung akzeptiert werden. Rosa Risiken hingegen sollten mit geeigneten Maßnahmen reduziert werden.

Bei dunkelrosa Risiken ist eine Behandlung fast immer zwingend notwendig. Außerdem wird hier in der Regel die Geschäftsführung über das Risiko in Kenntnis gesetzt.

Beispielhafte Risikomatrix zur Bewertung

Tipp
Die Größe der Risikomatrix kann frei gewählt werden. Es sollte aber immer sichergestellt sein, dass alle Risikokategorien klar definiert und abgegrenzt sind.

Zur Etappe
Zur Roadmap

Info: Strategien zur Risikobehandlung

Die Klassifizierung der Risiken bildet die Basis für die Risikobehandlung. Vier Behandlungsstrategien stehen zur Auswahl (siehe rechts). Die Wahl der Strategie und die Umsetzung der Maßnahmen müssen „verhältnismäßig“ sein – also effektiv und angemessen. Dabei sind geltende Standards, technische Machbarkeit, Kosten sowie erforderliche Ressourcen und benötigte Zeit zu berücksichtigen.

Beschreibung der Behandlungsstrategie

1. **Vermeiden**
   Das beste Risiko ist eines, das gar nicht erst auftritt. Dies kann beispielsweise erreicht werden, indem eine Komponente außer Betrieb genommen wird.

2. **Verringern**
   Viele Risiken lassen sich verringern, indem Schutzmaßnahmen umgesetzt werden. Diese können zum Beispiel aus Katalogen wie der ISO 27002 oder dem IT-Grundschutz kommen.

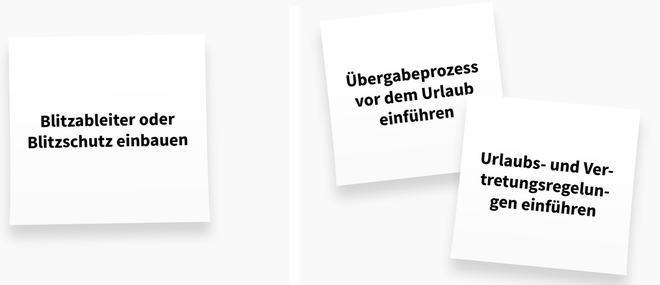
3. **Übertragen**
   Bestimmte Risiken können an Dritte übertragen werden. Das kann etwa durch Versicherungen oder (in begrenztem Umfang) durch Outsourcing geschehen.

4. **Akzeptieren**
   Risikoakzeptanz ist insbesondere dann sinnvoll, wenn Risiken hellrosa sind oder aber die Behandlung zu aufwendig oder aktuell nicht möglich ist. Dunkelrosa Risiken sollten erst ab einer gewissen Hierarchiestufe akzeptiert werden können, typischerweise durch die Geschäftsführung.

Wer legt die Risikobehandlung fest?
Damit die Geschäftsführung im Risikomanagement informierte Entscheidungen trifft, schreibt die NIS2 eine verpflichtende Schulung zur Informationssicherheit für die oberste Leitung vor. Die Kriterien für die Wahl der Behandlungsstrategie müssen mit der GF abgestimmt werden.

Beispielhafte Gefährdungen

Maßnahmen zur Reduktion der Eintrittswahrscheinlichkeit



Maßnahmen zur Reduktion der Auswirkungen

Zur Etappe
Zur Roadmap

Etappen-FAQ

Bin ich nicht viel zu klein für Risikomanagement?

Wer Risiken frühzeitig identifiziert und behandelt, verschleppt sie nicht unnötig und vermeidet oft sogar Technische Schulden.

Muss ich mich an einen der Risikomanagement-Standards halten?

Nein. Die Standards helfen, weil sie vorgefertigte Werkzeuge mitliefern. Aber man muss sie nicht komplett befolgen – vor allem wenn man (noch) keine Zertifizierung anstrebt.

Wie komplex ist Risikomanagement?

Man kann das Thema unendlich komplex machen – oder sich erst einmal auf die wichtigsten Dinge fokussieren. Dann lassen sich auch mit überschaubarem Aufwand gute Ergebnisse erzielen.

Wie ist die Beziehung zwischen Asset- und Risikomanagement?

