Machbarkeits- und Vergleichsstudie sowie Auswahlkriterien bzgl. Lösungseinsatz für ein SIEM-Betriebskonzept mit Schwerpunkt Angriffserkennung/-vermeidung (gemäß EnWG §11 (1d) und BSIG § 8a (1a))

Ver. 1.0

Schutzklasse: vertraulich!

Herausgegeben von der CONTROLNET GmbH

Von Dipl.-Ing. René Fiehl,

unter Mitarbeit von Dipl.-Soz.päd. (BA) Steffen Otto und M. Sc. pol. René Seidel.

August 2022, 151 Seiten, 73 Abbildungen,
mehr als 50 quantitative Vergleichs- bzw. Bewertungskriterien in der Produktmarktstudie

Zweck

Die Ergebnisse der Studie sind zur Information bestimmt. Sie entsprechen dem Kenntnisstand der Autoren zum Zeitpunkt der Veröffentlichung.

Vertraulichkeit

Autorisierte Nutzer des Dokumentes müssen einen Fremdzugriff eigenverantwortlich vermeiden. Es gelten die jeweils gültigen gesetzlichen Bestimmungen und Verpflichtungen zur Vertraulichkeit, zum Fernmelde- und Datengeheimnis, Datenschutzgesetze und Verordnungen (DSGVO, BDSG neu) sowie arbeitsrechtliche und unternehmensinterne Festlegungen in besonderem Maße.

Urheberrecht, Nutzungsrecht

Alle Rechte vorbehalten. Die unerlaubte Weitergabe, Verbreitung und Kopieerstellung stellt einen Urheberrechtsverstoß (§ 106 UrhG) dar.

Mit dem Erwerb der Studie erhält der Käufer ein nicht ausschließliches, nicht übertragbares, örtlich unbeschränktes und zeitlich unbegrenztes Nutzungsrecht an den Studieninhalten und -ergebnissen. Der Käufer ist berechtigt, zur internen Nutzung, in der zugelassenen Organisationseinheit, entsprechende Arbeitskopien zu erstellen.

Dem Käufer wird eingeräumt, Teile der Studie, auszugsweise gemäß Minimalprinzip und unter Wahrung der besonderen Schutzinteressen des Herausgebers, unter Angabe der Quelle wörtlich zu zitieren, wenn dies zur Erläuterung in der Stakeholdersphäre des Käufers erforderlich ist (vgl. § 51 UrhG). Bei einem solchen wörtlichen Zitat ist eine Quellenangabe gemäß § 63 UrhG erforderlich, die neben den urheberrechtsrelevanten Daten (Werk, Autor, Herausgabe) auch die genaue Fundstelle (z.B. Seitenzahl) enthält.

Das Nutzungsrecht gilt ausschließlich für den im Kaufvertrag bzw. im Rechnungsdokument bezeichneten Nutzungsnehmer und ausschließlich nur für dessen gültige Organisationseinheit zum Erwerbszeitpunkt der Studie. Davon nicht gedeckt sind weitere Konzerngesellschaften, Holdingstrukturen, Beteiligungsunternehmen und Tochtergesellschaften.

Ein übertragbares Nutzungsrecht kann mit dem Urheber/Herausgeber vertraglich vereinbart werden.

Nur der Urheber besitzt das ausschließliche Recht, sein Werk in unkörperlicher Form öffentlich wiederzugeben (Recht der öffentlichen Wiedergabe (§ 19a UrhG).

Haftungsausschluss

Die in diesem Dokument zur Vergleichsführung herangezogenen Lösungen der bezeichneten Hersteller wurden nach bestem und verfügbarem sowie zugänglichem Wissen beschrieben. Die vorgenommenen Bewertungen basieren auf öffentlich verfügbaren Informationen (Hersteller-Websites/Produktbeschreibungen, Presse- und Testbeiträge, Tagungspräsentationen, etc.), aus Teststellungsinstallationen, aus in aktivem Nutzungsbetrieb befindlichen Lösungen bei Referenzanwendern sowie auf Kauf- bzw. Projektanfragen, welche an Hersteller gerichtet wurden und darüber hinaus auch aus Rückmeldungen von zuverlässigen Fachquellen in entsprechenden Branchen- und Facharbeitskreisen. Es kann keine Gewähr für Voll-

Explizit wird darauf hingewiesen, dass mit dieser Studie keine Rechtsberatung gegeben wurde.

Marken- und Warenzeichen

Die in dieser Studie wiedergegebenen und gegebenenfalls durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

LEITMOTTO

für das Fachgebiet der Informationssicherheit und IT-Sicherheit
sowie für den Kontext dieser Arbeit:

›› Wenn ich etwas kennenlernte,
so betrachtete ich es nie als endgültig abgeschlossen,
sondern stets als verbesserbar. ‹‹

Professor Manfred von Ardenne

Wegbereiter moderner Broadcastmedien und Informationsübertragungen,
Erfinder des elektronischen Fernsehgerätes und des Raster-Elektronenmikroskopes

Vorwort

Unsere Experten für Leitsystem- und Feldleittechnik-Infrastrukturen sowie für OT-Netzwerke und Hochsicherheits-Lösungen sind insbesondere durch die Branchengruppe von Energieversorgern und Netzbetreibern (kritische Infrastrukturen) in den letzten Jahren sehr stark in verschiedenen Projekten, bei namhaften Unternehmen, von Übertragungsnetzbetreibern und Verteilnetzbetreibern bis hin zu Stadtwerken und deren Netzbetreiberstrukturen, tiefgründig involviert. Hier wurden Konzepte und Realisierungen zur Einführung und zum Betrieb sowie zur Verbesserung von Informationssicherheitsmanagementsystemen (ISMS) und zur Umsetzung von IT-Sicherheitsmaßnahmen von unserer Sparte „Consulting, Engineering und Audit“ umgesetzt.

Parallel und verzahnend wurden von unserer Sparte „Industrial & Energy Solutions“ Konzepte und Planungen sowie Realisierungen von zeitgemäßen und zukunftsfähigen Leitsystem- und Feldleitnetzwerken, Sicherheitsinfrastrukturen und deren Managementumgebungen (Monitoring, NOC, SOC) praktisch umgesetzt. Mit unserem „Neuen, flexiblen IEC61850-Netzwerk-Design“ haben wir alle unsere Kompetenzen genutzt, um für einen zentralen Verteilnetzbetreiber in den letzten 30 Monaten mehr als 12 Vorhaben im Bereich der Modernisierung von 110kV-Umspannwerken und deren OT-Netzwerk- und Security-Infrastrukturen, von der Stations-, Feld- und Prozessbusebene bis hin zu den Übergaben an die zentralen Informationsknoten und zum redundanten Leitsystem zu realisieren und diese, in Zusammenarbeit mit den arrivierten Herstellern der Feld- und Schutztechnik, erfolgreich in Betrieb zu setzen. Hierbei wurden mehr als 500 Switch- und Security-Komponenten verbaut, in Betrieb gesetzt und mit den aktuell erforderlichen und skalierbaren Sicherheitskonzepten und -funktionen versehen. Es wurden u.a. die deterministischen Protokolle MRP, HSR und PRP sowie im WAN-Transit die Protokolle EoSDH und MPLS eingesetzt.

Aus der Symbiose unserer erfahrenen genannten Sparten liegen nunmehr „brandaktuelle“, umfassende Technologie-, Hersteller- und Praxiserfahrungen vor, welche wir im Zusammenhang mit der Terminfrist des BSI zur Einführung von Angriffserkennung und -vermeidung bis zum 01.05.2023 (Vgl. EnWG §11 (1d) bzw. BSIG § 8a (1a)) zur Verfügung stellen möchten. Dies erfolgt vor dem Hintergrund, dass bisher vom BSI keine gültige Orientierungshilfe vorliegt und erst zum Herausgabezeitpunkt dieser Studie der „Community Draft einer Orientierungshilfe“ am 13.06.2022 veröffentlicht wurde. Somit konnten wir den „Community Draft der Orientierungshilfe“ bereits einer Bewertung unterziehen, welche in der vorliegenden Studie enthalten ist und welche wir in den Zusammenhang mit einer realistischen Strategie zur Erreichung einer sinnvollen „Erstwirksamkeit“, unter umfassender Erläuterung der Umfänge für eine tatsächliche, nur sukzessive zu erreichende „Vollwirksamkeit“ stellen.

Unsere Bewertungen und Konzeptvorschläge stützen sich vollständig auf die Interaktion mit unseren Kunden in der Bundesrepublik Deutschland, die hiesigen Regularien und Organisations- und Funktionsprozesse sowie die involvierten Stakeholder. Unter Wertschätzung und Kenntnis der global als Benchmark herangezogen Marktstudien von Gartner, für in Frage kommende Hersteller und Lösungen, wählen wir das Vorgehen, einer eigenen, von Pragmatik und Wirksamkeit gezeichneten Expertenbewertung unter den vorgenannten Erfahrungs- und Vernetzungsgrundlagen im spezifischen deutschen Markt.

Wir freuen uns, liebe Leser, mit dieser praxisorientierten Machbarkeits- und Vergleichsstudie die Lücke zwischen den allgemeinen Ausführungen der BSI-Orientierungshilfe zur Umsetzung von Angriffserkennungs- und -vermeidungssystemen hin zu praktisch durchführbaren Maßnahmen und Arbeitspaketen zu schließen und Ihnen damit eine Orientierung in dieser neuen und gewichtigen Anforderungs- und Sicherheitsdisziplin an die Hand geben zu können. Ebenso hoffen wir, dass wir Ihnen, vor dem anstehenden Fristhorizont zum 01.05.2023, wesentliche Zeitkontingente zur Einleitung eines zeitnahen Projekteinstieges eröffnen können, indem wir für Sie eine pragmatische Hersteller- und Produktbewertung verwertbar zur Seite stellen und Ihnen damit ermöglichen, konkrete Schutzmaßnahmen für Ihre Infrastrukturen und für Ihr Geschäftsmodell schnell und nachweisbar, mit einer Programmatik sowie den, für sie angepassten und wirksamen Funktionen sowie einem darauf basierenden stetigen Verbesserungskonzept umsetzen zu können.

