KuppingerCole Report

WHITEPAPER

von Matthias Reinwarth & Christopher Schütze | Juli 2019

KRITIS - Kritische Infrastrukturen verstehen und schützen

Organisationen oder Institutionen, die für die Öffentlichkeit wichtig sind, werden als Kritische Infrastrukturen (KRITIS = "Kritische Infrastrukturen") bezeichnet. Als solche unterliegen sie umfassenden und strengen Richtlinien, bestehend aus Gesetzen und Vorschriften. Ihr Ausfall oder ihre erhebliche Beeinträchtigung kann zu anhaltenden Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit oder anderen drastischen Folgen führen. Ihr Schutz und der Schutz der Öffentlichkeit erfordern geeignete Konzepte, Prozesse und Technologien.

von **Matthias Reinwarth**
mr@kuppingercole.com

von **Christopher Schütze**
chs@kuppingercole.com

Im Auftrag von CyberArk

Inhalt

Abbildungen

Tabellen

Weitere relevante Dokumente (in Englischer Sprache)

Leadership Compass: Privilege Management - 72330

Leadership Compass: Adaptive Authentication - 79011

Architecture Blueprint: Hybrid Cloud Security - 72552

Advisory Note: GRC Reference Architecture - 72582

Advisory Note: Big Data Security, Governance, Stewardship - 72565

KuppingerCole Hot Topic Area Privilege Management

1 Einführung

Die Abhängigkeit einer Gesellschaft von vernetzten Systemen wird für die Einwohner, Unternehmen und Regierung immer größer. Der Technologie-Thriller und weltweite Bestseller[1] "Blackout – Morgen ist es zu spät" des österreichischen Autors Marc Elsberg ist dabei nicht das erste Werk der Fiktion, das die Aufmerksamkeit einer breiten Öffentlichkeit auf dieses Thema lenkte. Am Beispiel eines groß angelegten und langanhaltenden Stromausfalls in Europa wird die Dynamik einer solchen Situation in einem spannungsdurchzogenen Roman beschrieben.

Aber nicht nur die Unterhaltungsbranche und Literatur haben sich mit diesem Thema auseinandergesetzt. Im Jahr 2010 veröffentlichte das "Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag" zusammen mit dem "Karlsruher Institut für Technologie (KIT)" einen umfassenden Bericht mit dem Titel "Gefährdung und Verletzbarkeit moderner Gesellschaften - am Beispiel eines großräumigen Ausfalls der Stromversorgung"[2]. Diese Studie beschrieb den Stromausfall als ein eindrucksvolles Beispiel für "kaskadierende Schadenseffekte". Der Bericht kam zu dem Ergebnis, dass die ausgelösten Folgen trotz geringer Eintrittswahrscheinlichkeit nicht "kontrolliert" und bestenfalls gemildert werden könnten. Die Empfehlung lautete, die Widerstandsfähigkeit der kritischen Infrastrukturbereiche kurz- und mittelfristig zu erhöhen.

Kritikalität ist der relative Grad, in dem eine Infrastruktur im Hinblick auf die Folgen, die eine Störung oder Fehlfunktion für die Versorgungssicherheit wichtiger Güter und Dienstleistungen für die Gesellschaft hat, wichtig ist.

Der Begriff "KRITIS" als Abkürzung für "**KRIT**ische **I**nfra**S**trukturen" ist eng mit der Bundesrepublik Deutschland als Staat und ihrer Gesetzgebung verbunden. Er zielt insbesondere auf die Bemühungen um eine Verringerung der potenziellen Anfälligkeit durch Verbesserung des Schutzes und der Widerstandsfähigkeit kritischer Infrastrukturen infolge des zunehmenden Ausmaßes der Abhängigkeit fast aller Lebensbereiche mit und von kritischen Infrastrukturen ab.

1 https://www.amazon.de/BLACKOUT-Morgen-ist-spät-Roman/dp/3442380294/ref=sr_1_1
2 http://www.tab-beim-bundestag.de/de/untersuchungen/u137.html

Dies spiegelt sich in einer Vielzahl von Initiativen, Gesetzen und Verordnungen wider, wie die folgenden europäischen und deutschen Beispiele zeigen:

- Im Jahr 2006 initiierte die Europäische Union das Europäische Programm zum Schutz kritischer Infrastrukturen (EPCIP).
- Im Jahr 2008 wurde die Richtlinie 2008/114/EC[3] "über die Identifizierung und Ausweisung kritischer europäischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern" auf EU-Ebene erlassen.
- Im Jahr 2016 bildete die "Richtlinie über die Sicherheit von Netzen und Informationssystemen (NIS-Richtlinie)" einen wichtigen Baustein der EU-weiten Gesetzgebung zur Cybersicherheit, die darauf abzielt, rechtliche Maßnahmen zur Verbesserung des allgemeinen Niveaus der Cybersicherheit in der EU durchzusetzen.
- Auf nationaler Ebene hat das BSIG[4] - "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" den Grundstein für die gesetzlichen und regulatorischen Anforderungen an kritische Infrastrukturen gelegt.
- Im Juli 2015 wurde das IT-SiG - "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" - zur Sicherung von IT-Systemen und digitalen Infrastrukturen, einschließlich kritischer Infrastrukturen in Deutschland, erlassen. Dieses wurde 2016 um die BSI-KritisV[5] - "BSI-Kritisverordnung" erweitert.
- Diese Dokumente wurden im Laufe der Zeit aktualisiert und erweitert, z.B. durch die Einbeziehung von Finanzen und Versicherungen, Gesundheit, Transport und Reisen in den Geltungsbereich der KritisV im Jahr 2017.

Über Europa hinaus wird dies natürlich auch als kritisches Thema betrachtet. Im Jahr 2015 untersuchte "Business Blackout"[6], ein gemeinsamer Bericht von Lloyd's Insurance und dem University of Cambridge's Centre for Risk Studies, das gleiche Szenario aus einem anderen Blickwinkel, indem es die Auswirkungen eines Cyberangriffs auf das US-Energienetz beleuchtete. Die Gesamtauswirkungen auf die US-Wirtschaft wurden auf 243 Mrd. USD geschätzt, wobei die Auswirkungen der sogenannten "extremsten Version" des prognostizierten Szenarios insgesamt mehr als 1 Billion USD betrugen.

3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114
4 https://www.buzer.de/gesetz/8987/index.htm
5 https://www.buzer.de/gesetz/12020/index.htm
6 https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

2 Definition kritischer Infrastrukturen

Die Definition von und Anforderungen an kritische Infrastrukturen, wie sie auf europäischer und insbesondere deutscher Ebene existieren, können in jeder Hinsicht als beispielhaft angesehen werden. Auch wenn sie vor allem für Betreiber kritischer Infrastrukturen in Deutschland von direkter Relevanz sind, können sie aufgrund des Detaillierungsgrades und der umfassenden Abdeckung einer Vielzahl von Branchen und Industrien als Grundlage für die Planung, den Betrieb und die Dokumentation belastbarer Architekturen in Europa und darüber hinaus dienen.

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder 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“[7].

Für das Gesamtbild ist es notwendig, zunächst eine allgemeine, einheitliche Definition von "Infrastrukturen" zu haben. Auf einem hohen Abstraktionsgrad sind Infrastrukturen Versorgungssysteme für unsere Gesellschaft, die grundlegende Güter und Dienstleistungen bereitstellen.

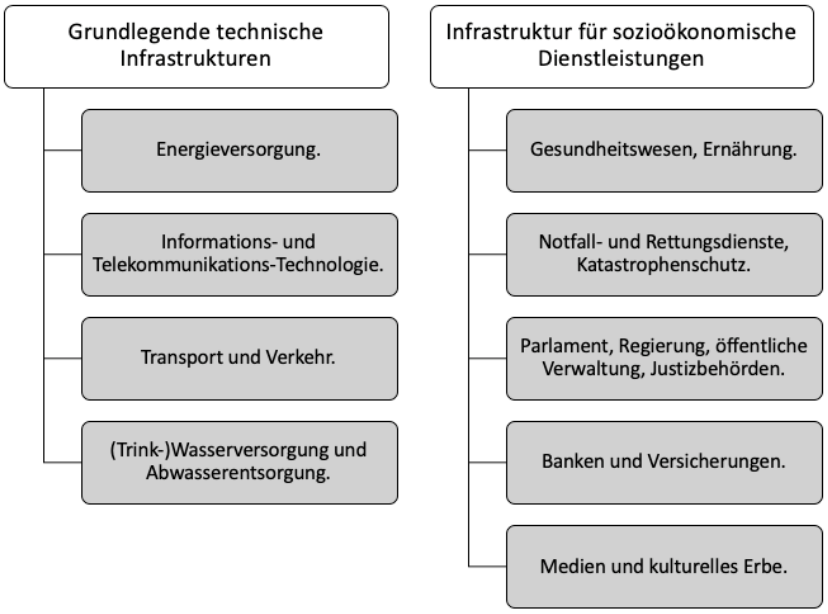

Abbildung 1: Zwei Bereiche und neun Sektoren definieren derzeit die Gesamtstruktur kritischer Infrastrukturen

7 https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html

Die derzeit gültige konzeptionelle Gliederung zum Schutz der für die Versorgung von Staat, Wirtschaft und Gesellschaft zentralen Versorgungs- und Dienstleistungseinrichtungen teilt die kritische Infrastruktur nun in neun Sektoren und 29 Industrien, die wiederum in zwei größere Bereiche unterteilt werden können. Die Abbildung 1 zeigt die zugrundeliegende Struktur.

Neun Sektoren und 29 Branchen gelten derzeit als kritische Infrastrukturen, darunter die Gesundheitsversorgung, Energieversorgung, der Verkehr und Finanzdienstleistungen.

