Minimalstandard für die Sicherheit der Informations- und Kommunikations-technologie (IKT) in der Gasversorgung

G1008 Ausgabe Mai 2024

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Energie BFE

Bundesamt für wirtschaftliche Landesversorgung BWL

Inhaltsverzeichnis

Einführung

2014 wurde eine gemeinsame Risiko- und Verwundbarkeitsanalyse der Erdgasversorgung[1] von Bund und den Gasversorgungsunternehmen durchgeführt, die sich auf die Prozesse konzentrierte, die die Gasversorgung der Industrie und der Schweizer Bevölkerung sicherstellen. Die Analyse ergab unter anderem, dass der Prozess der Gasversorgung zunehmend von IKT-Systemen abhängig ist. Die zunehmende Digitalisierung, insbesondere die Verbindung und Automatisierung von Systemen, führt zu Effizienzsteigerungen, macht den Versorgungsprozess komplexer und anfälliger für IKT-Systemausfälle, was nun zunehmend Einfluss auf die Gasversorgung haben kann.

Um die Schweizer Gasbranche angemessen vor möglichen IKT-Ausfällen zu schützen, haben das Bundesamt für wirtschaftliche Landesversorgung (BWL) und der Fachverband für Wasser, Gas und Wärme (SVGW) gemeinsam den IKT-Minimalstandard für die Gasversorgung (Empfehlung G1008) ausgearbeitet. Die erste Version wurde 2020 veröffentlicht und war als Rahmen gedacht, der es den Gasnetzbetreibern ermöglichen sollte, ihre eigenen Cyberrisiken zu bewerten und geeignete Massnahmen umzusetzen. In den folgenden Jahren wurde die Situation jedoch erheblich komplexer. COVID, der Krieg in der Ukraine, Energieversorgungsengpässe und die enorme Zunahme von Cyberangriffen haben das Gesicht unserer Gesellschaft grundlegend verändert. Um diesem veränderten Umfeld und der Zunahme von Cyberrisiken gerecht zu werden, wurde der IKT-Minimalstandard für die Gasversorgung (Empfehlung G1008) durch eine strengere Version ersetzt.

Diese neue Version «IKT-Minimalstandard für die Gasversorgung 2.0» wurde in Zusammenarbeit zwischen dem Bundesamt für wirtschaftliche Landesversorgung (BWL), dem Bundesamt für Energie (BFE), dem Verband der Schweizerischen Gasindustrie (VSG) und dem Fachverband für Wasser, Gas und Wärme (SVGW) erarbeitet und in einer Branchenvernehmlassung konsultiert. Im Gegensatz zur vorherigen Version, die als Empfehlung gedacht war, hat diese Norm das Ziel, für alle Betreiber von Rohrleitungsanlagen verbindlich zu sein[2]. Um einen effektiven und angemessenen Rahmen zu schaffen, wurden drei Schutzniveaus (A, B und C) geschaffen, die auf zwei Hauptkriterien basieren: der Druck des Netzes oder der Anlage (bar) in Verbindung mit der Leitungslänge (km) und der transportierten Energiemenge (GWh/Jahr). Für jedes Schutzniveau wurden die bestehenden 108 Massnahmen des *NIST Framework* (Programm für Cybersicherheit) sorgfältig überprüft und diesen eine Maturitätsstufe mit entsprechenden Anforderungen zugewiesen. Jeder Gasnetzbetreiber muss folglich die Anforderungen erfüllen, die dem Schutzniveau vergeben worden sind. Die zuständige Aufsichtsbehörde wird sicherstellen, dass die festgelegten Anforderungen erfüllt werden.

Das vorliegende Dokument ist in sechs Kapitel unterteilt. Das erste Kapitel definiert den Geltungsbereich und die Grenzen dieses Dokuments. Im zweiten Kapitel werden verschiedene Themen vorgestellt, um das Verständnis der Themen und Begriffe zu verbessern, die in diesem IKT-Minimalstandard verwendet werden. Kapitel drei konzentriert sich auf den Gassektor, indem es seine Struktur, die IKT-Prozesse und die Bewertung kritischer Aktivitäten erläutert. Im vierten Kapitel werden die verschiedenen Komponenten des Cybersicherheitsprogramms des IKT-Minimalstandards, der auf dem *NIST Framework* basiert, erläutert. Das fünfte Kapitel konzentriert sich auf die Schutzniveaus und die Anforderungen, die jeder Betreiber von Rohrleitungsanlagen erfüllen muss. Letztendlich schliesst das Kapitel sechs diesen Bericht mit den beigefügten Anhängen ab.

Es wird auch empfohlen, diesen IKT-Minimalstandard mit dem Excel Assessment Tool[3] des BWL und dem Begleitdokument[4] zu verknüpfen, um die Bewertung der einzelnen Massnahmen des Cybersicherheitsprogramms zu vereinfachen und das Verständnis des gesamten Cybersicherheitsprogramms zu fördern.

[1] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Bundesamt für wirtschaftliche Landesversorgung (BWL), Bern 2014.

[2] Verpflichtend durch die Revision der Verordnung über Sicherheitsvorschriften für Rohrleitungsanlagen (RLSV; SR 746.12).

[3] Es handelt sich um das Excel-Dokument "IKT-Minimalstandard-Assessment.Tool", das auf der Website des BWL verfügbar ist.

[4] Leitfaden für Gasnetzbetreiber (in Bearbeitung).

1 Geltungsbereich und Abgrenzungen

Dieser IKT-Minimalstandard konzentriert sich auf die kritischen Aktivitäten und die damit verbundenen IKT-Prozesse, die für die Gasversorgung der Schweiz erforderlich sind. Er ordnet ausserdem jedem Betreiber von Rohrleitungsanlagen (Gasnetzbetreiber) ein Schutzniveau (A, B oder C) nach definierten Kriterien zu. Jede Schutzstufe definiert spezifische Anforderungen, die der Gasnetzbetreiber in der entsprechenden Maturitätsstufe zu erfüllen hat. Der Geltungsbereich dieses Dokuments ist wie folgt definiert:

Geltungsbereich

- Dieser IKT-Minimalstandard richtet sich an alle Betreiber von Rohrleitungsanlagen, die der Verordnung über die Sicherheitsvorschriften für Rohrleitungsanlagen (RLSV; SR 746.12) unterliegen.
- IKT-Bedrohungen werden umfassend verstanden: von physischer Beschädigung über den Verlust oder die Manipulation von Daten bis hin zu Cyber-Angriffen in zerstörerischer Absicht. Es werden insbesondere auch jene Bedrohungen berücksichtigt, die im Rahmen der IKT-Verwundbarkeitsanalyse der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken identifiziert wurden[5]. Dieser IKT-Minimalstandard umfasst neben technischen Massnahmen auch die Ausbildung und Schulung der Mitarbeitenden sowie die *Governance*, um die Resilienz von wichtigen IKT-Systemen zu verbessern.
- Die Resilienz der Systeme soll branchenweit verbessert und standardisiert werden. Das angestrebte Ziel des minimalen Schutzniveaus besteht darin, zu verhindern, dass die Gasversorgung durch einen Cyber-Vorfall, der die Sicherheitsrichtlinien, die Integrität, Verfügbarkeit oder Vertraulichkeit verletzt, und somit das gesamte System erheblich beeinträchtigt werden kann.
- Der Standard konzentriert sich vor allem auf die ICS- (insbesondere SCADA), ERP-[6] und Kommunikationssysteme der IKT (IT und OT), welche die Überwachung der Netze bzw. Netzanlagen ermöglichen. Dazu zählen z.B. Laptops und Desktop-Computer, Telefone, Instandhaltungssoftware, Schnittstellen zu SCADA-Systemen, Drucker, Smart Metering, miteinander verbundene Geräte (*Internet of Things*) sowie Netzwerke und Systeme in Betriebsgebäuden, soweit diese nicht getrennt vom Gasnetzbetrieb betrieben werden.
- Je nach Schutzniveau muss jeder Gasnetzbetreiber die, in Kapitel 5.2 dieses Dokuments festgelegten, Anforderungen erfüllen.
- Dieser Minimalstandard muss von den Gasnetzbetreibern entweder intern durch kompetente Mitarbeiter oder extern durch ein spezialisiertes Unternehmen implementiert werden.
- Der VSG und der SVGW haben gemeinsam mit einer Arbeitsgruppe, die sich aus Vertretern der Branche zusammensetzt, die Schutzniveaus (A, B und C) und die entsprechenden Anforderungen (zu erreichende Maturitätsstufe für jede der Massnahmen des NIST Framework Core) definiert und durch die Revision der Verordnung über die Sicherheitsvorschriften für Rohrleitungsanlagen (RLSV; SR 746.12) verpflichtend gemacht.
- Es liegt in der Verantwortung der zuständigen Aufsichtsbehörde, die Umsetzung dieses IKT-Minimalstandards durch die Betreiber von Rohrfernleitungsanlagen zu überprüfen.

[5] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Bundesamt für wirtschaftliche Landesversorgung (BWL), Bern 2014.

[6] *Enterprise Ressource Planning System*: Das ERP-System ist eine komplexe Anwendung oder eine Vielzahl miteinander kommunizierender Anwendungssoftware- bzw. IT-Systeme, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden.

Abgrenzungen

- Nicht untersucht wurde der Fall, wenn die eigene Gasversorgung auch ohne IKT-Systeme in einem «manuellen Betrieb» aufrechterhalten werden kann. Trotzdem wird an dieser Stelle empfohlen, diese Möglichkeit zu erhalten oder (erneut) zu schaffen, falls es die Umstände zulassen. Der manuelle Betrieb ist essenziell für kritische Infrastrukturen – zumindest das geordnete Abschalten der Infrastruktur sollte zu jeder Zeit möglich sein.
- Dieser IKT-Minimalstandard konzentriert sich auf die IKT-Komponenten und deren grosser Abhängigkeit von der Stromversorgung. Ohne Strom würden die SCADA-Systeme, die Kompressionsstation, der Odorierungsprozess, die Bedarfsplanung und die Zollmessstationen nur manuell funktionieren, was eine erhebliche menschliche Kapazität erfordern würde. Es wird empfohlen, einen Notfallplan für jedes Versorgungssystem zu erstellen, um eine allgemeine Stromknappheit oder einen Stromausfall zu bewältigen.
- Um die Sicherheit der Anlagen zu gewährleisten, müssen die Massnahmen des IKT-Minimalstandards durch geeignete technische Massnahmen begleitet werden.
- Das vorliegende Dokument wurde nach aktuellem Wissensstand und mit grösster Sorgfalt erstellt. BWL, BFE, SVGW, VSG, Experten und Unternehmen, die an der Erstellung dieses Dokuments beteiligt waren, übernehmen keine ausdrücklichen oder stillschweigenden Gewährleistungen. Die Verantwortung für mögliche Schäden und für das ordnungsgemässe Funktionieren der Anlagen liegt bei dem Nutzer. Die Implementierung der in diesem Dokument empfohlenen Massnahmen ist keine Garantie für eine unfehlbare Cybersicherheit. Es wird daher empfohlen, über diesen Standard hinauszugehen, um sich optimal zu schützen.
- Endkunden, die kein Gas für Dritte verteilen oder transportieren, sind von diesem IKT-Minimalstandard nicht betroffen.

2 Situations- und Umfeldanalyse

Die Entwicklung der digitalen Welt hat den Aufschwung der Informations- und Kommunikationstechnologien (IKT) ermöglicht. Immer mehr Industrieunternehmen automatisieren und vernetzen ihre industriellen Kontrollsysteme (ICS[7]). Die Digitalisierung steigert die Produktivität und standardisiert die Ausführung der täglichen Aufgaben, aber sie schwächt auch die Zuverlässigkeit, Stabilität und Sicherheit der industriellen Systeme. Das Ziel des IKT-Minimalstandards für die Gasversorgung 2.0 liegt darin, die Cybersicherheit der Gasinfrastruktur zu stärken, um die Gasversorgung der Schweiz zu gewährleisten.

2.1 Die Entwicklung der Industrial Control Systeme (ICS)

Für Industrieunternehmen ist ein *Industrial Control System* (ICS) von entscheidender Bedeutung, da damit die industriellen Systeme gesteuert werden. Ein ICS besteht aus mehreren Steuerelementen, die elektrisch, mechanisch, hydraulisch oder pneumatisch sein können und zusammenwirken, um ein gemeinsames Ziel zu erreichen. Beispielsweise die Steuerung des Gastransports. Ein ICS ist in der Lage, sowohl Daten von variablen Prozessen oder den Zustand von Industriemaschinen zu erfassen als auch die Maschinen vor Ort oder aus der Ferne zu steuern[8]. Der Oberbegriff ICS ist ein Sammelbegriff und umfasst verschiedene Arten von Steuerungssystemen, darunter fällt auch das System *Supervisory Control And Data Acquisition* (SCADA)[9], das insbesondere in der industriellen Verteilung (einschliesslich des Gastransports) eingesetzt wird. Die Besonderheit eines Kontroll- und Datenerfassungssystems (SCADA) besteht darin, Betriebskontrollen über grosse Entfernungen mit Hilfe von Funkwellen, Satellitenübertragungen, Telefonnetz oder WAN[10] durchzuführen. Ein SCADA-System ermöglicht auch die Fernsteuerung verschiedener lokaler Vorgänge, wie das Öffnen und Schliessen von Ventilen oder Unterbrechern, das Sammeln von Daten von verschiedenen Sensoren, sowie die Überwachung von Feldeinheiten und die Möglichkeit, darauf zu reagieren[11].

2.2 Die Konvergenz zwischen Information Technology (IT) und Operational Technology (OT)

Innerhalb der Informations- und Kommunikationstechnologie (IKT) gibt es zwei Unterkategorien, die lange Zeit klar voneinander getrennt waren, aber in den letzten Jahren immer mehr zusammengewachsen sind. Es handelt sich um die *Information Technology* (IT) und die *Operational Technology* (OT). Die erste umfasst alle Informatiksysteme, die die tägliche Arbeit eines Unternehmens unterstützen (E-Mail, Drucker, Telefonie usw.). Die zweite wird für die operative Arbeit verwendet, die mit den industriellen Prozessen einer Organisation verbunden ist und für den korrekten Betrieb der ICS erforderlich ist (Sensoren, Thermometer, Industriemaschinen usw.). Um die Kosten zu senken und den Betrieb der ICS zu verbessern, wurde begonnen, die *Operational Technology* (OT) mit der *Information Technology* (IT) zu verschmelzen. Diese Konvergenz zwischen IT und OT hat es ermöglicht, industrielle Systeme über Netzwerke ferngesteuert zu automatisieren. Folglich können Standard IT-Kommunikationsprotokolle verwendet werden, um OT-Anlagen zu kontrollieren, in denen ICS implementiert sind. Die ICS gewinnen daher an Produktivität auf Kosten der Sicherheit, da sie externen Bedrohungen ausgesetzt sind, die von IT-Geräten ausgehen[12]. Das Ziel des IKT-Minimalstandards ist es daher, alle IKT-Geräte angemessen zu sichern und sicherzustellen, dass die ICS vor diesen "neuen" Risiken angemessen geschützt sind.

2.3 Die Abhängigkeit des Gassektors von IKT

In der Schweiz wird Gas hauptsächlich verwendet, um Wärmeenergie für Teile der Industrie zu erzeugen, um Anlagen zu betreiben und Privathaushalte zu beheizen. Die Gasversorgung in der Schweiz

[7] ICS: Industrial Control System (industrielle Kontrollsysteml)

[8] National Institute of Standards and Technology. “Glossary: industrial control system ICS”.