Asset Management und Risikomanagement haben große Synergien. Wenn ich meine Assets und Geschäftsprozesse sauber dokumentiert habe, fällt die Risikoanalyse viel leichter. Und wenn das Risikomanagement funktioniert, dann weiß ich genauer, wo ich im Asset Management zum Beispiel durch den Aufbau weiterer Ressourcen nachsteuern muss.

Zur Etappe

Zur Roadmap

Etappe

Incident Readiness

Zur Roadmap

Etappe

Incident Readiness

Relevanz: In dieser Etappe lernen Sie, Ihre Incident Readiness zu bewerten und zu optimieren, um im Ernstfall Ausfallzeiten und Schäden zu minimieren.

In dieser Etappe haben wir zentrale Themen zusammengefasst, die in Standards wie ISO 27035, IT-Grundschutz (DER-Bausteine) und NIST SP 800-61 detailliert beschrieben und für Ihre Incident Readiness unerlässlich sind. Sie erfahren, warum die systematische Erfassung von Assets sowie die Einrichtung von Logs und Backup-Architekturen essenzielle Bausteine darstellen. Mithilfe gezielter Fragen können Sie prüfen, ob Sie bereits wirksame Erstmaßnahmen und Notfallreaktionen – von Alarmierungskanälen bis zu Dos and Don'ts – definiert haben oder nachschärfen müssen. Abschließend unterstützen wir Sie dabei, klare Rollen und Verantwortlichkeiten festzulegen sowie Eskalationspfade zu etablieren.

Etappen FAQ >

Zur Roadmap

Etappenabschnitt

Vorbereitung

Erfahren, warum Standards, Asset Management und Logs essenziell für IR sind.

- Info: Relevante Dokumente und Standards >
- Übung: Reflexion zur Vorbereitung >

Etappenabschnitt

Erstmaßnahmen

Erfahren Sie, wie Sie No-go-Aktionen vermeiden und Dokumentationsvorlagen nutzen.

- Übung: Reflexion zu Erstmaßnahmen (1) >
- Übung: Reflexion zu Erstmaßnahmen (2) >

Etappenabschnitt

Eskalation

Erfahren Sie, wann Eskalationen starten.

- Übung: Reflexion zu Eskalationen >

Info: Relevante Dokumente und Standards

Sie müssen nicht von null beginnen, sondern können bei der Vorbereitung auf Security Incidents auf langjährig getestete Best Practices zurückgreifen. Internationale und nationale Standards wie ISO/IEC 27035, BSI DER und NIST SP 800-61 liefern umfassende Leitfäden zum Management von Sicherheitsvorfällen. Ergänzend definiert die NIS2-Richtlinie in Artikel 14 Anforderungen an Incident Readiness, die auch Start-ups helfen, auf Vorfälle zu reagieren.

NIST SP 800-61

NIST SP 800-61 Rev. 2 bietet praktische Empfehlungen zur Verbesserung der Reaktionsfähigkeit bei IT-Sicherheitsvorfällen und integriert dabei Überlegungen des NIST Cybersecurity Framework (CSF) 2.0 in die Risikomanagement-Aktivitäten. Dieser Ansatz unterstützt Organisationen dabei, sich auf Vorfälle vorzubereiten, die Anzahl und die Auswirkungen von Sicherheitsvorfällen zu reduzieren sowie die Effizienz und Effektivität ihrer Erkennungs-, Reaktions- und Wiederherstellungsmaßnahmen zu verbessern. Zudem wird empfohlen, ergänzende Online-Ressourcen zu nutzen, um weiterführende Informationen zur Implementierung der Empfehlungen und Überlegungen zu erhalten.

ISO-27035

Die ISO 27035 bietet Richtlinien für das Management von IT-Sicherheitsvorfällen. Teil 1 stellt grundlegende Konzepte und Prinzipien vor, um Vorfälle zu erkennen, zu melden, zu bewerten und darauf zu reagieren sowie aus ihnen zu lernen. Teil 2 bietet spezifische Anleitungen zur Planung und zur Vorbereitung auf Vorfälle, einschließlich der Aktualisierung von Richtlinien und der Etablierung von Beziehungen. Teil 3 beschreibt die operativen Aspekte des Vorfallsmanagements, einschließlich der Erkennung und Analyse sowie der Reaktion auf Sicherheitsvorfälle. Teil 4 behandelt die koordinierte Handhabung von Vorfällen über mehrere Organisationen hinweg.