Auf der Grundlage der in der Einleitung beschriebenen rechtlichen EU-Rahmenbedingungen haben viele Staaten Gremien geschaffen, die die Regulierung kritischer Infrastrukturen aktiv durchsetzen. In Deutschland gibt das BSI ("Bundesamt für Sicherheit in der Informationstechnik") entsprechende Richtlinien vor[8] und fungiert auch als Aufsichtsbehörde.

Die Betreiber kritischer Infrastrukturen in Deutschland sind verpflichtet, folgendes zu tun

- Benennung eines Kontaktweges (über den diese jederzeit erreichbar sind, z.B. eine E-Mail-Adresse);
- Berichterstattung über erhebliche[9] IT-Störungen;
- Implementierung von Schutzmaßnahmen nach dem "Stand der Technik";
- Nachweis dieser gegenüber dem BSI alle zwei Jahre;

Die zentrale Herausforderung besteht darin, die gesetzlichen Anforderungen nachweislich durch zuverlässige und sichere Systeme, Organisationen und Prozesse umzusetzen. Der notwendige Umsetzungsnachweis kann jedoch von vertrauenswürdigen Dritten in Form von Zertifizierungen, Prüfungen oder qualifizierten Audits erbracht werden.

[8] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/was_tun_node.html
[9] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html

3 Kritische Infrastrukturen in allen Branchen

Basierend auf den Definitionen des BSI für kritische Infrastrukturen hat das BBK ("Bundesamt für Bevölkerungsschutz und Katastrophenhilfe") eine Liste von Infrastrukturen, Organisationen und Branchen erstellt, die als kritische Infrastrukturen[10] eingestuft werden. Dazu gehören alle Bereiche des öffentlichen Interesses, die als potenzielle Schwachstelle für Deutschland angesehen werden können.

Gesetzgebung und Regulierung werden oft auf nationalstaatlicher Basis definiert und umgesetzt. Während die Kernvorschriften für jede kritische Infrastruktur gleich sind, besteht die Herausforderung für die einzelnen Branchen darin, dass die branchenspezifischen Anforderungen individuell definiert werden müssen. Dies macht es oft schwierig, von generischen Best Practices zu profitieren und schränkt Sektor-übergreifendes Handeln und konsistente Kommunikation ein. Die Sektor-spezifischen Bedürfnisse und Prozesse müssen stärker in den Mittelpunkt gerückt werden. In späteren Abschnitten dieses Dokumentes wird der Fokus auf ausgewählte Sektoren gelegt.

3.1 Verfeinerung der Anforderungen: B3S

Die Definition branchenspezifischer Anforderungen liegt in der Verantwortung der Branchen, ihrer Branchenverbände und einzelnen Schlüsselunternehmen als exemplarische Vertreter ihrer Branche. Diese Dokumente werden in Arbeitsgruppen der jeweiligen KRITIS-Abteilungen erstellt, die in den UP KRITIS (UP = "Umsetzungsplan") organisiert sind.[11] Der UP KRITIS ist eine öffentlich-private Zusammenarbeit zwischen Betreibern kritischer Infrastrukturen, ihren Verbänden und den zuständigen Behörden.

Der Aufgabenbereich der UP KRITIS-Industriearbeitsgruppen ist wesentlich größer, aber die Entwicklung und Aktualisierung von sogenannten B3S-Dokumenten (B3S = "Branchenspezifischer Sicherheitsstandard") ist eine ihrer wichtigsten Aufgaben.

B3S sind als so genannte "Orientierungshilfe" definiert und gelten als unterstützende Anleitung zur Umsetzung nach § 8a BSIG. Ihre Verwendung ist nicht zwingend vorgeschrieben, aber wo immer sie definiert sind, werden sie typischerweise als relevante Grundlage verwendet. Sie unterliegen einem klar definierten Lebenszyklus, der die Erstellung, Einreichung und Überprüfung von Prozessen zur Veröffentlichung umfasst. B3S-Dokumente müssen vom BSI genehmigt werden.

B3S sind derzeit nicht in allen Branchen verfügbar. Ihre Veröffentlichung ist von Branche zu Branche unterschiedlich: Einige Dokumente sind frei verfügbar, andere können gegen Entgelt als deutsche Industrienormen (DIN) erworben werden, andere sind nicht öffentlich und werden nur innerhalb der jeweiligen Branchen verbreitet. Das BSI dokumentiert einen Überblick[12] über die verfügbaren B3S-Dokumente.

10 https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Kritis/CI_Sektoren_Subsektoren.pdf
11 https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/UP_KRITIS_Fortschreibungsdokument.html
12 https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/B3S_BAKs/B3S_BAKs_node.html

Die Struktur dieser Dokumente ist vorgegeben und daher immer ähnlich. Sie umfassen in der Regel die folgenden Themen: Umfang, Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit), branchenspezifische Bedrohungssituation, Risikomanagement, Anwendungsanweisungen für Betreiber und Überprüfbarkeit der Umsetzung (Tests). Sie dienen als Sicherheitskatalog, der spezifische Anforderungen an die Systembetreiber enthält, die zur Erreichung der oben genannten Schutzziele umzusetzen sind. Es wird auf anerkannte, internationale Normen in den Bereichen IT-Sicherheit und der einzelnen Branchen Bezug genommen, deren Einhaltung empfohlen wird.

Die Betreiber kritischer Infrastrukturen müssen die Entwicklung, Kommunikation, Umsetzung und Dokumentation der Maßnahmen zur Umsetzung der Schutzziele innerhalb des Unternehmens sicherstellen. Sie bleiben für die Erfüllung der Sicherheitsziele verantwortlich, auch wenn Dritte beteiligt sind.

Branchenspezifische Sicherheitskataloge wurden als B3S-Dokumente erstellt und decken verschiedene Dimensionen der KRITIS-bezogenen Anforderungen ab, einschließlich der IT und über diese hinaus. Obwohl nicht obligatorisch, werden sie in der Regel als Grundlage für die Umsetzung herangezogen, sofern vorhanden.

3.2 Energie

Eine Schlüsselindustrie ist die Energieversorgung, zu der Strom, Gas und Öl gehören. Ein Notfall in diesem Bereich betrifft praktisch jede andere kritische Infrastruktur direkt.[13] Die Bundesnetzagentur hat den "IT-Sicherheitskatalog für Strom- und Gasnetze" veröffentlicht, um sicherzustellen, dass für Energieversorger ausreichende Prozesse und Aktivitäten definiert werden, die in dieser bereits regulierten Branche an die Stelle einer B3S treten.

Betroffene Betreiber sind verpflichtet, einen Netzstrukturplan zu erstellen, um aufzuzeigen, welche Anwendungen, Systeme und Komponenten existieren und welche Auswirkungen dies auf die Netzsteuerung haben kann. Eine darauf aufbauende Risikoanalyse muss durchgeführt werden. Dabei sind alle zentralen und dezentralen Anwendungen, Systeme und Komponenten zu berücksichtigen, die für einen sicheren Netzwerkbetrieb notwendig sind. Dazu gehören alle Telekommunikations- und IT-Systeme, die zur Netzsteuerung gehören und somit direkten Einfluss auf den Netzbetrieb haben. Aber auch Systeme, die nicht Teil des Netzleitsystems sind, können im Störungsfall eine Gefahr für die Sicherheit des Netzbetriebes darstellen, wie z.B. Messgeräte an Umspannwerken in Stromnetzen (anders als solche zum Zweck der Messung zur Verbrauchs- und Kostenermittlung).

[13] https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf

Zu den zu berücksichtigenden Kriterien gehören die Beeinträchtigung der Versorgungssicherheit, der Anteil der Betroffenen an der Gesamtbevölkerung, mögliche Risiken für Leib und Leben, mögliche Auswirkungen auf andere Infrastrukturen (z.B. vor- und nachgelagerte Netzbetreiber, Wasserversorgung), aber auch Risiken für Datensicherheit und Datenschutz oder finanzielle Auswirkungen. Die Schadenskategorien reichen von "kritisch" (existentiell bedrohlich, katastrophal) über "hoch" (erhebliche Schadensauswirkungen) bis "mäßig" (begrenzt und überschaubar).

Ursachen (absichtlich)	Ursachen (unbeabsichtigt)
Gezielte IT-Angriffe	Elementargefahren
Computerviren, Malware	Höhere Gewalt
Überwachung der Kommunikation	Organisatorische Mängel
Diebstahl von Computern	Menschliches Versagen
	Technischer Fehler
	Ausfall oder Beeinträchtigung anderer Infrastrukturen und externer Dienste, die für die Netzsteuerung relevant sind.
	Unerwünschte Angriffe und fehlgeleitete Malware

Tabelle 1: Mögliche Ursachen für Bedrohungen

Dabei sind viele Komponenten zu berücksichtigen, wie z.B. Netzwerkleitsysteme, Systeme zur dezentralen Überwachung, Parametrisierung, Konfiguration, Steuerung, Automatisierung und Programmierung, Datenarchivierungssysteme, Router, Switches und Firewalls, Kommunikationsendpunkte, Funksysteme, Steuerungen und SPS-Systeme (SPS = Speicherprogrammierbare Steuerung) einschließlich digitaler Sensor- und Betätigungselemente sowie Mess- und Zählgeräte.

Die Ziele liegen auf der Hand:

- IT-Systeme und die von ihnen unterstützten kritischen Prozesse müssen jederzeit beherrschbar sein.
- Technische Störungen können als solche identifiziert und behoben oder deren Behebung durch andere Mittel sichergestellt werden.
- Risiken durch IT-basierte Angriffe müssen durch geeignete Maßnahmen zum Schutz der relevanten Telekommunikations- und IT-Systeme bewertet und angegangen werden.

