Digitale Zwillinge von KRITIS
Potenziale und Anforderungen zur Erhöhung der IT-Sicherheit

Luise Lautenbach[1]

Das Konzept des Digitalen Zwillings im Industriekontext steckt zwar noch in seinen Kinderschuhen, die Technologie gewinnt in Industrie und Wirtschaft jedoch zunehmend an Bedeutung. Es handelt sich um virtuelle Repliken realer Systeme, die es ermöglichen, deren Betrieb und Risiken in Echtzeit zu überwachen, zu analysieren oder sogar zu steuern.

Auch im Bereich Kritischer Infrastrukturen (KRITIS) wurde das Potential des Digitalen Zwillings bereits erkannt. So bietet er eine vielversprechende Möglichkeit, die sensiblen IT-Systeme von KRITIS effizienter und widerstandsfähiger zu gestalten. Gleichzeitig sind Digitale Zwillinge mit ihrer hochvernetzten Verbindung zum realen System auch eine potenzielle Schwachstelle. Cyberkriminelle können sich hierüber Zugriff auf die realen Systeme verschaffen. Betreiber von KRITIS müssen die IT-Sicherheit der digitalen Repräsentanzen daher von Anfang an mitdenken.

Im folgenden Beitrag sollen die IT-sicherheitsrechtlichen Rahmenbedingungen, die beim Einsatz Digitaler Zwillinge von KRITIS zu berücksichtigen sind, beleuchtet werden. Dafür werden zunächst das Konzept des Digitalen Zwillings im Industrial Metaverse vorgestellt und seine Potentiale für KRITIS herausgearbeitet. Anschließend werden die IT-sicherheitsrechtlichen Vorgaben, die sich beim Einsatz im KRITIS-Bereich ergeben, geprüft. Der Fokus liegt dabei auf den Vorschriften des BSIG, das die zentrale gesetzliche Grundlage für IT-Sicherheit für Kritische Infrastrukturen bildet.

---

1 Die Autorin ist Rechtsanwältin bei Noerr PartG mbB im Bereich Data, Tech & Telecom. Sie dankt Herrn Tim Alexander Großmann, wissenschaftlicher Mitarbeiter bei Noerr PartG mbB, für die gelungene Unterstützung. Sämtliche Internetquellen wurden zuletzt am 12.10.2024 abgerufen.

A. Einführung – Digitale Zwillinge im Industriekontext

Das Metaversum ist neben künstlicher Intelligenz eines der zentralen aktuellen Entwicklungsfelder in der digitalisierten Welt von heute. Es ist – anders als die Umbenennung des Facebook-Konzerns in „Meta" vermuten lassen könnte – kein spezifisches Produkt eines einzelnen Unternehmens, sondern vielmehr die Bezeichnung für ein nicht einheitlich definiertes, umfassendes technologisches Konzept.[2] Im Kern ist dieses auf eine stärkere Einbindung virtueller Elemente in die wahrnehmbare physische Realität gerichtet – die digitale Welt soll mit der analogen Welt verschmelzen.

Ausgehend davon wird mit dem Begriff des Metaversums häufig eine virtuelle Welt mit digitalen Avataren und virtuellen Gegenständen assoziiert, welche regelmäßig mittels Datenbrillen und Extended-Reality-Technologien (XR) in 3D und in einer 360°-Perspektive visuell dargestellt wird.[3] In diesem „3D-Internet"[4] können Menschen, repräsentiert durch ihre Avatare, unabhängig von ihrem physischen Aufenthaltsort, in simulierten dreidimensionalen Konferenzräumen zusammenkommen,[5] an virtuellen Konzerten teilnehmen[6] oder touristische Attraktionen besuchen[7]. Diese Verbreitungstypen, welche teils als kommerzielles und als Verbraucher-Metaversum bezeichnet werden,[8] stellten den Menschen sowie den ihn repräsentierenden Avatar in den Mittelpunkt.

---

2 Vgl. *M. Kaulartz/A. Schmid/F. Müller-Eising*, Das Metaverse – eine rechtliche Einführung, RDi 2022, 521 (522).

3 Fraunhofer-Verbund IUK-Technologie, Technologien und Use Cases für das (Industrial) Metaverse – Fakt oder Fiktion?, Berlin 2020, abrufbar unter: https://www.iuk.fraunhofer.de/content/dam/iuk/de/Download/Technologien%20und%20Use%20Cases%20f%C3%BCr%20das%20(Industrial)%20Metaverse.pdf; *Kaulartz/Schmid/Müller-Eising*, Metaverse (Fn. 2), 522.

4 Fraunhofer IUK-Technologie, Use Cases (Fn. 3).

5 *K. Krause*, Meet Me In The Metaverse: The Future Of Virtual And In-Person Events, 20.10.2022, abrufbar unter https://www.forbes.com/councils/forbescommunicationscouncil/2022/10/20/meet-me-in-the-metaverse-the-future-of-virtual-and-in-person-events/.

