CYBERSICHERHEIT FÜR FERNWÄRME- UND FERNKÄLTEVERSORGUNGEN

NEU PUBLIZIERTER IKT-MINIMALSTANDARD

Immer mehr Industrieunternehmen automatisieren und vernetzen ihre Kontrollsysteme. Dadurch lässt sich zwar die Produktivität optimieren und alltägliche Aufgaben einfacher verrichten, aber die Cyberrisiken nehmen im gleichen Ausmass zu. Der neu publizierte «Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für die Fernwärme- und Fernkälteversorgung» unterstützt die Branche, ihre Widerstandsfähigkeit gegen Cyberrisiken zu erhöhen und sich gegen Angriffe zu wappnen.

Sven Peter, Bundesamt für wirtschaftliche Landesversorgung (BWL)
Stefan Güpfert, Schweizerischer Verein des Gas- und Wasserfaches (SVGW)*

RÉSUMÉ

CYBERSÉCURITÉ POUR L'APPROVISIONNEMENT DU CHAUFFAGE ET DU FROID À DISTANCE

La construction et l'extension des réseaux de chauffage et de froid à distance se poursuivent sans interruption en Suisse. Les réseaux thermiques acquièrent ainsi une importance systémique croissante pour l'alimentation du pays en chaleur et en froid. Dans ce contexte, ils attirent malheureusement aussi de plus en plus l'attention des cybercriminels qui essayent d'utiliser leur pertinence systémique accrue à des fins abusives (vol de données, chantage, etc.). C'est pourquoi l'Office fédéral pour l'approvisionnement économique du pays (OFAE) publie en collaboration avec la SSIGE et l'association Réseaux Thermiques Suisse (RETS) le standard de branche «Norme minimale pour garantir la sécurité des technologies de l'information et de la communication (TIC) requises pour l'approvisionnement du chauffage et du froid à distance» (recommandation SSIGE F1001). La norme minimale TIC est un programme d'amélioration de la cybersécurité. Ce programme permet aux exploitants de réseaux thermiques de se prémunir contre des erreurs de manipulation, d'améliorer le niveau de sécurité en cas de cyberattaque et de restaurer leurs systèmes si un accident se produit. Grâce à cette norme, les distributeurs de chaleur et de froid peuvent évaluer eux-mêmes leur profil de risque conformément aux particularités spécifiques à la branche des réseaux thermiques.

STEIGENDE BEDROHUNG DURCH CYBERRISIKEN

VERBREITUNG VON IKT

Die zunehmende Durchdringung und Vernetzung der Informations- und Kommunikationstechnologie (IKT) eröffnet unverzichtbare ökonomische wie auch gesellschaftliche Potenziale. Durch die fortschreitende Digitalisierung entstehen jedoch neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss.

Für kritische Infrastrukturen ist die Cybersicherheit von höchster Wichtigkeit. Gemäss der Nationalen Strategie zum Schutz kritischer Infrastrukturen 2018–2022 (SKI-Strategie) [1] des Bundes gilt die Fern- und Prozesswärme als einer von 27 kritischen Sektoren. Daher müssen diese Infrastrukturen angemessen geschützt werden. Den IKT-Systemen ist dabei besondere Beachtung zu schenken.

IKT-ABHÄNGIGKEIT

Wie die meisten anderen Industriebereiche sind auch die Betreiber von thermischen Netzen von IKT-Systemen abhängig. Die Vorteile der Digitalisierung liegen auf der Hand: Effizienzgewinne, höhere Verfügbarkeit der Anlagen sowie die Überwachung der Betriebsparameter. Allerdings erhöht die fortschreitende

** Kontakt: s.guepfert@svgw.ch, fernwaerme@svgw.ch* *(Titelbild: © AdobeStock)*

Digitalisierung auch die Komplexität des Versorgungsprozesses. So kann der Ausfall kritischer IKT-Systeme gravierende Auswirkungen auf den reibungslosen Betrieb der thermischen Netze haben und die Wärme- und Kälteversorgung in den betroffenen Gegenden, Städte oder Gemeinden des Landes stark beeinträchtigen.