Ein einfaches Beispiel: Das Hinzufügen einer neuen Konfiguration zu einem Sensor oder das Senden (aber auch das Verhindern des Sendevorgangs) eines kritischen Befehls an ein Ventil kann ein potenzielles Risiko für wesentliche Bereiche des gesamten Netzwerks darstellen. Dies erfordert angemessene Sicherheitsmaßnahmen auf praktisch jeder der oben genannten Systemebenen.

Zu den typischen Maßnahmen gehören:

- Der administrative Zugriff auf operative, dezentrale Systeme (Sensoren, Steuergeräte) muss geschützt und protokolliert werden.
- Das Verhalten automatisierter Systeme muss überwacht werden, um technische Fehler zu identifizieren oder Angriffsversuche (Hacking) zu erkennen.

- Administrative Endpunkte (Server, verteilte Systeme) müssen umfassend vor Malware und gezielten Angriffen geschützt werden.
- Personenbezogene Daten von Verbrauchern und Bürgern müssen jederzeit vor unerwünschter Verarbeitung geschützt werden.

3.3 Ernährung, Lebensmittel und Wasser

Die Aufrechterhaltung der Ernährung unterliegt ebenfalls den Bestimmungen der KRITIS. Eine zuverlässige Nahrungsmittelproduktion und die Versorgung der Bevölkerung über den Lebensmittelhandel sind unerlässlich. IT-Systeme berücksichtigen unter anderem die aktuelle Marktentwicklung: Produktion, Logistik, Groß- und Einzelhandel werden zunehmend vernetzt und automatisiert. Dies wird dynamisch gesteuert, typischerweise unterstützt durch komplexe Algorithmen, die den Bedarf basierend auf kontextabhängigen Informationen vorhersagen. Da Lieferanten in der Regel ohne nennenswerte Verluste für die Produktionssicherung nur noch über einen kleinen Bestand an Rohstoffen verfügen, sind sie von der Lieferkette abhängig.

Zu den kritischen Infrastrukturen im Ernährungsbereich gehören die Herstellung, Verarbeitung, Konservierung, Bestellung, Verteilung von Lebensmitteln und der Einzelhandel. Kritische Prozesse in all diesen Phasen werden zunehmend mit Hilfe unterstützender IT-Systeme umgesetzt. Eine ordnungsgemäße Risikoanalyse muss für diese durchgeführt und Prozesse und Systeme müssen angemessen geschützt werden.

Während die B3S-Anforderungen für den Lebensmittelhandel und die Lebensmittelindustrie nicht öffentlich zugänglich sind, sind die B3S-Anforderungen für die Wasserwirtschaft[14] klar definiert und veröffentlicht.

Zu den typischen Maßnahmen gehören:

- Bestell- und Kommunikationssysteme zur Aufrechterhaltung der Lieferkette müssen vor Malware und gezielten Angriffen geschützt werden.
- Die Kommunikation zwischen allen Beteiligten (Produktion, Verarbeitung, Aufbewahrung, Bestellung, Vertrieb und Handel) muss vor unbefugten Änderungen und Abholungen geschützt werden.
- Systeme zur Steuerung automatisierter Produktionsprozesse sind vor dem Einfluss Dritter zu schützen, auch vor Bedienungsfehlern. Menschliches Versagen muss somit verhindert werden.
- Steuer- und Messkomponenten in Kühl- und Transportsystemen sind vor technischen Störungen zu schützen.

Ein gut ausgeführtes und auditiertes ISMS (Information Security Management System), das den Anforderungen der DIN ISO/IEC 27001 entspricht, ist wiederum der Kern des Nachweises der Einhaltung der KRITIS-Anforderungen.

[14] https://www.dvgw.de/themen/sicherheit/it-sicherheit/

3.4 Transport

Einer der wichtigsten kritischen Bereiche ist der Verkehr. Der Verkehr ist in sechs wichtige Infrastrukturbereiche unterteilt: Luft, Wasser, See, Wasser, Schiene und Straße. Eine siebte Dimension ist die Logistik, die insbesondere sicherstellt, dass lebenswichtige Güter durch Deutschland transportiert werden. Sie ermöglicht den Transport von Gütern durch Koordination, Zwischenlagerung und rechtliche und kaufmännische Abwicklung.

Der Transport ist eng mit anderen Branchen verbunden, hat aber die Besonderheit, dass Teilbereiche als temporärer Ersatz füreinander dienen können. So kann beispielsweise der Transport per Hubschrauber im Falle einer Straßenblockade vorübergehend dazu beitragen, den tatsächlichen Vorfall zu mildern.

Eine Grundvoraussetzung für moderne arbeitsorientierte Volkswirtschaften, die auf die Mobilität von Gütern und Personen angewiesen sind, ist ein funktionierendes und effizientes Verkehrs- und Transportsystem.[15]

Zum Zeitpunkt der Erstellung dieses Dokuments war der Transportbereich durch die verfügbaren B3S-Dokumente nur wenig abgedeckt. Lediglich das B3S-Dokument über Verkehrsregelungs- und Leitsysteme im kommunalen Straßenverkehr lag als (kostenpflichtige) DIN-Norm vor. Die Dokumente über B3S im Luftverkehr und für Betreiber von öffentlichen Verkehrsmitteln und Schienenverkehr wurden beim BSI geprüft.

Die vom BSI im Jahr 2015 in Auftrag gegebene KRITIS-Sektorstudie[16] "Transport und Verkehr" liefert erste Empfehlungen, die mit denen anderer Branchen vergleichbar sind. Dazu gehören die Implementierung eines ISMS nach ISO 27001, die Implementierung von Maßnahmen nach BSI IT Grundschutz, Training, Sensibilisierung und branchenspezifischer Informationsaustausch zwischen Infrastrukturbetreibern.

Für typische Maßnahmen im Transport siehe Abschnitt 4.

15 https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/Sektoren/TransportundVerkehr/TransportundVerkehr_node.html

16 https://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/Sektorspezifisch/TuV/Sektorstudie_TuV.html

3.5 Gesundheitswesen

Die medizinische Versorgung mit ihren Abhängigkeiten von anderen kritischen Bereichen wird als kritische Infrastruktur eingestuft. Der Gesundheitssektor bezieht sich auf das gesamte Gesundheitssystem. Das Gesundheitswesen ist nicht so abhängig von der IT wie andere kritische Bereiche, aber dennoch ist eine moderne Leistungserbringung ohne IT undenkbar und unmöglich. Die Bereiche "Medizinische Versorgung", "Medikamente und Impfstoffe" und "Laboratorien" werden im Zusammenhang mit kritischen Infrastrukturen betrachtet. Auch im Notfall muss sichergestellt sein, dass Bürger und Behörden medizinische Versorgung erhalten können.

Die KRITIS-Sektorstudie "Kritische Infrastrukturen Gesundheitswesen"[17] vertiefte den Blick auf den gesamten Sektor und die Querabhängigkeiten zu verwandten KRITIS-Bereichen wie Wasser, Energie, Verkehr, Informations- und Kommunikationstechnologie.

Bei der Identifizierung kritischer Bereiche im Gesundheitswesen verwendet diese Studie eine zweidimensionale Matrix auf a) der Grundlage der Dringlichkeit der Leistung und b) der Anzahl der Fälle = betroffene Patienten. Je höher die Dringlichkeit und die Anzahl der gleichzeitig betroffenen Fälle, desto kritischer ist ein Gesundheitsdienst.

Der Ausfall von Information und Kommunikation ist ein kritisches Risiko, da er erhebliche Auswirkungen auf viele Aspekte der Gesundheitsversorgung hat, z.B. bei der Aufrechterhaltung der Versorgung mit medizinischen Dienstleistungen. Viele weitere Aspekte, die für ein funktionierendes Gesundheitssystem unerlässlich sind, müssen ebenfalls berücksichtigt werden. Dazu gehören:

- Patientenmanagement, Finanzen, klinische Dokumentation
- Bestellung von Medikamenten, Laborergebnisse
- Elektronische Patientenakte
- Organisation von Rettungseinsätzen

Für Krankenhäuser wurde bereits ein B3S-Leitfaden erstellt, weitere sind zum Zeitpunkt der Erstellung dieses Dokuments nicht verfügbar. Der im "Branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus" gewählte Ansatz ergänzt die gemeinsamen Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) um zwei weitere.

- „Patientensicherheit: Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen oder eines Schadens an Eigentum oder der Umwelt
- Behandlungseffektivität: Wirksame Behandlung des Patienten unter Benutzung ausgetauschter Informationen sowie die Anwendung wirksamer Gesundheitsmaßnahmen, durch die verantwortliche Organisation aufgrund des Informationsaustausches“[18]

[17] https://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/Sektorspezifisch/Gesundheit/Sektorstudie_Gesundheit.html
[18] https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/2018_12_18_532_ITSiG_Kritis_B3S_Einreichung_BSI.pdf

IT-Systeme werden nach der Zeitspanne kategorisiert, in der ihr Ausfall kompensiert werden kann. Das bedeutet, dass Systeme der Klasse 1, die nur für kurze Zeiträume nicht verfügbar sein dürfen, höchsten Schutz benötigen.

Zu den empfohlenen Maßnahmen (basierend auf den tatsächlichen Vorfällen, wie sie in der Sektorstudie dokumentiert sind) gehören:

- Alle operativen Systeme müssen vor Malware und gezielten Angriffen geschützt werden.
- Access Governance und Privilege Management müssen implementiert werden, um unerwünschte administrative Zugriffe (z.B. nach Beendigung des Arbeitsvertrags) zu verhindern.
- Patientendaten müssen durch Verschlüsselung, Identitäts- und Zugriffsmanagement, privilegierte Kontenverwaltung und die Umsetzung des Minimalprinzips ("Least Privilege") geschützt sein.
- Bestell- und Kommunikationssysteme zur Aufrechterhaltung der Arzneimittelversorgung müssen vor unbefugter Verwaltung oder Vandalismus geschützt werden.
- Die Kommunikation zwischen allen Beteiligten (Pharmaindustrie, Krankenhäuser, Behörden, Labors usw.) muss vor unbefugten Änderungen und Eingriffen geschützt werden.