BSI DER

Die DER-Bausteinserie im IT-Grundschutz-Kompendium bietet einen strukturierten Ansatz für den Umgang mit IT-Sicherheitsvorfällen. DER 2.1 behandelt die Reaktion auf und die Bewältigung von Sicherheitsvorfällen. DER 2.2 fokussiert auf die Vorsorge für die IT-Forensik zur Analyse digitaler Spuren. DER 2.3 konzentriert sich auf die Bereinigung weitreichender Sicherheitsvorfälle. Diese Vorgaben verbessern kontinuierlich die Fähigkeit einer Organisation, auf verschiedene Szenarien effektiv zu reagieren.

Zur Etappe

Zur Roadmap

Übung: Reflexion zur Vorbereitung

Im Abschnitt „Incident Readiness: Vorbereitung“ stehen drei zentrale Säulen im Fokus: Assets, Logs und Backups. Nur wer seine kritischen Systeme kennt, sämtliche Ereignisdaten lückenlos erfasst und funktionsfähige Wiederherstellungsmechanismen vorhält, kann im Ernstfall schnell und gezielt reagieren. Reflexionsfragen helfen dabei, den aktuellen Reifegrad zu ermitteln und Schwachstellen frühzeitig aufzudecken.

Ihr werdet über eine Ransomware-Nachricht informiert. Pickt euch ein beliebiges Asset (z. B. client4711) raus. Wo steht das System (logisch und physisch)?

Ich bin eine Beispielantwort

Tipp
Gerne einen „schwierigen“ Fall nehmen, z. B. Asset in Außenstelle, Homeoffice Tochtergesellschaft etc.

Bei der forensischen Untersuchung braucht ihr Logs. Wo wisst ihr z.B. nicht, wie ihr an die Logs kommt?

Firewall

Proxy

Netzwerk Switches

Applikations-Server

Cloud-Dienste

SIEM/Monitoring

Endpoint Devices

Mailserver

Tipp
Vergessen Sie nicht „exotische“ Anwendungen und Systeme, die aber kritisch für Ihre Haupt-Geschäftsprozesse sind.

Wie sicher sind eure Backups gegen Ransomware?

100% air-gapped, getestet

Keine Ahnung

Tipp
Achten Sie auf Schreibrechte: Kontrolliert der Domain-Admin auch Backups, droht ein gleichzeitiger Angriff.

Übungsablauf

Nutzen Sie die Reflexionsfragen zu Assets, Logs und Backups zur Diskussion.

Moderieren Sie im Team eine strukturierte Runde.

Sammeln Sie die Antworten sichtbar (Whiteboard, digitales Board) und markieren Sie offene Lücken oder Unsicherheiten.

Erstellen Sie am Ende gemeinsam eine Prioritätenliste der nächsten Schritte zur Schließung der identifizierten Lücken.