BEDEUTUNG DER ICS

In der Fernwärme- und Fernkälteversorgung werden die meisten operativen Vorgänge durch ein industrielles Kontrollsystem (*Industrial Control System*, ICS) gesteuert. Diese Systeme bestehen aus mehreren Steuerkomponenten, die zu einer sicheren, zuverlässigen und nachhaltigen Energieversorgung zusammenwirken. Ihre Aufgabe ist es, die Daten verschiedener Prozesse oder den Zustand von Industriemaschinen zu erfassen und diese Maschinen vor Ort oder aus der Ferne zu steuern und zu überwachen. Dadurch kommt den ICS eine zentrale Bedeutung zu und sie müssen unbedingt gegen Cyberbedrohungen und Datendiebstahl geschützt werden (*Box*).

ICS-DETAIL: OT- UND IT-KONVERGENZ

ICS betrifft seit einigen Jahren weltweit alle Industriezweige. Um die Kosten zu senken und die Prozesskontrolle zu verbessern, verschmelzen die operativen Technologien (OT) vermehrt mit den Informationstechnologien (IT). Diese Konvergenz von IT und OT ermöglicht es, industrielle Systeme zu verbinden und zu automatisieren. In der Folge können nun OT-Anlagen, in denen ICS implementiert sind, mithilfe von Standard-IT-Kommunikationsprotokollen ferngesteuert werden. Die ICS erhöhen folglich die Produktivität auf Kosten der Sicherheit, da sie den externen Bedrohungen, die normalerweise IT-Geräte betreffen, stärker ausgesetzt sind. Das Ziel des IKT-Minimalstandards ist es daher, alle IKT-Geräte (sowohl IT als auch OT) ausreichend zu sichern und so zu gewährleisten, dass die ICS vor diesen «neuen» Risiken angemessen geschützt sind [2].

ZUNAHME VON CYBERANGRIFFEN

Dank Entwicklungen im Bereich digitaler Technologien lässt sich der Schutz der IKT-Systeme zwar grundsätzlich verbessern, aber gleichzeitig wachsen die Cyberrisiken. Dies stellt auch für die Fernwärme- und Fernkälteversorgungen eine zunehmende Bedrohung dar. Grösse oder Bedeutung eines Unternehmens spielen bei Cyberangriffen keine Rolle; häufig erfolgen sie zufällig oder geschehen dort, wo sich dafür «einfache Gelegenheiten» bieten. Aufgrund der fortschreitenden Digitalisierung werden solche Situationen immer häufiger auftreten.

SCHUTZ MIT DEM IKT-MINIMALSTANDARD

Eine wirksame Bewältigung der Cybersicherheitsprobleme erfordert ein klares Verständnis der aktuellen Sicherheitsherausforderungen sowie der verfügbaren Gegenmassnahmen. Der neu publizierte «Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für die Fernwärme- und Fernkälteversorgung» zeigt der Branche nicht nur Wege auf, sich vor Cyberangriffen zu schützen, sondern auch Möglichkeiten, sich nach einem Vorfall möglichst rasch wieder zu erholen. Innerhalb dieses Sicherheitsrahmens stufen Unternehmen ihr Risiko selbstständig ein und setzen geeignete Massnahmen um.

UMSETZUNG DES IKT-MINIMALSTANDARDS

Mit einem einheitlichen, standardisierten Vorgehen im Bereich Cybersicherheit können die Unternehmen ihre IKT-Systeme möglichst adäquat schützen und den Schutz zudem kontinuierlich ausbauen. Der IKT-Minimalstandard gibt praktische Handlungsanweisungen für die Umsetzung dieses Cybersicherheitsprogramms. Die für die thermischen Netze verantwortlichen Unternehmen sind angehalten, ihre Risiken mit dem IKT-Minimalstandard selbst zu identifizieren und ihre Risikobereitschaft selbstständig zu definieren. Sie können diesen Standard entsprechend ihrer Grösse und Ressourcen sowie den Bedrohungen, mit denen sie konfrontiert sind, umsetzen. Letztlich sei darauf hingewiesen, dass es in der eigenen Verantwortung der Unternehmen liegt, für einen sicheren Betrieb der thermischen Netze zu sorgen.

IKT-MINIMALSTANDARD UND BRANCHENSTANDARDS

ENTSTEHUNG DES IKT-MINIMALSTANDARDS

Der IKT-Minimalstandard ist ein Programm für die Cybersicherheit, das vom Bundesamt für wirtschaftliche Landesversorgung (BWL) im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) [3] ausgearbeitet wurde. Der Standard ermöglicht es jeder Organisation, ein akzeptables (Minimal-) Schutzniveau zu erreichen, das ihren Bedürfnissen und Ressourcen entspricht und sie angemessen gegen Risiken wappnet.