3.6 Finanzen und Versicherungen

Während andere kritische Infrastrukturen immer noch materielle Güter und Dienstleistungen umfassen, wird der Bereich des Finanz- und Versicherungssektors fast vollständig durch Informations- und Kommunikationssysteme kontrolliert und unterhalten. Im Finanz- und Versicherungswesen existieren viele wichtige Dienstleistungen und Produkte nur virtuell und digital. Relevante Daten und Fakten werden in IT-Systemen verarbeitet und in Datenspeichern gespeichert, die über ein Netzwerk zugänglich sind. Das eigentliche Produkt ist somit nicht direkt überprüfbar, sondern nur durch seine Auswirkungen auf die Prozesse, z.B. als Kontoauszug oder im Kreditkartenzahlungsprozess.

Der Bereich Finanzen und Versicherungen gliedert sich in vier Hauptbereiche: Banken, Börsen, Versicherungen und Finanzdienstleister. Wenn die Infrastruktur, die Software oder die Kommunikationsinfrastruktur nicht reibungslos funktionieren, kann dies zu hohen Verlusten auf den Finanzmärkten und damit zu hohen Verlusten für die Volkswirtschaften oder die Gesellschaft im Allgemeinen führen. Es muss sichergestellt sein, dass die unterstützende IT genau und sicher funktioniert und insbesondere, dass Benutzer, d.h. Kunden, reguläre Mitarbeiter und Personen mit administrativen Zugriffsrechten, die Systeme nicht negativ beeinflussen können. Die Destabilisierung durch Angriffe und nationale oder globale Krisen gehören zu den Hauptrisiken für diesen Bereich der kritischen Infrastruktur.

Der Zusammenbruch von Lehman Brothers (obwohl nicht durch KRITIS-relevante Ursachen bedingt) im Jahr 2008 und die folgende globale Finanzkrise sind ein relevantes Beispiel dafür, welche Dominoeffekt-Szenarien mit angemessenen Kontrollen verhindert werden sollen. Dies war ein wirklich globaler Vorfall mit direkten oder indirekten Auswirkungen auf mehr oder weniger alle. Es kam zu einem Dominoeffekt, und selbst Unternehmen, die nicht direkt mit Lehman Brothers verbunden waren, waren von fallenden Aktienkursen betroffen und begannen zu schwanken.

Die KRITIS-Anforderungen an den Finanzsektor zielen insbesondere darauf ab, zu verhindern, dass diese Art von kaskadierenden Auswirkungen durch böswillige oder fehlerhafte Nutzung der IT verursacht werden.

Unternehmen im Finanzdienstleistungssektor können als Vorbilder und Quellen für bewährte Verfahren angesehen werden, insbesondere für die Umsetzung angemessener Kontrollen der Informationstechnologie und Telekommunikation.

Der seit langem bestehende regulatorische Druck in diesen Bereichen, z.B. durch die Anforderungen der BaFin (Bundesanstalt für Finanzdienstleistungsaufsicht), stellt sicher, dass der Anteil der möglicherweise nicht erfüllten Anforderungen von KRITIS für Finanzinstitute und die verschiedenen Versicherungsbranchen in der Regel am geringsten ist. Damit können diese als Lieferanten für Best Practices fungieren, da sie den notwendigen Wandel viel früher als andere Sektoren durchlaufen haben. Die BaFin als Regulierungsbehörde für das Finanzdienstleistungsgeschäft in Deutschland hat kürzlich ihre Anforderungsdokumente aktualisiert und erweitert. Die "Bankaufsichtliche Anforderungen an die IT - BAIT" und die "Versicherungsaufsichtliche Anforderungen an die IT - VAIT" definieren klar und deutlich eine Reihe von Anforderungen, die als Blaupause für die Implementierung von Kontrollen zur KRITIS-Compliance verstanden werden können.

Zu den Anforderungen von BAIT und VAIT, die auch für die KRITIS-Konformität von Vorteil sind, gehören:

- Zuverlässige Identitäten für alle Benutzer mit einem kompletten Lebenszyklus
- Einheitliche Benutzerrechteverwaltung
- Verwendung von organisatorischen und funktionalen Berechtigungen
- Grundsatz der geringsten Privilegien (Minimalprinzip)
- Funktionstrennung (Segregation of Duties)
- Regelmäßige Rezertifizierung von Berechtigungsvergaben
- Regelmäßige Überprüfung der Berechtigungsdefinitionen
- Anforderung, Genehmigung und Dokumentation von Berechtigungen
- Überwachung und Analyse der vergebenen Berechtigungen
- Verwaltung von technischen, nicht personalisierten Konten

Die Überarbeitung des BAIT 2017 beinhaltet einen zusätzlichen Abschnitt, der ein KRITIS-Sicherheitsziel definiert, das von den Banken erreicht werden soll: "Unter KVP-Ziel ist hier die Aufrechterhaltung der Versorgungssicherheit der Gesellschaft für die in § 7 BSI-KritisV genannten kritischen Dienstleistungen (Bargeldversorgung, kartengestützte Zahlungstransaktionen, konventionelle Zahlungstransaktionen und Clearing und Abwicklung von Wertpapier- und Derivatgeschäften) zu verstehen, da der Ausfall oder die Beeinträchtigung dieser Dienstleistungen zu schwerwiegenden Versorgungsstörungen oder Bedrohungen für die öffentliche Sicherheit führen könnte."[19]

Typische Maßnahmen zur Erreichung dieses Ziels sind:

- Sichere Kreditkartenzahlungssysteme durch die Implementierung und Überprüfung der PCI-DSS-Anforderungen (einschließlich Privilege Access Management).
- Schutz der Kernbankensysteme vor Malware und gezielten Angriffen.
- Schutz der Bargeldversorgung, indem Geldautomaten-Systeme gehärtet und vor der Ausnutzung von Betriebsfehler durch Dritte geschützt werden. Menschliches Versagen und Vandalismus müssen verhindert werden.

[19] https://www.bafin.de/dok/10445406

4 Transportspezifisches Bedrohungsszenario (Eisenbahn)

Mögliche Angriffe auf die Informationstechnologie und Kommunikation sind wichtig zu verstehen. Die DB (Deutsche Bahn) wird als Vertreter des Verkehrssektors ausgewählt. Dieses dennoch theoretische Beispiel veranschaulicht die möglichen Bedrohungen durch IT-Störungen.

4.1 Definition des Szenarios

Die DB besteht aus mehreren Unternehmen, die die verschiedenen Bereiche Transport, Steuerung und Logistik abdecken. Es gibt Unternehmen für den Personenfernverkehr, den öffentlichen Personennahverkehr, den Schienengüterverkehr und ein Eisenbahninfrastrukturmanagementunternehmen. Die IT selbst lässt sich in vier Bereiche unterteilen, die miteinander verbunden sind und zusammenlaufen:

- Personenbeförderung (Ticketkauf, Kontrolle im Zug, WiFi im Zug,....)
- Güterverkehr und Logistik
- Infrastruktur (Züge, Weichen, Signale, Aufzüge)
- Gruppenleitung (Verwaltung, Buchhaltung, Management)

Das Zusammenspiel der einzelnen Bereiche wird anhand eines realen Szenarios veranschaulicht, das anschließend mit anderen Anwendungsfällen abgestimmt werden kann:

Ein DB-Kunde sucht mit seinem Smartphone nach einer Verbindung für die Fahrt von Stuttgart nach Köln. Er wählt ein 1. Klasse-Ticket, reserviert einen Platz und bezahlt per Kreditkarte. Die Informationen, auf welcher Strecke sein Zug abfährt, werden sofort angezeigt und in der mobilen DB-Applikation aktuell gehalten. Sie wird ihn rechtzeitig darüber informieren, dass der Zug einige Minuten zu spät kommt.

Dieses einfache Beispiel kann aus einer anderen Perspektive betrachtet werden. Wenige Tage vor der Buchung der Zugfahrt durch den Kunden ändert ein DB-Mitarbeiter über eine interne Verwaltungsseite eine Zugverbindung. Einige Verbindungen von Stuttgart nach Köln müssen aufgrund von Wartungsarbeiten später eine alternative Route nutzen. An dem Tag, an dem der Kunde die Zugfahrt bucht, kennzeichnet die Streckenüberwachung einen Streckenabschnitt „rot“ für einen Zug von Berlin nach Stuttgart aufgrund eines kleineren Notfalls. Dadurch wird die ursprüngliche Route blockiert, was dazu führt, dass andere Züge zu spät fahren. Ein erfahrener Dispatcher kann die Verzögerungen so gering wie möglich halten. Nach 15 Minuten ist die Strecke wieder frei.

4.2 Analyse und Kontrolle

Dieses Beispiel enthält viele Prozesse, die IT-gestützt sind und daher angemessen geschützt werden müssen. Dazu gehören Authentifizierungsprozesse für Kunden, die sich an einem Portal anmelden und etwas kaufen. Es gibt Authentifizierungsprozesse für Mitarbeiter, die Änderungen an kritischen Elementen vornehmen und aktiv in die Steuerung und Planung von Signalanlagen und Schaltern eingreifen.