Zur Etappe

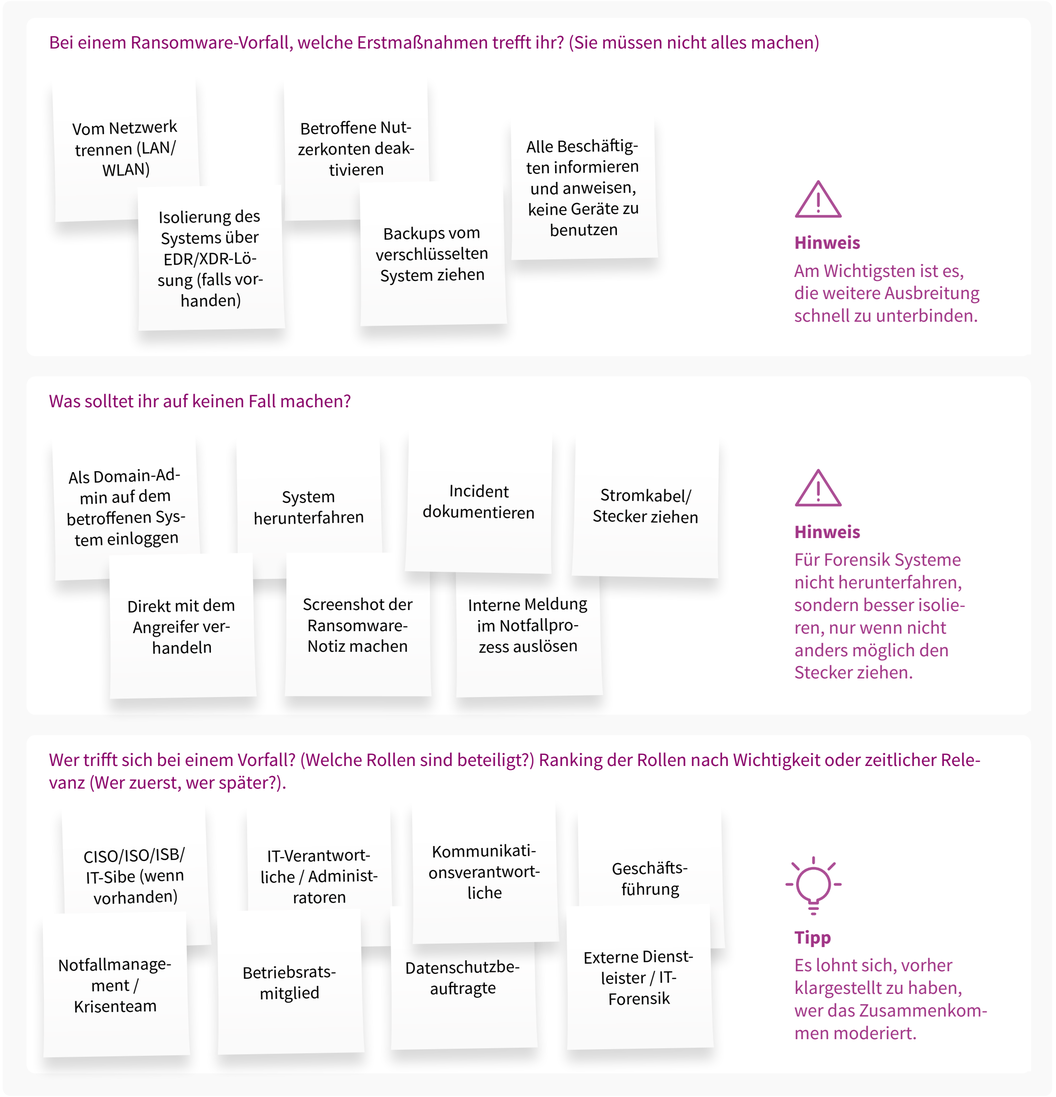
Zur Roadmap

Übung: Reflexion zu Erstmaßnahmen (1)

Die folgenden Reflexionsfragen sind essenziell, um sicherzustellen, dass Ihre Organisation im Ernstfall schnell, korrekt und koordiniert agiert. Indem Sie sich systematisch mit den Erstmaßnahmen auseinandersetzen, klären Sie, welche unmittelbaren Schritte Leben, Infrastruktur und Reputation schützen. Die Sammlung von Dos and Don'ts verhindert Fehlentscheidungen unter Druck und schafft eine klare Handlungsbasis. Durch die Definition des Teams legen Sie Verantwortlichkeiten fest und vermeiden Lücken in der Reaktion. Schließlich garantieren abgestimmte Kommunikationskanäle, dass alle Beteiligten jederzeit informiert sind und kein Wissen verloren geht. Nur so entwickeln Sie eine belastbare Incident Readiness, die im Notfall den Unterschied zwischen rascher Eindämmung und eskalierendem Schaden ausmachen kann.

Zur Etappe

Zur Roadmap



Übungsablauf

Nutzen Sie die Reflexionsfragen zu Erstmaßnahmen, Verantwortlichkeiten und Kommunikationskanälen.

Moderieren Sie im Team eine strukturierte Runde.

Sammeln Sie die Antworten sichtbar (Whiteboard, digitales Board) und markieren Sie offene Lücken oder Unsicherheiten.

Fassen Sie am Ende gemeinsam eine Prioritätenliste der nächsten Schritte zur Schließung der identifizierten Lücken.

Übung: Reflexion zu Erstmaßnahmen (2)

Die folgenden Reflexionsfragen sind essenziell, um sicherzustellen, dass Ihre Organisation im Ernstfall schnell, korrekt und koordiniert agiert. Indem Sie sich systematisch mit den Erstmaßnahmen auseinandersetzen, klären Sie, welche unmittelbaren Schritte Leben, Infrastruktur und Reputation schützen. Die Sammlung von Dos and Don'ts verhindert Fehlentscheidungen unter Druck und schafft eine klare Handlungsbasis. Durch die Definition des Teams legen Sie Verantwortlichkeiten fest und vermeiden Lücken in der Reaktion. Schließlich garantieren abgestimmte Kommunikationskanäle, dass alle Beteiligten jederzeit informiert sind und kein Wissen verloren geht. Nur so entwickeln Sie eine belastbare Incident Readiness, die im Notfall den Unterschied zwischen rascher Eindämmung und eskalierendem Schaden ausmachen kann.