Die Betrachtungen und Ergebnisse in der vorliegenden Studie sind auch auf andere Branchen vollständig und im Sinne der Aufrechterhaltung von Geschäftskontinuität und Wettbewerbsfähigkeit anwendbar.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre und die Ableitung eines für Ihre Struktur und Erfordernisse angemessenen und wirksamen Umsetzungskonzeptes.

Weimar, im August 2022

René Fiehl
Steffen Otto
René Seidel

Inhalt

1 Management Summary

Der erforderliche Einsatz von zeitgemäßen Informations- und Automationstechnologien zur sicheren Netzführung und zum sicheren Schnittstellenaustausch in der Energiewirtschaft sowie deren weiterer Ausbau bildet eine wesentliche Grundlage für die erfolgreiche Geschäftsfähigkeit dieses gesellschaftlichen Infrastrukturbereiches zur Daseinsvorsorge (Public Services) und die diesem Geschäftsfeld anhängige komplexe Regulariensphäre und Stakeholderlandschaft.

Es ist bekannt, dass durch die zunehmende Erhöhung digitaler Funktions- und Geschäftsprozesse in Gesellschaft und Wirtschaft auch das Schwachstellen- sowie Bedrohungspotential und damit die Risiken durch automatisierte, ungezielte sowie gezielte Angriffe sowie durch den Eintrag von Schadcode massiv ansteigen. In nie dagewesener Art und Weise sind in den Jahresscheiben 2019 bis 2022 vorbezeichnete Schwachstellen, durch Angriffe und Schadcodeeintrag sowie folgenden Datenverlust oder -diebstahl, ausgenutzt worden, mit dem Ergebnis, das eine beträchtliche Anzahl namhafter Unternehmen, Behörden, Institute, Politiker und auch Privatpersonen penetriert wurden und hierbei immense Schäden für die Betroffenen sowie auch für deren Verantwortungsfeld- und Dienstleistungsbereiche entstanden sind. Ferner sind im globalen Maßstab nicht gewünschte Einflussnahmen auf Wirtschaft, Gesellschaft und das Finanzsystem durch, auf unsicheren Infrastrukturen basierenden Zugriffen, Diebstahl und Manipulation im digitalen Raum zu verzeichnen. Mit den nachfolgenden Nennungen sollen einige Belegbeispiele auf nationaler Ebene angeführt werden. Von Angriffen und z.B. der Einschleusung von Ransomware (Verschlüsselungstrojaner) waren z.B. betroffen: Technische Werke Ludwigshafen, Stadtwerke Wismar, Landkreis Anhalt-Bitterfeld, Abfallservice Landkreis Gotha, Kammergericht Berlin, Stadt Frankfurt/M., Tegut Lebensmittelkette, Autovermietung Buchbinder, Kranhersteller Palfinger, Automationsunternehmen Pilz, Funke Mediengruppe, Modeunternehmen Marco Polo, SRH-Klinik-Gruppe, verschiedene Unfallkassen-Institutionen bundesweit, welche kritikale, personenbezogene Sozialdaten verarbeiten, und viele mehr. Im internationalen Maßstab soll auszugweise auf nachfolgende Sicherheitsvorfälle mit enormen Schadensauswirkungen hingewiesen werden bei: Acer, Bombardier, Colonial Pipeline, Eversource Energy, United States federal government data breach.

Die Eigenverantwortung für das kritische Infrastrukturfeld der Energiewirtschaft gebietet, dass entsprechende Konzepte und Systeme durch die Betreiber zum Einsatz gebracht werden müssen, mit welchen derartige Angriffe detektiert und vermieden werden können, um die gesellschaftsrelevanten Infrastrukturen zur Daseinsvorsorge aufrecht zu erhalten. Hierzu hat die Bundesregierung im Juli 2015 das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 1.0) in Kraft gesetzt und daraus ist dann in der Folge, insbesondere für den KRITIS-Sektor der Energiewirtschaft, die Verpflichtung zur Einführung eines Informationssicherheitsmanagementsystems (ISMS), auf Basis des IT-Sicherheitskataloges 1a, zum 31.01.2018 sowie die Umsetzung des IT-Sicherheitsgesetzes 2.0 (IT-SiG 2.0) vom 18. Mai 2021 entstanden. Letzteres definiert explizit bestimmte Mindeststandards für KRITIS-Kernkomponenten und -Prozesse. Gemäß EnWG §11 (1d) besteht für Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als kritische Infrastruktur bestimmt wurden (BSIG § 8a (1a), die Verpflichtung zur Einrichtung von Systemen zur

Angriffserkennung und -vermeidung, mit einer Umsetzungspflicht bis zum 01.05.2023. Einher geht die Verpflichtung zur Aufbewahrung von anonymisierten Protokolldaten für einen Zeitraum von 18 Monaten, als Nachweisinstrumentarium an die BNetzA sowie das BSI.

In Folge der dargestellten Bedrohungslagen sowie unter den regulatorisch vorgegebenen Verpflichtungen besteht nun die Aufgabe zur Einführung einer angemessenen und wirkungsvollen Lösung zur Angriffserkennung und -vermeidung. Diese umfasst konzeptbedingt auch das Feld der Schwachstellendetektion, da es keine allumfassende Einzellösung gibt und vor allen Dingen auch interne Organisations- und Durchführungsprozesse, mit Verzahnung z.B. zum ISMS, einzubeziehen und zu etablieren sind. Anzumerken ist, dass es sich bei den einzuführenden Mechanismen zur Netzüberwachung, um Angriffe wirkungsvoll erkennen und abwehren zu können, um eine sehr komplexe Materie handelt. Sie ist in etwa vergleichbar mit der Netzführung und dem Netzbetrieb für die generischen Strom- und Gas-Verteilinfrastrukturen. Daraus kann abgeleitet werden, dass die Aufgaben nicht alleine durch Produkteinkäufe umgesetzt werden können, sondern damit umfassende Implementierungs- und Infrastrukturmaßnahmen sowie ein stetiger und langfristiger Betriebsführungsprozess im Zusammenhang stehen. Vor den oben aufgezeigten Umsetzungsfristen gilt es, eine angemessene Basis-Wirksamkeit (Erstwirksamkeit) nachzuweisen, deren Verbesserung in weiterfüh-

Die Betrachtungen in dieser Vergleichsstudie sind wesentlich und erforderlich, da es sich bei den zu tätigenden Investitionen in die betrachteten Kaufprodukte oder Open-Source-Lösungen um relevante Investitionen, Aufwände und daraus resultierende Betriebskosten handelt. Sie sollen somit als fundierte Entscheidungsgrundlage dienen.

2 Einführung

Das Erreichen eines hohen Sicherheitsniveaus stellt einen sukzessiven, lebendigen Prozess dar, für dessen Umsetzung es erfahrener Spezialisten bedarf. Ad-hoc-Maßnahmen erbringen nur minimale Effekte, was am Beispiel von 400.000! täglich neu hinzukommenden Schadcodeprogrammen verdeutlicht werden soll. Neben Schadprogrammen existieren eine Vielzahl weiterer, diffiziler Penetrations- und Störereignisse im Zusammenwirken Mensch, Unternehmen und Digitaler Raum. Zur wirksamen Absicherung bedarf es neben einer Digitalstrategie eines fundierten, nachhaltigen Sicherheitskonzeptes, welches die Grundlage für alle digitalen und existentiellen Funktionsprozesse des Unternehmens bildet.

Mit der Verpflichtung zur Einrichtung von Systemen zur Angriffserkennung und -vermeidung, mit einer Umsetzungspflicht bis zum 01.05.2023, kommt auf die betroffenen Netzbetreiber ein neues und sehr gewichtiges Prozess- und Technikfeld zu. Es lässt sich am besten mit der aktuell durch die Netzbetreiber umgesetzten Disziplin der Netzführung und des Netzleitstellenbetriebes, vom Grundkonzept her, vergleichen. Dieser Vergleich offenbart, dass zur Umsetzung, neben technischen State-of-the-Art-Systemen und -Lösungen, auch ein umfassendes Fachverständnis und Erfahrungen sowie Strukturen und Prozesse neu aufgebaut und bereitgestellt werden müssen.

Vor dem Hintergrund der in der Gesellschaft und Wirtschaft anstehenden Vakanzen bzgl. entsprechender hochspezialisierter Personalprofile stellt die Aufgabe für alle Größen der betroffenen Unternehmen eine Herausforderung dar, welche jedoch für den sicheren und stabilen Netzbetrieb, unabdingbar ist.

Vor dem Zeithorizont der Umsetzungsfrist gilt es nun zu eruieren und zu bewerten, welche Lösungen, in welchem Umfang sinnvoll und wirksam einzusetzen sind oder ob bereits erste Voraussetzungen vorliegen, mit einem anzupassenden Bestandskonzept in dieses gewichtige Aufgabenfeld einzusteigen.

nicht präsent bzw. wurde noch nicht in dieser Dimension praktiziert und muss nun, durch die regulatorisch verpflichteten KRITIS-Unternehmen, entsprechend neu etabliert und zukünftig eingeordnet werden.

Die nachfolgende Abbildung (Abb. 2-1) soll den sehr hohen Stellenwert von Informationssicherheit, als zentrale Dimension der Daseinsvorsorge, der Unternehmensexistenz sowie als Wettbewerbsvorteil, herausarbeiten und die betroffenen Ressourcenbereiche visualisieren.