6 *B. Marr*, The World Of Metaverse Entertainment: Concerts, Theme Parks, And Movies, 27.07.2022, abrufbar unter https://www.forbes.com/sites/bernardmarr/2022/07/27/the-world-of-metaverse-entertainment-concerts-theme-parks-and-movies/.

7 *M. Constantin/G. Genovese/K. Munawar/R. Stone*, Tourism in the metaverse: Can travel go virtual?, 04.05.2023, abrufbar unter: https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/tourism-in-the-metaverse-can-travel-go-virtual.

8 Bundesverband der Deutschen Industrie, Das industrielle Metaverse – Chancen für die Industrie, 06.06.2023 abrufbar unter https://bdi.eu/artikel/news/das-industrielle-me

Demgegenüber gibt es auch ein sogenanntes *Industrial Metaverse*[9], was die Digitalisierung, Virtualisierung und Vernetzung der industriellen Produktion auf eine neue Ebene hebt. Es verbindet reale Produktionsprozesse mit einer virtuellen Welt, in der diese Prozesse simuliert, überwacht und optimiert werden können. Es basiert dabei auf dem Einsatz fortschrittlicher Technologien, die eine nahtlose Integration und Interaktion zwischen der physischen und der digitalen Welt ermöglichen. Hierzu gehören insbesondere Künstliche Intelligenz, maschinelles Lernen, *Augmented Reality* (AR), *Blockchain* sowie *Cloud-Computing*.[10]

Im Vordergrund des *Industrial Metaverse* stehen realitätsgetreue virtuelle Abbildungen von realen Systemen und Prozessen. Solche Abbildungen werden auch als Digitale Zwillinge bezeichnet. Sie werden auch als das „Herzstück" des *Industrial Metaverse* bezeichnet,[11] mit dem die Hoffnung einer „neuen Ära in der industriellen Produktion und Kooperation" verbunden wird.[12]

Wenngleich sich ihre volle praktische Bedeutung wohl erst in der näheren Zukunft entfalten wird, finden Digitale Zwillinge im *Industrial Metaverse* bereits heute in verschiedensten Wirtschaftssektoren Verwendung.[13] Nur beispielhaft sei in diesem Zusammenhang auf BMW verwiesen, das die „Omniverse-Plattform" von NVIDIA nutzt, um mithilfe Digitaler Zwillinge den Planungsprozess neuer Fabriken zu optimieren.[14]

---

taverse-chancen-fuer-die-industrie. Im Englischen sind die Bezeichnungen consumer metaverse sowie enterprise metaverse geläufig, vgl. *K Whiting*, Consumer, enterprise or industrial? The 3 main ways we are using the 'metaverse' explained, 17.02.2023 abrufbar unter: https://www.weforum.org/agenda/2023/02/metaverse-use-cases-industrial-consumer-enterprise/.

9 Deutsch: Industrielles Metaversum.

10 Bundesverband der Deutschen Industrie, Chancen (Fn. 8).

11 Bundesverband der Deutschen Industrie, Chancen (Fn. 8).

12 Bundesverband der Deutschen Industrie, Das Industrial Metaverse als wichtiger Chancenträger für die Industrie von morgen, 22.4.2024, abrufbar unter: https://bdi.eu/publikation/news/das-industrial-metaverse-als-wichtiger-chancentraeger-fuer-die-industrie-von-morgen.

13 Etwa *A. Kung, C. Baudoin, K. Tobich*, Report of TWG Digital Twin: Landscape of Digital Twin Standards, 09.06.2022, S. 1, abrufbar unter: https://www.standict.eu/digital-twin-standards-report.

14 BMW, Pressemitteilung: BMW Group auf der NVIDIA GTC: Produktion im künftigen Werk Debrecen läuft schon virtuell, 21.03.2023, abrufbar unter: https://www.press.bmwgroup.com/deutschland/article/detail/T0411467DE/bmw-group-auf-der-nvidia-gtc:-produktion-im-kuenftigen-werk-debrecen-laeuft-schon-virtuell?language=de.

Auch der Gesetzgeber – sowohl auf nationaler als auch auf europäischer Ebene – nimmt in verschiedenen Zusammenhängen auf das Konzept des Digitalen Zwillings im Industriekontext Bezug und bringt damit prinzipielles Bewusstsein für diese technologische Entwicklung zum Ausdruck.[15]

I. Definition und technische Grundlagen

Bislang existiert keine einhellig anerkannte Definition zum Digitalen Zwilling, zumal Überschneidungen mit verwandten Begriffen wie digitalen Modellen, Simulationen und dem Internet of Things (IoT) bestehen.