[9] Falco, J., Scarfone, k. & Stouffer, K. (2013). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology.

[10] Es handelt sich um ein Weitverkehrsnetzwerk, das die Datenübertragung an eine grosse Anzahl von Benutzern über ein viel grösseres geographisches Gebiet als das LAN ermöglicht.

[11] National Institute of Standards and Technology. “Glossary: Supervisory Control and Data Acquisition SCADA".

[12] Balmelli, Laurent. « Build a Cyber Security Program for Industrial Control Systems ». *Medium*, 14. Februar 2020.

umfasst die folgenden vier Hauptetappen: Beschaffung, Transport, Verteilung und Verbrauch. Da die Schweiz über keine Gasförderung verfügt, ist das Land auf Importe aus dem Ausland angewiesen. Das Gas gelangt über ein weites Pipelinenetz (rund 190'000 Kilometer Fernleitungsnetz) in die Schweiz. Dank der zentralen Lage der Schweiz innerhalb Europas erfolgt die Gasversorgung über mehrere Achsen (Genf, Basel, Thurgau bzw. St. Gallen). Im Übrigen spielt die Schweiz innerhalb des europäischen Gasnetzes mit der Verdichterstation Ruswil eine Schlüsselrolle. Dank dieser Station lässt sich Gas bei Bedarf durch die Alpen nach Italien oder Deutschland weiterleiten.

Das Schweizer Pipelinenetz wird hauptsächlich über SCADA-Systeme (*Supervisory Control and Data Acquisition*) gesteuert, die eine Vielzahl von Sensoren zur Netzüberwachung, -analyse und -verwaltung sowie zur Datenerfassung einsetzen. Die SCADA-Systeme ermöglichen zum Beispiel die Fernüberwachung sämtlicher Druckreduzier- und Messstationen (DRM). Diese senken den Druck ab, um das gemessene Gas bis zum Verbrauchsort zu befördern. Bei einem Ausfall der SCADA-Systeme wären die verantwortlichen Unternehmen mangels Netzwerktransparenz nicht mehr in der Lage, die Verwaltung des Transportnetzes zu gewährleisten, und könnten somit auch nicht mehr aus der Ferne intervenieren. Neben den SCADA-Systemen sind auch weitere Kommunikationsinstrumente wie E-Mail, mobile Kommunikation, VoIP und teilweise Funkkommunikation für die Gasunternehmen wichtig. Ohne diese Instrumente sind sie nicht mehr in der Lage, effizient mit dezentralisierten (verteilten) Anlagen zu kommunizieren und auftretende Störungen zu beheben.

2.4 Die Zunahme von Cyberangriffen

Die digitale Welt hat die Industrie mit intelligenten Kontrollsystemen revolutioniert, vernetzt und damit produktiver gemacht, aber sie hat diese Systeme auch neuen Bedrohungen ausgesetzt. Alle Sektoren sind von Cyberangriffen betroffen, auch die Gasindustrie. Cyber-Angriffe hängen nicht von der Grösse oder Bedeutung des Unternehmens ab - sie geschehen oft sogar zufällig - weil eine günstige Gelegenheit geboten wird. Aufgrund der fortschreitenden Digitalisierung werden sich solche Situationen immer häufiger ergeben. Immer mehr Gasnetzbetreiber vernetzen ihre Steuerungssysteme mit dem Internet, um beispielsweise durch Fernüberwachung Kosten zu sparen oder flexibler zu werden. Dies kann zu neuen Verwundbarkeiten führen, die von Hackern ausgenutzt werden, um z. B. Daten zu stehlen, fremde IKT-Ressourcen zu nutzen oder die Kontrolle über kritische Anlagen zu übernehmen. Zum Beispiel werden bei Angriffen mit *Ransomware* Computernetzwerke oder Kontrollsysteme blockiert und nach Zahlung eines Lösegelds wieder freigegeben. Solche Angriffe verursachen erheblichen Schaden und kosten viel Geld.

Die grossen amerikanischen Erdöl- und Gasnetzbetreiber waren bereits mit solchen Bedrohungen konfrontiert. So legte beispielsweise im April 2018 ein Cyber-Angriff beim bedeutenden US-Energiekonzern *Energy Transfer Partners* ETP das verantwortliche System für den elektronischen Datenaustausch (EDI) lahm, das für die Kundentransaktionen innerhalb des Pipelinenetzes verantwortlich ist. Laut ETP beeinträchtigte die Störung die Transaktionen nicht, weil der Software-Ausfall durch interne Ressourcen erfolgreich kompensiert werden konnte[13]. Anfang 2018 nutzte eine Hacker-Gruppe eine Malware namens «Triton», um in ein vorwiegend von AKW-Betreibern sowie Erdöl- und Gasunternehmen verwendetes industrielles Steuerungssystem (*Industrial Control System,* ICS) einzudringen. Das betreffende Unternehmen entdeckte den Angriff, als die Hacker-Gruppe versuchte, gewisse Sensoren umzuprogrammieren, was zur Aktivierung des Sicherheitsmodus und zur automatischen Abschaltung des Systems führte. Dadurch konnte das Unternehmen verhindern, dass sämtliche Anlagen gehackt wurden[14]. Diese Beispiele zeigen, dass derartige Bedrohungen sehr real sind. Um solche und weitere Gefahren möglichst zu beschränken, müssen die IKT-Systeme in der Gasversorgung hohen Sicherheitsanforderungen erfüllen. Die Einführung eines verbindlichen Standards für Cybersicherheit ermöglicht den Gasnetzbetreibern, den Schutz ihrer IKT-Systeme zu optimieren und den Schutz kontinuierlich zu verbessern.

[13] Digital Guardian: *Gas Pipeline Company Recovers From Cyberattack,* 5. April 2018.

[14] The Guardian: *Triton – hackers take out safety systems in «watershed» attack on energy plant,* 15. Dezember 2017 (Stand: 6. Mai 2019).

2.5 Identifizierung kritischer Aktivitäten

Dieser IKT-Minimalstandard für die Gasversorgung 2.0 stützt sich auf bestehende und bewährte Grundlagen wie das *NIST Framework Core*[15]*,* sowie die Risiko- und Verwundbarkeitsanalyse zur Gasversorgung des Bundesamts für wirtschaftliche Landesversorgung[16]. Der IKT-Minimalstandard bezweckt ein einheitliches Vorgehen zu schaffen, um vergleichbare Resultate in der Branche zu erzielen und das Sicherheitsniveau der IKT-Systeme in der Gasversorgung zu erhöhen.

Um die wichtigen Sektoren, die als kritisch für die Landesversorgung gelten, wirksamer zu schützen, werden alle branchenspezifischen IKT-Minimalstandards auf demselben Cybersicherheitsprogramm und denselben Sicherheitsmassnahmen basieren. Folglich gelten für den IKT-Minimalstandard für die Gasversorgung 2.0 die gleichen Voraussetzungen wie für die Strom-[17], Trinkwasser[18]- und Fernwärmeversorgung[19].

Die Besonderheiten zwischen den branchenspezifischen IKT-Minimalstandards besteht darin, die kritischen Aktivitäten in dem spezifischen Bereich zu erkennen. Auf Grundlage der Risiko- und Verwundbarkeitsanalyse des Gassektors[20] durch das BWL und die Gasexperten wurden die Marktstruktur und der Versorgungsprozess des Sektors analysiert, um die kritischen Aktivitäten und die damit verbundenen IKT-Systeme zu definieren. Diese Identifizierung ermöglicht es, bestimmte Massnahmen des Cybersicherheitsprogramms zu priorisieren, damit die Gasnetzbetreiber die Sicherheit der Elemente, die für den Betrieb ihrer Anlagen unerlässlich sind, gewährleisten können. Damit eine Aktivität als kritisch eingestuft werden kann, muss sie zwei Bedingungen erfüllen: Sie muss von den IKT-Systemen abhängig und für den Versorgungsprozess unerlässlich sein. Im Falle von Gas wurden neun kritische Aktivitäten identifiziert: Handel, Nominierung, Zollmessstellen, Odorierung, Netzwerkmanagement, Kompression, Lagerbewirtschaftung, Kundendaten und Kommunikationstools. Diese kritischen Aktivitäten werden in Kapitel 3.3 ausführlich erläutert.

Es ist wichtig, darauf hinzuweisen, dass der IKT-Minimalstandards für die Gasversorgung 2.0 nicht nur die kritischen Aktivitäten identifiziert. Da es sich um ein Dokument handelt, das im Rahmen der Revision der Verordnung über die Sicherheit von Rohrleitungsanlagen (RLSV) verbindlich vorgeschrieben werden soll, sind die Schutzniveaus und die daraus resultierenden Anforderungen nur für den IKT-Minimalstandard für die Gasversorgung 2.0 verbindlich.

[15] In den USA entwickelter Verfahrensrahmen zur Unterstützung öffentlicher und privater Organisationen bei der Verbesserung ihrer Cyber-Sicherheit. Der Rahmen umfasst fünf Funktionen: Identifizieren *(Identify)*, Schützen *(Protect)*, Erkennen *(Detect)*, Reagieren *(Respond)* und Wiederherstellen *(Recover)*.

[16] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Bundesamt für wirtschaftliche Landesversorgung (BWL), Bern 2014.

[17] Handbuch Grundschutz für «Operational Technology» in der Stromversorgung. Verband der Schweizer Elektrizitätsunternehmen (VSE), Aarau 2018.

[18] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Wasserversorgung. Schweizerischer Verein des Gas- und Wasserfaches (SVGW), Zürich 2019.

[19] Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für Fernwärme- und Fernkälteversorgung. Bundesamt für wirtschaftliche Landesversorgung BWL, Bern 2023.

[20] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Bundesamt für wirtschaftliche Landesversorgung (BWL), Bern 2014.

3 Kritische Prozesse und Aktivitäten im Gassektor

In diesem Kapitel werden die Marktstruktur, die Versorgungsprozesse und die kritischen Aktivitäten des Gassektors beschrieben. Ziel ist es, den IKT-Minimalstandard optimal auf den Gassektor zuzuschneiden.

3.1 Marktzusammensetzung

Der Schweizer Gasmarkt ist nach wie vor stark segmentiert und umfasst rund 100 Lokalgesellschaften, die die privaten und gewerblichen Endkonsumentinnen und -Konsumenten beliefern. Zur Optimierung der Gasbeschaffung und des Gastransports haben sich die Lokalgesellschaften in vier Regionalgesellschaften zusammengeschlossen. Diese haben den Auftrag, Gas für die Lokalgesellschaft zu beschaffen und zu transportieren. Zur weiteren Optimierung und zur Erzielung von Skaleneffekten besteht das Unternehmen Swissgas als gemeinsame Dienstleistungsplattform der vier Regionalgesellschaften. Inzwischen ist wichtigstes Geschäftsziel der Swissgas die Gewährleistung der transportseitigen Versorgungssicherheit und des wettbewerbsfähigen Netzbetriebs. Swissgas ist z.B. mit 51 % an der Transitgas AG beteiligt und betreibt ein Hochdruck-Leitungsnetz mit 260 km Länge. Die regionalen Beschaffungsgesellschaften und weitere Importeure beschaffen Gas auf dem EU-Grosshandels-Markt und importieren dies in die Schweiz, um den schweizerischen Bedarf bestmöglich zu decken. Die Regionalgesellschaften sind neben dem technischen Betrieb der Leitungen im Gastransport und im Gashandel tätig. Das Unbundling zwischen Transport und Handel erfolgt mit unterschiedlichen Ansätzen (Abbildung 1).

Die Schweiz liegt im Zentrum des europäischen Pipelinenetzes. Transitgas, im Besitz von "Swissgas", "FluxSwiss" und zu einem sehr kleinen Teil Uniper Global Commodities SE, ist für den Betrieb des Schweizer Abschnitts zwischen Deutschland und Italien zuständig, um Nord- und Südeuropa zu verbinden. Dieser Abschnitt bildet auch das Rückgrat des Schweizer Pipelinenetzes, wird über ihn doch bis zu drei Viertel, der von der Schweiz importierten, Gasmenge transportiert[21]. Transitgas ist auch für den Betrieb der Verdichterstation Ruswil zuständig, die den für den Transport erforderlichen Druck sicherstellt.

Der Gassektor setzt sich aus mehreren Organisationen zusammen, die spezifische Aufgaben wahrnehmen. Zu den wichtigsten Akteuren gehören:

- Hochdrucknetz-Betreiber (> 5 bar und Durchmesser > 6 cm) sind Transitgas, Swissgas, die Regionalgesellschaften und AIL. Das Bundesamt für Energie (BFE) ist für die Überwachung des Hochdrucknetzes zuständig. Dies geschieht in Zusammenarbeit mit dem Eidgenössischen Rohrleitungsinspektorat (ERI), welches die technische Aufsicht führt.
- Das Niederdrucknetz (≤ 5 bar) wird von Lokalgesellschaften verwaltet. Die Kantone sind für die Überwachung des Niederdrucknetzes zuständig. Dies geschieht in Zusammenarbeit mit dem Technischen Inspektorat des Schweizerischen Gasfaches (TIGS), welches die technische Aufsicht führt.
- Im Sinne der Interessenvertretung der Gaswirtschaft unterstützt der Verband der Schweizerischen Gasindustrie (VSG) seine Mitglieder in den Bereichen Politik, Marketing, Öffentlichkeitsarbeit und Ausbildung. Der Fachverband für Wasser, Gas und Wärme (SVGW) vertritt alle Lokalgesellschaften.

[21] *Risikobewertung Erdgasversorgung Schweiz. Bundesamt für Energie (BFE), 2014, Bern.*

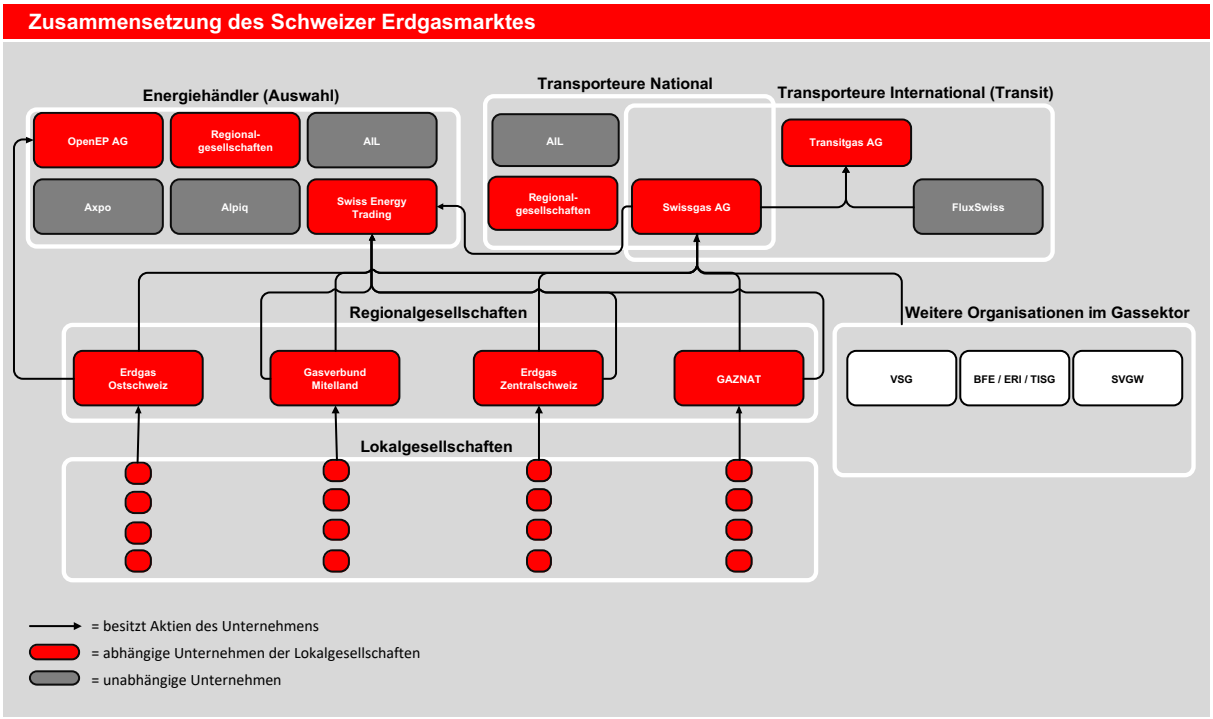

Abbildung 1: Struktur des Schweizer Gasmarkts (vereinfachte Darstellung)

3.2 Prozess der Gasversorgung

Die Gasversorgung der Schweiz wurde in fünf Teilprozesse (Beschaffung, Produktion, Transport, Verteilung, Verbrauch) unterteilt, die jeweils verschiedene Aktivitäten umfassen. Der Gesamtprozess der Gasversorgung ist in Abbildung 2 detailliert dargestellt.