Mögliche Bedrohungen in diesem Szenario können wie folgt kategorisiert werden:

	Technische Fehler	**Menschliches Versagen**	**Kriminelle oder terroristische Handlungen**
Sprach- und Datenübertragung	Ausfall oder technische Fehlfunktion von Infrastruktur-komponenten	Menschliches Versagen, z.B. bei umfangreichen Konfigurationsänderungen von Infrastrukturkomponenten	Vorsätzliche Manipulation oder Cyber-Angriffe auf Infrastrukturkomponenten
Datenspeicherung und -verarbeitung			

Tabelle 2: Bedrohungen für infrastruktur- und kommunikationskritische Bereiche

Im Hinblick auf die Anforderungen der IT an die Dienste "Sprach- und Datenübertragung" und "Datenspeicherung und -verarbeitung" gilt es, unerwünschte Ereignisse oder Zustände zu verhindern oder zumindest zu erkennen und zu steuern. In diesem Fall geht es der IT insbesondere darum, wer wann, warum und in welchem Umfang welche Maßnahmen durchführen darf. Dabei geht es nicht um traditionelles Identitätsmanagement, sondern um die Verfügbarkeit des Dienstes im Allgemeinen.

In dem beschriebenen Szenario hat der Dispatcher Änderungen an der Konfiguration eines Systems vorgenommen. Auf technischer Ebene wurden dem Dispatcher über ein Berechtigungssystem die notwendigen Zugriffsrechte erteilt. Unabhängig davon, ob es sich um eine Standardberechtigung und -funktion oder bereits um eine weitreichende Änderung des Eisenbahnsystems handelt, muss sichergestellt sein, dass eine automatisierte Richtlinie oder eine dritte Person diese Konfigurationsänderung bestätigt oder dass eine automatisierte oder manuelle Überwachung stattfindet.

Zum Schutz der IT und damit der kritischen Infrastruktur müssen bestimmte Voraussetzungen für den Zugriff von Benutzern mit privilegierten Berechtigungen erfüllt sein. Dazu gehören

- Beschränkung des Zugriffs für bestimmte Benutzer auf ausgewählte Systeme
- Widerruf des Zugangs bei nicht mehr benötigter Nutzung
- Einfache, sichere und automatisierte Passworteingabe, idealerweise mehrstufige Authentifizierung

- Zentralisierte Verwaltung von Zugriffsrechten in heterogenen Netzwerken
- Präzises Audit für jede Aktion von privilegierten Benutzern

Diese Anforderungen stellen sicher, dass menschliche Fehler reduziert und vorsätzlicher Missbrauch ausgeschlossen wird. Im beschriebenen Szenario erfordert eine Änderung des Zugfahrplans, die erhebliche Auswirkungen auf das Gesamtsystem haben könnte, die Genehmigung und/oder Überwachung einer anderen Person.

4.3 Szenariobasierte Risikoanalyse

Das oben genannte Beispiel zeigt, dass die kontinuierliche Durchführung einer angemessenen Risikobewertung eine zentrale Herausforderung für den Schutz kritischer Infrastrukturen ist. Die Verwendung von Use Cases und Szenarien kann bei der Risikobewertung und der Identifizierung geeigneter Maßnahmen unterstützen.

Die folgenden Szenarien veranschaulichen die erforderliche Breite und Tiefe der Analyse:

- Im Falle eines Fehlers oder Systemausfalls muss eine geeignete Wiederherstellungsstrategie vorhanden sein und die richtigen Personen schnellen Zugriff auf die zugrunde liegenden Systeme und Konfigurationen haben. Sogenannte "Break-the-glass"-Szenarien sind für kritische Infrastrukturen von hoher Bedeutung und ermöglichen den sofortigen Zugriff auf die Verwaltung oder den Neustart von Kernsystemen.
- Wartungsverträge mit Lieferanten, die kritische Funktionen als Dienstleistung anbieten, sind eine besondere Herausforderung. Es ist sicherzustellen, dass deren Mitarbeiter keine anderen als die erforderlichen Arbeiten an den Systemen durchführen.
- Neben dem Schutz vor vorsätzlichem Missbrauch durch den Mitarbeiter muss sichergestellt sein, dass das absichtliche Abfangen von Zugangsdaten oder einer laufenden Login-Sitzung durch so genannte Man-in-the-Middle-Angriffe verhindert wird, bei denen der Angreifer vorgibt, das Zielsystem für den Benutzer und der Benutzer für das Zielsystem zu sein.

5 Schutz der IT in kritischen Infrastrukturen

Kritische Infrastrukturen unterscheiden sich in ihren jeweiligen Kerngeschäftsfeldern erheblich. Das Wissen und die Erfahrung von erfahrenen Ingenieuren und einer Vielzahl von Experten ist daher notwendig, um die verschiedenen Aspekte der jeweiligen Geschäftsprozesse angemessen zu schützen und zu erhalten. Als zentraler und immer wichtiger werdender gemeinsamer Nenner ist jedoch jede kritische Infrastruktur zunehmend von der Informationstechnologie abhängig.

Die Gewährleistung der Sicherheit großer kritischer Infrastrukturen führt zu mehr IT. Um branchenspezifische Sicherheitsanforderungen umsetzen zu können, werden zunehmend IT-Sicherheitssysteme eingesetzt, die als technisches Mittel auch systeminterne Schwachstellen und die daraus resultierenden Bedrohungen kontrollieren.

5.1 IT ist für KRITIS von entscheidender Bedeutung

IT-basierte Systeme sind unverzichtbare Elemente für Steuerungs- und Überwachungssysteme aller Art. Viele wesentliche Prozesse in der Logistik oder der modernen Energieversorgung wären heute ohne die Unterstützung der IT nicht mehr möglich. IT dient der Automatisierung oder zur Unterstützung bei manuellen Vorgängen. Gerade in Notfällen unterstützt sie, schnell und automatisch Maßnahmen auswählen und umsetzen zu können.

Allen geschäftsunterstützenden und sicherheitsrelevanten Systemen ist gemeinsam, dass sie auch auf allen Ebenen angemessen geschützt werden müssen. Dies gilt insbesondere für die unerwünschte Nutzung oder den Missbrauch durch Mitarbeiter und Kunden, Benutzer und Administratoren oder den zweifelsfrei zu erkennenden, externen Angreifer. In einer weitgehend automatisierten und verteilten Infrastruktur muss diese Kontrolle auch für technische Systeme (Sensoren, Aktoren) mit eigener dezentraler und autonomer Identität gelten.

IT-Sicherheit und Cyber-Resilienz können als der gemeinsame Nenner aller Sektoren angesehen werden. Über die individuellen, branchenspezifischen Anforderungen hinaus werden Best Practices für IT-Kontrollen und deren Management empfohlen.

IT-Sicherheit ist ein „Schwächstes-Glied-Szenario“: Der Verteidiger muss viele verschiedene Systeme und Komponenten schützen, während der Angreifer nur eine - oder wenige - Schwachstellen identifizieren muss, um in kritische IT und damit kritische Infrastrukturen einzudringen. Dies führt zur Notwendigkeit einer adäquaten Sicherheitsarchitektur als Teil der Gesamt-IT-Architektur. Diese muss Risiken, Bedrohungen und Schwachstellen adressieren, ohne das Unternehmen zu beeinträchtigen, für das es entwickelt wurde.

5.2 ISMS als Kernstück der KRITIS-Konformität

Ein gemeinsamer Nenner aller relevanten Richtlinien, einschließlich der B3S-Dokumente und z.B. des "IT-Sicherheitskatalogs für Strom- und Gasnetze", ist die ordnungsgemäße Dokumentation der bestehenden Infrastruktur, gefolgt von einer gründlichen Risikoanalyse zur Identifizierung der zu schützenden Prozesse und Systeme sowie der umzusetzenden Kontrollen.

Es gibt also eine zentrale Anforderung an alle Anbieter kritischer Infrastrukturen: Die obligatorische Einrichtung eines ISMS (Information Security Management System), das die Anforderungen der DIN ISO/IEC 27001 in der aktuellen Fassung erfüllt. Die isolierte Umsetzung einzelner Maßnahmen (Antivirensoftware, Firewalls, etc.) wird als unzureichend erachtet. Vielmehr ist ein umfassender, kontinuierlicher und nachhaltiger Ansatz erforderlich, um die jeweiligen Schutzziele zu erreichen. Seine Leistung und Wirksamkeit werden überprüft und gegebenenfalls angepasst. Seine Umsetzung und Verwendung unterliegen einer Auditierung.

5.3 Threat intelligence und moderne Security Operations Centers

Über die notwendigen Maßnahmen für eine reine KRITIS-Checklistenkonformität hinaus werden die bisher genannten Maßnahmen zunehmend als nicht ausreichend angesehen. Das oberste Ziel ist es, einen kontinuierlichen Schutz zu gewährleisten. Cyberkriminelle entwickeln ständig die Werkzeuge, Techniken und Prozesse (WTPs) weiter, mit denen sie ihre Opfer, einschließlich kritischer Infrastrukturen, angreifen. Sie nutzen ein hoch entwickeltes, kommerzielles Ökosystem, um sowohl bestehende als auch neue, bisher ungenutzte WTPs gemeinsam zu nutzen.

Insbesondere die Betreiber kritischer Infrastrukturen müssen in hohem Maße auf aktuelle Bedrohungen vorbereitet sein. Deshalb ist Threat Intelligence ein wesentlicher Bestandteil der Cyberabwehr und der Reaktion auf Security Vorfälle (Incidents). Sie liefert Informationen über Bedrohungen, WTPs und die Geräte, die von Cyber-Angreifern eingesetzt werden, über die Systeme und Informationen, auf die sie abzielen, sowie andere bedrohungsbezogene Informationen, die ein besseres Lagebild bieten. Diese Informationen müssen zeitnah, relevant, genau, spezifisch und nutzbar sein. Security Operations Centers (SOC) gewinnen zu diesem Zweck immer mehr an Bedeutung, da sie die zeitnahe Verfügbarkeit von umsetzbarer Threat Intelligence in einer Form bereitstellen und nutzen, die leicht ausgewertet werden kann, um nicht nur bekannte, sondern auch neue und aufkommende Angriffsmuster zu erkennen.