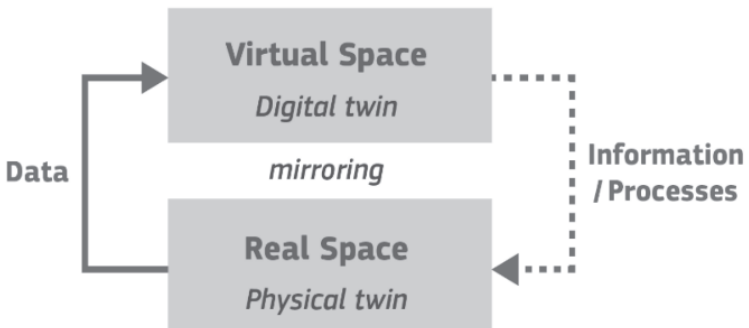
Nach dem hier zugrunde gelegten Verständnis handelt es sich bei einem Digitalen Zwilling um die virtuelle Abbildung eines realen Systems, die mit dem realen System verknüpft ist und dieses in allen relevanten Aspekten – je nach Synchronisationsintervall – möglichst in Echtzeit abbildet.[16] Der entscheidende Unterschied zu klassischen Simulationsmodellen besteht

15 Auf nationaler Ebene s. die Begründung der Bundesregierung zum Gesetz für die Wärmeplanung und zur Dekarbonisierung der Wärmenetze, BT-Drs. 20/8654, S. 93; ferner fördern verschiedene Bundesministerien unterschiedliche Projekte zu digitalen Zwillingen, s. etwa Bundesministerium für Digitales und Verkehr, Digitale Zwillinge für Infrastruktur, Bau, Wohnen – von Theorie und Konzeption in die Praxis, 07.02.2024, abrufbar unter: https://bmdv.bund.de/DE/Themen/Digitales/Building-Information-Modeling/Digitale-Zwillinge/digitale-zwillinge.html, sowie Bundesministerium für Wirtschaft und Klimaschutz, Der digitale Zwilling, abrufbar unter: https://www.bmwk.de/Redaktion/DE/Artikel/Digitale-Welt/GAIA-X-Use-Cases/der-digitale-zwilling.html. Auf EU-Ebene s. insb. das Positionspapier der EU-Kommission vom 11.7.2023 zum Thema „Web 4.0 and virtual worlds", COM(2023) 442/final.

16 In der Sache ebenso ISO/IEC 30173: „*the digital representation of a target entity with data connections that enable convergence between the physical and digital states at an appro :priate rate of synchronization.*", vgl. IEC, Internationally agreed concepts and terminology for digital twins, abrufbar unter https://www.iec.ch/blog/internationally-agreed-concepts-and-terminology-digital-twins; ähnlich etwa *E. Brucherseifer/H. Winter/ A. Mentges/ M. Mühlhäuser/M. Hellmann*, Digital Twin conceptual framework for improving critical infrastructure resilience, at 2021, 1062 (1067); *O. C. Madubuike/C. J. Anumba/R. Khallaf*, A review of digital twin applications in construction, ITcon 27 (2022), 145 (147).

demzufolge in der Verknüpfung zwischen Digitalem Zwilling und realem System.[17]

Das Konzept des Digitalen Zwillings setzt sich mithin aus drei Elementen zusammen: Dem realen System, seinem virtuellen Gegenstück sowie der Kommunikationsplattform als Schnittstelle zwischen den beiden anderen Elementen.[18] Die Kommunikationsplattform umfasst dabei einmal die Datenübertragung vom realen System hin zum Digitalen Zwilling. Zum anderen erlaubt sie die nutzergesteuerte oder automatisierte Einwirkung auf das reale System.[19]



Quelle: Frascolla, Digital Twins and Standards – Destination Earth Initiative, Trans Continuum Initiative, BDVA and STA4DESTINE, 22.11.2022, https://european-big-data-value-forum.eu/wp-content/uploads/2022/10/Digital-Twins-and-Standards-Frascolla_v3.pdf, Folie 6

17 *Madubuike/Anumba/Khallaf*, digital twin (Fn. 16), 147; *L. Wright/S. Davidson*, How to tell the difference between a model and a digital twin, Advanced Modeling and Simulation in Engineering Sciences, 2020 vol. 7, 13 (3); angesichts der Terminologie ist zu beachten, dass auch das abgebildete reale System gegebenenfalls digitale Elemente, namentlich Software, enthalten kann, vgl. *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1068.

18 *Madubuike/Anumba/Khallaf*, digital twin (Fn. 16), 148.

19 Aufgrund dieser Differenzierung unterscheidet *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1068 f. zwischen vier Komponenten des digitalen Zwillings. Im Rahmen dieses Beitrags wird die Kommunikationsplattform hingegen als ein Element bezeichnet.