Um die Schweiz mit Gas zu versorgen, muss dieses zunächst beschafft werden. Der Handel mit Gas wird von Energiehändlern auf dem europäischen Energiemarkt abgewickelt. Es gibt zwei Arten von Lieferverträgen: langfristige (mit Laufzeiten zwischen fünf und zehn Jahren) und kurzfristige (mit Laufzeiten von einem Tag bis drei Jahren). Langfristige Kontrakte erlauben es, auf Grundlage von Verbrauchsschätzungen vordefinierte Mengen zu kaufen. Kurzfristige Verträge werden hingegen genutzt, um die Versorgung an den momentanen spezifischen Bedarf anzupassen. Im Gashandel lässt sich somit die zu liefernde Gasmenge festlegen. Zusätzlich ist die «Nominierung» des Gases erforderlich, d. h. die Bestimmung der Netzkapazität und -verfügbarkeit für die gekaufte Gasmenge und die Festlegung der Transportroute des Gases bis zum Verbrauchsort.

Gas ist grösstenteils ein fossiler Energieträger (die Menge an produziertem, in die Schweizer Pipelines eingespeistem Biogas, ist derzeit noch vernachlässigbar). Es wird aus den Gasfeldern gefördert, aufbereitet und direkt oder als regasifiziertes LNG (*liquefied natural gas*) in das europäische Pipelinenetz eingespeist. Mangels ausreichender Rohstoffvorkommen auf ihrem Staatsgebiet, muss die Schweiz ihr gesamtes Gas importieren. Die Schweiz ist also für den Teilprozess «Produktion» auf die Förderländer angewiesen.

Das europäische Fernleitungs-Pipelinenetz erstreckt sich von Norwegen bis Italien und von Portugal bis Russland. In diesem Netz wird das Gas in der Regel mit einem Druck von 40 bis 80 bar transportiert. Es erreicht die Schweiz über einen der Grenzübergangspunkte. Die Leitung von Transitgas durchquert die Schweiz und verbindet Nord- und Südeuropa. Von besonderer Bedeutung ist die Verdichterstation Ruswil, wo das Gas komprimiert wird, um es durch die Alpen transportieren zu können. Normalerweise erfolgt der Transport von Norden nach Süden. Durch den sogenannten "Reverse Flow" in die umgekehrte Richtung ergibt sich eine höhere Flexibilität.

Das Schweizer Pipelinenetz ist rund 19’000 Kilometer lang und weist unterschiedliche Druckniveaus auf. Der Druck variiert im Transportnetz (Swissgas, Regionalgesellschaften und Transitgas) zwischen 5 und 80 bar und im Verteilnetz (Lokalgesellschaften) zwischen 20 mbar und 5 bar. Zur Steuerung der verschiedenen Druckniveaus verfügt das Schweizer Netz über eine Reihe von Druckreduzier- und Messstationen (DRM). Sie ermöglichen die Druckabsenkung, damit das Gas mit dem richtigen Druck

an den Verbrauchsort befördert wird. Für ein optimales Netzmanagement werden die Funktionsweise und die Koordination der mit den Teilprozessen Transport und Verteilung verbundenen Tätigkeiten von einem SCADA-System gesteuert und überwacht. Das System evaluiert und sammelt eine grosse Menge von Daten, mit denen die *Dispatching*-Mitarbeitenden den Gasstrom im Netz bestmöglich regulieren können.

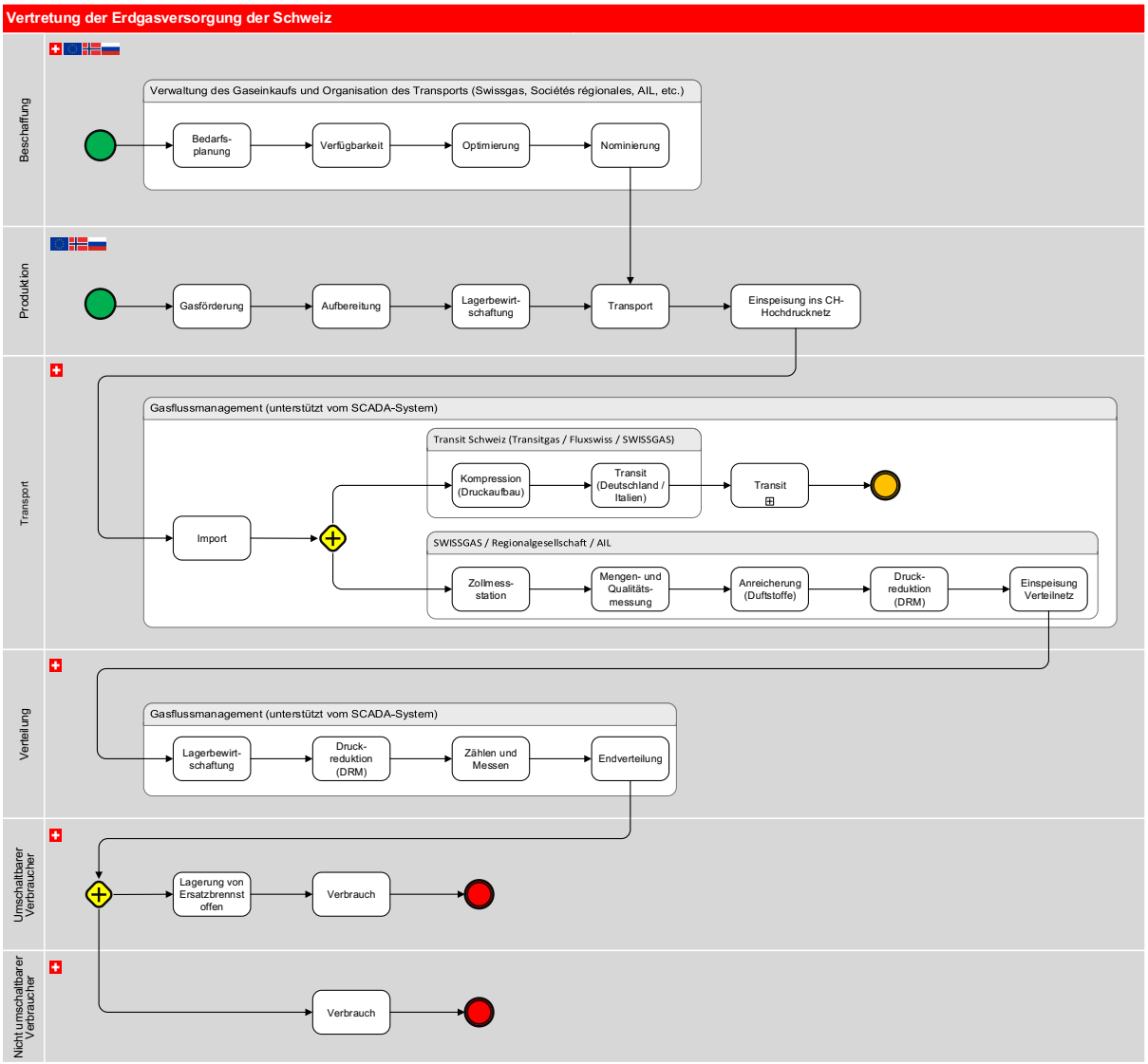

Abbildung 2: Prozess der Gasversorgung (vereinfachte Darstellung)

Der Gasverbrauch unterscheidet sich je nach Konsumentengruppe. Gas wird hauptsächlich zu Wärmezwecken wie die Beheizung von Gebäuden verwendet, kann aber auch als Kraftstoff für Fahrzeuge genutzt werden. Weitere Anwendungsbeispiele sind die Industrie (Wäschereien, Ziegeleien, Einbrennlackierereien) und das Gewerbe (Bäckereien, Gaststätten, Gastronomiebetriebe), deren Tätigkeiten einen hohen Bedarf an Wärmeenergie resp. Bedarf an hohen Temperaturen haben. Im Gasversorgungsprozess wird zwischen verschiedenen Anlagetypen unterschieden. Manche Anlagen sind mit einem (unterbrechbaren) Gas-/Öl-Zweistoffbrenner ausgerüstet und können so je nach Bedarf von einem Brennstoff auf den anderen umschalten. Die übrigen «nicht unterbrechbaren» Anlagen werden hingegen ausschliesslich mit Gas betrieben und sind somit von diesem Energieträger abhängig. Da die Schweiz wie erwähnt über keine Gasspeicher verfügt, ist eine Lagerung von Gas im Land nicht möglich. Einzig die Tagesspeicherkapazitäten (das in den Pipelines vorhandene Gas) bilden eine begrenzte Reserve, die je nach Jahreszeit mehr oder weniger schnell aufgebraucht ist. (Im Winter hält diese Gasreserve ungefähr eine Stunde lang, im Sommer gegebenenfalls mehrere Stunden.)

3.3 Kritische Aktivitäten

Bei der Anpassung des Minimalstandards an einen Sektor muss zunächst festgelegt werden, welche Elemente (sowohl bei der Umsetzung des Standards als auch im Tagesgeschäft) besondere Aufmerksamkeit erfordern. Eine Aktivität wird als kritisch eingestuft, wenn sie zwei Voraussetzungen erfüllt: Abhängigkeit von IKT-Systemen und Unverzichtbarkeit für den Versorgungsprozess (d. h. ohne die Aktivität ist die Versorgung des Landes nicht mehr gewährleistet). Die an der Ausarbeitung dieses Minimalstandards beteiligten Fachleute haben die kritischen Aktivitäten des Erdgassektors auf Grundlage der vom BWL durchgeführten Risiko- und Verwundbarkeitsanalyse zur Erdgasversorgung[22] identifiziert. Sämtliche kritischen Aktivitäten sowie alle relevanten Gasakteure und damit verbundenen IKT-Systeme sind in Abbildung 3 dargestellt.

Hinweis: Obwohl im Folgenden die kritischen Aktivitäten der Beschaffung auf nationaler Ebene dargestellt werden, ist es unerlässlich, die kritischen Aktivitäten innerhalb der Unternehmen selbst zu identifizieren. Es ist daher die Pflicht eines jeden Betreibers, festzulegen, welche Aktivitäten für seinen Betrieb kritisch sind.

Handel

Die erste Etappe der Gasversorgung ist der Kauf des Rohstoffs im Rahmen des Gashandels. Dieser wird auf dem europäischen Energiemarkt abgewickelt, auf dem Gaslieferanten, Energiehändler und Gasnetzbetreiber als Akteure zusammentreffen. Sie handeln miteinander, um die benötigten Gasmengen auf Grundlage kurz- oder langfristiger Verkaufsbedingungen zum bestmöglichen Preis zu beziehen. Das Einkaufsmanagement erfolgt digital mithilfe spezifischer IKT-Systeme (Handels- und Abwicklungssystem). Eine längere Störung des Handels- und Abwicklungssystem oder der Kommunikationskanäle würde die Gasbeschaffung und den Transport erschweren oder gar verunmöglichen. Die Sicherstellung des Landes kann durch vorsorgliche Massnahmen wie verbindliche Zuordnung der Verantwortlichkeiten für Versorgungssicherheit, Diversifikation bei Beschaffung und Transport, Backup-IT und Kommunikationssystem und/oder nationale Notfall-Reserveverträge gestützt werden.

Nominierung

Nach der Beschaffung des Gases muss es in die Schweiz transportiert werden. Der physikalische Fluss wird unterstützt von SCADA-Systemen, der kommerzielle Fluss wird unterstützt durch Beschaffungs- und Abwicklungstools sowie Bilanzierungs/Nominationsplattformen von Marktgebietsverantwortlichen und TSO's im In- und Ausland. Zu diesem Zweck führen die Gasversorger eine Nominierung durch. Dabei werden die Transportroute des Gases bis zum Verbrauchsort sowie die Kapazität und Verfügbarkeit der benutzten Netze ermittelt. Im Rahmen der Nominierung sind ausserdem die Ein- und Ausspeisepunkte der einzelnen Netze anzugeben, durch die das Gas strömt. Mit anderen Worten geht es darum, den Gasimport zu organisieren. Die Nominierung erfolgt digital über Transportmanagementsysteme. Bei einer Störung der IKT-Systeme wären die Gastransportunternehmen nicht mehr in der Lage, den Gastransport zu steuern und den Import des Rohstoffs zu gewährleisten.

Zollmessstation (Einsatz eines SCADA-Systems)

Mit den Zollmessstationen lassen sich an den Ein- und Ausspeisepunkten eines Netzes Messungen durchführen. Bei der Einleitung in die Schweiz muss das Gas eine Zollmessstation passieren, damit die tatsächlich ins Land importierte Gasmenge präzise ermittelt und die Rechnung entsprechend angepasst werden kann. An den Zollmessstationen werden zudem die Qualität und die Zusammensetzung des Gases gemessen. Die entsprechenden gemessenen Daten werden von SCADA-Systemen erfasst. Bei einer Störung würde die Verbindung zu den Zollmessstationen unterbrochen werden. Da die Gasversorgung der Schweiz von den Gasnetzbetreibern abhängt, wird die Tätigkeit der Zollmessstationen als kritische Aktivität eingestuft. Manuelle Vorgänge sind grundsätzlich möglich, erfordern aber signifikant höheren personellen Aufwand.

Odorierung (Einsatz eines SCADA-Systems)

Gas ist von Natur aus farb- und geruchlos und somit für den Menschen nicht wahrnehmbar, was diesen Energieträger besonders gefährlich macht. Zur Lösung dieses Problems wird Gas künstlich odoriert, d. h. mithilfe einer chemischen Verbindung namens Tetrahydrothiophen (THT) mit einem bestimmten

[22] Risiko- und Verwundbarkeitsanalyse des Teilsektors Erdgasversorgung. Bundesamt für wirtschaftliche Landesversorgung (BWL), Bern 2014.