Abb. 2-1: Informationssicherheit: Definition und Stellenwert

Das Informationssicherheitsmanagement, umzusetzen durch ein funktionsfähiges und wirksames ISMS sowie durch folgende ISMS-Praxistransformation (technische und organisatorische Detailumsetzungen) ist nunmehr zum Kernprozess- und Existenzmanagement avanciert. Damit repräsentiert es einen primären Geschäftsprozess und Erfolgsfaktor für die zunehmend digitalen Wirtschafts-

3 Studie

3.1 Ziel der Studie

Für die konkrete weiterführende Konzepterstellung zur regulatorisch auferlegten und verpflichtenden Einführung von Angriffserkennungs- und -vermeidungssystemen sollen relevante Zusammenhänge und Konzepte sowie mögliche Produkte (Lösungen) aufgezeigt und bewertet werden.

Ergänzend sollen aus der tiefen Kenntnis der Branchen Energie und Versorgung (Energy und Utility), deren Organisation und Prozessen sowie den vorhandenen technischen Bestandskonzepten, mögliche Handlungsempfehlungen oder auch Alternativen für eine pragmatische, stufenweise sowie wirksame und regulatorisch haltbare Zielerreichung herausgearbeitet werden.

Von zentraler Bedeutung bei den in dieser Studie beleuchteten Feldern, Herstellern und Produkten ist eine realistische und wirksame Transformation der Funktionen und Nutzenaspekte insbesondere für die in der Bundesrepublik Deutschland angewendeten Informationssicherheitsstandards DIN ISO/IEC 27001, DIN ISO/IEC 27019, ISO/IEC 27002:2013, ISO/IEC 27002:2022 und IEC 62443.

3.2 Scope der Studie

3.2.1 Sektoren und Branchen

Die Studie legt ihren zentralen Scope auf das Feld der Operational IT (OT) der nachfolgend bezeichneten Branchen und Einheiten:

- Kritische Infrastrukturbetreiber gemäß KRITIS-Rechtsverordnung vom 01.01.2022 (KRITIS-Verordnung 1.5 bzw. auch als KRITIS-Verordnung 2.0 bezeichnet), im Kontext definierter und aktualisierter Schwellenwerte für die Infrastrukturen,
- Energiewirtschaft (Strom, Gas, Öl, Fernwärme),
- Erzeugungsanlagen/Kraftwerke,
- Stadtwerke,
- Energienetzbetreiber,
- Versorgungsunternehmen sowie Handelsunternehmen für Strom und Gas,
- Hersteller und Zulieferer für diese Branchen.

Die o.g. Branchen werden gemäß den in 4.1 detailliert bezeichneten Regularien, gemäß Artikelgesetz IT-SiG 2.0, zur Einführung derartiger Systeme zum 01.05.2023 verpflichtet. Damit gehören diese Bereiche, neben z.B. Wirtschaftsbereichen, welche aus Eigeninteresse bereits über derartige Lösungen verfügen (z.B. Pharma-, Chipindustrie, Luftfahrt – siehe auch 2), zu den ersten Branchenfeldern in der Bundesrepublik Deutschland, die verbindlich mit derartigen technischen und organisatorischen Maßnahmen beauflagt sind.

Darüber hinaus sind die in der vorliegenden Studie geführten Betrachtungen vollständig anwendbar für die Sektoren (Branchen):

- Transport (Logistik),
- Verkehr (ÖPNV),
- Gesundheit,

- Automotive, u.a.

Nachfolgend erfolgt eine Wiedergabe der Definition des Begriffes „Kritische Infrastrukturen (KRITIS)“:

- *Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.*

Eine Übersicht der gesellschaftlichen, existentiellen und kritischen Infrastrukturbereiche findet sich in Abb. 3-1 (Vgl. auch KRITIS-V und UP-KRTIS, www.upkritis.de).

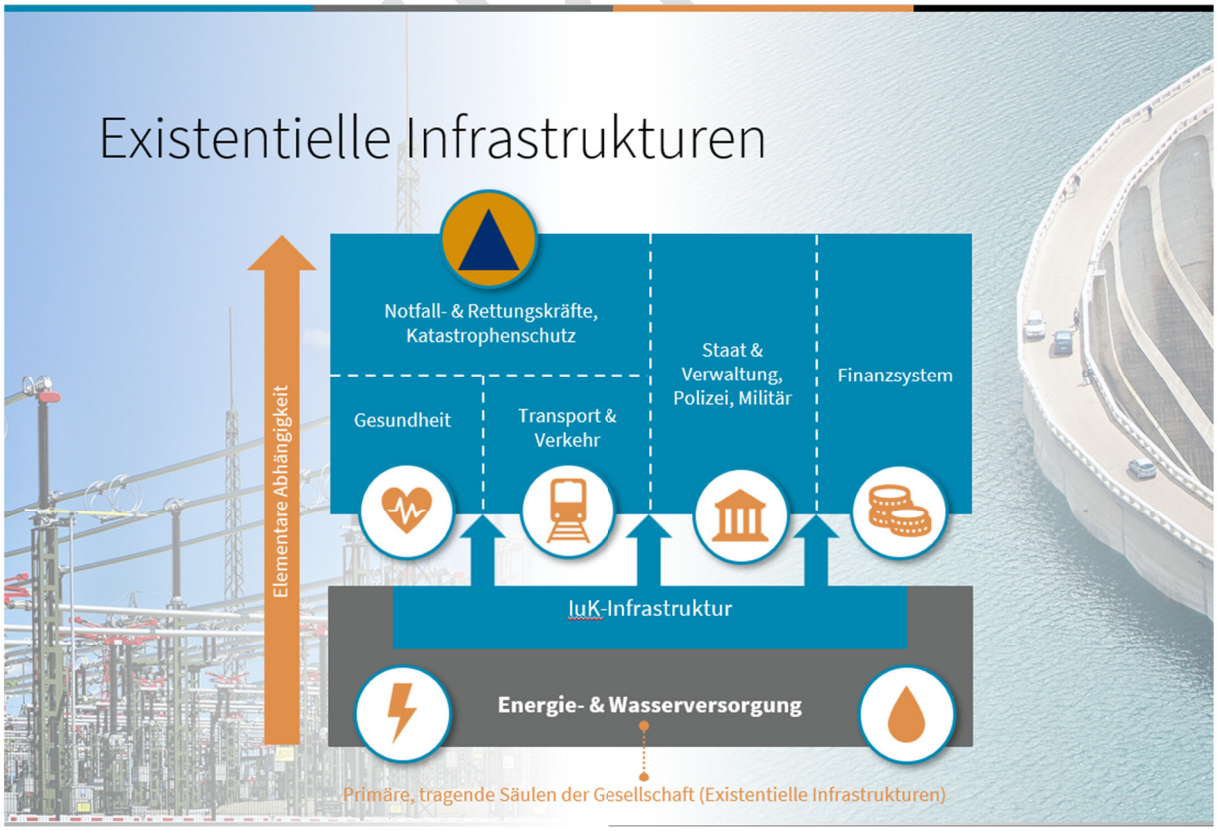


Abb. 3-1: Kritische Infrastrukturen (KRITIS-Sektoren) gemäß UP-KRITIS (IT-SiG 1.0)

Aufgaben und Verantwortung der KRITIS-Sektoren	
• Aufrechterhaltung gesellschaftlicher Funktionen und Ordnung (Daseinsvorsorge, Resilienz) • Gewährleistung der eigenen Geschäftsgrundlage und Schutz geistigen Kapitals	• Bereitstellung eines „Fundamentes“ für andere Nutzer (Institutionen, Kunden) und deren Dienste („Carrier“ für weitere gesellschaftliche Daseins-Funktionen).

Tab. 3-1: Übersicht wesentlicher Kernaufgaben der KRITIS-Bereiche

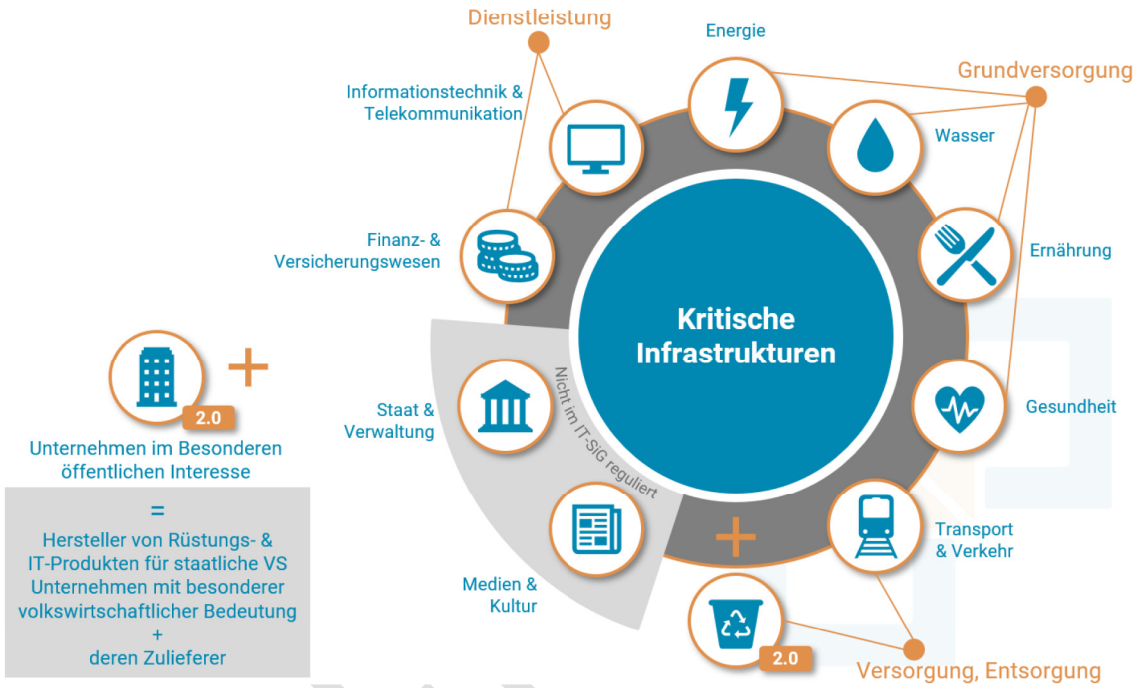


Abb. 3-2: Kritische Infrastrukturen (8 KRITIS-Sektoren) gemäß KRITIS-V (IT-SiG 2.0)

3.2.2 OT-Infrastrukturen für den sicheren Netzbetrieb

Zur Steuerung von Netz- und Anlagenführungsprozessen werden in Umspannwerken und Schalthäusern der Energieversorger und Netzbetreiber Stationsautomatisierungsanlagen (Fernwirktechnik, Schutztechnik) eingesetzt. Diese stellen die informationstechnische Verbindung zwischen den Betriebsmitteln der Primär- und Sekundärtechnik im Umspannwerk her und ermöglichen somit die Akkumulation und Verarbeitung von Messwerten, die Projizierung des Anlagen- und Netzabbildes in der zentralen Netzleitstelle und sie gewährleisten das korrekte und plausible Absetzen von Befehlen zur Prozesssteuerung (Ausführung von Schalthandlungen). Sie repräsentieren somit eines der wesentlichen Kernsysteme moderner Energieverteilungsanlagen. Nach dem eingeführten Informationssicherheitsmanagementsystem (ISMS) klassifizieren sich Stationsautomatisierungsanlagen, als Systeme zur Netzsteuerung, sowohl als Assetgüter (Anlagevermögen), als auch als Informationswerte (geistiges Kapital).