II. Einsatzfelder

Im Industriebereich bieten Digitale Zwillinge eine Vielzahl von Verwendungsmöglichkeiten. In der Designphase können beispielsweise Entwicklung und Erprobung neuer Produkte und Prozesse in einer risikofreien, virtuellen Umgebung durchgeführt werden, bevor diese in die reale Produktion überführt werden.[20] Dies führt zu einer Minimierung von Risiken und Fehlern in der Produktentwicklung und -fertigung und damit zu einer Reduzierung von Kosten und Zeitaufwand.[21] Bei bestehenden Strukturen eignet sich der Einsatz Digitaler Zwillinge hingegen für die präzise und umfassende Simulation und Optimierung von Produktionsprozessen, indem sie reale Anlagen und Systeme in einer virtuellen Umgebung abbilden und deren Verhalten unter verschiedenen Bedingungen simulieren.[22] Hierdurch lassen sich reale Systeme und Prozesse über deren gesamte Lebensdauer analysieren, steuern und optimieren.[23] So können Unternehmen beispielsweise potenzielle Engpässe frühzeitig erkennen und Produktionsabläufe effizienter gestalten.[24] Zudem erlauben Digitale Zwillinge eine vorausschauende Wartung, da durch kontinuierliche Echtzeitüberwachung und Analyse

20 *Dietz/L. Hagemann/C. v. Hornung/G. Persul*, Employing Digital Twins for Security-by-Design System Testing, in: Association for Computing Machinery (Hrsg.), Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (SaT-CPS '22), New York 2022, S. 97 (97 f.).

21 So vermeldete McKinsey bereits im Jahr 2022, dass ein Unternehmen seine Kapital- und Betriebskosten durch den Einsatz digitaler Zwillinge um 10 % senken konnte, vgl. McKinsey, Digital twins: The foundation of the enterprise metaverse, Oktober 2022, abrufbar unter: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-twins-the-foundation-of-the-enterprise-metaverse.

22 *N. Attoh-Okine*, ASME J. Risk Uncertainty Part B. Mar 2024, 10(1), 010301, Paper No. RISK-24–1015; *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1063.

23 *Brucherseifer/Winter/Mentges/Mühlhäuser/Hellmann*, Framework (Fn. 16), 1063; Fraunhofer IOSB, Digitale Zwillingssysteme – das Schlüsselkonzept für Industrie 4.0, abrufbar unter: https://www.iosb.fraunhofer.de/de/geschaeftsfelder/automatisierung-digitalisierung/anwendungsfelder/digitaler-zwilling.html.

24 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Der Digitale Zwilling in der Netz- und Elektrizitätswirtschaft, VDE Studie, Offenbach am Main 2023, S. 24, abrufbar unter: https://www.vde.com/resource/blob/2257516/cce234dea484fc0b1943774391752d8a/studie-digitaler-zwilling---download-data.pdf; B. Wicha-Krause/J. Poos/B. Kreft Namen in Grün?, Wenn der Digitale Zwilling hinkt – ohne Daten keine aussagekräftigen Ergebnisse, BET Webmagazin, 19.06.2023, abrufbar unter: https://www.iec.ch/blog/internationally-agreed-concepts-and-terminology-digital-twins.

von Betriebsdaten mögliche Ausfälle prognostiziert und rechtzeitig Gegenmaßnahmen ergriffen werden können.[25]

B. Digitale Zwillinge von KRITIS

I. KRITIS als Rückgrat der Gesellschaft

KRITIS bilden das Rückgrat moderner Gesellschaften. Sie stellen grundlegende Dienstleistungen und Ressourcen bereit, auf die nahezu alle anderen Lebensbereiche angewiesen sind. Ihr reibungsloser Betrieb ist daher essenziell für die Aufrechterhaltung von Sicherheit, Wohlstand und gesellschaftlicher Ordnung. Insoweit besteht die besondere Verantwortung dieser Systeme darin, auch in Krisenzeiten ihre Funktionsfähigkeit sicherzustellen und die Grundversorgung der Gesellschaft zu gewährleisten.

Dies macht KRITIS zu einem sensiblen Ziel. In einer zunehmend vernetzten und digitalisierten Welt sind deren IT-Systeme verstärkt Cyberangriffen ausgesetzt.[26] Als zentrale Pfeiler der öffentlichen Sicherheit und Ordnung bedarf es daher besonderer Maßnahmen, um die Resilienz von KRITIS zu erhöhen und mögliche Ausfälle zu minimieren. Ihr Schutz und ihre Widerstandsfähigkeit rückt daher vermehrt in den Fokus moderner Sicherheitsstrategien.

II. IT-Sicherheit durch Digitale Zwillinge?

In diesem Kontext gewinnt das bislang weitgehend ungenutzte Potenzial leistungsfähiger Digitaler Zwillinge zunehmend an Bedeutung. Jenseits ihrer allgemeinen Vorzüge bieten Digitale Zwillinge nämlich weitreichende Möglichkeiten, um ein konstant hohes IT-Sicherheitsniveau zu etablieren. So lassen sich Sicherheitslücken, potenzielle Angriffswege und Schwach-

25 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Elektrizitätswirtschaft (Fn. 24), S. 24.