Geruch versetzt. Die Odorierung ist eine spezifische Aufgabe der Zollmessstationen, die mit SCADA-Systemen den THT-Gehalt im Gas messen. Ist dieser zu tief, leiten sie weiteres THT ein. Selbst bei einer Störung des Systems wäre die Gasversorgung gewährleistet. Die Odorierung ist jedoch aus Rechts- und Sicherheitsgründen obligatorisch, weshalb diese Aktivität zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus als kritisch eingestuft wird.

Management des Schweizer Pipelinenetzes (Einsatz eines SCADA-Systems)

Das Management des Schweizer Pipelinenetzes ist der wichtigste Bestandteil der in Abbildung 2 dargestellten Teilprozesse «Transport» und «Verteilung». SCADA-Systeme erfassen sämtliche Netzdaten und ermöglichen so die Fernüberwachung des gesamten Netzes über die internen Schnittstellen der einzelnen Gastransportunternehmen. Das Netzmanagementsystem umfasst alle mittels SCADA-Systems betriebenen Elemente (Zollmessstation, Odorierung, Druckreduzier- und Messstation usw.). Auf diese Weise hat jedes Gastransportunternehmen den Gesamtüberblick über sein Netz: vom Gasimport bis zur Verteilung. Bei einer Störung dieses Systems und je nach ihrer Dauer, wären die Gastransportunternehmen nicht mehr in der Lage, ihre Aktivitäten korrekt zu steuern. Die sichere Gasversorgung des Landes wäre somit nicht mehr gewährleistet. Manuelle Vorgänge sind grundsätzlich möglich, erfordern aber signifikant höheren personellen Aufwand.

Kompression (Einsatz eines SCADA-Systems)

Für die Gaskompression ist hauptsächlich Transitgas, genauer gesagt die Verdichterstation Ruswil, zuständig. Auf nationaler Ebene sorgt der Kompressionsprozess für den erforderlichen Druck im Hochdrucknetz, damit das Gas bis zum Verbrauchsort befördert werden kann. Auf internationaler Ebene gewährleistet dieser Prozess einen ausreichend hohen Druck, um das Gas durch die Alpen zu transportieren. Die Kompression wird ausschliesslich durch SCADA-Systeme gesteuert, womit eine 100-prozentige Abhängigkeit von IKT-Systemen besteht. Eine Störung des Kompressionsprozesses auf nationaler Ebene hätte zur Folge, dass in den Wintermonaten sich in Teilen des Schweizer Netzes nicht mehr ein ausreichendes Druckniveau gewährleisten liesse, womit ggf. einige Netzbereiche nicht mehr mit Gas versorgt werden könnten. Auf internationaler Ebene würde eine Störung des Kompressionsprozesses zwar die Versorgung der Schweiz nicht direkt beeinträchtigen, hätte aber negative Folgen für das europäische Netz. Um die korrekte Funktionsweise des Netzes sicherzustellen, die Reputation der Schweiz zu wahren und die Erfüllung ihrer vertraglichen Verpflichtungen zu gewährleisten, wurde die Kompression als kritische Aktivität eingestuft.

Tagesspeicherkapazitäten und Kundendaten

Über das Management der Tagesspeicherkapazitäten und die Verwaltung der Kundendaten können die Lokalgesellschaften auf Schwankungen des Gasverbrauchs reagieren. Unterschreitet die verfügbare Gasmenge einen bestimmten Schwellenwert, können einzelne Versorger die Gasnachfrage über die Tagesspeicherkapazitäten regulieren und sich so vorübergehend auf den jeweiligen Bedarf einstellen. Mittels der Kundendatenverwaltung erhalten die Lokalgesellschaften zudem einen Gesamtüberblick über den effektiven Gasverbrauch. Wird mit einem hohen Verbrauch gerechnet, nutzen die Lokalgesellschaften die Kundendaten, um die Gasverteilung bestmöglich anzupassen. In einem solchen Fall können sie beispielsweise Unternehmen mit unterbrechbaren Anlagen informieren, dass sie unter Umständen auf Ölbetrieb umschalten müssen. Bei einer Störung dieser IKT-Systeme hätten die Gasnetzbetreiber Probleme, die Gasverteilung zu gewährleisten, was die sichere Gasversorgung gefährden würde.

Kommunikationssysteme

Hierunter fallen alle für die Kommunikation verwendeten IKT-Systeme, insbesondere die Sprachkommunikation über *Voice over IP* (VoIP), der elektronische Datenaustausch (EDI, *Electronic Data Interchange* nach dem weltweiten GS1-Standard), der E-Mail-Verkehr und die mobile Kommunikation. Auch die Telekommunikationsinfrastrukturen, welche Kommunikation und Datenaustausch ermöglichen, sind ein wichtiges Element, das es zu berücksichtigen gilt. Insbesondere muss das Abhängigkeitsverhältnis, das zwischen Telekommunikationsprovider und Gasnetzbetreiber bestehen kann, reguliert werden, um sicherzustellen, dass die Telekommunikationsinfrastrukturen angemessen geschützt werden. Die Kommunikationssysteme spielen daher für die internen und externen Beziehungen der Gasnetzbetreiber eine wesentliche Rolle. Ohne diese Systeme und ihre Infrastruktur liesse sich die sichere Gasversorgung nicht gewährleisten. Manuelle Vorgänge sind grundsätzlich möglich, erfordern aber signifikant höheren personellen Aufwand.

Druckreduzier- und Messstationen

Die Druckreduzier- und Messstationen (DRM) sind für den Prozess der Gasversorgung essenziell. Ihre Aufgabe besteht darin, den Druck des Gases zu reduzieren, damit es vom Transportnetz in das Verteilnetz eingeleitet werden kann. Obwohl DRM für den Gastransport unerlässlich sind, weisen sie mehrere Elemente auf, die ihre Kritikalität einschränken. Das elektronische Druckreduziersystem der DRM wird durch ein (IKT-unabhängiges) pneumatisches System unterstützt. Ausserdem verfügen die DRM über eine Sicherungsvorrichtung zur Speicherung des letzten Messwerts, wodurch Unterbrüche vermieden werden. Des Weiteren können vor Ort auch manuelle (allerdings sehr arbeitsintensive) Kontrollen durchgeführt werden. Angesichts dieser Elemente sind DRM unabhängig von IKT-Systemen und werden daher nicht als kritische Aktivität angesehen. Dies ist jedoch keine absolute Wahrheit, da einige DRM aufgrund ihrer Konzeption als kritische Aktivität angesehen werden können. Jede Organisation ist dafür verantwortlich, den Kritikalitätsgrad ihrer DRM zu definieren und festzulegen, ob sie als kritische Aktivität betrachtet werden oder nicht.

Darstellung von kritischen Aktivitäten in Bezug auf Akteure und zugehörige IKT-Systeme

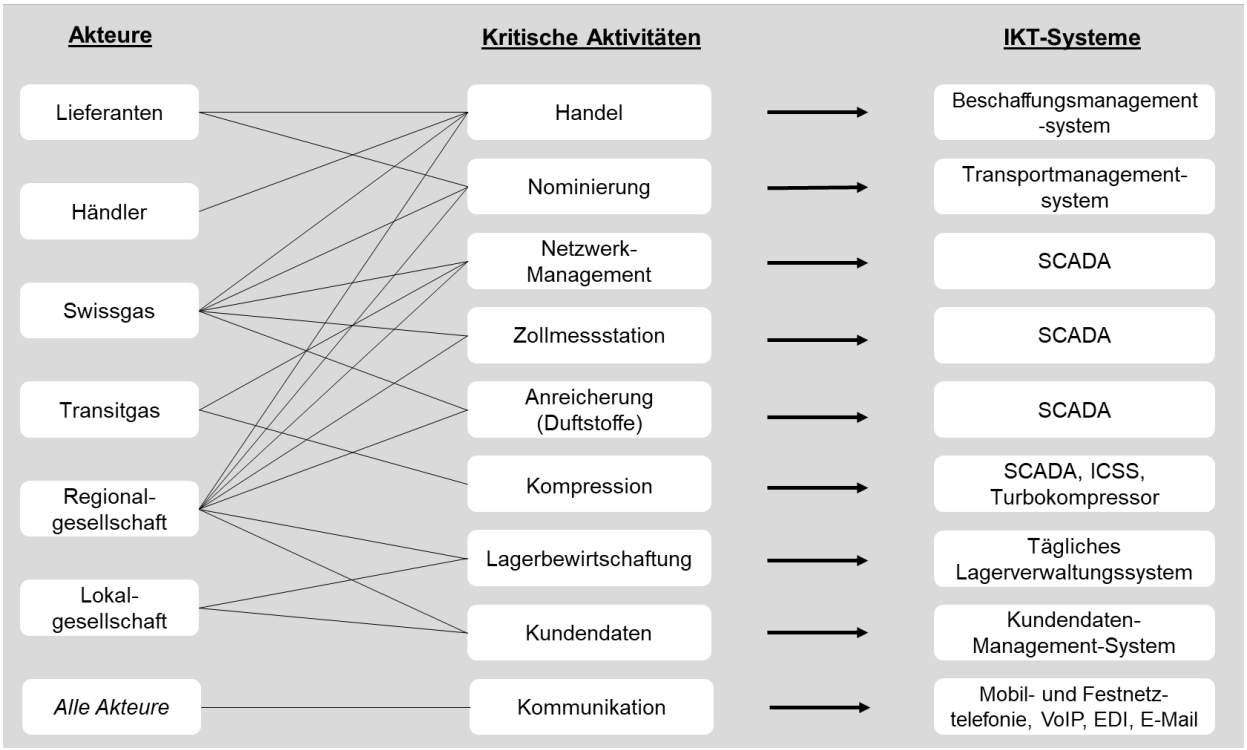

Abbildung 3: Beziehungen zwischen den Gasakteuren, den kritischen Aktivitäten und den verwendeten IKT-Systemen (vereinfachte Darstellung)

4 Cyber-Sicherheitsprogramm des IKT-Minimalstandards

Dieses Kapitel behandelt die spezifischen Aspekte des IKT-Minimalstandards für die Gasversorgung 2.0. Die CIA-Triade[23] ist die Grundlage jedes Cybersicherheitsprogramms. Danach wird besonders auf das *NIST Framework*, der Basis des IKT-Minimalstandard, eingegangen. Als nächstes gibt es eine detaillierte Beschreibung der Grundlagen, Funktionen und Massnahmen des *NIST Framework*. Des Weiteren wird empfohlen, das Begleitdokument[4] zu lesen, um weitere Informationen über den Cybersicherheitsrahmen des IKT-Minimalstandards zu erhalten.

4.1 Die Grundlegenden Konzepte der Cybersicherheit

Im Bereich der Cybersicherheit und insbesondere der Datensicherheit gibt es drei Grundprinzipien, die die Einführung einer Sicherheitspolitik regeln. Dabei handelt es sich um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten (Abbildung 4). Der IKT-Minimalstandard bildet hier keine Ausnahme und jede Massnahme in seinem Cybersicherheitsprogramm zielt darauf ab, das Sicherheitsniveau mindestens eines dieser drei Konzepte zu verbessern. Die Vertraulichkeit als erste Säule, war lange Zeit ein Symbol für Sicherheit, was bedeutet, dass nur autorisierte Systeme und Personen auf Daten und Informationen zugreifen können. Um Organisationen vor Cyberrisiken zu schützen, reicht es nicht aus, nur auf die Vertraulichkeit zu achten. Es ist auch wichtig, die Integrität der Daten zu gewährleisten, was bedeutet, dass die Daten zu jeder Zeit vollständig und korrekt sein müssen, damit keine falschen Entscheidungen auf der Grundlage falscher Informationen getroffen werden. Das letzte Element ist die Verfügbarkeit der Daten, was bedeutet, dass eine Organisation jederzeit Zugang zu ihren Daten haben muss. Dies ist von entscheidender Bedeutung, denn selbst wenn die Daten vertraulich und integer aber nicht zugänglich sind, sind sie nicht nützlich. Diese drei Prinzipien bilden daher die Grundlage für eine Infrastruktur, die wirksam gegen Cyberrisiken geschützt ist. Die Anwendung dieses Modells ist für jedes Cybersicherheitsprogramm von entscheidender Bedeutung, da es sich auf die Sicherheit und den Schutz von Daten konzentriert.

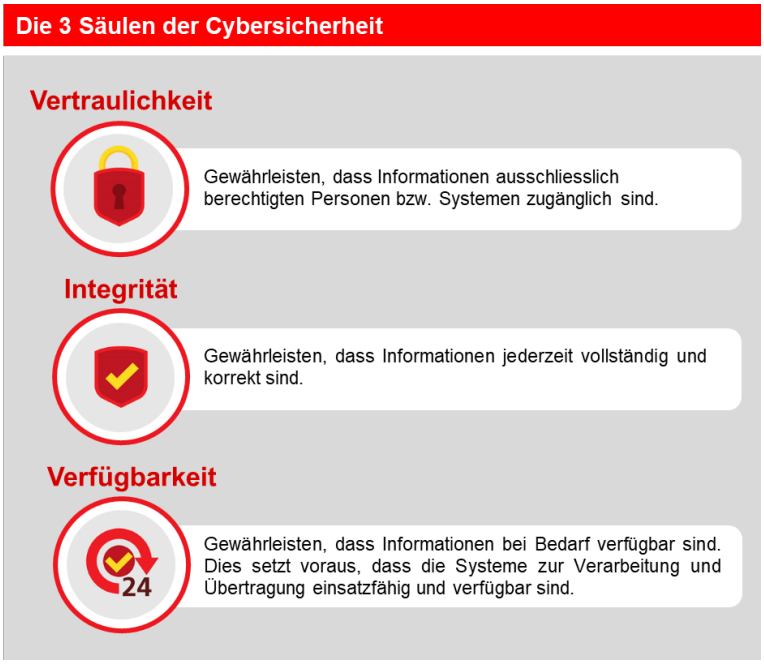

Abbildung 4: CIA-Triade

[23] Es handelt sich um drei grundlegende Konzepte, die die Vertraulichkeit (Confidentiality), die Integrität (*Integrity*) und die Verfügbarkeit (*Availability*) von Daten umfassen.

4.2 Der NIST Framework als Cybersicherheitsprogramm

Der IKT-Minimalstandard basiert auf dem *NIST Framework*; welches zur Reduzierung von Cyberrisiken für kritische Infrastrukturen entwickelt[24] worden ist. Diese amerikanische Methode, die vom *National Institute of Standards and Technology* (*NIST*) veröffentlicht wurde, zeigt einen umfassenden gesamtheitliche Ansatz, damit eine kontinuierliche Überprüfung der IKT-Systeme auf ihre Cybersicherheit durchgeführt werden kann. Das Ziel des NIST Framework ist es, den Betreibern kritischer Infrastrukturen und allen anderen Organisationen, die von IKT-Systemen abhängig sind, ein Instrument an die Hand zu geben, mit dem sie unabhängig und selbständig ihre Widerstandsfähigkeit gegenüber IKT-Risiken erhöhen können.

Das Ziel des NIST-Cybersecurity Framework ist es, einen Rahmen für die effektive Erhöhung des Schutzniveaus gegen Cyberrisiken zu schaffen. Um dies zu erreichen, basiert das Programm für Cybersicherheit auf einem Ansatz, der auf dem akzeptablen Risiko und der *Defense-in-Depth*-Strategie beruht. Es bietet auch eine ausgewogene Sicherheitskombination aus gemeinsamer IT und spezifischen Sicherheitskontrollen der OT, während es technologisch neutral ist. Darüber hinaus ist das *NIST Framework* mit anderen internationalen Standards wie ISO 2700x kompatibel.