5.4 Privilegiertes Zugriffsmanagement integriert mit IAM

Die Ursache für die meisten dokumentierten Angriffe sind kompromittierte privilegierte Benutzerkonten. Dies wird in der Regel dadurch erleichtert, dass diese Konten keinem festen Lebenszyklus unterliegen und es keine präzise Überwachung der Anzahl der bestehenden Management-Accounts gibt.

Die Integration von Identitäts- und Zugriffsmanagement und Privilegiertem Zugriffsmanagement auf architektonischer Ebene ermöglicht die Definition und Bereitstellung einer Vielzahl von Governance- und Verwaltungsprozessen. Die folgende Abbildung gibt einen Überblick über die erforderlichen Grundkomponenten. Für ein umfassendes Bild des Themenbereichs Privileged Access Management lesen Sie bitte den KuppingerCole-Bericht 72330 Leadership Compass Privilege Management[20].

Abbildung 2: Übersicht der funktionalen Komponenten zur Verwaltung privilegierter Benutzer

Das IAM-System eines Unternehmens ist der Ausgangspunkt für die Verwaltung von Identitäten und die Vergabe von Berechtigungen. Der Access Manager ist für die Überprüfung und Implementierung definierter Richtlinien für privilegierte Benutzer verantwortlich. Auf dieser Grundlage bietet der Session Manager die Möglichkeit, die Sitzung eines Benutzers zu analysieren, zu verwalten und zu beenden und gleichzeitig die Sitzungsisolation als wichtige Sicherheitsschicht hinzuzufügen. Die Passwörter für Systeme werden im Password Vault gespeichert, damit auch ein privilegierter Benutzer nie das aktuelle Passwort kennt, sondern nur über den Access Manager Zugriff auf die für ihn verwalteten Zielsysteme hat.

[20] https://www.kuppingercole.com/report/lc72330

Bei der Anwendung dieses Konzepts auf das oben beschriebene Transportbeispiel übernimmt das IAM die grundlegende Aufgabe, den Zugriff für den Dispatcher auf Systeme wie Mail-, Computer- und Dateifreigaben freizugeben. Darüber hinaus kann das operative Dispositionssystem als privilegiertes System nur über den Access Manager aufgerufen werden, und der Session Manager überwacht die spezifischen Aktionen, die bei der Änderung eines Zeitplans durchgeführt werden. Der Password Vault enthält die Passwörter für das Dispositionssystem, die der Benutzer nicht einsehen kann. Dadurch wird sichergestellt, dass in diesem vereinfachten Szenario (nur) der benannte Dispatcher alle erforderlichen Operationen durchführen kann, während das erforderliche Maß an Sicherheit, Kontrolle und Audit gewährleistet ist.

6 Schutz kritischer Infrastrukturen mit den Sicherheitslösungen von CyberArk

Anforderungen an die Cybersicherheit für kritische Infrastrukturen haben oft einen anderen Fokus als der Schutz der traditionellen Unternehmens-IT. Eine solide Cybersicherheitsstrategie, die marktführende und hochmoderne Lösungen nutzt, unterstützt kritische Infrastrukturen und ist ein wichtiger Baustein in einem umfassenden Schutzkonzept für KRITIS.

Unternehmen, die kritische Infrastrukturen bereitstellen, benötigen einen einheitlichen Ansatz für die Verwaltung, Kontrolle und Überwachung des Zugriffs auf und des Betriebs auf diesen Systemen. Zu den wesentlichen Kernfunktionalitäten, die erforderlich sind, gehören die privilegierte Passwortkontrolle und -verwaltung, die Isolation und Überwachung von Sitzungen sowie eine begleitende Bedrohungsanalyse. Jedes einzelne System im Rahmen der KRITIS-Anforderungen hat ein entsprechend hohes Schutzniveau, damit es nicht zum Ziel wird.

Privileged Access Management ist eine Reihe von kritischen Cybersicherheitskontrollen, die sich mit dem Management von Sicherheitsrisiken befassen, die mit einem privilegierten Zugriff in einem Unternehmen verbunden sind. Die Kontrolle privilegierter Benutzer, erweiterter Zugriffsrechte und gemeinsam genutzter Konten erfordert eine gut integrierte Lösung, die aus Risikominimierung, klar definierten Prozessen und durchdachter Implementierung besteht.

Privilegierte Zugriffsmanagement-Tools sind so konzipiert, dass sie eine Vielzahl von Anwendungsszenarien abdecken, die für kritische Infrastrukturen typisch sind. Das Zusammenspiel mit operativen Systemen, deren Steuerung, Überwachung und Konfiguration durch Techniker, Administratoren, aber auch automatisierte Prozesse soll im täglichen Betrieb, aber auch in Ausnahmefällen oder Notfällen sichergestellt werden. Um dies zu erreichen, sind sichere Systeme und Prozesse erforderlich, z.B. für

- die Verwendung von gemeinsam genutzten Konten,
- die Überwachung von privilegierten Aktivitäten und
- die kontrollierte temporäre Erweiterung von Zugriffsrechten.

6.1 Übersicht

CyberArk bietet eine End-to-End-Lösung für privilegierte Zugriffssicherheit auf einer einzigen, gut integrierten Plattform. Sie bietet eine kritische Schicht von IT-Sicherheitstools zum Schutz von Daten, Infrastruktur und Ressourcen im gesamten Unternehmen, in verteilten Umgebungen und in der Cloud. Die CyberArk-Lösung ist ein wichtiger Baustein für die Implementierung robuster Controls zur Erfüllung zentraler Anforderungen von KRITIS an die IT-Infrastruktur in allen Branchen.

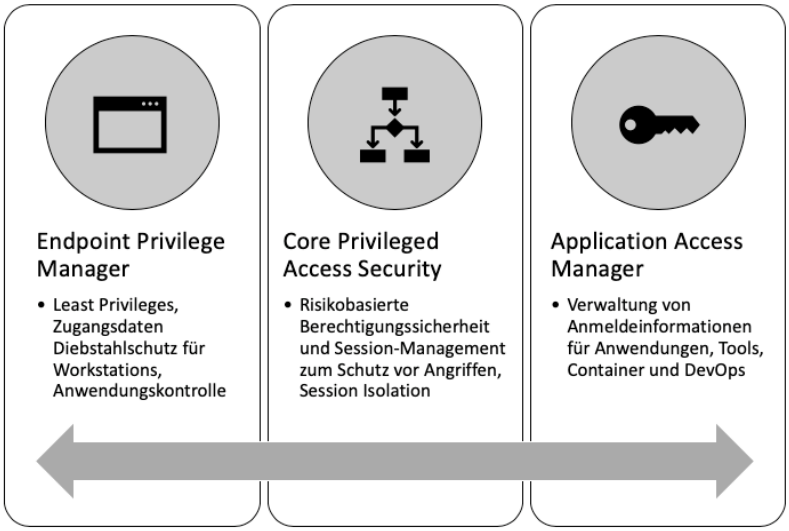

Abbildung 3: Lösungen und Produkte von CyberArk

- Privileged Account Security (PAS)[21] bietet ein mehrstufiges Kernportfolio, einschließlich privilegierter Passwortverwaltung, Sitzungsisolierung und -aufzeichnung, Durchsetzung des Minimalprinzips und privilegierter Datenanalyse. PAS hilft gegen fortgeschrittene persistente Bedrohungen (APTs = Advanced Persistent Threats) und Bedrohungen durch Insider.
- Der Application Access Manager (AAM)[22] kümmert sich um das Management von Passwörtern und Schlüsseln für Anwendungen, Tools, Container und DevOps-Szenarien und lässt sich gut mit Drittanwendungen integrieren.
- Der Endpoint Privilege Manager (EPM)[23] bietet eine zusätzliche kritische Schutzschicht auf dem Arbeitsplatz als Endpunkt, um die Sicherheit zu erhöhen.

21 https://www.cyberark.com/products/privileged-account-security-solution/core-privileged-account-security/
22 https://www.cyberark.com/products/privileged-account-security-solution/application-access-manager/
23 https://www.cyberark.com/products/privileged-account-security-solution/endpoint-privilege-manager/

Das CyberArk-Portfolio umfasst eine vollständig integrierte Umgebung für On-Premise-, Hybrid- und Cloud-Szenarien. Durch dieses komplementäre Produktportfolio steht eine umfassende Funktionalität zur Verwaltung privilegierter Konten für den Einsatz in kritischen Infrastrukturen zur Verfügung. Dies ermöglicht einen integrierten, aber modularen Ansatz zur Definition und kontinuierlichen Weiterentwicklung eines umfassenden risikoorientierten Konzepts zur Identifizierung und Implementierung wirksamer Kontrollen, die für den Schutz kritischer Infrastrukturen unerlässlich sind.

6.2 Schutz des Endpunktes

Obwohl diese Tatsache oft übersehen wird, beginnt Privileged Access Security am Endpunkt, egal ob es sich um die Desktop-Workstation oder einen Backend-Server handelt. Der Endpoint Privilege Manager (EPM) von CyberArk stellt sicher, dass vertrauenswürdigen Anwendungen erweiterte Zugriffsrechte als Teil der Richtlinienanwendung gewährt werden, während die Administratorrechte unmittelbar nach der Verwendung entzogen werden. Dadurch wird die Angriffsfläche deutlich reduziert.