26 Beispielsweise wurde im Jahr 2020 das IT-System eines Düsseldorfer Krankenhauses angegriffen. Der Angriff führte dazu, dass Patienten nicht rechtzeitig behandelt werden konnten. Die Folgen gingen so weit, dass eine Patientin durch diesen IT-Angriff verstarb, vgl. *K. Kerkmann/L. Nagel*, Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf, 18.09.2020, abrufbar unter https://www.handelsblatt.com/technik/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html.

stellen in einer sicheren, virtuellen Umgebung identifizieren und testen, ohne dass die realen Systeme außer Betrieb genommen werden müssen.[27] Dies ist besonders bei kritischen Systemen von Vorteil, wo auch nur kurze Ausfallzeiten erhebliche gesellschaftliche und wirtschaftliche Folgen haben können. Ein weiterer Vorteil besteht darin, dass eine durch Penetrationstests herbeigeführte Beschädigung des Digitalen Zwillings unschädlich ist. Dieser kann einfach zurückgesetzt werden.[28] Schlussendlich können Digitale Zwillinge umfangreiche Trainingsdaten bereitstellen, die Systeme zur Erkennung und Vermeidung von Angriffen stärken.[29] Diese Daten ermöglichen es beispielsweise, maschinelles Lernen und Künstliche Intelligenz zu nutzen, um Bedrohungen frühzeitig zu erkennen und darauf zu reagieren. Insoweit überrascht nicht, dass Digitale Zwillinge im Bereich von KRITIS vermehrt in den Fokus von Wirtschaft und Forschung rücken.[30]

Allerdings gehen mit ihrem Einsatz auch beachtliche Risiken einher. Durch ihre Verknüpfung bzw. den Datenaustausch mit dem realen System sind sie potenziell ebenso anfällig für Cyberangriffe wie die realen Systeme. Klassische Gefahren wie Identitätsdiebstahl, das Ausspähen von Betriebs- und Geschäftsgeheimnissen sowie die Verschlüsselung von Daten und an-

27 *Arrow*, Digital Twin: Die erste reale Anwendung des Metaverse, 12.09.2022, abrufbar unter: https://www.arrow.de/research-and-events/articles/digital-twin-the-first-real-application-of-the-metaverse.

28 *A. Giehl*, Digitale Zwillinge und ihr Potenzial für sichere Betriebstechnik (OT), 28.10.2022, abrufbar unter: https://www.cybersecurity.blog.aisec.fraunhofer.de/digitale-zwillinge-und-ihr-potenzial-fuer-sichere-betriebstechnik-ot/.

29 *Giehl*, Betriebstechnik (Fn. 28).

30 Verband der Elektrotechnik Elektronik Informationstechnik e.V., Elektrizitätswirtschaft (Fn. 24), S. 1 ff.; *C. Bischofberger*, Digital twins and the smart grid, e-tech, 03/2022, abrufbar unter: https://etech.iec.ch/issue/2022-03/digital-twins-and-the-smart-grid; Bundesverband der Energie- und Wasserwirtschaft e.V., Digitale Doppelgänger: Neue Chancen für die Wasserwirtschaft?, 13.3.2023, abrufbar unter: https://www.bdew.de/online-magazin-zweitausend50/generation/digitale-doppelgaenger-neue-chancen-fuer-die-wasserwirtschaft/; *M. Neumann*, Was Digital Twins für die Telekommunikationsbranche bedeuten, 28.6.2024, abrufbar unter: https://newroom-connect.com/blog/was-digital-twins-fuer-die-telekommunikationsbranche-bedeuten/; PWC, Der digitale Zwilling in der Medizin, abrufbar unter https://www.pwc.de/de/gesundheitswesen-und-pharma/der-digitale-zwilling-in-der-medizin.html; *Denga*, ZBB 2023, 280 (284); IT-Finanzmagazin, Digital Twin Technologie-Report: Finanzsektor setzt voll auf digitale Zwillinge, 28.8.2023, abrufbar unter: https://www.it-finanzmagazin.de/altair-studie-finanzsektor-setzt-voll-auf-digitale-zwillinge-160027/; Deutsches Zentrum für Luft- und Raumfahrt e. V., Simulationsmethoden für Digitale Zwillinge, abrufbar unter: https://www.dlr.de/de/pi/ueber-uns/abteilungen/simulationsmethoden-fuer-digitale-zwillinge.

schließende Erpressung können folglich auch den Digitalen Zwilling betreffen.[31] Im schlechtesten Fall können Cyberkriminelle über den Digitalen Zwilling auch Zugriff auf das reale System erhalten und die Steuerung übernehmen bzw. Ausfälle provozieren.