Konkret basiert das *NIST Framework* auf 108 Massnahmen in 23 Kategorien und fünf Funktionen: identifizieren, schützen, entdecken, reagieren und wiederherstellen. Diese fünf Funktionen spiegeln die Philosophie des *NIST Framework* wider, das Cybersicherheit als einen dynamischen Prozess betrachtet, der regelmässige Kontrollen und einen kontinuierlichen Verbesserungsprozess erfordert (Abbildung 5). Die Implementierung des IKT-Minimalstandards besteht darin, alle Massnahmen des *NIST Framework* von 0 bis 4 (Maturitätsstufen) zu bewerten. Diese Diagnose ermöglicht es jeder Organisation, ihre Stärken und Schwächen zu bestimmen und geeignete Sicherheitslösungen durch die Verbesserung von Massnahmen oder Funktionen zu implementieren, die unterhalb der definierten Werte liegen. Die Bewertung dieser Massnahmen bietet den Gasnetzbetreibern einen umfassenden Sicherheitsrahmen, um das Sicherheitsprogramm der Organisation kontinuierlich anzupassen.

Die 5 Funktionen und 23 Kategorien des *NIST Framework Core*

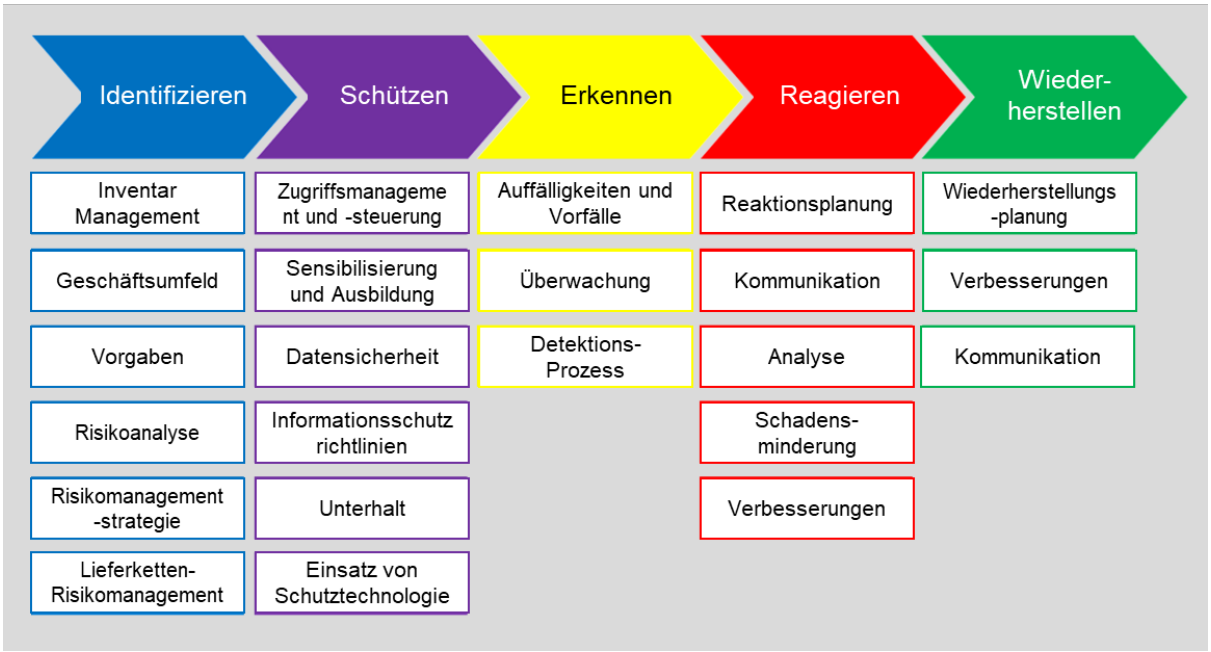

Abbildung 5: Struktur des NIST Framework Core

[24] National Institute of Standards and Technology. *An Introduction to the Components of the Framework*. https://www.nist.gov/cyberframework/online-learning/components-framework.

4.3 Die Funktionen des NIST Framework Core

Dieser Cybersicherheitsrahmen besteht aus fünf Funktionen des *NIST Framework Core* (Abbildung 6). Sie bilden das Rückgrat, auf dem alle anderen Komponenten aufgebaut sind. Sie wurden ausgewählt, weil sie das Kernmaterial einer erfolgreichen Cybersicherheitsprogramms repräsentieren. Diese Elemente ermöglichen eine effektive Identifizierung von Cyberrisiken und über die Risikobewertung eine angemessene Beurteilung des Sicherheitsrisikos. Sie sind ausserdem in 23 Kategorien unterteilt, um alle Massnahmen des *NIST Framework Core* zu klassifizieren

Identifizieren

Im Rahmen des Identifizierens im NIST-Framework werden Vermögenswerte, Bedrohungen und Schwachstellen erfasst. Dies ermöglicht die Bewertung von Risiken und deren Auswirkungen auf geschäftliche Ziele. Die Identifizierung ist ein kontinuierlicher Prozess, der regelmässiges Monitoring erfordert. Unternehmen konzentrieren ihre Ressourcen auf die Bereiche mit den höchsten Risiken. Ziel ist es, eine effektive Grundlage für die Cybersicherheitsstrategie zu schaffen.

Schützen

Diese Funktion umfasst Massnahmen zur Gewährleistung eines angemessenen Schutzes inklusive Sicherheitskontrollen für alle IKT-Ressourcen der Organisation. Insbesondere geht es um technische Prozesse wie Anti-Virus, DMZ, Netzwerkarchitektur oder auch organisatorische Aspekte wie die Sensibilisierung der Mitarbeitenden für Cyberrisiken. Ziel ist es, den Schaden, der durch eine potenzielle Bedrohung verursacht wird, zu vermeiden oder zu begrenzen.

Erkennen

Sobald die IKT-Elemente identifiziert und die entsprechenden Schutzmassnahmen angewendet wurden, ist eine kontinuierliche Überwachung der Sicherheit der Infrastruktur erforderlich. Ziel dieser Funktion ist es, ein effektives und zielgerichtetes Überwachungssystem für IKT-Elemente zu implementieren, um Bedrohungen frühzeitig zu erkennen und so die Auswirkungen eines Cybervorfalls zu vermeiden oder abzumildern.

Reagieren

Innerhalb dieser Funktion werden Massnahmen ergriffen, um Sicherheitsverfahren anzupassen, wenn Cyber-Bedrohungen erkannt werden. Das Ziel ist es, angemessen auf einen Cybervorfall zu reagieren und gleichzeitig die Auswirkungen auf das Unternehmen zu minimieren. Idealerweise sollten detaillierte und genehmigte Verfahren vorhanden sein, um den Vorfall so effizient wie möglich zu lösen.

Wiederherstellen

Diese Funktion beinhaltet Massnahmen zur Wiederherstellung aller Fähigkeiten, die durch einen Cybersecurity-Vorfall beeinträchtigt wurden. Es geht darum, Resilienzpläne zur Wiederherstellung der Infrastruktur der Organisation anzuwenden, damit sie schnell wieder einen normalen Arbeitsrhythmus aufnehmen kann. Diese Funktion ist von entscheidender Bedeutung, damit die IKT-Elemente eines Unternehmens auf einer soliden Basis neu gestartet werden können und somit die Auswirkungen eines Cybersicherheitsvorfalls reduziert werden.

Abbildung 6: Funktionen des NIST Framework Core

4.4 Die Massnahmen des NIST Framework Core

Dieses Kapitel enthält alle Massnahmen des *NIST Framework Core*, die im Rahmen des IKT-Minimalstandards zu bewerten sind. Jede Massnahme wird kurz beschrieben. Es wird empfohlen, zusätzlich zu diesem IKT-Minimalstandard das Begleitdokument[25] und das Excel Assessment Tool zu [26] nutzen, um das Verständnis zu verbessern. Ersteres bietet eine Beschreibung der Massnahmen durch präzise Definitionen, Kontextualisierung und explizite Beispiele. Das Excel-Tool wurde speziell entwickelt, um die Bewertung der Massnahmen zu erleichtern.

4.4.1 Identifizieren – *Identify*

4.4.1.1 Inventarmanagement – Asset Management

Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.

Bezeichnung	Aufgabe
ID.AM-1	Erarbeiten Sie einen Inventarisierungsprozess, der sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar Ihrer IKT-Betriebsmittel (Assets) vorhanden ist.
ID.AM-2	Inventarisieren Sie all Ihre Softwareplattformen, -Lizenzen und -Applikationen innerhalb Ihrer Organisation.
ID.AM-3	Organisatorische Kommunikation und Datenflüsse werden abgebildet.
ID.AM-4	Externe Informationssysteme werden katalogisiert.
ID.AM-5	Ressourcen (z. B. Hardware, Geräte, Daten, Zeit, Personal und Software) werden basierend auf ihrer Klassifizierung, Kritikalität und ihrem Geschäftswert priorisiert.
ID.AM-6	Cybersecurity-Rollen und -Verantwortlichkeiten für die gesamte Belegschaft und externe Stakeholder (z. B. Lieferanten, Kunden, Partner) sind festgelegt.

Tabelle 1: Aufgaben ID.AM

4.4.1.2 Geschäftsumfeld – Business Environment

Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet. Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten.

[25] Achtung, wird später im Detail festgelegt

[26] Es handelt sich um das Excel-Dokument "IKT-Minimalstandard-Assessment.Tool", das auf der Website des BFL verfügbar ist: https://www.bwl.admin.ch/bwl/de/home/bereiche/ikt/ikt_minimalstandard.html

Bezeichnung	Aufgabe
ID.BE-1	Die Rolle ihres Unternehmens innerhalb der (kritischen) Versorgungskette ist identifiziert, dokumentiert und kommuniziert.
ID.BE-2	Die Bedeutung der Organisation als kritische Infrastruktur und ihre Position innerhalb des kritischen Sektors ist identifiziert und kommuniziert.
ID.BE-3	Die Ziele, Aufgaben und Aktivitäten innerhalb der Organisation sind bewertet und priorisiert.
ID.BE-4	Abhängigkeiten und kritische Funktionen für die Bereitstellung kritischer Dienste sind festgelegt.
ID.BE-5	Für alle Betriebszustände (z. B. unter Zwang/Angriff, während der Wiederherstellung, im Normalbetrieb) sind die Anforderungen an die Widerstandsfähigkeit zur Unterstützung der Erbringung kritischer Dienste festgelegt.

Tabelle 2: Aufgaben ID.BE

4.4.1.3 Vorgaben – Governance

Die *Governance* regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen aus dem Geschäftsumfeld eingehalten werden.

Bezeichnung	Aufgabe
ID.GV-1	Vorgaben zur Informationssicherheit sind im Unternehmen festgelegt und kommuniziert.
ID.GV-2	Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit sind mit internen Rollen (z.B. aus dem Riskmanagement) sowie externen Partnern koordiniert.
ID.GV-3	Stellen Sie sicher, dass Ihr Unternehmen alle gesetzlichen und regulatorischen Vorgaben im Bereich der Cyber-Sicherheit erfüllt, inkl. Vorgaben zum Datenschutz.
ID.GV-4	Stellen Sie sicher, dass Cyber-Risiken Teil des unternehmensweiten Risikomanagements sind.

Tabelle 3: Aufgaben ID.GV

4.4.1.4 Risikoanalyse – Risk Assessment

Die Organisation kennt die Auswirkungen von Cyber-Risiken auf die Geschäftstätigkeit, auf Betriebsmittel und Individuen, inklusive Reputationsrisiken.

Bezeichnung	Aufgabe
ID.RA-1	Identifizieren Sie die (technischen) Verwundbarkeiten Ihrer Betriebsmittel und dokumentieren Sie diese.
ID.RA-2	Aktuelle Informationen über Cyber-Bedrohungen werden durch regelmässigen Austausch in Foren und Gremien erhalten.
ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyber-Bedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen auf die Geschäftstätigkeit und bewerten Sie ihre Eintretenswahrscheinlichkeit.
ID.RA-5	Bewerten Sie die Risiken für Ihre Organisation, basierend auf den Bedrohungen, Verwundbarkeiten, Auswirkungen (auf die Geschäftstätigkeit) und Eintretenswahrscheinlichkeiten.
ID.RA-6	Definieren Sie mögliche Sofortmassnahmen bei Eintritt eines Risikos und priorisieren Sie diese.

Tabelle 4: Aufgaben ID.RA

4.4.1.5 Risikomanagementstrategie – Risk Management Strategy

Legen Sie die Prioritäten, Einschränkungen und die maximal akzeptablen Risiken Ihrer Organisation fest. Beurteilen Sie Ihre operativen Risiken auf dieser Grundlage.

Bezeichnung	Aufgabe
ID.RM-1	Etablieren Sie Risikomanagementprozesse, managen Sie diese aktiv und lassen Sie sich diese von den beteiligten Personen / Anspruchsgruppen bestätigen.
ID.RM-2	Definieren und kommunizieren Sie die maximal akzeptablen Risiken Ihrer Organisation.

Bezeichnung	Aufgabe
ID.RM-3	Stellen Sie sicher, dass die maximal tragbaren Risiken unter Berücksichtigung der Bedeutung Ihrer Organisation als Betreiber einer kritischen Infrastruktur bewertet werden. Berücksichtigen Sie dazu auch die sektorspezifischen Risikoanalysen.

Tabelle 5: Aufgaben ID.RM

4.4.1.6 Lieferketten-Risikomanagement – Supply Chain Risk Management

Legen Sie die Prioritäten, Einschränkungen und maximalen Risiken fest, die Ihre Organisation in Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist.

Bezeichnung	Aufgabe
ID.SC-1	Prozesse für das Risikomanagement in der Cyber-Supply-Chain sind identifiziert, etabliert, bewertet, verwaltet und von den organisatorischen Interessenvertretern vereinbart.
ID.SC-2	Lieferanten und Dienstleister von Informationssystemen, Komponenten und Dienstleistungen werden identifiziert, nach Prioritäten geordnet und anhand eines Risikobewertungsprozesses für die Cyber-Lieferkette bewertet, siehe ID.SC-1.
ID.SC-3	Verträge mit Lieferanten und Drittparteien verpflichten diese, Massnahmen, zur Erfüllung der Ziele des Cybersicherheitsprogramms und des Cyber-Lieferketten Risikomanagement Plans der Organisation umzusetzen und einzuhalten.
ID.SC-4	Etablieren Sie ein Monitoring, um sicherzustellen, dass all Ihre Lieferanten und Dienstleister ihre Verpflichtungen gemäss den Vorgaben erfüllen. Lassen Sie sich dies regelmässig in Audit-Berichten oder technischen Prüfergebnissen bestätigen.
ID.SC-5	Definieren Sie mit Ihren Lieferanten und Dienstleistern Reaktions- und Widerherstellungsprozesse nach Cybersecurity-Vorfällen. Testen Sie diese Prozesse in Übungen.

Tabelle 6: Aufgaben ID.SC

4.4.2 Schützen – *Protect*

Zugriffsmanagement und S-teuerung – Access Control

Stellen Sie sicher, dass der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte und auch nur für zulässige Aktivitäten möglich ist.