SCHAFFUNG VON BRANCHENSTANDARDS

Ursprünglich war der IKT-Minimalstandard ein allgemeines Programm für Cybersicherheit, das allen Organisationen, Unternehmen und Firmen zur Verfügung gestellt wurde. 2018 trat eine neue Version der NCS-Strategie mit neuen Zielen

Fig. 1 Erst gab es nur den allgemeinen IKT-Minimalstandard, später folgten die sektorspezifischen Minimalstandards, darunter für Trinkwasser, Gas und nun auch für thermische Netze.

in Kraft. Eine der neuen Aufgaben, die dem BWL übertragen wurden, ist die Erstellung von sektorspezifischen IKT-Minimalstandards (Branchenstandards). Dabei geht es darum, den allgemein gültigen IKT-Minimalstandard an die verschiedenen kritischen Sektoren zur Versorgung des Landes anzupassen, damit diese ein ausreichendes Sicherheitsniveau erreichen können, das ihren Besonderheiten Rechnung trägt *(Fig. 1)*. Zu diesem Zweck arbeitet das BWL mit einem oder mehreren Verbänden der betreffenden Branche zusammen, um ein qualitativ hochwertiges Dokument zu erstellen, das den Erwartungen und Bedürfnissen des jeweiligen Sektors entspricht. Im Fall des «Minimalstandards für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) für die Fernwärme- und Fernkälteversorgung» hat das BWL eng mit dem SVGW[1] (Empfehlung F1001) und Thermische Netze Schweiz (TNS [vormals VFS], IKT-Minimalstandard Fernwärme) zusammengearbeitet.

GEMEINSAMES CYBERSICHERHEITS-PROGRAMM DER BRANCHENSTANDARDS

Die Branchenstandards basieren alle auf dem gleichen Cybersicherheitsprogramm und empfehlen daher die gleichen Sicherheitsmassnahmen. Sie sind jedoch an die jeweilige Branche angepasst, indem sie deren kritische Aktivitäten identifizieren. Das gemeinsame Cybersicherheitsprogramm aller Branchenstandards erleichtert den Austausch zwischen den verschiedenen Sektoren. Zudem können dadurch Organisationen, die in verschiedenen Bereichen tätig sind (z. B. städtische Querverbundunternehmen), durchgehend die gleichenLösungen einsetzen. Die Identifizierung der kritischen Aktivitäten ermöglicht die Priorisierung bestimmter Massnahmen des Cybersicherheitsprogramms. Dadurch können Organisationen die für das Funktionieren ihrer Infrastruktur unerlässlichen Elemente gezielt sichern.

CYBERSICHERHEITSPROGRAMM: NIST FRAMEWORK CORE

RISIKOMANAGEMENT UND DEFENSE-IN-DEPTH

Der von BWL, TNS und SVGW erstellte IKT-Minimalstandard setzt das Cybersicherheitsprogramm *NIST Framework Core* [4] um. Dieses stützt sich auf zwei Konzepte: Risikomanagement und *Defense-in-Depth*-Strategie. Die Analyse eines akzeptablen Risikos ist für eine Organisation von entscheidender Bedeutung, da sie dadurch die Kernmassnahmen des *NIST Framework Core* an ihre eigenen Bedürfnisse anpassen kann (Branche, Grösse, Ressourcen und Bedrohungen).

Bei der *Defense-in-Depth*-Strategie wiederum handelt es sich um einen vom militärischen Prinzip abgeleiteten Ansatz, wonach ein komplexes, vielschichtiges Verteidigungssystem schwieriger zu überwinden ist als eine einfache Barriere. Ziel dieser Strategie ist es daher, mehrere Sicherheitsmassnahmen auf unterschiedlichen Schutzniveaus anzuwenden (die z. B. vom Netzwerkschutz über den Schutz physischer Elemente bis hin zur Ausbildung des Personals reichen) und so potenzielle Angreiferinnen und Angreifer zur Überwindung einer Vielzahl komplexer Sicherheitshindernisse zu zwingen.

GRUNDPRINZIPIEN DER CYBERSICHERHEIT

Im Bereich der Cybersicherheit gibt es drei Grundprinzipien, die die Einführung einer Sicherheitsrichtlinie regeln. Dabei handelt es sich um die Verfügbarkeit, Integrität und Vertraulichkeit von Daten.