Zur Etappe

Zur Roadmap

Wie alarmiert ihr diese Personen?

- Microsoft Teams
- WhatsApp
- Signal

Tipp
Nicht vergessen: normale Kommunikation meiden, um Angreifer auszuschließen.

Wo trefft ihr euch?

- Spezieller Raum
- VC
- Verschlüsselte TelCo

Tipp
Nicht vergessen, dass die normale räumliche Infrastruktur eingeschränkt nutzbar sein könnte (z. B. Zutrittskarten).

Wie kommuniziert und dokumentiert ihr während des Vorfalls?

- Vorfallformular laut Notfallplan
- Eigenes Wiki oder Incident Management Tool
- Per E-Mail-Protokoll
- Excel-Sheet oder Word-Datei
- Noch kein definiertes Format

Tipp
Dokumentationsort vorab festlegen und Dokumente ransomware-sicher zugänglich aufbewahren.

Übungsablauf

Nutzen Sie die Reflexionsfragen zu Erstmaßnahmen, Verantwortlichkeiten und Kommunikationskanälen.

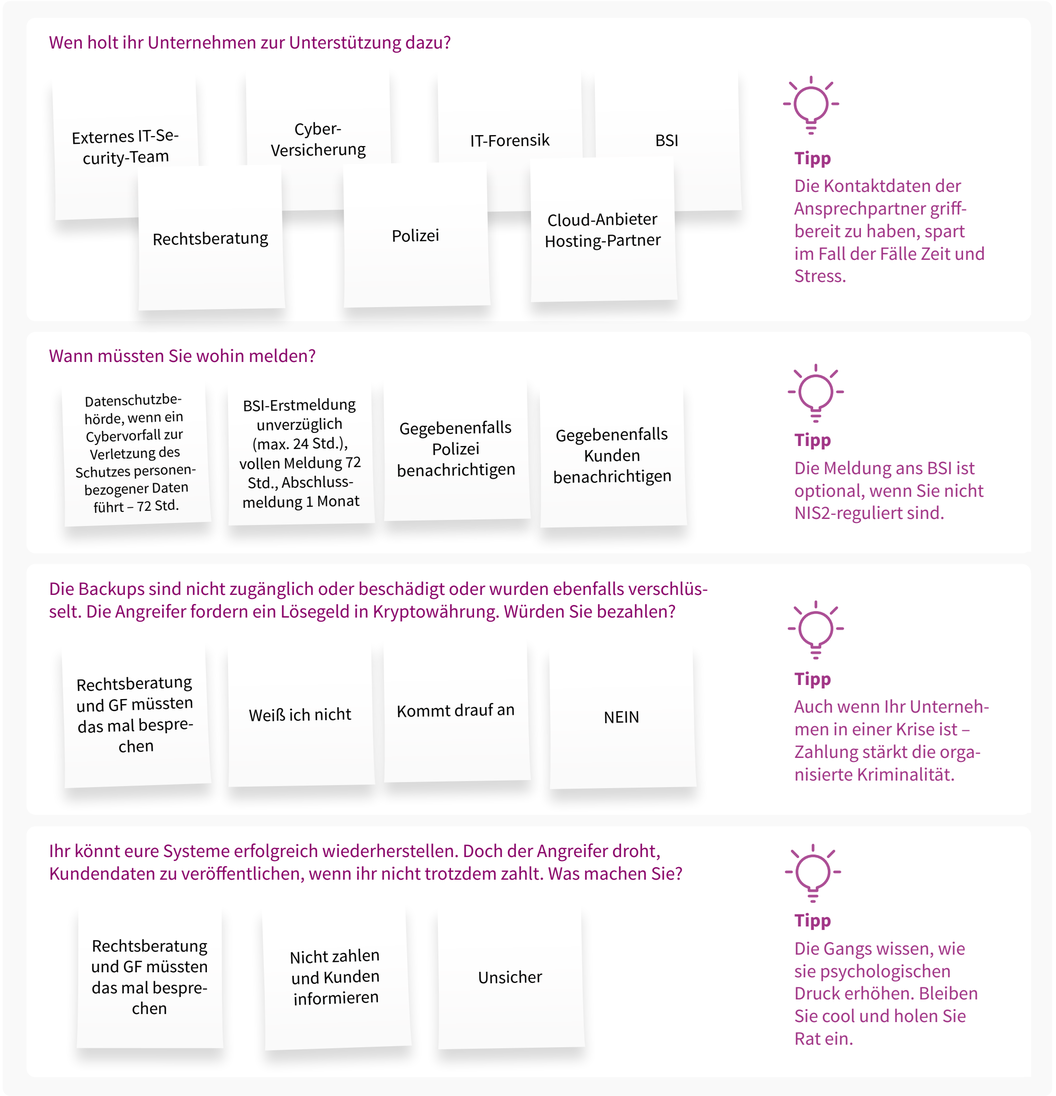
Moderieren Sie im Team eine strukturierte Runde.