Bezeichnung	Aufgabe
PR.AC-1	Etablieren Sie einen klar definierten Prozess zur Erteilung und Verwaltung von Berechtigungen und Zugangsdaten für Benutzer, Geräte und Prozesse.
PR.AC-2	Stellen Sie sicher, dass nur autorisierte Personen physischen Zugriff auf die IKT-Betriebsmittel haben. Sorgen Sie mit (baulichen) Massnahmen dafür, dass die IKT-Betriebsmittel vor unautorisiertem physischem Zugriff geschützt sind.
PR.AC-3	Etablieren Sie Prozesse zur Verwaltung der Fernzugriffe.
PR.AC-4	Definieren sie Zugriffsberechtigungen und Autorisierungen unter Berücksichtigung der Grundsätze der geringsten Rechte und der Aufgabentrennung.
PR.AC-5	Stellen Sie sicher, dass die Integrität Ihres Netzwerks geschützt ist. Segregieren Sie ihr Netzwerk logisch und physisch, wo notwendig und sinnvoll.
PR.AC-6	Stellen Sie sicher, dass digitale Identitäten überprüft und bestätigt sind und nur bestätigten Berechtigungsstufen und Zugangsdaten zugeordnet sind.
PR.AC-7	Die Authentifizierung von Benutzern, Geräten und anderen Vermögenswerten (z. B. Ein-Faktor- oder Mehr-Faktor-Authentifizierung) erfolgt entsprechend dem Risiko der Transaktion (z. B. Sicherheits- und Datenschutzrisiken für Einzelpersonen und andere Unternehmensrisiken).

Tabelle 7: Aufgaben PR.AC

4.4.2.1 *Sensibilisierung und Ausbildung – Awareness and Training*

Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Cyber-Sicherheit angemessen geschult und informiert sind. Sorgen Sie dafür, dass sie ihre sicherheitsrelevanten Aufgaben gemäss den definierten Vorgaben und Prozessen ausführen.

Bezeichnung	Aufgabe
PR.AT-1	Stellen Sie sicher, dass alle Mitarbeitenden bezüglich Cyber-Sicherheit informiert und geschult sind.
PR.AT-2	Stellen Sie sicher, dass Anwender/innen mit höheren Berechtigungsstufen sich ihrer Rolle und Verantwortung besonders bewusst sind.
PR.AT-3	Stellen Sie sicher, dass sich alle beteiligten Akteure ausserhalb Ihres Unternehmens (Lieferanten, Kundschaft, Partner) ihrer Rolle und Verantwortung bewusst sind.
PR.AT-4	Stellen Sie sicher, dass sich alle Führungskräfte ihrer besonderen Rolle und Verantwortung bewusst sind.
PR.AT-5	Stellen Sie sicher, dass die Zuständigen für physische Sicherheit und Informationssicherheit sich ihrer besonderen Rolle und Verantwortung bewusst sind.

Tabelle 8: Aufgaben PR.AT

4.4.2.2 *Datensicherheit – Data Security*

Stellen Sie sicher, dass Informationen, Daten und Datenträger so verwaltet werden, dass die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gemäss der Risikostrategie der Organisation geschützt werden.

Bezeichnung	Aufgabe
PR.DS-1	Stellen Sie sicher, dass gespeicherte Daten geschützt sind (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit).
PR.DS-2	Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.
PR.DS-3	Stellen Sie sicher, dass für Ihre IT-Betriebsmittel ein formaler Prozess etabliert ist, der die Daten bei Entfernung, Verschiebung oder Ersatz der Betriebsmittel schützt.
PR.DS-4	Stellen Sie sicher, dass Sie bezüglich der Verfügbarkeit der Daten über ausreichende Kapazitätsreserven verfügen.
PR.DS-5	Stellen Sie sicher, dass adäquate Massnahmen gegen den Abfluss von Daten (Datenlecks) implementiert sind.
PR.DS-6	Etablieren Sie einen Prozess, um Firmware, Betriebssysteme, Anwendungssoftware und Daten hinsichtlich ihrer Integrität zu verifizieren.
PR.DS-7	Stellen Sie eine IT-Umgebung für das Entwickeln und Testen zur Verfügung, die komplett unabhängig von den produktiven Systemen ist.
PR.DS-8	Etablieren Sie einen Prozess, um die eingesetzte Hardware hinsichtlich ihrer Integrität zu verifizieren.

Tabelle 9: Aufgaben PR.DS

4.4.2.3 *Informationsschutzrichtlinien – Information Protection Processes and Procedures*

Stellen Sie sicher, dass Daten während der Übertragung (vor Verletzungen der Vertraulichkeit, Integrität und Verfügbarkeit) geschützt sind.

Bezeichnung	Aufgabe
PR.IP-1	Erstellen Sie eine Standardkonfiguration für die Informations- und Kommunikationsinfrastruktur sowie für die industriellen Kontrollsysteme. Stellen Sie sicher, dass diese Standardkonfiguration typische Sicherheitsprinzipien (z. B. N-1-Redundanz, Minimalkonfiguration usw.) einhält.
PR.IP-2	Etablieren Sie einen Lebenszyklus-Prozess für den Einsatz von IKT-Betriebsmitteln.
PR.IP-3	Etablieren Sie einen Prozess zur Kontrolle von Konfigurationsänderungen.
PR.IP-4	Stellen Sie sicher, dass Sicherungen (Backups) Ihrer Informationen regelmässig durchgeführt, bewirtschaftet und getestet werden (Rückspielbarkeit der Backups testen).
PR.IP-5	Stellen Sie sicher, dass Sie alle (regulatorischen) Vorgaben und Richtlinien hinsichtlich der physischen Betriebsmittel erfüllen.
PR.IP-6	Stellen Sie sicher, dass Daten gemäss den Vorgaben vernichtet werden.

Bezeichnung	Aufgabe
PR.IP-7	Stellen Sie sicher, dass Ihre Informationsschutzprozesse kontinuierlich weiterentwickelt und verbessert werden.
PR.IP-8	Tauschen Sie sich bezüglich der Effektivität verschiedener Schutztechnologien mit Ihren Partnern aus.
PR.IP-9	Etablieren Sie Prozesse zur Reaktion auf eingetretene Vorfälle. (*Incident Response Planning, Business Continuity Management, Incident Recovery, Disaster Recovery*).
PR.IP-10	Testen Sie die Reaktions- und Wiederherstellungspläne.
PR.IP-11	Etablieren Sie Aspekte der Cybersecurity bereits in den Personalrekrutierungsprozess (z.B. durch die Etablierung von Background-Checks/Personensicherheitsprüfungen).
PR.IP-12	Entwickeln und implementieren Sie einen Prozess zum Umgang mit erkannten Schwachstellen.

Tabelle 10: Aufgaben PR.IP

4.4.2.4 Unterhalt – Maintenance

Stellen Sie sicher, dass Unterhalts- und Reparaturarbeiten an Komponenten des IT- und / oder des ICS-Systems gemäss den geltenden Richtlinien und Prozessen durchgeführt werden.

Bezeichnung	Aufgabe
PR.MA-1	Stellen Sie sicher, dass der Betrieb, die Wartung und allfällige Reparaturen an den Betriebsmitteln aufgezeichnet und dokumentiert werden (Logging). Stellen Sie sicher, dass diese zeitnah durchgeführt werden und nur unter Einsatz von geprüften und freigegebenen Mitteln erfolgen.
PR.MA-2	Stellen Sie sicher, dass Unterhaltsarbeiten an Ihren Systemen, die über Fernzugriffe erfolgen, aufgezeichnet und dokumentiert werden. Stellen Sie sicher, dass kein unautorisierter Zugriff möglich ist.

Tabelle 11: Aufgaben PR.MA

4.4.2.5 Einsatz von Schutztechnologie – Protective Technology

Installieren Sie technische Sicherheitslösungen, um die Sicherheit und Resilienz Ihres Systems und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Bezeichnung	Aufgabe
PR.PT-1	Definieren Sie Vorgaben zu Audits und Log-Aufzeichnungen. Erstellen und prüfen Sie die Logs regelmässig gemäss den Vorgaben und Richtlinien.
PR.PT-2	Stellen Sie sicher, dass Wechseldatenträger geschützt sind und dass sie nur gemäss den Richtlinien eingesetzt werden.
PR.PT-3	Stellen Sie sicher, dass Ihr System so konfiguriert ist, dass jederzeit eine Minimalfunktionalität gewährleistet wird.
PR.PT-4	Stellen Sie sicher, dass Ihre Kommunikations- und Steuernetzwerke geschützt sind.
PR.PT-5	Stellen sie sicher, dass Mechanismen (z.B. Ausfallsicherheit, Lastenausgleich, Hot-Swap) implementiert sind, um die Anforderungen an die Ausfallsicherheit in normalen und ungünstigen Situationen zu erfüllen.

Tabelle 12: Aufgaben PR.PT

4.4.3 Erkennen − *Detect*

4.4.3.1 Auffälligkeiten und Vorfälle – Anomalies and Events

Stellen Sie sicher, dass Auffälligkeiten (abnormales Verhalten) und sicherheitsrelevante Ereignisse zeitgerecht erkannt werden und dass sich das Personal der potenziellen Auswirkungen solcher Vorfälle bewusst ist.

Bezeichnung	Aufgabe
DE.AE-1	Definieren Sie Standardwerte für zulässige Netzwerkoperationen und die zu erwartende Datenflüsse für Anwender/innen und Systeme. Überprüfen Sie diese Werte fortlaufend.
DE.AE-2	Stellen Sie sicher, dass entdeckte Cyber-Sicherheitsvorfälle hinsichtlich ihrer Ziele und ihrer Methoden analysiert werden.

Bezeichnung	Aufgabe
DE.AE-3	Stellen Sie sicher, dass Informationen zu Cybersecurity-Vorfällen aus verschiedenen Quellen und Sensoren aggregiert und aufbereitet werden.
DE.AE-4	Bestimmen sie die Auswirkungen möglichen Ereignissen.
DE.AE-5	Definieren sie Schwellenwerte die für Vorfallswarnungen festgelegt sind.

Tabelle 13: Aufgaben DE.AE

4.4.3.2 Überwachung – Security Continuous Monitoring

Stellen Sie sicher, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Abständen überwacht wird, um einerseits Cyber-Sicherheitsvorfälle zu erkennen und andererseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Bezeichnung	Aufgabe
DE.CM-1	Etablieren Sie ein kontinuierliches Netzwerkmonitoring, um potentielle Cybersecurity-Vorfälle zu entdecken.
DE.CM-2	Etablieren Sie ein kontinuierliches Monitoring/Überwachung aller physischen Betriebsmittel und Gebäude, um Cybersecurity-Vorfälle entdecken zu können.
DE.CM-3	Die Aktivitäten der Mitarbeiter werden überwacht, um potenzielle Cybersicherheitsvorfälle zu erkennen.
DE.CM-4	Stellen Sie sicher, dass Schadsoftware erkannt werden kann.
DE.CM-5	Stellen Sie sicher, dass Schadsoftware auf Mobilgeräten erkannt werden kann.
DE.CM-6	Stellen Sie sicher, dass die Aktivitäten von externen Dienstleistern überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können.
DE.CM-7	Überwachen Sie ihre Systeme laufend, um sicherzustellen, dass Aktivitäten/Zugriffe von unberechtigten Personen, Geräten und Software erkannt werden.
DE.CM-8	Führen Sie Verwundbarkeitsscans durch.

Tabelle 14: Aufgaben DE.CM

4.4.3.3 Detektionsprozesse – Detection Processes

Prozesse und Handlungsanweisungen zur Erkennung von Cyber-Sicherheitsvorfällen werden gepflegt, getestet und unterhalten.

Bezeichnung	Aufgabe
DE.DP-1	Definieren Sie klare Rollen und Verantwortlichkeiten, sodass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat.
DE.DP-2	Stellen Sie sicher, dass die Detektionsprozesse die Vorgaben und Bedingungen erfüllen.
DE.DP-3	Testen Sie Ihre Detektionsprozesse.
DE.DP-4	Kommunizieren Sie erkannte Vorfälle an die zuständigen Stellen (Lieferanten, Kundschaft, Partner, Behörden usw.).
DE.DP-5	Verbessern Sie Ihre Detektionsprozesse kontinuierlich.

Tabelle 15: Aufgaben DE.DP

4.4.4 Reagieren − *Respond*

4.4.4.1 Reaktionsplanung – Response Planning

Erarbeiten Sie einen Reaktionsplan im Hinblick auf erkannte Cyber-Sicherheitsvorfälle. Stellen Sie sicher, dass dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Bezeichnung	Aufgabe
RS.RP-1	Stellen Sie sicher, dass der Reaktionsplan während oder nach einem erkannten Cyber-Sicherheitsvorfall korrekt und zeitnah durchgeführt wird.

Tabelle 16: Aufgaben RS.RP

4.4.4.2 Kommunikation – Communication

Stellen Sie sicher, dass Ihre Reaktionsprozesse mit den internen und externen Anspruchsgruppen abgestimmt sind. Sorgen Sie dafür, dass Sie im Ereignisfall falls notwendig und angemessen Unterstützung durch staatliche Stellen erhalten.

Bezeichnung	Aufgabe
RS.CO-1	Stellen Sie sicher, dass alle Personen ihre Aufgaben bezüglich der Reaktion und der Reihenfolge ihrer Handlungen auf eingetretene Cybersecurity-Vorfälle kennen.
RS.CO-2	Definieren Sie Kriterien für Meldungen und stellen Sie sicher, dass Cybersecurity-Vorfälle gemäss diesen Kriterien gemeldet und bearbeitet werden.
RS.CO-3	Teilen Sie Informationen und Erkenntnisse zu detektierten Cybersecurity-Vorfällen gemäss den definierten Kriterien.
RS.CO-4	Die Koordinierung mit allen Beteiligten und den Anspruchsgruppen erfolgt im Einklang mit den Reaktionsplänen gemäss den vordefinierten Kriterien.
RS.CO-5	Es werden regelmässig freiwillig Informationen mit externen Akteuren ausgetauscht, um das Bewusst-sein hinsichtlich der aktuellen Cybersicherheitssituation zu steigern.

Tabelle 17: Aufgaben RS.CO

4.4.4.3 Analyse – Analysis

Stellen Sie sicher, dass regelmässig Analysen durchgeführt werden, die Ihnen eine adäquate Reaktion auf Cyber-Sicherheitsvorfälle ermöglichen.

Bezeichnung	Aufgabe
RS.AN-1	Stellen Sie sicher, dass Benachrichtigungen aus Detektionssystemen berücksichtigt und Nachforschungen ausgelöst werden.
RS.AN-2	Stellen sie sicher, dass die Auswirkungen eines Cybersecurity-Vorfalls bekannt ist und verstanden wird.
RS.AN-3	Führen Sie nach einem eingetretenen Vorfall forensische Analysen durch.
RS.AN-4	Kategorisieren Sie eingetretene Vorfälle gemäss den Vorgaben im Reaktionsplan.
RS.AN-5	Richten sie Prozesse ein, um Schwachstellen, die der Organisation aus internen und externen Quellen (z. B. interne Audits, Sicherheitsbulletins oder Sicherheitsforscher) bekannt werden, zu empfangen, zu analysieren und darauf zu reagieren.

Tabelle 18: Aufgaben RS.AN

4.4.4.4 Schadensminderung – Mitigation

Handeln Sie so, dass die weitere Ausbreitung eines Cyber-Sicherheitsvorfalls verhindert und der mögliche Schaden verringert wird.