Stationsautomatisierungsanlagen sind aus technologischen Gründen sowie auch dem Betriebskonzept folgend sehr stark mit Informations- und Datenverarbeitungstechnologien (Hardware, Software, Netzwerk, Betreiberkonzept) durchsetzt. Diese Technologien sind zeitgemäß und

zukunftsfähig. Dementsprechend müssen Systeme der OT und Prozess-IT (PIT) höchste Anforderungen an die Informationssicherheit, die IT-Sicherheit und in Teilbereichen auch an den Datenschutz erfüllen.

Das verbindlich ab dem 31.01.2018 bei den Energieversorgern und Netzbetreibern einzuführende Informationssicherheitsmanagementsystem (ISMS) nach DIN ISO/IEC 27019 soll folgende Ziele maßgeblich unterstützen:

- die gesellschaftliche Daseinsvorsorge verbindlich und wirksam sicherstellen,
- Versorgungssicherheit gewährleisten,
- Informationen entsprechend ihrem Schutzbedarf handhaben.

Für den Bereich Netzführung ist ein jederzeit verfügbares sowie integres Netzabbild (Beobachtbarkeit) sowie die Steuerbarkeit des Netzes und der Betriebsmittel von immens hoher und existentieller Bedeutung. Dementsprechend muss sichergestellt werden, dass die Kernsysteme der Energieverteilung jederzeit hochsicher und sehr stabil betrieben werden können (IS/IT-Security, Safety).

Die vorliegende Studie und geführten Betrachtungen fokussieren sich auf folgende Zonen- und Infrastrukturbereiche der OT (Stationsautomatisierungsanlagen der Energieversorger und Netzbetreiber), gemäß Defense-in-Depth-Prinzip:

Sicherheitszone	Purdue-Referenzebene	Systembereich	Beispiele
Sehr hoch	Prozessebene	***Netzführungsinfrastrukturen PIT***	Netzleitstelle, Ersatznetzleitstelle, weitere zentrale Notfallsysteme
Hoch	Steuerungsebene	***Informationsknoten OT***	WAN-Netzwerke zur Datenübertragung von dezentralen Stationen an die zentrale Leitsysteminfrastruktur
Hoch	DMZ	***Transitnetzwerke***	Eigene oder externe Netzwerkressour-
	OT extern		Schnittstellenaustausch

Tab. 3-2: Übersicht der Sicherheitszonen der beteiligten Teilsysteme am sicheren Netzbetrieb

Anhand der aufgestellten Tabelle (Tab. 3-2) soll ein Sicherheitsgrundsatz verdeutlich werden, nachdem es gilt komplexe Systeme in Teilsysteme zu zerlegen, um diese beherrschbar zu machen und

3.4 Nutzen der Studie

Interessenten sowie die verpflichteten Branchen erhalten mit der vorliegenden Studie eine aktuelle Gesamtbetrachtung und Verknüpfung der erforderlichen Regularien, Prozesse und möglichen sowie wirksamen Technologien und Lösungen zur Etablierung und Aufrechterhaltung von Informationssicherheit und IT-Sicherheit durch Etablierung von Systemen zur Angriffserkennung und -vermeidung. Diese Systeme sollen mit der Einführung und einer nachhaltigen kontinuierlichen Verbesserung (Ausbau, Reifegradverbesserung) den Betrieb zur funktionalen und prozessualen Sicherstellung der zentralen und kritischen Infrastrukturen zur gesellschaftlichen Daseinsvorsorge verbindlich unterstützen und sicherstellen (sicherer Netzbetrieb gemäß IT-SiG 2.0).

Die Inhalte und Ergebnisse der Studie können den Aufstellungsprozess sowie die Etablierung von Systemen zur Angriffserkennung und -vermeidung inhaltlich und insbesondere unter Zeitaspekten stark befördern (Einführungsfrist zum 01.05.2023). In diesem Zusammenhang stehen die nachfolgend bezeichneten Effekte und Nutzenoptionen, in Weiterverwertung der Ergebnisse, zur Verfügung:

1. Schnelle Absicherung und Erreichung eines adäquaten Sicherheitsniveaus der Infrastrukturen zur gesellschaftlichen Daseinsvorsorge (Herstellung einer sinnvollen Erstwirksamkeit),
2. Wesentliche Einsparung von Zeit und Terminmaßnahmen im Zusammenhang mit der Anbieter- und Lösungsauswahl für Angriffserkennungs- und -vermeidungssysteme, vor dem zeitnah anstehenden Fristhintergrund zur Einführungsverpflichtung am 01.05.2023,
3. Effektive und zielführende Aufstellung eines Kernteams zur Konzept- und Lösungseinführung auf Basis der vorbereiteten Inhalte und Herstellen einer schnell verfügbaren und gemeinsamen Handlungs- und Faktengrundlage,
4. Know-how-, Konzept- und Verfahrensunterstützung zur Lösungsbeurteilung und zur Anbieterbewertung,
5. Umfassende Bereitstellung von Bewertungskriterien zum Lösungsvergleich (Produktmarktstudie),
6. Planungs- und Ausschreibungsunterstützung: konkrete Inhalte und Aufbereitungen verwendbar als Ausschreibungsrahmen,
7. Einordnung der Funktionen und Zusammenhänge sowie der erforderlichen Aufgaben zur Überwachung, Auswertung und Reaktion, im Rahmen des Incident Managements (SIEM und SOC),
8. Systematische und kontinuierliche Verbesserung des Reifegrades von Informationssicherheit und IT-Sicherheit (Härtung und Prüfung),
9. Etablierung und Ausbau eines Analyse-Grid zur Detektion von kritischen Ereignissen,
10. Erhöhung von Business Continuity und Resilienz,
11. Bereitstellung und Verbesserung von Nachweisen für umgesetzte und zu verbessernde Maßnahmen, als Audit-Nachweise für entsprechende Informationssicherheitsstandards und -managementsysteme.

Zusammenfassend können mit den in der vorliegenden Studie durchgeführten Betrachtungen, die folgenden, existentiellen Sicherheits- und Stabilitätsfunktionen, im Rahmen eines realistischen und wirksamen Umsetzungsprozesses, bereitgestellt werden:

- Visibilität schaffen (Protokollieren und Detektieren),
- Business Continuity sicherstellen und Resilienz schaffen (Vertraulichkeit, Integrität, Verfügbarkeit),
- nicht ausschließbare Notfälle und Havarien planbar und mit einer offensiven Sicherheitsstrategie begegnen (Reagieren).

3.5 Positionierung zu Mindestanforderungen

Häufig werden von durch Regularien verpflichteten Wirtschaftsbereichen Fragen nach einer Bereitstellung einer Handlungsanleitung zur Umsetzung von „Mindestanforderungen“ an Regulierer und Dienstleister gestellt. Wir erachten dieses Vorgehen, im Kontext IS/IT-Sicherheit, nicht als tatsächlich zielführend, zur Erreichung eines hohen sowie resilienten Funktions- und Sicherheitsstatus an die Anlagen, Applikationen und zu Grunde liegenden Netze. Der Begriff „Mindestanforderungen“ impliziert leider zu oft, eine reine Nachweisführung (umgangssprachlich: „Persilschein“) zu betrachteten Maßnahmen, welche aber noch nicht oder nur in geringem Umfang realisiert wurden und dementsprechend wenig Schutz und Erstwirksamkeit liefern. Besser ist es, wenn ein Konzept und die dazu gehörenden Anwendungen (Tools) eine tatsächlich messbare und damit belegbare Erstwirksamkeit bereitstellen können. Sollten dabei das verwendete Konzept und die Produkte sinnvolle

Um diese Empfehlung nochmals zu untersetzen, werden anbei einige ausgewählte Treiber einer solchen Philosophie aufgeführt, für welche es sich lohnt, dieses Konzept zu etablieren und aufrecht zu erhalten:

- Schutz der geistigen Werte eines Unternehmens (Know-how, Prozesse, Patente, Netzelemente Risiken, Zusammenhänge, …),
- Marktführerschaft erlangen und ausbauen,
- Wettbewerbsfähigkeit sichern,
- Aufrechterhaltung von Reputation,
- Unterstützung und Absicherung wichtiger externer Experten- und Dienstleiterzugriffe,
- Übergang von einer defensiven, hin zu einer offensiven Sicherheitsstrategie.