Verfügbarkeit
Sicherstellen, dass die Informationen jederzeit verfügbar sind.

Integrität
Sicherstellen, dass die Informationen jederzeit vollständig und richtig sind.

Vertraulichkeit
Sicherstellen, dass die Informationen nur für autorisierte Personen oder Systeme zugänglich sind.

FUNKTIONEN DES NIST

Auch das *NIST Framework Core* baut auf diesen drei Grundprinzipen auf. Die Massnahmen des Programms zielen darauf ab, das Sicherheitsniveau in mindestens einem der drei Bereiche zu verbessern. Der Kern des *NIST Framework Core* besteht aus rund 100 Schutzmassnahmen, die in fünf Funktionen unterteilt sind: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen. *(Fig. 2)*.

IMPLEMENTIERUNGSEBENEN (TIERS) ZUR BEWERTUNG DER MASSNAHMEN

Jede der rund 100 Massnahmen kann auf einer Skala von 0 bis 4 bewertet werden *(Fig. 3)*. Das auf der Website des BWL verfügbare Bewertungs-Tool [5] hilft bei der Bestimmung der Implementierungsebene jeder einzelnen Massnahme. Es stellt verschiedene Profile zur Verfügung *(Fig. 4)*, die es ermöglichen, z. B. die in den verschiedenen Funktionen erreichten Schutzniveaus. Durch die visuelle Darstellung erhalten Unternehmen einen Überblick über ihr individuelles Schutzniveau vor Cyberrisiken und können die Stärken und Schwächen ihrer Cybersicherheit identifizieren. Massnahmen oder Funktionen, die unter ihren Erwartungen und

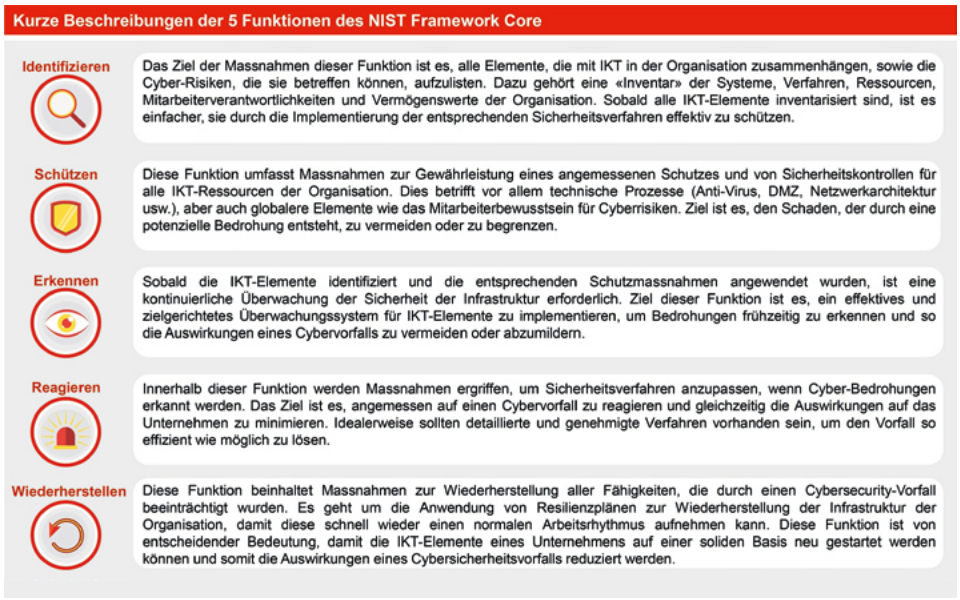

Fig. 2 Kern und Philosophie des NIST Framework Core.