Bezeichnung	Aufgabe
RS.MI-1	Stellen Sie sicher, dass Cybersecurity-Vorfälle eingegrenzt werden können und die weitere Ausbreitung unterbrochen wird.
RS.MI-2	Stellen Sie sicher, dass die Auswirkungen von Cybersecurity-Vorfällen gemindert werden können.
RS.MI-3	Stellen Sie sicher, dass neu identifizierte Verwundbarkeiten reduziert oder als akzeptierte Risiken dokumentiert werden.

Tabelle 19: Aufgaben RS.MI

4.4.4.5 Verbesserungen – Improvements

Verbessern Sie die Reaktionsfähigkeit Ihrer Organisation auf eingetretene Cyber-Sicherheitsvorfälle regelmässig, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RS.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus vorangegangenen Cyber-Sicherheitsvorfällen in Ihre Reaktionspläne einfliessen.
RS.IM-2	Aktualisieren Sie Ihre Reaktionsstrategien.

Tabelle 20: Aufgaben RS.IM

4.4.5 Wiederherstellen − *Recover*

4.4.5.1 Wiederherstellungsplanung – Recovery Planning

Stellen Sie sicher, dass die Wiederherstellungsprozesse so gepflegt und durchgeführt werden (können), dass eine zeitnahe Wiederherstellung der Systeme gewährleistet ist.

Bezeichnung	Aufgabe
RC.RP-1	Stellen Sie sicher, dass der Wiederherstellungsplan nach einem eingetretenen Cybersecurity-Vorfall korrekt durchgeführt werden kann.

Tabelle 21: Aufgaben RC.RP

Verbesserungen – Improvements

Verbessern Sie Ihre Wiederherstellungsprozesse laufend, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Bezeichnung	Aufgabe
RC.IM-1	Stellen Sie sicher, dass Erkenntnisse und Lehren aus früheren Cybersecurity-Vorfällen in Ihre Wiederherstellungspläne einfliessen.
RC.IM-2	Aktualisieren Sie Ihre Wiederherstellungsstrategien.

Tabelle 22: Aufgaben RC.IM

Kommunikation – Communication

Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern wie Internet-Service-Providern, *Cyber Emergency Response Teams* (CERT), Behörden, Systemintegratoren usw.

Bezeichnung	Aufgabe
RC.CO-1	Stellen Sie sicher, dass Ihre öffentliche Wahrnehmung aktiv angegangen wird.
RC.CO-2	Stellen Sie sicher, dass Ihre Organisation nach einem eingetretenen Cybersecurity-Vorfall wieder positiv wahrgenommen wird.
RC.CO-3	Kommunizieren Sie alle Ihre Wiederherstellungsaktivitäten an die internen Anspruchsgruppen, insbesondere auch an das Management/die Geschäftsleitung.

Tabelle 23: Aufgaben RC.CO

4.5 Bestimmen und definieren von Maturitätsstufen (*Tiers*)

Das *NIST Framework Implementation Tiers* umfasst mehrere Maturitätsstufen, welche das Sicherheitsrisiko und den Komplexitätsgrad des Managementansatzes beurteilen. Diese beschreiben die Ausbaustufe (Schutzniveau), die implementiert wird. Diese Stufen reichen von «nicht umgesetzt» (*Tier 0*) bis dynamisch (*Tier 4*). Um den eigenen Maturitätsgrad festzulegen (Tier-Level), muss eine Organisation den Risikomanagementprozess, die Infrastruktur, die IT/OT-Architektur, die Art von möglichen Bedrohungen sowie die rechtlichen und regulatorischen Anforderungen und ihre organisatorischen Vorgaben genau kennen.

Die folgenden Abschnitte enthalten detaillierte Beschreibungen der vier Maturitätsstufen (*Tiers*) und werden durch Abbildung 7 ergänzt, die die Hauptmerkmale jede Stufe vereinfacht darstellt.

Wichtiger Hinweis zu n/a: nicht anwendbar

- Diese Massnahme kann nicht bewertet werden, da sie sich nicht auf die betreffende Organisation bezieht und daher nicht angewendet werden kann. Es ist jedoch notwendig, zu begründen, warum diese Massnahme nicht umgesetzt werden kann.
- Beispiel: Ein Unternehmen verzichtet auf die Nutzung bestimmter Dienstleistungen. In diesem Fall werden die Unterkategorien, die sich ausschliesslich auf diese Dienstleistungen beziehen, nicht auf sie angewendet. Wenn das Unternehmen z. B. darauf verzichtet, die Fernwartung zu ermöglichen, ist PR.MA-2 als N/A zu definieren und eine Begründung anzugeben.

***Tier 0*: nicht umgesetzt**

- Dies ist die niedrigste Stufe, die einem nicht vorhandenen Schutz entspricht. Die Massnahmen wurden nicht umgesetzt, es gibt keinen Prozess und es wurde keine Massnahmen ergriffen.

***Tier 1*: Partiell umgesetzt, nicht vollständig definiert und abgenommen**

- Das *Tier*-Level 1 entspricht nicht dokumentierten Risikomanagementprozessen und organisatorischen Cybersicherheitsanforderungen. Daher werden Cybersicherheitsrisiken typischerweise ad hoc oder reaktiv behandelt.
- Es besteht ein integriertes Risikomanagementprogramm auf Organisationsebene, aber kein institutionalisiertes Bewusstsein für Cybersicherheitsrisiken oder einen unternehmensweiten Ansatz zu deren Bewältigung.
- In der Regel verfügt die Organisation keine Mechanismen, um die Informationen zur Cybersicherheit zu koordinieren. Wenn Cybersicherheitsrisiken auftreten, verfügt die Organisation keine standardisierten Verfahren zum Informationsaustausch oder zur Koordinierung der Zusammenarbeit mit externen Partnern.

***Tier 2*: Partiell umgesetzt, vollständig definiert und abgenommen**

- Organisationen, die sich in Tier-Level 2 einstufen, verfügen in der Regel über Verfahren zum Risikomanagement, um Cybersicherheitsrisiken zu begegnen. Sie werden jedoch als spezifische Anweisungen verstanden, die die Mitarbeiter befolgen müssen.
- Auf organisatorischer Ebene sind Cybersicherheitsrisiken in das Risikomanagement des Unternehmens integriert und auf allen Unternehmensebenen ist ein gewisses Bewusstsein vorhanden. Allerdings fehlt es solchen Organisationen häufig an unternehmensweiten Ansätzen zur Verwaltung und Sensibilisierung für aktuelle und zukünftige Cybersicherheitsrisiken.
- Genehmigte Verfahren und Prozesse sind definiert und implementiert. Die Mitarbeiter verfügen über ausreichende Ressourcen, um ihre Aufgaben im Zusammenhang mit der Cybersicherheit zu erfüllen. Innerhalb der Organisation werden Informationen über Cybersicherheit auf informeller Basis ausgetauscht.
- Die Organisation ist sich ihrer Verantwortung im allgemeinen Umfeld bewusst und kommuniziert mit externen Partnern (z.B. Kunden, Lieferanten, Dienstleistern usw.) über Fragen der Cybersicherheit. Es gibt jedoch keine standardisierten Verfahren, um mit diesen Partnern zusammenzuarbeiten oder den Austausch von Informationen auszutauschen.

***Tier 3*: Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch**

- Organisationen der *Tier*-Level 3 verfügen über offiziell genehmigte Risikomanagementpläne als auch Anforderungen für deren Umsetzung im gesamten Unternehmen.
- Gültige Richtlinien des Unternehmens regeln Cybersicherheitsrisiken. Die standardmässig erfassten Cybersicherheitsrisiken sowie die Anforderungen für den Umgang mit ihnen werden regelmässig aktualisiert. Diese Aktualisierungen berücksichtigen Änderungen in den geschäftlichen Anforderungen, technischen Entwicklungen, politischen Veränderungen oder sich verändernde Bedrohungslandschaften (zum Beispiel durch neue Akteure).
- Die Verfahren und Prozesse für den Umgang mit diesen neuen Risiken sind schriftlich festgelegt. Die Organisation verwendet standardisierte Methoden, um auf Veränderungen der Risiken zu reagieren. Die Mitarbeiter verfügen über die Kenntnisse und Fähigkeiten, die sie zur Erfüllung dieser Aufgaben benötigen.
- Die Organisation weiss, dass sie von externen Partnern abhängig ist und tauscht regelmässig Informationen mit ihnen aus. Das Management kann Entscheidungen als Reaktion auf Vorfälle treffen.

***Tier 4:* Dynamisch umgesetzt, kontinuierlich überprüft, verbessert**

- Das *Tier*-Level 4 bedeutet, dass eine Organisation alle Anforderungen der *Tier*-Level 1-3 vollständig erfüllt und darüber hinaus ihre eigenen Verfahren, Methoden und Fähigkeiten kontinuierlich überprüft und bei Bedarf verbessert. Diese kontinuierliche Verbesserung basiert auf der vollständigen Dokumentation aller Cybersicherheitsvorfälle.
- Die Organisation analysiert vergangene Vorfälle und zieht daraus die notwendigen Lehren, indem sie ihre eigenen Verfahren und die von ihr verwendeten Sicherheitstechnologien dynamisch an den Fortschritten bei den Cybersicherheitstechnologien oder veränderte Bedrohungssituationen anpasst.
- Das Cybersicherheitsrisikomanagement ist ein integraler Bestandteil der Unternehmenskultur.
- Der Risikomanagementprozess integriert kontinuierlich die Erkenntnisse aus früheren Vorfällen, Informationen aus externen Quellen und die laufende Überwachung der eigenen Systeme und

Netzwerke.

- Das Unternehmen hat standardisierte Verfahren eingeführt, um Informationen mit Partnern ständig auszutauschen.

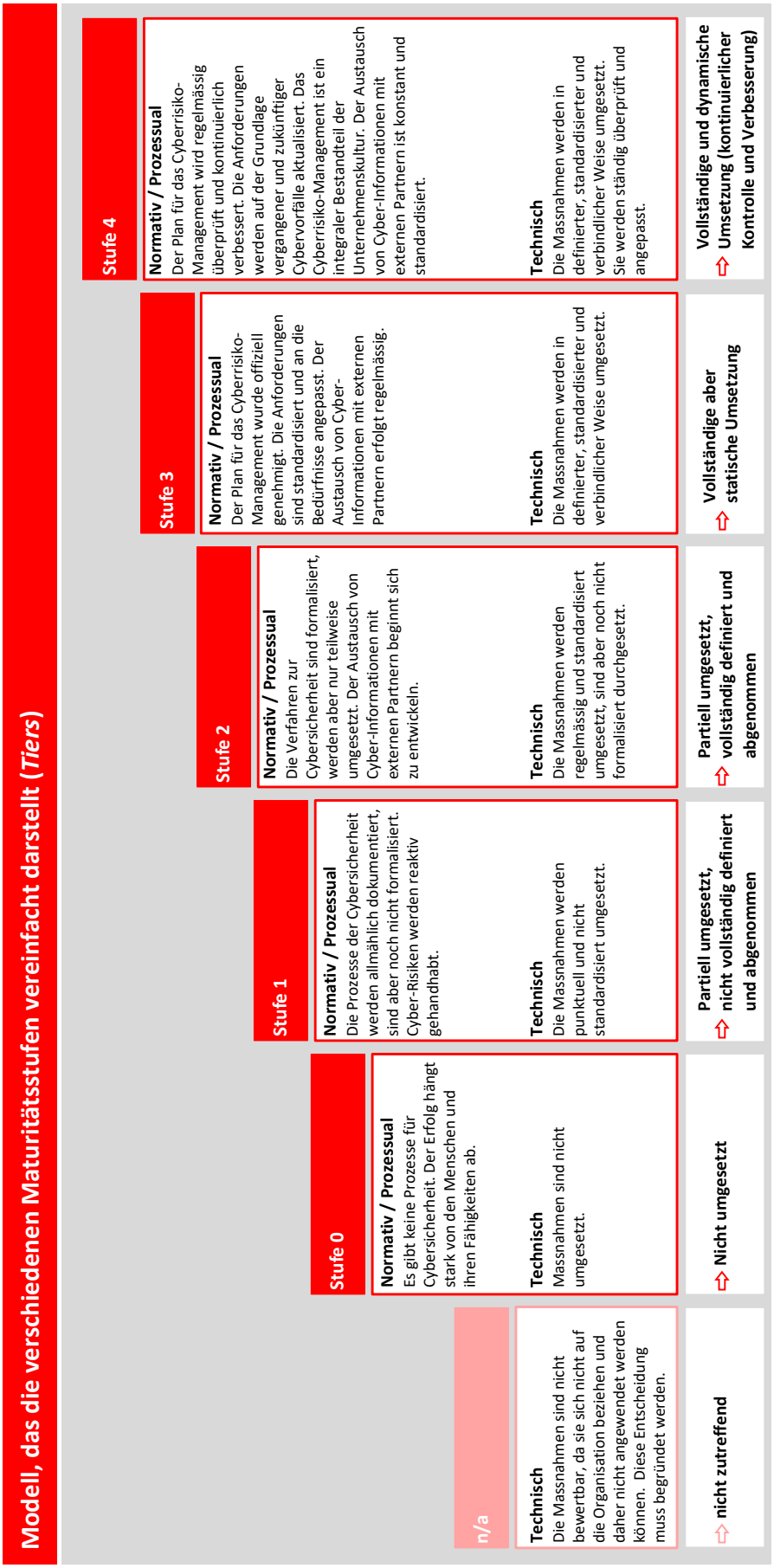

Abbildung 7: Zusammenfassung der Maturitätsstufen (Tiers)

5 Schutzniveaus und Anforderungen

Die Revision der Verordnung über die Sicherheitsvorschriften für Rohrleitungsanlagen (RLSV; SR 746.12) zielt darauf ab, den IKT-Minimalstandard für Betreiber von Rohrleitungsanlagen verbindlich zu machen. Das bedeutet, dass die zur Anwendung dieses Standards verpflichteten Parteien ein bestimmtes Schutzniveau bei der Umsetzung von Massnahmen zu erreichen haben. Um das Prinzip der Verhältnismässigkeit zu berücksichtigen und den Bedürfnissen der Gasbranche bestmöglich zu entsprechen, wurden drei Schutzniveaus definiert (A, B und C). Jedes Schutzniveau entspricht einer spezifischen Maturitätsstufe, so dass die Anforderungen gestaffelt werden können.

5.1 Schutzniveaus

Es werden Kriterien definiert, um Gasnetzbetreiber nach ihren Bedürfnissen, ihrer Kritikalität und ihren Ressourcen zu unterscheiden. Die Schutzniveaus gelten nur für Betreiber von Rohrleitungsanlagen. Die Endkunden sind von dieser Verpflichtung ausgenommen.

Kriterien		Schutzniveau A	Schutzniveau B	Schutzniveau C
Druck des Netz- oder Anlagenbetrieb (bar) und Leitungslänge (km):	> 5 bar und > 15 km	X		
Transportierte Energiemenge:	> 2'600 GWh/Jahr	X		
	> 400 GWh/Jahr und ≤ 2'600 GWh/Jahr		X	
	≤ 400 GWh/Jahr			X

Energie in GWh/Jahr: basierend auf dem Durchschnitt der letzten fünf Kalenderjahre

Abbildung 8: Kriterien für Schutzniveaus

Mit den oben genannten Kriterien (Abbildung 8) können den Unternehmen definierten Schutzniveau zugewiesen werden: nämlich A, B oder C. Wenn ein Gasnetzbetreiber die Kriterien eines Schutzniveaus erfüllt, muss er die entsprechenden Anforderungen erfüllen (siehe Kapitel 5.2). Die transportierte Energie umfasst die Gesamtmenge an Gas, die durch die Rohrleitungsanlagen transportiert wird. Dies umfasst sowohl das Volumen, das an die Endkunden verteilt wird, als auch das Volumen, das an andere Gasnetzbetreiber weitergeleitet wird (Rolle des zwischengeschalteten Transporteurs).