Eine praktische Anwendung dieser Attribute lässt sich mit dem in 3.2.2 eingeführten Domänen-Begriff bewerkstelligen. Hierbei werden zuerst die Anlagen- und Infrastrukturbereiche mit der höchsten Risikopriorität behandelt, gehärtet und in eine dauerhafte Überwachung aufgenommen. Dann folgen wichtige Transit-Netzelemente (Zonen-Firewalls), welche in kritikalen Bereichen

4 Definitionen, Einordnung

Nachfolgend werden zum gemeinsamen, einheitlichen Verständnis wichtige Definitionen sowie auch weiterführende Erläuterungen sowie Einordnungen gegeben. Auf diesen beruhen die in diesem Konzept durchgeführten Darstellungen und Bewertungen.

Das Dokument fokussiert in der aktuellen Fassung primär auf die Regularien, welche aus den Energiewirtschaftsgesetz (EnWG) gemäß §11 hervorgehen und die hierüber verpflichteten Betreiber von Energieversorgungsnetzen und Energieanlagen betreffen. Diese sind von den technischen und organisatorischen Umfängen identisch zu den Anforderungen an Betreiber von Energieversorgungsnetzen und Energieanlagen, welche nach der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur gelten (Schwellenwert-Klassifizierung, KRITIS).

Grundsätzlich gelten die Ausführungen in diesem Dokument ebenfalls für viele andere Branchen.

4.1 Angriffe und Bedrohungen

An dieser Stelle werden einige einführende Ausführungen zu möglichen Angriffsformen dargestellt, welche einen grundsätzlichen Überblick über die sehr umfangreiche und komplexe Materie geben sollen.

4.1.1 Allgemeine Angriffstypen

- Supply Chain Angriffe,

– Systemdesign durch Hersteller (Hardware, Software; Performance und Robustheit).

sein, bei welchem die Sicherheitszonen, welche einen hohen und sehr hohen Schutz gewährleisten

nen bereits einige der o.g. Angriffsvektoren, von vorne herein, eliminiert werden.

Abb. 4-1: Wesentliche Angriffsvektoren sowie deren Schadenspotenzial

4.1.3 Kritische Infrastrukturumgebungen der Energiewirtschaft

Zu den kritischen Infrastrukturumgebungen zählen z.B. folgende Teilsysteme (Vgl. auch IT-SiKat 1a (Technologiekategorien)):

– LAN-Netzwerke zum Leitstellenbetrieb (SCADA),

– WAN-Netzwerke zur Leitsystem- und Stationskommunikation

lisierung, Alarmierung, Logging, ...),

4.1.4 Zu erwartende Angriffsformen

Mit der notwendigen Zunahme an vernetzten, digitalen Konzepten sowie deren Infrastrukturbasis können zwei wesentliche Vektoren identifiziert werden. Diese sind:

fer), anwendbar.

4.1.4.1 Branchenspezifische Angriffe

Anbei erfolgt eine kurze Aufzählung grundsätzlicher Angriffsformate:

4.1.4.2 Allgemeine Angriffsoptionen aus der verwendeten, technologischen Infrastruktursphäre

Anbei erfolgt eine kurze Aufzählung grundsätzlicher Angriffsformate:

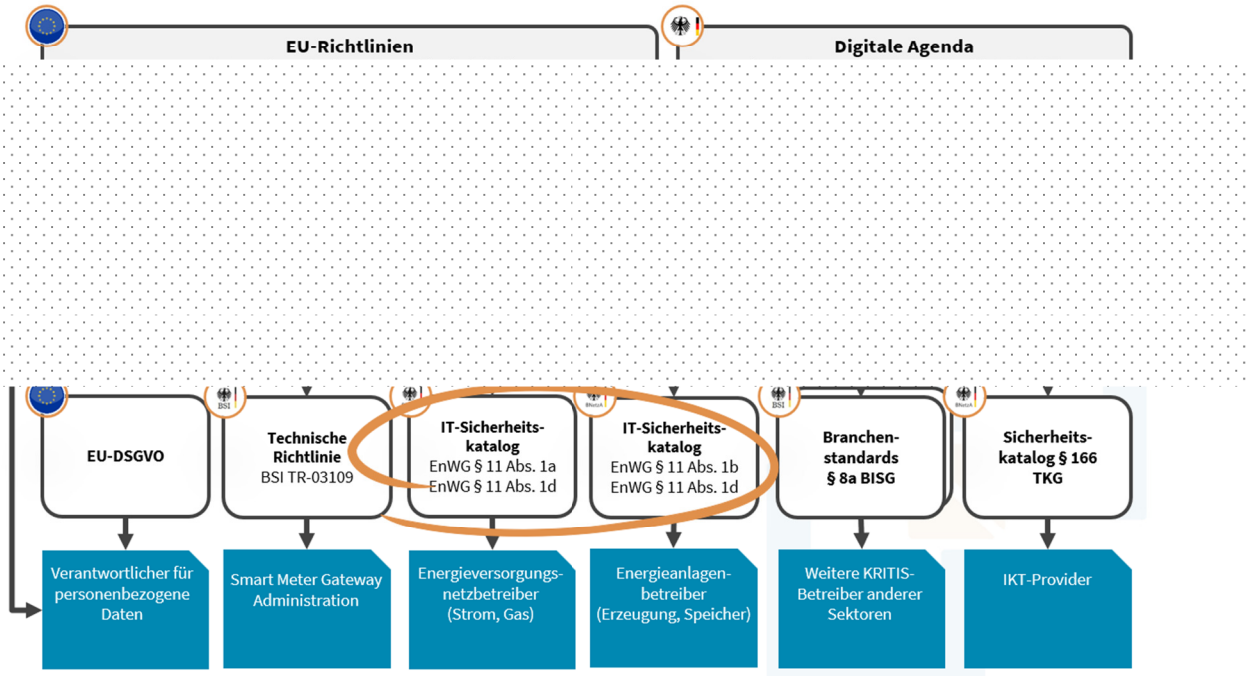
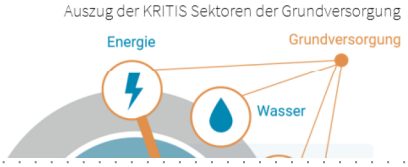


Abb. 5: Regularien in der Bundesrepublik Deutschland in der Übersicht

Die BSI-KritisV definiert nahezu alle Stufen der energiewirtschaftlichen Wertschöpfungskette als kritische Infrastruktur. Sofern nicht Schwellwerte eine Einordnung gemäß BSIG § 10 Abs. 1 festlegen, so ist für die meisten anderen Strukturgrößen das EnWG gemäß §11 Abs. 1a heranzuziehen. Für jeweils beide Zugehörigkeiten kann die in Abb. 6 aufgestellte Übersicht (gesamten Wertschöpfungskette der Energieversorgung) zur Eigenpositionierung herangezogen werden.



Wertschöpfungskette des KRITIS-Sektors Energie

Abb. 6: Stufen der energiewirtschaftlichen Wertschöpfungskette, im Kontext der Einordnung nach KRITIS (BSIG § 10 Abs. 1) oder gemäß der Zugehörigkeit weiterer gesellschaftlicher Bereiche zur Daseinsvorsorge (EnWG § 11 Abs. 1a bzw. 1b)

4.4 Präzisierende Umfangdarstellung eines wirksamen Konzeptes zur Angriffserkennung und -vermeidung

Angriffserkennung und Schwachstellenmanagement

Im EnWG §11 Absatz 1d wird der Begriff Angriffserkennung primär verwendet und der Begriff Angriffsvermeidung nur tangiert, ohne näher auf technische Spezifikationen oder Umsetzungen einzugehen. In diesem Dokument wird unter Angriffserkennung und Angriffsvermeidung, in Auslegung des EnWG § 11 Absatz 1d und eines wirksamen Schutzkonzeptes (Stand der Technik), verstanden:

- **Angriffserkennung** in Form von Mustererkennung und Analyse von Verkehrsströmen (z.B. IDS),
- **Anomalieerkennung** in Form von unerwarteten Abweichungen oder Aktivitäten auf einem System, welche auf einen Fehler oder eine Manipulation hindeuten können (z.B. Asset Changes, unerwartete Protokolle, IP-Adressen, IP/MAC-Changes, Netzwerkqualitätsveränderun-

enz“. Mit den durch die neue Normveröffentlichung ISO/IEC 27002:2022 im Zusammenhang stehenden weiterführenden Anpassungen korrespondierender Normwerke (z.B. ISO/IEC 27001) ist davon

5 Grundlegende Betrachtungen zur Auswahl von Lösungen zur Angriffserkennung- und -vermeidung

5.1 Marktsituation

Am Markt existieren eine Vielzahl von Lösungen, zumeist mit dem Gesamtfokus auf eine umfassende „Security Incident and Event Management"-Gesamtlösung (SIEM), welche i.d.R. auf große Strukturkonzepte von Konzernunternehmen, mit globalem Handlungshorizont und Regularien, zielen. Derartige Lösungen sind in den letzten Jahren 5-10 Jahre insbesondere für den Finanzsektor, für die Automobilbranche, für Pharma- sowie Luftfahrt- und Raumfahrtunternehmen entstanden und hinsichtlich ihrer Funktionen sehr stark erweitert worden. Es sind Modulkonzepte verfügbar, welche ausnahmslos eine gesamtheitliche Enterprise-Sicht und Konzernsicherheit adressieren. I.d.R. muss zur Etablierung und Partizipierung bereits zu Beginn eine sehr hohe Investition für die Gesamtplattform getätigt werden, an welche dann verschiedene weitere Module gekoppelt werden können. Die übergeordnete Plattform ermöglicht seitens der namhaften Hersteller die Applizierung der Lösung auf die jeweilige Kundenbranche. Daher werden eine Vielzahl internationaler Security-Standards (Frameworks) unterstützt, wie z.B. ISO 27001, 27019, IEC62443, PCI DSS, NIST, FISMA, AWWA, NERC, HIPAA, DISA, ISO/IEC 27002 und SOX.