Sammeln Sie die Antworten sichtbar (Whiteboard, digitales Board) und markieren Sie offene Lücken oder Unsicherheiten.

Fassen Sie am Ende gemeinsam eine Prioritätenliste der nächsten Schritte zur Schließung der identifizierten Lücken.

Übung: Reflexion zu Eskalationen

In diesem Abschnitt „Eskalation“ reflektieren Sie, welche internen und externen Experten Sie im Ernstfall hinzuziehen, ab welchem Punkt Sie behördliche und regulatorische Stellen informieren müssen und wie Sie im sensiblen Kontext von Ransomware-Zahlungen rechtlich und strategisch verantwortungsvoll entscheiden. Eine klare Eskalationsstrategie stellt sicher, dass Entscheidungen nicht verzögert, Compliance-Anforderungen erfüllt und finanzielle wie reputationsbezogene Risiken minimiert werden.



Übungsablauf

Nutzen Sie die Reflexionsfragen zu Meldungen, Ransomware-Zahlungen und Unterstützungsanfragen.

Moderieren Sie im Team eine strukturierte Runde.

Sammeln Sie die Antworten sichtbar (Whiteboard, digitales Board) und markieren Sie offene Lücken oder Unsicherheiten.

Erstellen Sie am Ende gemeinsam eine Prioritätenliste der nächsten Schritte zur Schließung der identifizierten Lücken.

Zur Etappe

Zur Roadmap

Etappen-FAQ

Warum ist Incident Management wichtig?

Incident Management (insbesondere, aber nicht nur für Security Incidents) ist wichtig, um IT-Störungen und Sicherheitsvorfälle schnell zu erkennen, Schäden zu begrenzen und den Geschäftsbetrieb aufrechtzuerhalten sowie Compliance- und Reputationsrisiken zu minimieren.

Lieber „zu viel“ alarmieren als „zu wenig“?

Beides ist nicht optimal: Überalarmierung führt zu Alarmmüdigkeit und verpassten echten Vorfällen, Unteralarmierung zu unentdeckten Angriffen. Stattdessen sollten Sie Alarme fein justieren, durch Korrelation und Priorisierung nur relevante Ereignisse melden sowie regelmäßig Schwellenwerte und Playbooks überprüfen.

Was versteht man unter einem „(Security) Incident“?

Ein Security Incident ist jedes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen beeinträchtigen kann. Intern sollten Sie die Definition konkretisieren (z. B. Unterscheidung nach Schweregrad, betroffenen Prozessen und Systemen) und im Team regelmäßige Awareness Sessions durchführen, damit alle Beschäftigten Incidents frühzeitig erkennen und melden.

Wie sieht Incident Response aus, wenn man ausschließlich Cloud-Services nutzt?

Die Vorgehensweise hängt vom jeweiligen Cloud-Provider ab. Aktivieren Sie in jedem Fall zentrale Logging-Dienste wie CloudTrail, Azure Monitor oder Cloud Logging und leiten Sie die Logs in ein SIEM zur Aggregation und Analyse weiter. Nutzen Sie API-basierte Playbooks und SOAR-Inte-grationen für automatisierte Reaktionen. Schützen Sie Admin-Accounts durch das Prinzip „Least Privilege“, verpflichtendes MFA und rollenbasierte Zugriffsverwaltung. Legen Sie einen „Breakglass“-Account als Notfallzugang offline an, bewahren Sie seine Anmeldedaten sicher auf und protokollieren Sie jede Nutzung lückenlos.

Zur Roadmap