Betreiber von Gasanlagen (Rohrleitungsanlagen) mit einem Druck von mehr als 5 bar und einer Leitungslänge von über 15 Kilometern werden automatisch der Schutzstufe A zugeordnet. Bei anderen Gasnetzbetreibern wird der Durchschnittswert der transportierten Energie der letzten fünf Jahre berücksichtigt. Wenn dieser Wert höher als 2.600 GWh pro Jahr liegt, gilt dies auch als Schutzstufe A. Schutzniveau B liegt zwischen mehr als 400 GWh und bis und mit 2.600 GWh pro Jahr. Schutzniveau C gilt für einen Wert bis und mit 400 GWh pro Jahr. Um bei der Identifizierung des entsprechenden Schutzniveaus zu helfen, bietet Abbildung 9 eine grafischere Darstellung dieses Prozesses.

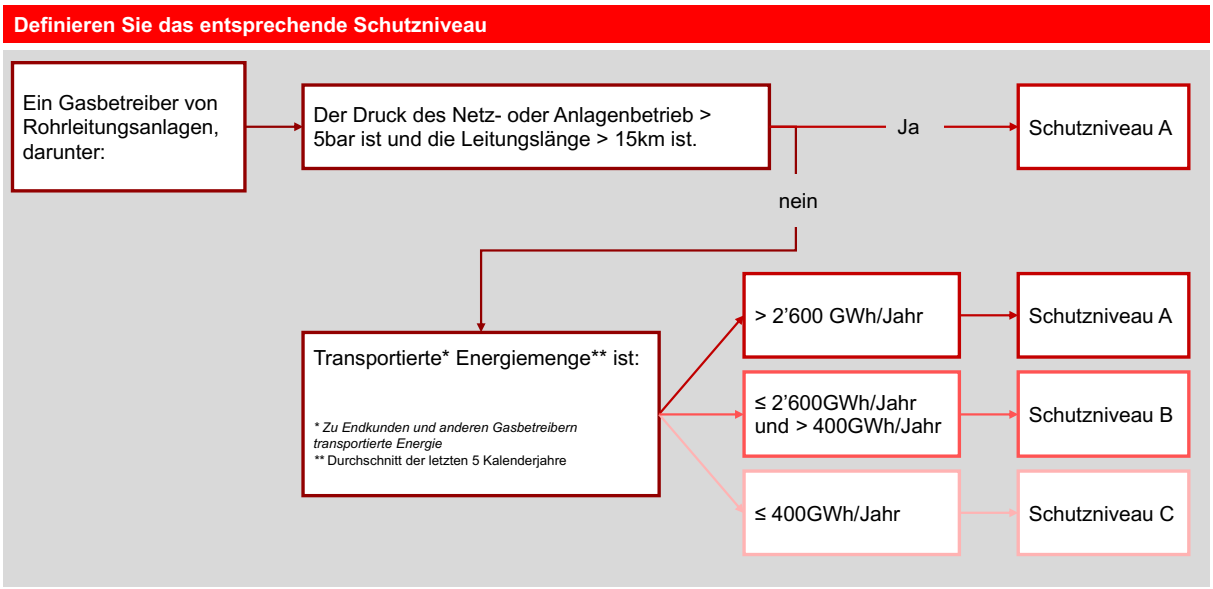

Abbildung 9: Definieren Sie das entsprechende Schutzniveau

5.2 Die Anforderungen an die Schutzniveaus

Die Schutzniveaus definieren die erreichenden Anforderungen an den Maturitätsstufe der Massnahmen des *NIST Framework Implemetions Tiers*, die im IKT-Minimalstandard für die Gasversorgung 2.0 behandelt werden. Die Anforderungen der Schutzstufe A sind die strengsten und richten sich an die wichtigsten Unternehmen der Gasversorgung. Die Niveaus B und C beinhalten niedrigere Anforderungen, sie gelten für mittlere und kleine Akteure. Die Anforderungen werden anhand der verschiedenen Maturitätsstufe (*Tiers*) definiert, wie es in Kapitel 4.5 beschrieben wird.

Nur ungefähr vierzig der hundertacht Massnahmen, die dieser IKT-Minimalstandard umfassen, sind für das Schutzniveau C erforderlich. Nur die höher priorisierten Massnahmen sind aufgrund des Grundsatzes der Verhältnismässigkeit davon umzusetzen. Weiter sind Massnahmen, die nicht zwingend vorgeschrieben sind, werden jedoch weiterhin dringend zur Umsetzung empfohlen.

Die folgenden Maturitätsstufe müssen mindestens erreicht werden:

Massnahmen	Schutzniveau A	Schutzniveau B	Schutzniveau C
Identifizieren (ID = Identify)			
ID.AM-1	3	3	3
ID.AM-2	3	3	2
ID.AM-3	3	3	2
ID.AM-4	3	3	–
ID.AM-5	3	3	–
ID.AM-6	3	4	3
ID.BE-1	3	2	–
ID.BE-2	3	2	–
ID.BE-3	3	3	–
ID.BE-4	3	3	–
ID.BE-5	3	2	–
ID.GV-1	3	4	3
ID.GV-2	3	3	3
ID.GV-3	3	4	3
ID.GV-4	3	3	–
ID.RA-1	3	2	–
ID.RA-2	3	3	–
ID.RA-3	3	3	–

Massnahmen	Schutzniveau A	Schutzniveau B	Schutzniveau C
ID.RA-4	3	3	–
ID.RA-5	3	2	–
ID.RA-6	3	2	–
ID.RM-1	3	2	–
ID.RM-2	2	3	–
ID.RM-3	2	3	–
ID.SC-1	3	3	–
ID.SC-2	3	3	–
ID.SC-3	2	3	3
ID.SC-4	2	2	–
ID.SC-5	3	2	–
Schützen (PR = Protect)			
PR.AC-1	3	3	2
PR.AC-2	3	3	2
PR.AC-3	4	4	3
PR.AC-4	3	3	2
PR.AC-5	3	3	2
PR.AC-6	3	3	2
PR.AC-7	3	3	2
PR.AT-1	4	3	3
PR.AT-2	4	3	3
PR.AT-3	3	3	–
PR.AT-4	4	3	3
PR.AT-5	3	3	–
PR.DS-1	4	2	–
PR.DS-2	3	4	2
PR.DS-3	2	3	–
PR.DS-4	2	2	–
PR.DS-5	3	2	–
PR.DS-6	3	2	–
PR.DS-7	3	2	–
PR.DS-8	2	2	–
PR.IP-1	4	2	2
PR.IP-2	2	3	–
PR.IP-3	3	3	–
PR.IP-4	4	4	3
PR.IP-5	3	4	3
PR.IP-6	2	3	–
PR.IP-7	2	2	–
PR.IP-8	2	2	–
PR.IP-9	3	2	2
PR.IP-10	3	2	–
PR.IP-11	3	2	–
PR.IP-12	3	2	–
PR.MA-1	2	3	–
PR.MA-2	2	3	2
PR.PT-1	3	2	–
PR.PT-2	3	4	3
PR.PT-3	3	3	–

Massnahmen	Schutzniveau A	Schutzniveau B	Schutzniveau C
PR.PT-4	4	3	3
PR.PT-5	3	2	–
Erkennen (DE = Detect)			
DE.AE-1	2	2	–
DE.AE-2	3	2	–
DE.AE-3	3	2	–
DE.AE-4	3	2	–
DE.AE-5	3	2	–
DE.CM-1	3	3	2
DE.CM-2	2	3	2
DE.CM-3	2	2	–
DE.CM-4	3	3	2
DE.CM-5	3	3	2
DE.CM-6	1	2	–
DE.CM-7	3	2	2
DE.CM-8	4	2	–
DE.DP-1	3	4	2
DE.DP-2	3	2	–
DE.DP-3	3	3	–
DE.DP-4	2	2	–
DE.DP-5	3	2	–
Reagieren (RS = Respond)			
RS.RP-1	3	3	2
RS.CO-1	2	3	2
RS.CO-2	3	4	2
RS.CO-3	3	2	–
RS.CO-4	2	2	–
RS.CO-5	2	2	–
RS.AN-1	3	3	–
RS.AN-2	2	3	–
RS.AN-3	3	2	–
RS.AN-4	2	2	–
RS.AN-5	2	2	–
RS.MI-1	3	3	2
RS.MI-2	3	2	2
RS.MI-3	3	2	2
RS.IM-1	3	3	–
RS.IM-2	3	3	–
Wiederherstellen (RC = Recover)			
RC.RP-1	3	3	2
RC.IM-1	3	2	–
RC.IM-2	3	2	–
RC.CO-1	2	1	–
RC.CO-2	2	1	–
RC.CO-3	2	1	–

Tabelle 24: Anforderungen, die für jedes Schutzniveau erreicht werden müssen

6 Anhänge

6.1 Glossar

Abkürzung	Beschreibung
BABS	Bundesamt für Bevölkerungsschutz
BACS / NCSC	Bundesamt für Cyber-Sicherheit / Nationales Zentrum für Cybersicherheit
BFE	Bundesamt für Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)
BWL	Bundesamt für wirtschaftliche Landesversorgung
DMZ	Demilitarized Zone, Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten (wird oft benutzt, um eine logische Trennung zwischen zwei Netzwerkzonen sicherzustellen)
DRM	Druckreduzier- Messstation
EDI	Electronic Data Interchange
ENISA	European Union Agency for Network and Information Security
ERI	Eidg. Rohrleitungsinspektorat
ERP	Enterprise Ressource Planning-System
ICS	Industrial Control Systems
IKT	Informations- und Kommunikationstechnologie (dt. elektronische Datenverarbeitung EDV)
IP	Internet Protocol
ISA	International Society of Automation
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnologie, hier insbesondere Office-IT / Büroautomation. Alles was nicht OT betrifft.
Kommunikationsnetzwerk	Netzwerk des zur internen Daten- und Sprachkommunikation.
MELANI	Melde- und Analysestelle Informationssicherung (Informatiksteuerungsorgan des Bundes)
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NIST	National Institute of Standards and Technology
OT	Operational Technology (insbesondere SCADA-Systeme)
PC	Personal Computer
PLC	Programmable Logic Controller
Produktionssteuerung	Siehe SCADA
SCADA	Supervisory Control and Data Acquisition, Überwachen und Steuern technischer Prozesse. Zum SCADA-System gehören neben der Steuerung und Überwachung auch die Sensoren, Leitungen, Computer und Leitstelle des (Produktions-) Systems. Gemeint sind insbesondere Kommissioniersysteme, Produktionssteuerungssysteme der Verarbeiter, sowie Kassensysteme der Detailhändler. Der Begriff "SCADA" wird hier synonym zum Begriff "ICS" verwendet.
SVGW	Fachverband für Wasser, Gas und Wärme

Abkürzung	Beschreibung
TISG	Technisches Inspektorat des Schweizerischen Gasfaches
VoIP	Voice over IP
VPN	Virtual Private Network
VSG	Verband der Schweizerischen Gasindustrie
WAN	Wide Area Network
WL	Wirtschaftliche Landesversorgung

6.2 Abbildungsverzeichnis

6.3 Tabellenverzeichnis

Impressum

Autor/Autorin der ersten Version (2020)

Name	Vorname	Organisation	Funktion
Peter	Sven	BWL	Hauptautor / Projektleitung
Caduff	Daniel	BWL	Co-Autor / Fachexperte / Quality Assurance
Ernst	Philippe	SVGW	Co-Autor / Fachexperte / Quality Assurance
Balmelli	Laurent	Kader der WL	Fachexperte / Quality Assurance
Modolell	Diego	SVGW	Fachexperte / Quality Assurance
Reichart	Karsten	SVGW	Fachexperte / Quality Assurance
Favarger	Hervé	SIG	Fachexperte / Quality Assurance
Cornu	Philippe	Holdigaz	Fachexperte / Quality Assurance
von Vivis	Marcel	Swisscom	Fachexperte / Quality Assurance
Häni	Reto	Deloitte	Fachexperte / Quality Assurance
Nyffeler	Gregor	EWZ	Fachexperte / Quality Assurance
Martin	Andre	GVM	Fachexperte / Quality Assurance
Munaron	Renato	A.EN	Fachexperte / Quality Assurance
Henry	Stéphane	OFEN	Fachexperte / Quality Assurance
von Ah	Matthias	Swissgas	Fachexperte / Quality Assurance
Angelini	Danilo	Transitgas	Fachexperte / Quality Assurance
Wolf	Andreas	EGO	Fachexperte / Quality Assurance
Rossat	Pierre-André	GAZNAT	Fachexperte / Quality Assurance

Autor/Autorin der zweiten Version (2024)

Name	Vorname	Organisation	Funktion
Peter	Sven	BWL	Hauptautor / Projektleitung
Käser	Hans-Peter	BWL / BACS	Co-Autor / Fachexperte / Quality Assurance
Räz	Barbara	BWL	Co-Autorin / Fachexpertin / Quality Assurance
Henry	Stéphane	BFE	Co-Autor / Fachexperte / Quality Assurance
Bonvin	Marc	BFE	Co-Autor / Fachexperte / Quality Assurance
Angelini	Danilo	Transitgas	Fachexperte / Quality Assurance
Bächtiger	Roger	ERI	Fachexperte / Quality Assurance
Breitschmied	Sandra	GVM	Fachexpertin / Quality Assurance
Cavegn	Dominik	EGO	Fachexperte / Quality Assurance
Decurtins	Daniela	VSG	Fachexpertin / Quality Assurance
Geiger	Christoph	Swissgas	Fachexperte / Quality Assurance
Korosec	Wolfgang	Stadt SG	Fachexperte / Quality Assurance
Kühni	Marcel	Regionalwerke	Fachexperte / Quality Assurance
Marra	Sylvia	Oiken	Fachexpertin / Quality Assurance
Menard	Caroline	SIG	Fachexpertin / Quality Assurance
Niehörster	Christof	VSG	Fachexperte / Quality Assurance
Reichart	Karsten	SVGW	Fachexperte / Quality Assurance
Monn	Remo	GAZNAT	Fachexperte / Quality Assurance
Schäfer	Charles	GVM	Fachexperte / Quality Assurance
Schüle	Roman	GVM	Fachexperte / Quality Assurance
Spörri	Hans	IBB	Fachexperte / Quality Assurance
Von Ah	Matthias	Swissgas	Fachexperte / Quality Assurance
Weber	Lukas	EGO	Fachexperte / Quality Assurance
Weber	Markus	Swissgas	Fachexperte / Quality Assurance
Wolf	Andreas	EGO	Fachexperte / Quality Assurance

Herausgeber

Fachverband für Wasser, Gas und Wärme SVGW
Grütlistrasse 44, CH-8027 Zürich
info@svgw.ch, https://www.svgw.ch/de
Telefon +41 44 288 33 33

Organisationen, die an der Entwicklung beteiligt sind:

Bundesamt für wirtschaftliche Landesversorgung (BWL),
Bundesamt für Energie (BFE),
Verband der Schweizerischen Gasindustrie (VSG) und
Fachverband für Wasser, Gas und Wärme (SVGW).