Dem oben skizzierten Lösungsansatz stehen weitere Konzepte am Markt zur Seite, welche verschiedene Teilaspekte berücksichtigen und auf die jeweilige Herkunfts- und Spezialisierungshistorie des Herstellers zurückzuführen sind. Zu diesen zählen z.B. die Felder Logging, Monitoring, Anomaliede-

tallisieren sich jedoch zwei Konzepte heraus. Das eine fokussiert sich auf die Bereitstellung einer übergeordneten Integrationsplattform für verschiedene darunter liegende andere Open-Source-Lösungen für die zu erbringenden Aufgaben. Das andere orientiert sich daran, dass sinnvolle Funktionen, in einem Framework ähnlichen Konzept, bereits im Kontext SIEM, Angriffserkennung und Schwachstellenmanagement bereitgestellt werden. Ein Open-Source-Einsatz ist i.d.R. mit einer sehr hohen Expertise und Eigenverantwortung verbunden.

„Erstwirksamkeit“ nachzugehen oder auf eine „Vollwirksamkeit“ einer einzelnen Systemumgebung (Domäne), bis hin zu kompletten Infrastrukturbereichen zu erzielen.

5.5 SOC und SIEM: Einordnung

An dieser Stelle sollen einige Ausführungen zum zentralen Sicherheitsmanagement gemacht werden. Der Themenkomplex ist überaus anfordernd und er kann an dieser Stelle nur angerissen werden.

Das Sicherheitsmanagement stellt eine zentrale Disziplin des Systemmanagements gemäß ISO 10164 und ISO 10040 dar und, neben weiteren wichtigen Systemmanagementfunktionen (Vgl.

lichkeiten, aber auch Komplexitäten zur Übergabe von Ereignissen aus der Entstehungsdomäne an ein SOC, aufzeigen,

Insbesondere, wenn ein SOC-Konzept aus der OT-Domäne eines Energieversorgers nach extern vergeben werden soll, um die Ereignisse (Incidents, Incident Management) einem standardisiert organisierten IT-SOC zuzuführen, müssen folgende Prämissen berücksichtigt werden:

1. Es ist ein operatives Modell für den SOC-Betrieb festzulegen. Hierbei ist zu unterscheiden,

dent- und Change Managements. Im Falle eines kritischen Ereignisfundes sind die

Es sind Kombinationen der in 1. und 2. dargelegten Methodiken sowie auch eine arbeitsteilige Organisation und Delegation mit externen, verpflichteten Dienstleistern, möglich.

ner offensiven Sicherheitsstrategie (siehe Tab. 5-1) bei welcher die Anzahl der Vektoren stetig bewertet und minimiert wird und bei welcher schnell die Auswirkungen überschaut werden können, um Gegenmaßnahmen und Changes (Reaktion) einzuleiten.

Zur offensiven Sicherheitsstrategie			
Strategie	**Konzept**	**Methodik**	**Sicherheitsgewinn**
Defensiv	Sicherheitsbewertung von „innen nach außen"	Reaktiv (Angreifer bereits im Netz tätig bzw. Changes bereits initiiert)	Mittel bis hoch
Offensiv	Sicherheitsbewertung von „innen nach außen" und von „außen nach innen"	Proaktiv (Angreifer werden abgehalten, Changes werden unterbunden)	sehr hoch bis maximal (sehr hohe Sicherheit mit Frühwarnung)

Tab. 5-1: Effekte einer Lösung mit impliziten SIEM-Funktionen: Erreichung einer „Offensiven Sicherheitsstrategie"

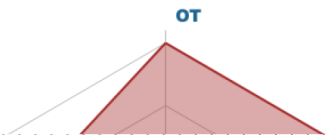
Abschließend darf ein aktuell im Markt stehender Zusammenhang nicht verschwiegen werden. Der

Grund der Rolle für die gesellschaftliche Daseinsvorsorge (kritische Infrastruktur), eine gewisse „Fach- und Sprachtransformation" (Branchenfokussierung), welche als zentraler Erfolgsfaktor für derartige operative Betriebsmodelle angesehen werden kann.

6.3 Explizite Lösungen zur Angriffserkennung

6.3.1 *Claroty Inc.: „Claroty Continuous Threat Detection" (CTD)*

6.3.1.1 *Hersteller*

Hersteller:	Claroty Inc. 488 Madison Avenue New York, NY 10022
Sitz:	USA
Nächster Vertriebsstandort:	Claroty-Vertrieb DACH-Region, München
Website:	https://www.claroty.com
Hersteller-Präferenzen für Technologiedomänen:	
	Enterprise

6.3.1.2 *Einordnung des Produktfokus*

Beschreibung	Bewertung	Bemerkung
OT-Einsatzfeld	☒ Ja ☐ Nein	
OT-Schwachstellen	☒ Ja ☐ Nein	Claroty Security Feed
IT-Schwachstellen	☒ Ja ☐ Nein	grundsätzlich gegeben (CVE/CVSS).
Angriffsmustererkennung	☒ Ja ☐ Nein	

Anomalieerkennung	☒ Ja ☐ Nein	
Ausbaufähigkeit zum Enterprise SIEM	☒ Ja ☐ Nein	Mit Ergänzungslösung; Übergabe-

6.3.1.3 Grundkonzept

Beschreibung	Bewertung	Bemerkung
Aktives Schwachstellenmanagement	☒ Ja ☐ Nein	Zusatzmodul: Claroty Edge
Passives Schwachstellenmanagement	☒ Ja ☐ Nein	Claroty Security Feed
Offline Security Feed, Aktualisierung für isolierte Zonen	☒ Ja ☐ Nein	GPG-verschlüsselte Signaturen liegen für Vertragskunden vor

6.3.1.4 Zusammenfassung der Kernfunktionen

Anbei werden die Kernfunktionen, welche für die geplante Anwendung als Angriffserkennungs- und -vermeidungssystem zur Verfügung stehen sollen, aufgeführt:

Beschreibung	Bewertung	Bemerkung
Passives Schwachstellenmanagement	☒ Ja ☐ Nein	
Asset-Discovery und -Change	☒ Ja ☐ Nein	

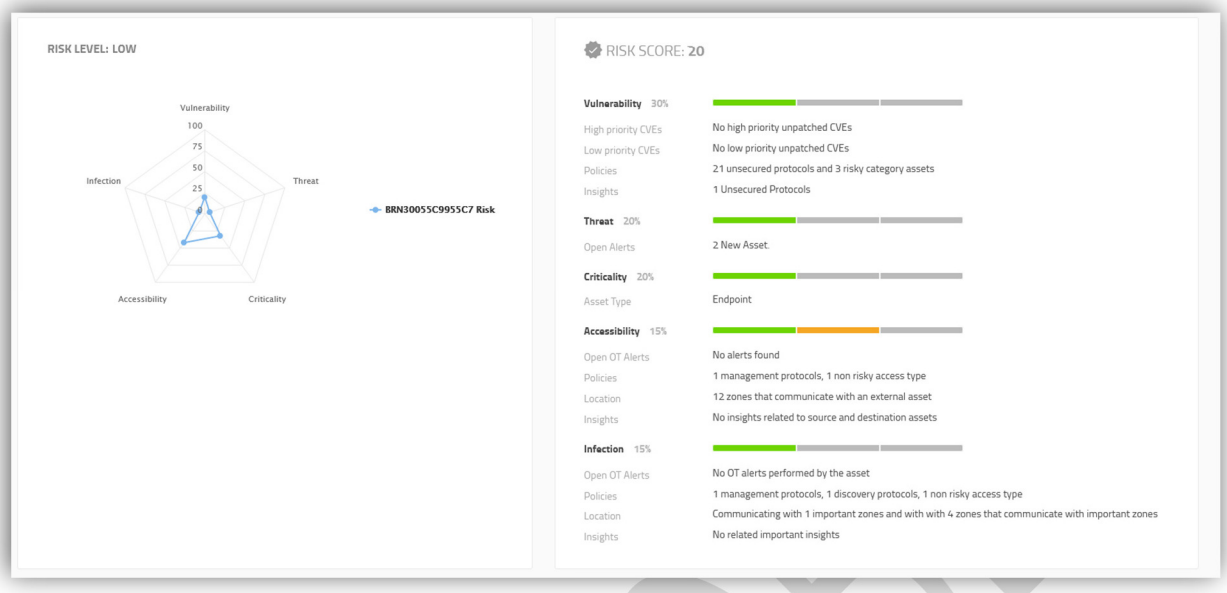


Abb. 6-2: Risiko-Assessment-Report

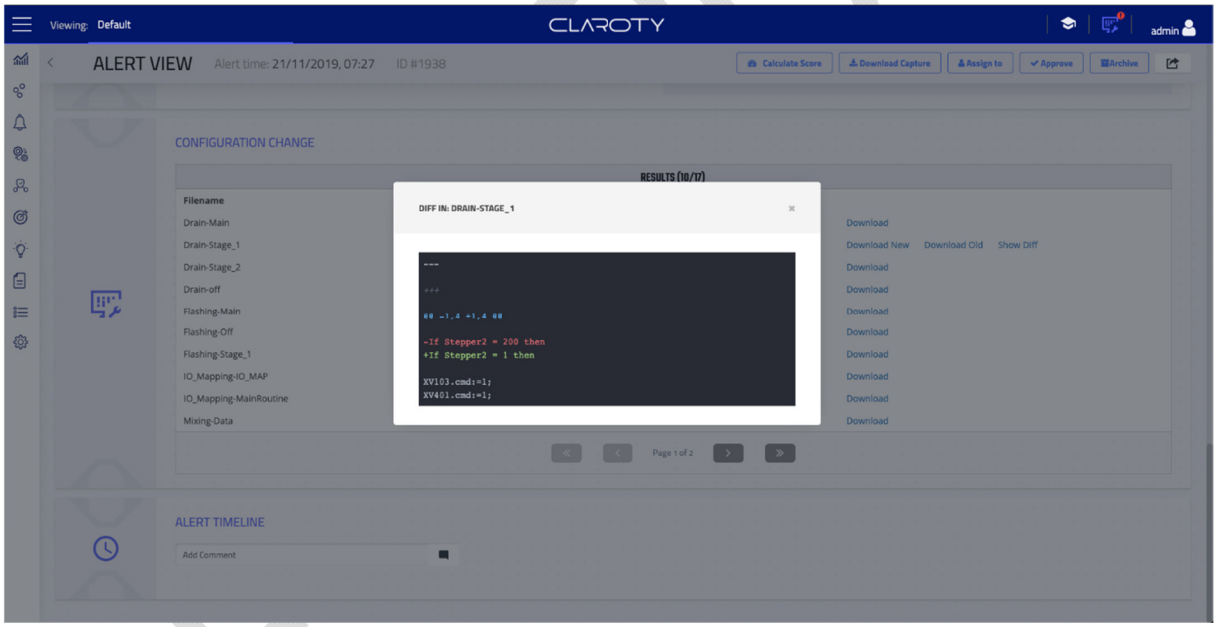


Abb. 6-3: Alarmansicht einer detektierten Konfigurationsänderung (Asset Change Detection)