Ergänzend zum Schutz von Anmeldeinformationen bietet das EPM eine Verhaltensanalyse, um festzustellen, ob versucht wird, Anmeldeinformationen vor dem Zugriff auf einen Endpunkt zu stehlen. In diesem Fall wird der Zugriff beendet und der Benutzer isoliert.

Berechtigungsmanagement	Anwendungskontrolle	Schutz vor Identitätsdiebstahl
• Entfernt lokale Administratorrechte von Geschäftsanwendern, um die Angriffsfläche zu reduzieren und kritische Schwachstellen zu minimieren. • Erweitert die Berechtigungen für autorisierte Anwendungen bei Bedarf. • Separiert die Verwaltungsaufgaben auf Windows-Servern, um die Berechtigungen bei Bedarf zu isolieren.	• Automatisiert das Blockieren der Ausführung nicht genehmigter Anwendungen. • „Greylisting“ unbekannter Anwendungen, die dann im eingeschränkten Modus ausgeführt werden. • Schutz vor unbekannten Risiken durch den Service Application Risk Analysis.	• Erkennen und Blockieren von vermuteten Versuchen des Diebstahls von Berechtigungen • Schutz der Anmeldeinformation im Betriebssystems-, Browser- und File-Cache. • Einschränkung eines Angreifers auf einen einzigen Endpunkt und Vermeidung von lateral movement (Verbreitung auf andere Systeme).

Tabelle 3: Funktionen von Endpoint Privilege Manager

6.3 Privilegierte Berechtigungsverwaltung, Sitzungsverwaltung und privilegierte Bedrohungsanalyse

Der Schutz und die Kontrolle von Anmeldeinformationen sind buchstäblich die zentrale Herausforderungen in jeder kritischen Infrastruktur. Die enge Integration von KRITIS in die Normenfamilie ISO 27000 macht somit den dies fordernden Anhang A.9.2.3 der ISO27001 "Management of Privileged Access Rights" zu einer zentralen Anforderung.

Der CyberArk Enterprise Password Vault wird zum Schutz und zur Verwaltung von Anmeldeinformationen für interaktive und Servicekonten verwendet. Die detaillierte Berechtigungsverwaltung stellt sicher, dass privilegierte Benutzer die entsprechende Berechtigung zum Ausführen der gewünschten Funktion haben. Die Anmeldeinformationen werden an einem zentralen und sicheren Ort („secure digital vault“ = „sicherer digitaler Tresor“) für alle angeschlossenen Systeme gespeichert. Passwörter und Schlüssel werden nach definierbaren Regeln gedreht.

Der Privileged Session Manager wird zur Steuerung und Überwachung von Sitzungen verwendet. Es verbindet den privilegierten Benutzer mit dem erforderlichen Administratorkonto, ohne die Anmeldeinformationen für das privilegierte Konto direkt zugänglich zu machen. Die Möglichkeit, privilegierte Sitzungen aufzuzeichnen und/oder zu überwachen, kann dazu beitragen, verdächtige Aktivitäten in Echtzeit zu verhindern oder Beweise ex post zu liefern. Die automatisierte Risikobewertung kann einzelne Sitzungen priorisieren, die vom Sicherheitsteam überwacht werden sollten.

Darüber hinaus isoliert es den Computer des Benutzers vom Zielsystem, was verhindert, dass sich potenzielle Malware auf dem Computer des Benutzers befindet, um das Zielsystem zu infizieren. Diese Isolierung ist ein wichtiger Sicherheitsgewinn.

Die privilegierte Bedrohungsanalyse („Privileged Threat Analytics“) kombiniert die Vermeidung und die Erkennung von Bedrohungen mit der Reaktion auf diese. Access Analytics sammelt und analysiert Daten von mehreren Plattformen mit dem höchsten Risikopotenzial für das Unternehmen. Mit statistischen Modellen, Machine Learning und „User and Entity Behavior Analytics“ (UEBA) werden verdächtige Aktivitäten erkannt. Diese können dann manuell oder automatisch gestoppt oder vom Sicherheitsteam überwacht werden. Die Anbindung an bestehende SIEM-Systeme für den bidirektionalen Datenaustausch bietet darüber hinaus erweiterte Möglichkeiten, Unregelmäßigkeiten oder Systemänderungen zu finden.

6.4 Applikationszugriffe mit Application Access Manager schützen

Eine besondere Herausforderung in der kritischen Infrastruktur ist die Vielzahl von zentralen und dezentralen Anwendungen, Systemen und Komponenten. Betreiber kritischer Infrastrukturen verlassen sich bei der Bereitstellung ihrer Produkte und Dienstleistungen in der Regel sowohl auf kommerzielle als auch auf intern entwickelte Anwendungen. Dazu gehören zum einen die für den sicheren Betrieb der Infrastruktur notwendigen Kernsysteme und alle dafür notwendigen Telekommunikations- und IT-Systeme, wie zum Beispiel die direkte, aktive Netzsteuerung.

Aber auch Systeme, die nicht direkt Teil der Netzsteuerung sind, deren Ausfall die Sicherheit des Netzbetriebs gefährden könnte (z.B. IT-basierte Infrastruktur), müssen berücksichtigt, gesteuert und überwacht werden.

Verwaltete Systeme werden immer dynamischer in Größe und Struktur und erfordern zunehmend automatisierte IT-Infrastrukturen und DevOps-Methoden zur Verwaltung der Komplexität. Während Kernsysteme und ihre IT-Umgebungen weitgehend statisch sind, können andere, wie beispielsweise hochverteilte Sensornetzwerke und containerisierte Umgebungen, sehr dynamisch sein. Der manuelle Zugriff ist die Ausnahme. So müssen neben den Rechten von menschlichen Nutzern mit erhöhtem Zugriff auch die Berechtigungen von Systemen und Diensten - so genannte technische Konten - verwaltet werden. Jede Anwendung, jeder Sensor und jedes aktive Element, jedes Skript und jedes Automatisierungswerkzeug benötigt daher eine vertrauenswürdige, nicht personalisierte Identität und auf dieser Basis eine kontrollierte und nachvollziehbare privilegierte Authentifizierung und Autorisierung für den Zugriff auf Systeme, Anwendungen und Daten. Es ist sicherzustellen, dass diese sensiblen Identitäten einem Lebenszyklus unterliegen und bei Bedarf verwendet, modifiziert und dokumentiert werden. Außerdem darf nur die genehmigte Anwendung, das Skript oder System auf die Identität zugreifen und den Zugriff anfordern.

CyberArk Application Access Manager (AAM) ist eine Lösung zur Kontrolle, Verwaltung und Auditierung aller beschriebenen nicht-menschlichen privilegierten Zugriffe auf Anwendungen, die sowohl in statischen als auch in dynamischen Umgebungen ausgeführt werden. Dies ist insbesondere in heterogenen Umgebungen (lokal, hybrid, containerisiert oder Multi-Cloud) notwendig. Es bietet starke Authentifizierung, die konsistente Anwendung von Zugriffsrichtlinien durch rollenbasierte Zugriffskontrollen auf nicht-menschliche Identitäten und arbeitet gleichzeitig nahtlos mit der zentralen privilegierten Credential-Management-Lösung von CyberArk für menschliche Identitäten zusammen. Damit ist AAM ein zentraler Baustein, um Skalierbarkeit, Verfügbarkeit, Redundanz und Zuverlässigkeit sowie Überwachung und Alarmierung zu erreichen und letztlich die Business Continuity der Anwendungen und Dienste, die kritische Infrastrukturen unterstützen und verwalten, sicherzustellen.

6.5 Cloud- und Hybrid-Umgebungen

Selbst für Betreiber kritischer Infrastrukturen bringt die Verlagerung von Prozessen, Aufgaben und Workloads in die Cloud erhebliche Optimierungs- und Effizienzmöglichkeiten. Aber die Cloud erweitert auch die Angriffsfläche, so dass ungeschützte privilegierte Konten sowie technische Anmeldeinformationen zu gefährlichen Sicherheitslücken werden. Besondere Sicherheitsherausforderungen durch Cloud-Umgebungen und Automatisierung müssen in diesem Zusammenhang durch geeignete Maßnahmen mitigiert werden. Cloud-Anwender sollten bedenken, dass diese Sicherheit eine *gemeinsame* Herausforderung zwischen dem Cloud Service Provider (CSP) und dem Anwender ist. Insbesondere im Hinblick auf die KRITIS-Sicherheitsanforderungen kann die Verantwortung nicht auf den Cloud Service Provider übertragen werden.

Auch hier ist das CyberArk-Portfolio entsprechend vorbereitet für Multi-Cloud- und hybride Einsatzszenarien. Während die zugrunde liegenden Konzepte weitgehend gleichbleiben, müssen Umfang und Umsetzung angepasst werden. Jeder Zugriff auf Managementkonsolen muss als privilegiert betrachtet werden. Alle Zugriffspfade (Root- und Admin-Konten, API-Schlüssel, automatisierte Skripte) müssen durch Best Practices für den Umgang mit privilegierten Konten geschützt werden, indem die geringsten Privilegien genutzt werden sowie Passwort-Vaulting, Multifaktor-Authentifizierung, Session-Isolation, Passwort-Rotation, Session-Monitoring, etc. eingesetzt werden. Dasselbe gilt natürlich für alle administrativen Konten in Software-as-a-Service (SaaS)-Umgebungen.

Das Cloud-Gegenstück zur schlechten Angewohnheit, fest kodierte Anmeldeinformationen (Benutzername und Passwort) für technische oder Servicekonten in Skripten zu verwenden, sind API-Schlüssel in Skripten oder Konfigurationsdateien. API-Schlüssel dürfen niemals direkt zugänglich sein und müssen daher in einem sicheren digitalen Tresor geschützt werden, so dass nur autorisierte Benutzer und Anwendungen sie abrufen und verwenden können, während sie dem Minimalprinzip folgen.