[1] *BWL und SVGW haben bereits gemeinsam die IKT-Minimalstandards für Trinkwasser (Empfehlung W1018) und für Gas (Empfehlung G1008) erarbeitet und publiziert.*

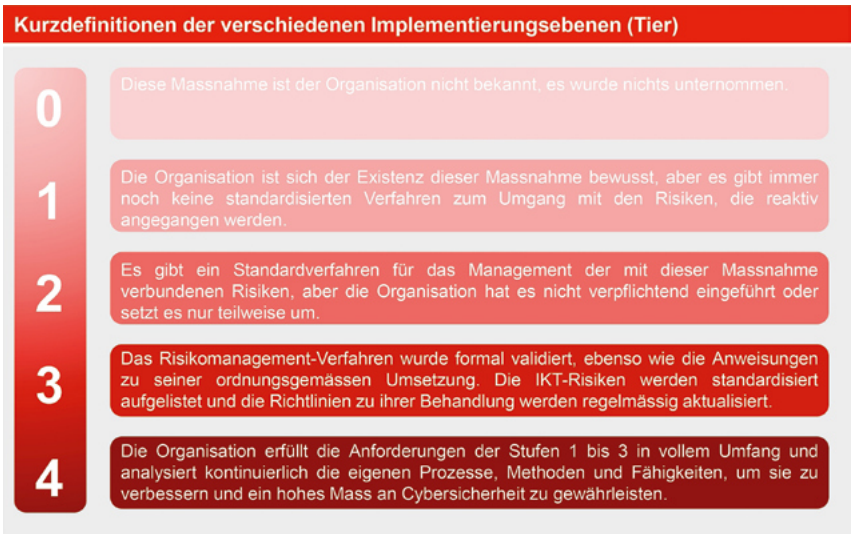

Fig. 3 Jede Massnahme kann auf einer Skala von 0 bis 4 bewertet werden.

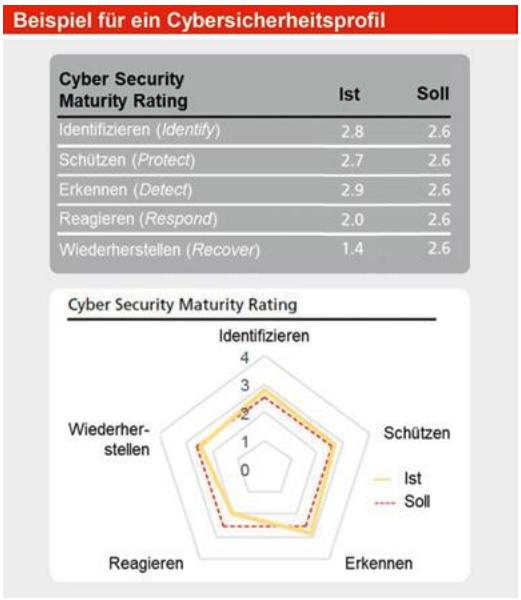

Fig. 4 Durch eine visuelle Darstellung (unten) erhalten Unternehmen einen schnellen Überblick über ihr individuelles Schutzniveau.

Anforderungen liegen, können, basierend auf diesen Erkenntnissen, durch die Implementierung konkreter Verbesserungen der Schutzlösung verbessert werden. Damit bildet die Bewertung der Massnahmen einen umfassenden Sicherheitsrahmen, der es Organisationen ermöglicht, ihr Sicherheitsprogramm kontinuierlich an ihre Bedürfnisse anzupassen.

KRITISCHE AKTIVITÄTEN

DEFINITION

Damit eine Aktivität als kritisch eingestuft wird, muss sie folgende Bedingungen erfüllen:

- Sie muss von IKT-Systemen abhängig sein (kann nicht manuell ausgeführt werden).
- Sie muss für den Versorgungsprozess unerlässlich sein, d. h., wenn sie nicht mehr ausgeführt wird, wird der gesamte Versorgungsprozess der Organisation blockiert.
- Sie gefährdet im Falle einer IKT-Störung Menschenleben *(Safety)*.

AUTOMATISIERUNGSPYRAMIDE

Zum besseren Verständnis wurden die kritischen Aktivitäten den entsprechenden Ebenen der Automatisierungspyramide [6] zugeordnet. Mit dem Konzept werden die verschiedenen IT-Ebenen (Anwendungen und Systeme) klassifiziert *(Fig. 5)*. Mit Blick auf die generischen Konzepte der Automatisierung soll die Pyramide sichtbar und verständlich machen, welche Technologien innerhalb eines Industriesektors verwendet werden. Die Pyramide ist in fünf Ebenen unterteilt, die jeweils eine bestimmte Art von Information, das System oder einen Zeitpunkt im Prozess darstellen.