Ein weiteres Risiko birgt der sogenannte "gefälschte digitale Zwilling": Bei diesem Angriffsmittel schaffen Cyberkriminelle durch erbeutete Daten virtuelle Kopien realer Systeme und nutzen diese beispielsweise für *Social Engineering*-Angriffe.[32] Solche gefälschten Zwillinge gefährden nicht nur die Integrität und Sicherheit von KRITIS, sondern können auch das Vertrauen in die Authentizität und Verlässlichkeit der digitalen Repräsentationen untergraben.

Der Einsatz Digitaler Zwillinge im Bereich von KRITIS geht somit sowohl mit Chancen als auch Risiken für die IT-Sicherheit einher. Betreiber, die diese Technologie in Betracht ziehen, sollten nicht nur angemessene Sicherheits- und Überwachungsmaßnahmen ergreifen, sondern müssen auch die rechtlichen Anforderungen, die sich an den Einsatz Digitaler Zwillinge stellen, eruieren und implementieren.

C. Rechtliche Rahmenbedingungen

Mit der DSGVO, der KI-Verordnung[33] sowie diversen anderen Rechtsakten hat die EU bereits einen starken Rechtsrahmen geschaffen, der potenzielle Bereiche des *Industrial Metaverse,* und damit auch den Einsatz Digitaler Zwillinge, reguliert. Im Kontext von KRITIS muss jedoch auch das IT-Sicherheitsrecht besonders in den Blick genommen werden.

Maßgebend ist hierfür das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG).[34] Es bildet den Grundstein der KRITIS-

31 PWC, Neue Risiken an der Schnittstelle von Metaverse und digitalen Zwillingen, abrufbar unter: https://www.pwc.de/de/cyber-security/neue-risiken-an-der-schnittstelle-von-metaverse-und-digitalen-zwillingen.html.

32 PWC, Risiken (Fn. 31); auch als „*Evil Digital Twin*" betitelt.

33 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

34 Des Weiteren enthalten Spezialgesetze wie das TKG (bspw. §§ 165, 166 TKG) und das EnWG (§ 11 EnwG) IT-Sicherheitspflichten. Eine detaillierte Darstellung dieser

Regulierung in Deutschland. Es regelt nicht nur die Aufgaben, Befugnisse und Zuständigkeiten des Bundesamts für Sicherheit in der Informationstechnik (BSI), sondern legt auch Pflichten für Unternehmen im Bereich von KRITIS fest, um ein nationales IT-Sicherheitsniveau zu gewährleisten.

I. Digitaler Zwilling als KRITIS i. S. d. § 2 Abs. 10 BSIG

Wenn ein Digitaler Zwilling KRITIS virtuell abbildet, liegt zunächst die Annahme nahe, dass auch er automatisch zu KRITIS wird. Eine solche pauschale Einordnung verbietet sich jedoch. Da der Digitale Zwilling vielfältige Einsatzmöglichkeiten bietet, die aber nicht zwangsläufig von hoher Bedeutung für die Allgemeinheit sind, ist vielmehr zu prüfen, ob der Digitale Zwilling die Tatbestandsvoraussetzungen von KRITIS erfüllt.

Ausgangspunkt für die Frage, ob Infrastrukturen „kritisch" sind, ist die Legaldefinition in § 2 Abs. 10 S. 1 BSIG. Darin werden KRITIS bestimmt als Einrichtungen, Anlagen oder Teile davon, die einem der dort genannten Sektoren angehören und kumulativ von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 2 Abs. 10 S. 1 BSIG).

1. Kritische Infrastruktur

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) konkretisiert den Rechtsbegriff, indem sie „unter Festlegung" von kritischen Dienstleistungen, Anlagenkategorien und bedeutenden Versorgungsgraden, die sich durch Schwellenwerte messen lassen, bestimmt werden.

Die Einordnung als KRITIS nach dem BSIG und der BSI-KritisV erfolgt insofern nach folgendem Schema:[35] Es muss kumulativ (i) eine kritische Dienstleistung in einem der Sektoren nach § 2 Abs. 10 S. 1 Nr. 1 BSIG vorliegen, (ii) zu deren Erbringung eine Anlage, die einer in der BSI-KritisV festgelegten Anlagenkategorie zuzuordnen ist, betrieben wird und (iii) de-

Gesetze geht jedoch über den Zweck dieses Beitrags hinaus und wird daher von der Untersuchung ausgeklammert.