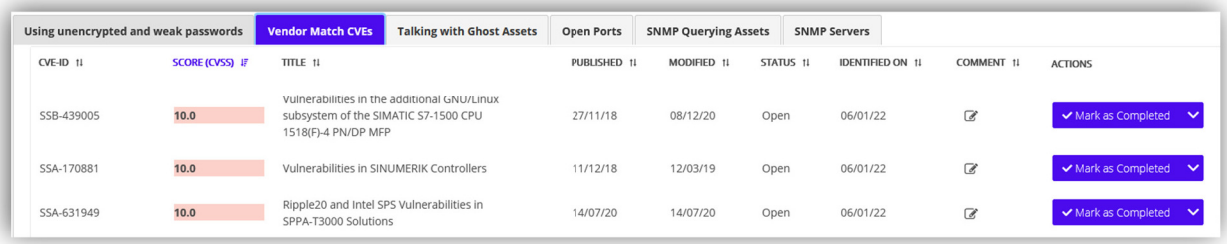


Abb. 6-4: Schwachstellendetektion mit Asset-Mapping (CVE- und CVSS-Darstellung)

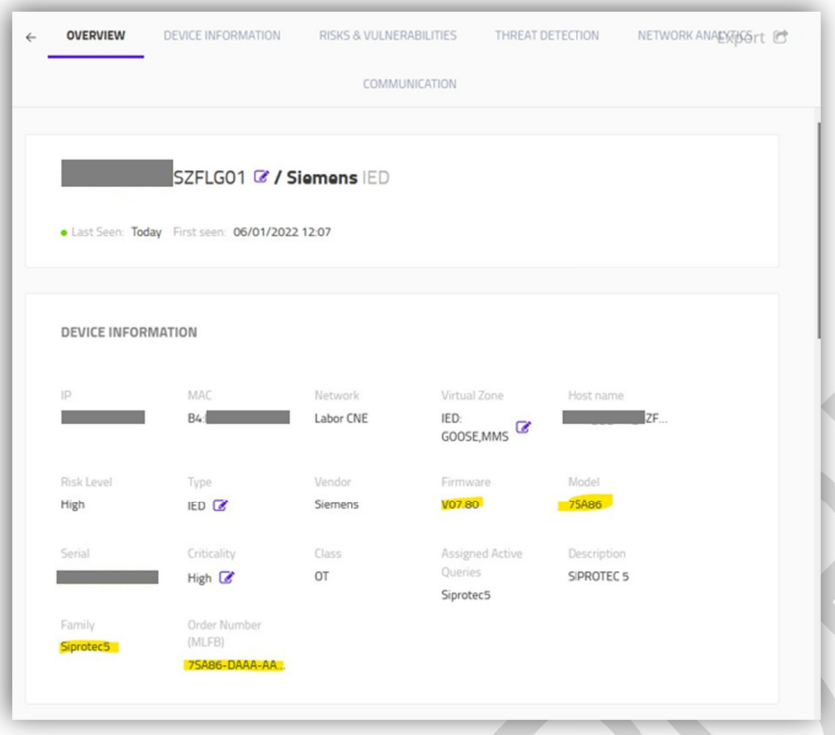


Abb. 6-9: **In Zusammenarbeit mit dem Entwicklungsteam von Claroty Inc. sowie einem deutschen Integrator wurde für EVU bzw. Netzbetreiber übliche, in der BRD vorhandene, Feldgerätetechnik implementiert (gezeigtes Beispiel: Digitales Schutzgerät „Siemens Siprotec 5“)**

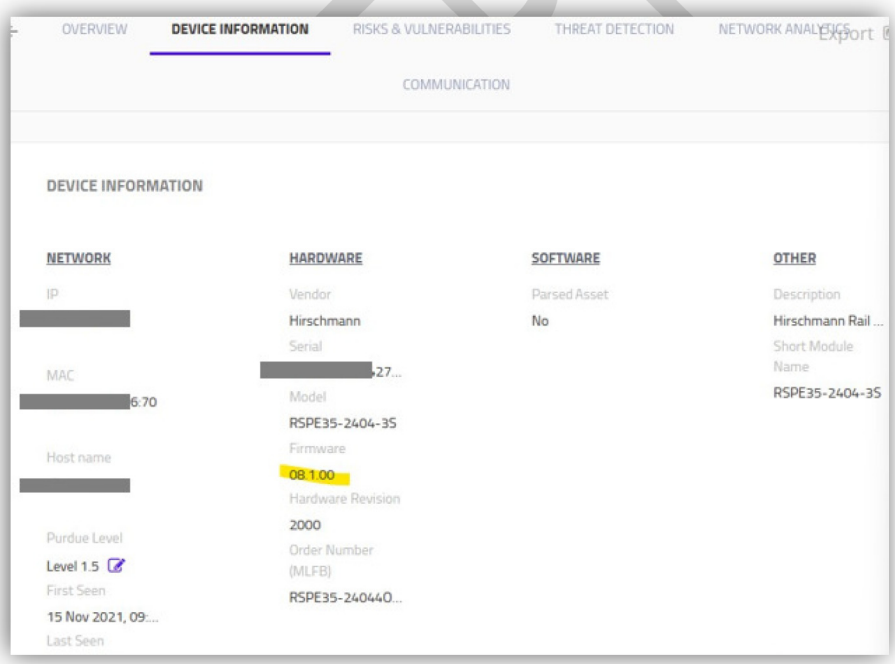
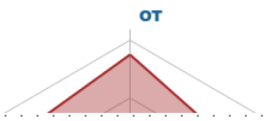


Abb. 6-10: **In Claroty implementiertes Komponenten-Management für OT-Netzwerkkomponenten „Belden/ Hirschmann“, im Kontext mit dem ISMS-Patch- und -Lifecycle Management**

6.3.5 Tenable Inc.: „tenable.ot und tenable.sc"

6.3.5.1 Hersteller

Hersteller:	Tenable Inc. 7021 Columbia Gateway Drive Suite 500 Columbia
Sitz:	USA
Nächster Vertriebsstandort:	Tenable Network Security GmbH, München
Dach-/Mutterkonzern:	-
Website:	https://de.tenable.com
Hersteller-Präferenzen für Technologiedomänen:	

6.3.5.2 Einordnung des Produktfokus

Beschreibung	Bewertung	Bemerkung
OT-Einsatzfeld	☒ Ja ☐ Nein	Modul: tenable.ot
OT-Schwachstellen	☒ Ja ☐ Nein	Modul: tenable.ot
Ausbaufähigkeit zum Enterprise SIEM	☒ Ja ☐ Nein	Modul: tenable.sc, tenable.ep

Rubrik der Grundsatzbewertung 1/2

Kategorie		*Explizite Lösungen* zur Angriffs- und Anomalierkennung mit weiteren umfassenden Funktionsmodulen und Anwendungsoptionen							*Alternative Lösungen* Teilbereiche anwendbar und je nach Konzept auch weiterführend auszubauen		Eruierung einer Log-Lösung
Funktionen		Claroty „CTD"		Rhebo „Industrial Protector"	Omicron „StationGuard"	Tenable „tenable.ot", „tenable.sc"					
Einsatzfeld	OT	ja	ja	ja	ja	ja	ja	ja	ja	ja	ja
	IT	ja	ja	nein	nein	ja	ja	ja	ja	ja	ja
SIEM-Komponenten	Asset-Erkennung	ja	ja	ja	ja	ja	ja	ja	*möglich*	ja	nein
	A										
	A										
	S										
	K										
	&										
	D										
	P										
	I										
	R										
	C										
Beitrag zu ISMS-Prozessen (organisatorisch / formell)	A										
	S										
	C										
	P										
	L										
	I										
	R										
	R										

Rubrik der Hauptbewertungskriterien 3/5

Lfd. Nr.	Kategorie	Anforderung	Wertungskriterium	*Explizite Lösungen* zur Angriffs- und Anomalierkennung mit weiteren umfassenden Funktionsmodulen und Anwendungsoptionen												*Alternative Lösungen* Teilbereiche anwendbar und je nach Konzept auch weiterführend auszubauen				Eruierung einer Log-Lösung	
				Claroty „CTD"				Rhebo „Industrial Protector"		Omicron „Station Guard"		Tenable „tenable.ot", „tenable.sc"									
			AK 100 Pkte., WK max.	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?
24.	Beitrag zu IS-Security- sowie zu ISMS-Prozessen	Möglichkeit der einfachen und schnellen Benutzung von Einzel-funktionen für die Startphase bzw. im Rahmen einer Strategie der Erstwirksamkeitserhöhung („Insel-benutzung von Modulen/Funktio-nen")	WK5	5	☒ erfüllt	4	☒ erfüllt	2	☒ erfüllt	4	☒ erfüllt	5	☒ erfüllt	5	☒ erfüllt	4	☒ erfüllt	2	☒ erfüllt	2	☒ erfüllt	0	☐ erfüllt
25.	Beitrag zu IS-Security- sowie zu ISMS-Prozessen	Risikobewertung der Assets	WK5	5	☒ erfüllt	5	☒ erfüllt	2	☒ erfüllt	0	☐ erfüllt	5	☒ erfüllt	5	☒ erfüllt	5	☒ erfüllt	2	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt
26.	Beitrag zu IS-Security- sowie zu ISMS-Prozessen	Lifecycle-Management	WK3	3	☒ erfüllt	2	☒ erfüllt	0	☐ erfüllt	0	☐ erfüllt	2	☒ erfüllt	1	☒ erfüllt	3	☒ erfüllt	1	☒ erfüllt	3	☒ erfüllt	0	☐ erfüllt
27.	Beitrag zu IS-Security- sowie zu	Vordefinierte, dienliche Reports	WK5	5	☒ erfüllt	4	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt	4	☒ erfüllt	5	☒ erfüllt	5	☒ erfüllt	3	☒ erfüllt	3	☒ erfüllt	0	☐ erfüllt
28.																							
29.																							
30.																							
31.																							
32.																							