KRITISCHE AKTIVITÄTEN VON THERMISCHEN NETZEN

Zum besseren Verständnis der verschiedenen kritischen Aktivitäten bei thermischen Netzen *(Fig. 6)* wurden diese in zwei Gruppen unterteilt:

- Die erste Gruppe umfasst alle kritischen Aktivitäten organisatorischer Natur, also Tätigkeiten, die sich auf den Verwaltungsbetrieb einer Organisation auswirken.
- Bei der zweiten Gruppe handelt es sich um kritische Aktivitäten operativer Natur, die spezifisch mit den industriellen Prozessen zusammenhängen.

Die Unterscheidung zwischen organisatorischen und operativen Aufgaben ist im Zusammenhang mit der Konvergenz von Informationstechnologien (IT) und operativen Technologien (*Operational Technology*, OT) entscheidend.
Jede kritische Aktivität ist in *Figur 6* kurz beschrieben, sodass ihre Funktion auch ohne weitere Hilfsmittel verständlich ist. Ebenfalls werden die dafür jeweils notwendigen IKT-Systeme angegeben. Auch zeigt die Grafik, ob eine Aktivität in Bezug auf die Gefährdung von Menschenleben *(Safety)* relevant ist und auf welcher Ebene der Automatisierungspyramide sie

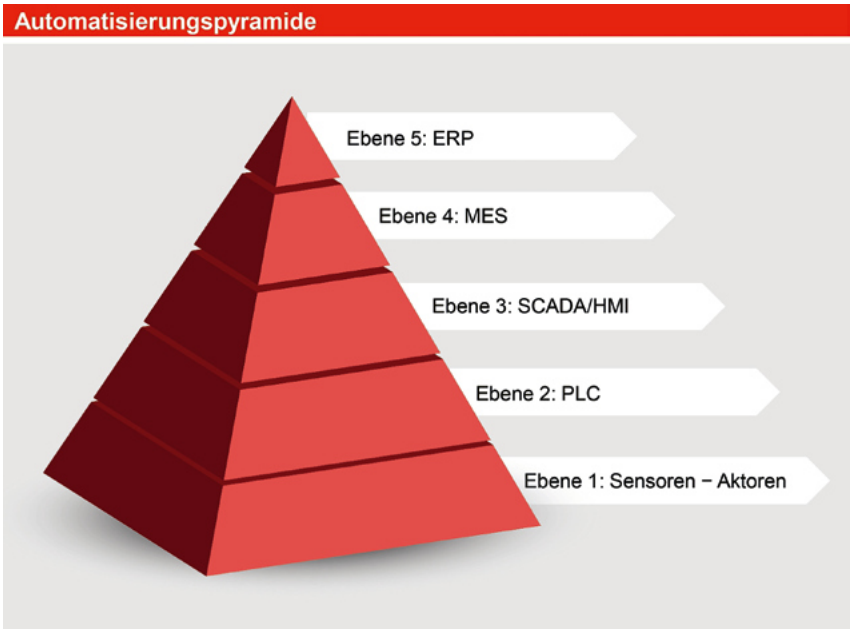

Fig. 5 Die Pyramide klassifiziert die verschiedenen IT-Ebenen eines Sektors.