Da die Automatisierung eine Schlüsselrolle für Skalierbarkeit und dynamische Infrastruktur spielt, ist es wichtig, dass die automatische Bereitstellung neuer Cloud-Serverinstanzen sicher ist. Die Verwendung sicherer REST-APIs zum Speichern und Abrufen von Anmeldeinformationen in einem sicheren digitalen Tresor stellt sicher, dass alle neuen Anmeldeinformationen ab dem Zeitpunkt der Bereitstellung einer Ressource geschützt sind.

Dies ist von noch größerer Bedeutung, wenn Software nach einem DevOps-Paradigma entwickelt, getestet, eingesetzt und betrieben wird. Leistungsstarke Tool Chains im Entwicklungs- und Deploymentprozess ermöglichen hochautomatisierte Prozesse, wenn diese angemessen umgesetzt werden. Das CyberArk-Portfolio bietet die erforderlichen Tools zur Sicherung der DevOps-Pipeline. Dazu gehören Mechanismen zum Sichern des Zugriffs auf alle Tool-Administrationskonten und -Konsolen, zum Anwenden der Prinzipien der Mindest- oder "just in time"-Privilegien und zum Wechseln, Überwachen und Aufzeichnen von essentiellen Aktionen menschlicher und automatisierter Benutzer.

7 Wichtige Maßnahmen für den Zugriff auf privilegierte Berechtigungen

Die Implementierung von Cyber-Resilienz als Grundlage für die Einhaltung der KRITIS-Anforderungen ist nicht vollständig deckungsgleich mit den Maßnahmen, die die Anforderungen der klassischen Cybersicherheit erfordern. Business Continuity wird in fast allen Fällen als wichtiger angesehen als z.B. Effizienz oder die Vermeidung von Leaks. Der Einfluss des Privileged Access Managements (und damit der Nutzen von Investitionen in diesem Bereich) auf die Gesamtrisikominderung ist im Vergleich zu anderen Arten von IT- und Sicherheitstechnologien außergewöhnlich hoch.

Vergleicht man die klassische Cybersicherheit mit dem Schutz kritischer Infrastrukturen, zeigt sich eine grundlegende Verschiebung der wesentlichen Zieldefinition: Die Cybersicherheit schützt Daten und Systeme vor unerwünschtem Zugriff durch böswillige Dritte. Dies schließt eine vorübergehende Abschaltung als letztes Mittel nicht aus. Kritische Infrastrukturen hingegen müssen in erster Linie dauerhaft, zuverlässig und nachhaltig funktionieren. Daher ist das Hauptziel hier vielmehr die kontinuierliche Bereitstellung von Diensten bei voller Integrität.

Die Aufrechterhaltung der Funktionsfähigkeit einer kritischen Infrastruktur steht daher im Mittelpunkt aller Angriffsszenarien, von absichtlichen Angriffen bis hin zum versehentlichen Missbrauch. Letztendlich muss die elementare Rolle der IT-Cybersicherheit als Querschnittsfunktion in allen anderen kritischen Infrastrukturen gut verstanden werden. Jeder IT-Ausfall ist als kritisch einzustufen, da die IT fast überall als Steuerungssystem fungiert. Die Anwendung eines risikobasierten Ansatzes auch bei der Auswahl valider IT-Sicherheitstechnologien zur Erfüllung der KRITIS-Anforderungen führt zu einem klaren Ergebnis. Lösungen zum Schutz, zur Verwaltung und Überwachung privilegierter Konten wie Administratoren und technische Konten können wesentliche Risiken für hochkritische Systeme innerhalb einer Infrastruktur sofort minimieren.

Zusätzlich und unabhängig von der tatsächlichen KRITIS-Branche, in der sich ein Unternehmen befindet, empfiehlt KuppingerCole folgende Maßnahmen:

- **Implementation von Zugriffsbeschränkungen für privilegierte Benutzer.**

  Kritische Berechtigungen dürfen nur bei Bedarf zugewiesen werden und es muss sichergestellt sein, dass ein Benutzer keine unbemerkten Aktionen ausführt. Mindestens die folgenden drei der in Abschnitt 5.3 definierten Anforderungen sollten berücksichtigt werden.

  - Beschränkung des Zugriffs für bestimmte Benutzer auf ausgewählte Systeme
  - Zugang temporär gewähren und widerrufen, wenn er nicht mehr benötigt wird.
  - Eine zentralisierte Verwaltung von Zugriffsrechten in heterogenen Netzwerken

- **Privileged Access Security über den traditionellen Administrator hinaus.**
  Es gibt im Wesentlichen zwei Arten von privilegierten Benutzern. Beide müssen berücksichtigt werden, da die Grenzen zwischen beiden Typen immer stärker verwässern.
  - **Privilegierte IT-Anwender** - diejenigen, die Zugang zur IT-Infrastruktur haben, die das Unternehmen unterstützt. Dieser Zugriff wird IT-Administratoren im Allgemeinen über Administratorrollen gewährt, die Systemkonten, Softwarekonten oder Betriebskonten verwenden.
  - **Privilegierte Geschäftsanwender** - diejenigen, die Zugang zu sensiblen Daten und Informationsbeständen wie Personalakten, Gehaltsabrechnungen, Finanzinformationen und dem geistigen Eigentum des Unternehmens usw. haben. Diese Art von Zugriff wird typischerweise den Anwendungsbenutzern über Geschäftsrollen über die Anwendungskonten zugewiesen. In kritischen Infrastrukturen spielen ERP-Systeme wie SAP typischerweise eine wichtige Rolle und müssen daher in eine umfassende Sicherheits- und Resilienz-Architektur eingebunden werden.

- **Training und Sensibilisierung.**
  Mit der kontinuierlichen Personalfluktuation, mit sich ändernden Infrastrukturen und einfach nur im Laufe der Zeit geht das aktuelle Wissen in Unternehmen, insbesondere über Sicherheitssysteme, deren Nutzung und Notwendigkeit verloren. Die Bedeutung von Training und Sensibilisierung kann nicht hoch genug eingeschätzt werden. Stellen Sie Ihren Administratoren und privilegierten Geschäftsanwendern stets die aktuellen Informationen zur Verfügung, um erwartete und unerwartete Ereignisse angemessen zu bewerten und darauf zu reagieren.

- **Berücksichtigung der Risiken einer vernetzten Welt.**
  Jede einzelne kritische Infrastruktur ist direkt oder indirekt mit anderen Infrastrukturen verbunden und es entsteht ein komplexes Geflecht von Abhängigkeiten. Das bedeutet, dass indirekte, abgeleitete Risiken, die interdependente Infrastrukturen füreinander schaffen können, im Krisenfall ebenfalls berücksichtigt werden müssen. Und es bedeutet auch, dass die Zusammenarbeit über einzelne kritische Infrastrukturen hinweg sehr effektiv sein kann, zum Beispiel bei der Erstellung umfassender Risikobewertungen oder Bedrohungsanalysen.

Und unabhängig von KRITIS:

- **Nehmen Sie an, KRITIS-relevant zu sein, auch wenn Sie es nicht sind.**
  Diejenigen, die diesen Bericht bis zu diesem Abschnitt gelesen haben und keine KRITIS-relevante Infrastruktur betreiben (weil sie außerhalb Deutschlands liegen oder nicht als KRITIS-relevant eingestuft sind), sehen höchstwahrscheinlich den Nutzen und die Herausforderungen für den Betrieb einer hochsicheren und robusten Infrastruktur. Warum überdenken Sie nicht Sicherheit, Schutz und Business Continuity aus diesem etwas anderen Blickwinkel? Nutzen Sie die damit verbundenen KRITIS-Anforderungen als Benchmark, die Ihnen helfen können, Ihre organisatorische Reife zu erhöhen. Nur weil Sie nicht zur Einhaltung verpflichtet sind, bedeutet das nicht, dass über Ihre individuellen, verbindlichen Anforderungen hinauszugehen, kein geeignetes Mittel zur Verbesserung Ihrer eigenen Richtlinien, Organisationen, Systeme, Infrastrukturen und Prozesse sein kann. Das Beste, was Sie mit Ihrer eigenen IT machen können, ist, nicht darauf zu warten, dass die gesetzlichen Regelungen nach dem ersten kritischen Vorfall in Kraft treten.

8 Urheberrechte

Die Zukunft der Informationssicherheit - heute

KuppingerCole unterstützt IT-Profis mit herausragender Expertise bei der Definition von IT-Strategien und in relevanten Entscheidungsprozessen. Als führendes Analystenunternehmen liefert KuppingerCole herstellerneutrale Informationen aus erster Hand. Unsere Dienstleistungen ermöglichen es Ihnen, sich sicher und wohl zu fühlen, wenn Sie Entscheidungen treffen, die für Ihr Unternehmen wichtig sind.

KuppingerCole, gegründet 2004, ist ein globales Analystenunternehmen mit Hauptsitz in Europa, das sich auf Informationssicherheit und Identitäts- und Zugriffsmanagement (IAM) konzentriert. KuppingerCole steht für Kompetenz, Ideenführerschaft, hohen Praxisbezug und eine herstellerneutrale Sicht auf die Marktsegmente der Informationssicherheit, die alle relevanten Aspekte abdeckt: Identitäts- und Zugriffsmanagement (IAM), Governance & Auditing Tools, Cloud- und Virtualisierungssicherheit, Informationsschutz, Mobile sowie Software-Sicherheit, System- und Netzwerksicherheit, Sicherheitsüberwachung, Analytik & Reporting, Governance sowie Organisation & Richtlinien.

Für weitere Informationen wenden Sie sich bitte an **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Deutschland

Telefon +49 (211) 23 70 77 - 0
Fax+49 (211) 23 70 77 - 11
www.kuppingercole.com