Rubrik der Hauptbewertungskriterien 5/5

Lfd. Nr.	Kategorie	Anforderung	Wertungskriterium	*Explizite Lösungen* zur Angriffs- und Anomalierkennung mit weiteren umfassenden Funktionsmodulen und Anwendungsoptionen												*Alternative Lösungen* Teilbereiche anwendbar und je nach Konzept auch weiterführend auszubauen				Eruierung einer Log-Lösung	
				Claroty „CTD"				Rhebo „Industrial Protector"		Omicron „Station Guard"		Tenable „tenable.ot", „tenable.sc"									
			AK 100 Pkte., WK max.	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?	Punkte	erfüllt?
48.	Betrieb des Systems	Aufwandsunterstützung für Alarmanalysen (Effizienz, Einfachheit der Anwendung)	WK4	3	☒ erfüllt	2	☒ erfüllt	1	☒ erfüllt	2	☒ erfüllt	2	☒ erfüllt	3	☒ erfüllt	2	☒ erfüllt	2	☒ erfüllt	3	☒ erfüllt	0	☐ erfüllt
49.	Betrieb des Systems	Unterstützung bei der Alarmanalyse durch leister	WK3	1	☒ erfüllt	1	☒ erfüllt	3	☒ erfüllt	2	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt	1	☒ erfüllt	0	☐ erfüllt
50.	Betrieb des Systems	Intuitive E oberfläch																					
51.	Betrieb des Systems	Dezidierte zept (RBA																					
52.	Betrieb des Systems	AD/LDAP- tegration																					
53.	Betrieb des Systems	On-Premi gesichert																					
54.	Betrieb des Systems	Laufende über Nutz Monate, 2 fügbar)																					
	Zwischensumme:																						
	Gesamtsumme WK:																						
	Gesamtsumme AK:																						
	Gesamtbewertung:		683																				

Tab. 7-2: Tabelle für das quantitative Hauptbewertungsverfahren

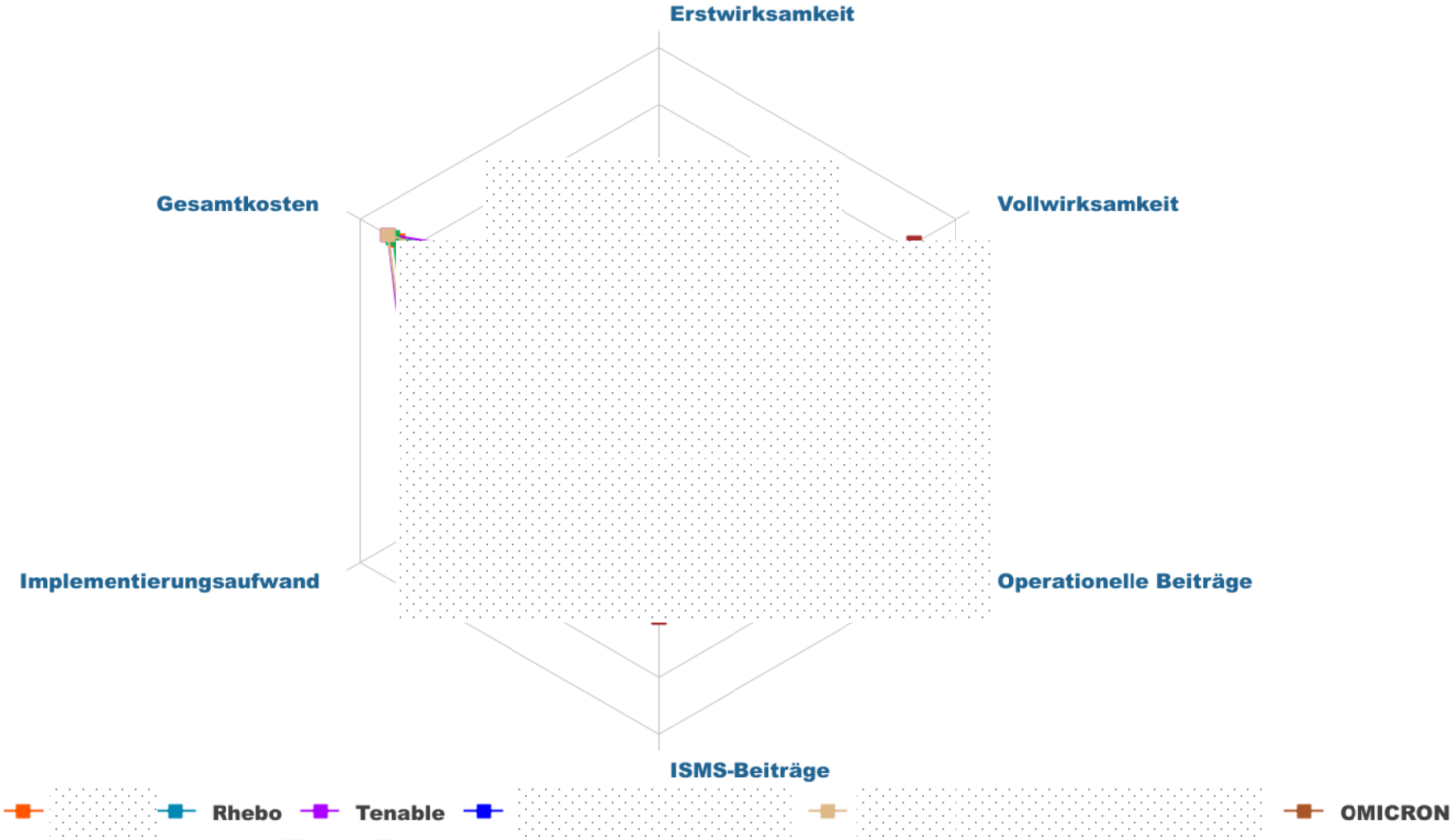


Abb. 8-1: Best-Practice-Bewertung der in den Vergleich einbezogenen Lösungen. Die Basis bilden die in Kapitel 6 und 7 geführten Lösungsvergleiche.

15 Kontaktaufnahme

Kontaktaufnahme	
Postadresse:	CONTROLNET GmbH, Bauhausstraße 7c, 99423 Weimar
Email:	expertscontact@controlnet.de

Über uns	
	CONTROLNET GmbH offeriert eine unabhängige, innovative Expertenstruktur für den Energie- und Versorgungssektor, für die industrielle OT sowie für Informations- und IT-Sicherheit. Wir verfügen über fundierte Erfahrungen in der Planung, Auslegung und dem Schutz von Industrieanlagen, Steuerungssystemen und kritischen Infrastrukturen und wir haben uns sehr tiefgründige Fähigkeiten in den Bereichen Informationssicherheit gemäß DIN ISO/IEC 27001/27019, in der Auditierung sowie auch zu energiespezifischen Workflows erarbeitet, um eine sichere, stabile und resiliente netzwerkbasierte Prozess- und Applikationsinfrastruktur betreiben zu können. Unser Team lebt Informationssicherheit und wir treiben Fortschritt sowie Innovation an, um die Wettbewerbsfähigkeit und Marktführerschaft unserer Kunden zu sichern. Hierzu arbeiten wir intensiv mit unseren Zielbranchen, Herstellern sowie mit Distributoren und insbesondere mit verlässlichen und unsere Werte teilenden Fachexperten langfristig zusammen. Unsere Experten verfügen über ein sehr umfassendes Know-how in Consulting, Entwicklung, Integration von OT- und SCADA-Infrastrukturen sowie auch in der Unternehmensberatung. Wir bringen einen „Rundumblick“ ein, welcher den Fokus beginnend bei den zu erreichenden unternehmerischen Zielen, über Technologieeinsatz und Technikkonzept, bis hin zu Prozessen, Resilienz und Regularien spannt. Dabei bringen wir auch unkonventionelle und neue Ansätze ein, um eine passfähige und nutzbringende Lösung für unsere Kunden bereitzustellen und den Lösungserfolg zu sichern. Die Erfahrungen zur Bereitstellung unseres Expertenwissens rekrutieren sich zwischenzeitlich aus einer Tätigkeitsepoche von mehr als 30 Jahren, in welchen unsere führenden Spezialisten in den Branchen Luft- und Raumfahrt, Energieversorgung, IT, Carrier und ISP sowie Informations- und IT-Sicherheit tätig sind. Während dieser Tätigkeiten wurden insbesondere Plattformprojekte für Energieversorger und nationale Carrier umgesetzt, indem mehrere Unternehmen ab Anfang der 90iger Jahre aufgebaut und in den vergangenen 25 Jahren verschiedene Lösungen im Bereich Netzmanagement, Monitoring, Analyse sowie auch im Feld von Umbrella- und Meta-Plattformen (DCN, OSS, NOC, SOC) erfolgreich geplant, implementiert und betrieben wurden.