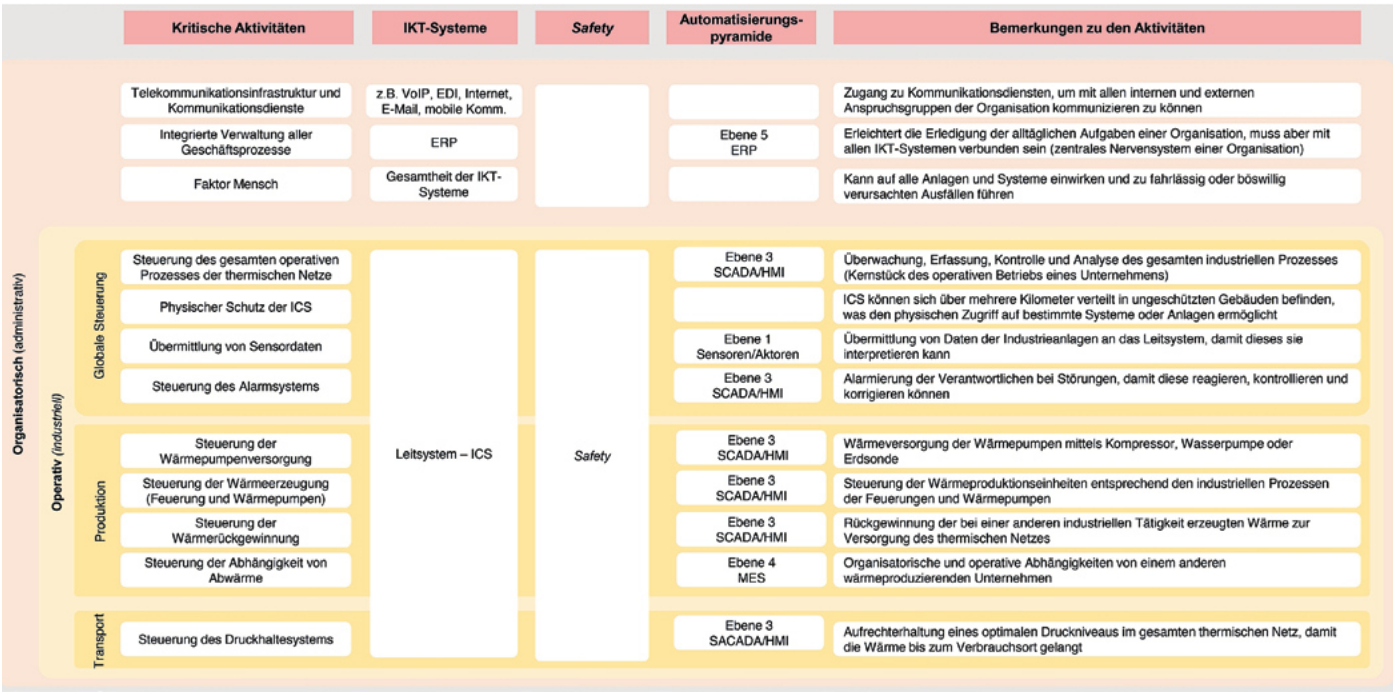

Fig. 6 Kurze, übersichtliche Beschreibung der kritischen Aktivitäten innerhalb von thermischen Netzen und die dazugehörigen IKT-Systeme.

angesiedelt ist. Es wird darauf hingewiesen, dass alle kritischen Aktivitäten im IKT-Minimalstandard für die Fernwärme- und Fernkälteversorgung in *Kap. 2.4* ausführlich erläutert werden.

ÜBERSICHT ÜBER DIE IM ARTIKEL VERWENDETEN ABKÜRZUNGEN

IKT	Informations- und Kommunikations-techologien
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
NIST	National Institute of Standards and Technology
ICS	Industrial Control System
IT	Information Technology
OT	Operation Technology
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken
ERP	Enterprise Resource Planning
MES	Manufacturing Execution System
SCADA	Supervisory Control and Data Acquisition
HMI	Human Machine Interface
PLC	Programmable Logic Controller
BWL	Bundesamt für wirtschaftliche Landesversorgung
TNS	Verband Thermische Netze Schweiz (ehemals Verband Fernwärme Schweiz)

FAZIT

Cybersicherheit sollte nicht als Zustand, sondern als dynamischer Prozess betrachtet und entsprechend angegangen werden. Mit anderen Worten: Eine absolute Sicherheit von IKT-Systemen ist nie erreicht. Sie ist ein Ziel, das ständig überprüft werden muss. Zudem sollte sie Gegenstand eines kontinuierlichen Verbesserungsprozesses sein.

Der Artikel gibt einen Überblick über den IKT-Minimalstandard, indem einige Themen der Cybersicherheit kurz behandelt werden. Wer sich eingehender mit dem Thema auseinandersetzen möchte, dem ist die Lektüre des IKT-Minimalstandard für die Fernwärme- und Fernkälteversorgung empfohlen. Er ist auf Deutsch und auf Französisch erhältlich und kann im SVGW-Shop kostenlos als Empfehlung F1001 heruntergeladen werden.

www.svgw.ch/shopregelwerk

BIBLIOGRAPHIE

[1] *Bundesrat (2017): Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022*

[2] *Balmelli, L. (2020): «Build a Cyber Security Program for Industrial Control Systems». Medium, 14 février 2020. https://medium.com/@laurentbalmelli/build-a-cyber-security-program-for-industrial-control-systems-5026064aa633 (20. Februar 2020)*

[3] *Informatiksteuerungsorgan des Bundes ISB (2018): Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022*

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

[5] *https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html*

[6] *Realpars (2018): «What is the Automation Pyramid?», 11. Juni 2018. https://realpars.com/automation-pyramid/ (Stand: 7.7.2022)*