35 Nach *V. Vogel/N. Ziegler*, Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie, International Cybersecurity Law Review, 2023 vol. 4, 1 (6).

ren Versorgungsgrad durch Bemessung der entsprechenden Schwellenwerte als bedeutend anzusehen ist.

a) Kritische Dienstleistung

Was unter einer kritischen Dienstleistung zu verstehen ist, definiert § 1 Abs. 1 Nr. 3 BSI-KritisV. Danach handelt es sich um Dienstleistungen zur Versorgung der Allgemeinheit in den jeweiligen Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Die nähere Bestimmung kritischer Dienstleistungen erfolgt in den §§ 2 – 9 BSI-KritisV für jeden Sektor durch Aufzählung der maßgeblichen Dienstleistungen und deren weitere Unterteilung.

Die Prüfung, ob eine kritische Dienstleistung vorliegt, bleibt zwar dem konkreten Einzelfall vorbehalten. Der Einsatz Digitaler Zwillinge kommt jedoch bei der Erbringung kritischer Dienstleistungen in sämtlichen Sektoren in Betracht.[36] Nur beispielhaft sei in diesem Zusammenhang etwa die Stromversorgung als kritische Dienstleistung im Energiesektor genannt, die sich gemäß § 2 Abs. 1–2 BSI-KritisV aus der Stromerzeugung, dem Stromhandel, der Stromübertragung und der Stromverteilung zusammensetzt.

b) Anlage, die einer Anlagenkategorie zuzurechnen ist

Liegt eine kritische Dienstleistung vor, rückt der Digitale Zwilling in den Fokus der Prüfung. Zu prüfen ist, ob der Digitale Zwilling eine Anlage darstellt, die sich einer in der BSI-KritisV festgelegten Anlagenkategorie zuordnen lässt.

Als Anlage bezeichnet man gemäß § 1 Abs. 1 Nr. 1 BSI-KritisV (i) Betriebsstätten und sonstige ortsfeste Einrichtungen, (ii) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen sowie (iii) Software und IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind. Die Legaldefinition der BSI-KritisV orientiert sich damit im Wesentlichen

36 Siehe zu den sektorübergreifenden Einsatzfeldern Digitaler Zwillinge bereits oben unter Punkt B. II.

am immissionsschutzrechtlichen Begriffsverständnis einer Anlage i. S. d. § 3 Abs. 5 BImSchG und ist daher weit auszulegen.[37]

Aus systematischer Sicht folgt hieraus, dass – anders als § 2 Abs. 10 BSIG vermuten lässt – es sich bei Anlagen und Einrichtungen nicht um unterschiedliche Kategorien handelt. Vielmehr fungiert der Begriff der Anlage als Oberbegriff.[38] Das erscheint auch insoweit konsequent, als dass die BSI-KritisV nur auf Teile einer Anlage, nicht aber auf Teile einer Einrichtung abstellt.[39]

Legt man die Legaldefinition des § 1 Abs. 1 Nr. 1 BSI-KritisV zugrunde, ist der Digitale Zwilling als Software bzw. IT-Dienst im Sinne von § 1 Abs. 1 Nr. 1 lit. c) BSI-KritisV und damit als Anlage einzustufen; vorausgesetzt, er ist für die Erbringung einer kritischen Dienstleistung notwendig.

Zu der Frage, wann von einer Notwendigkeit für die Erbringung der kritischen Dienstleistung auszugehen ist, gibt die BSI-KritisV keine Anhaltspunkte. Zielsetzung des Verordnungsgebers ist jedoch die Identifizierung jener Anlagen, deren Funktionsfähigkeit für die Versorgung der Allgemeinheit erhalten werden muss, um eine Inanspruchnahme der Notversorgung von vornherein zu verhindern.[40] Ausweislich der Verordnungsbegründung sollen damit zwei Arten von Anlagen nicht vom Anlagenbegriff erfasst sein; selbst, wenn sie die entsprechenden Schwellenwerte erreichen. Dies betrifft zum einen Anlagen, die ausschließlich der Notversorgung, nicht aber dem Regelbetrieb dienen.[41] Zum anderen sollen aber auch solche Anlagen ausgeschlossen sein, die allein für die Versorgung betriebsinterner Prozesse genutzt werden, etwa im Konzernverbund.[42]

37 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

38 Wohl auch *Ritter* in D. Kipker/P. Reusch/S. Ritter (Hrsg.), Recht der Informationssicherheit, München 2023, BSIG § 2 Rn. 29: „[E]*ine scharfe Abgrenzung zwischen diesen Begriffen* [ist] *nicht immer möglich*".

39 Vgl. § 7 Abs. 7, § 8 Abs. 3, § 9 Abs. 3 BSI-KritisV.

40 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

41 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

42 Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6: „*Der Anlagenbegriff wird nur insoweit eingegrenzt, als eine Anlage im Sinne dieser Rechtsverordnung zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung notwendig sein muss. Nicht erfasst sind somit Anlagen, die zur Versorgung ausschließlich betriebsinterner Prozesse z. B. innerhalb eines Konzernverbunds dienen (Selbstversorgung).*" Im Wesentlichen ebenso im Zuge der Erweiterung durch § 1 Abs. 1 Nr. 1 lit. c BSI-KritisV Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 40.

Doch wann ist ein betrieblicher Prozess als nicht (nur) betriebsintern – und damit als notwendig zur Erbringung der kritischen Dienstleistung – anzusehen? Dieses Notwendigkeitskriterium ist in der juristischen Fachwelt bisher kaum näher beleuchtet worden. Einerseits könnte man den Begriff der Notwendigkeit eng auslegen und nur auf solche betrieblichen Prozesse beziehen, die selbst bei Berücksichtigung kompensatorischer Maßnahmen nicht hinweggedacht werden können, ohne dass die Erbringung der kritischen Dienstleistung beeinträchtigt würde. In diesem Sinne ließe sich von einem theoretischen Notwendigkeitsbegriff sprechen.[43] Demgegenüber kann das Notwendigkeitserfordernis auch weiter verstanden werden, sodass ihm all jene Anlagenbestandteile unterfielen, die im konkreten Fall für die Erbringung der kritischen Dienstleistung genutzt werden. Dies entspräche einem faktischen Notwendigkeitsbegriff.[44]

Richtigerweise ist das Kriterium der Notwendigkeit nicht in einem theoretischen, sondern in einem faktischen Sinne zu verstehen.[45] Ein solches versorgungsfunktionales Begriffsverständnis entspricht dem vom Gesetzgeber verfolgten Zweck, die Allgemeinheit vor dem partiellen oder vollständigen Ausfall kritischer Dienstleistungen zu schützen.[46] Maßgeblich ist folglich, ob die bestehende Versorgungskette bis zum betroffenen Bürger bedroht bzw. durch einen potentiellen Cyberangriff beeinträchtigt werden könnte.[47] In der Konsequenz sind vom Anlagenbegriff auch solche Anlagen erfasst, die sowohl für die Erbringung der kritischen Dienstleistung sowie für die Selbstversorgung parallel genutzt werden. Dies gilt selbst dann, wenn der Nutzungsanteil für die Selbstversorgung überwiegt.[48]

Ob die Nutzung eines Digitalen Zwillings ausgehend von den soeben dargelegten Maßstäben einen nicht ausschließlich betriebsinternen und damit für die kritische Dienstleistung notwendigen Prozess darstellt, kann nur im Einzelfall und in Abhängigkeit von dessen konkreter Funktions- und Verwendungsweise beurteilt werden. Im Folgenden sollen jedoch einige allgemeine, auf typisierte und praktisch besonders bedeutsame Fallkonstellationen bezogene Einschätzungen getroffen werden.

---

43 So *M. Glade* in D. Kipker/P. Reusch/S. Ritter (Hrsg.), Recht der Informationssicherheit, München 2023, BSI-KritisV § 1 Rn. 13.
44 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
45 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
46 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
47 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.
48 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 13.

Dient der Digitale Zwilling ausschließlich zu Analysezwecken, kann sein Einsatz grundsätzlich hinweggedacht werden, ohne dass die Erbringung der kritischen Dienstleistung beeinträchtigt würde. Ein störungsbedingter Ausfall der durch den Digitalen Zwilling ermöglichten und durchgeführten Analysetätigkeit würde die Versorgung der Allgemeinheit grundsätzlich nicht gefährden. Die bloße Analyse der Realdaten bleibt vielmehr ein betriebsinterner Vorgang. Besonders deutlich wird dies dann, wenn anhand der Analysedaten mögliche Prozessoptimierungen (manuell oder automatisiert) entwickelt und vorgeschlagen werden. Das BSIG und die BSI-KritisV zielen nämlich nicht auf eine betriebswirtschaftliche Optimierung interner Prozesse, sondern auf die Gewährleistung eines sicherheitstechnischen Minimalstandards bei der Erbringung kritischer Dienstleistungen.[49]

Damit ist auch der Einsatz Digitaler Zwillinge zur bloßen fortlaufenden Entwicklung bestehender Systeme und Prozesse nicht notwendig i. S. d. § 1 Abs. 1 Nr. 1 BSI-KritisV. Dies gilt erst recht für die Verwendung Digitaler Zwillinge in der initialen Entwicklungsphase, denn zu diesem Zeitpunkt fehlt es bereits an der Erbringung einer kritischen Dienstleistung.

Weniger eindeutig fällt die Beurteilung aus, soweit der Digitale Zwilling zu Überwachungszwecken eingesetzt wird. Denn die Überwachung des realen Systems ermöglicht, dass drohende oder eingetretene Störungen frühzeitig erkannt, begrenzt und abgestellt werden können. Im Gegensatz zur reinen Analysetätigkeit besteht bei der Nutzung Digitaler Zwillinge zu Überwachungszwecken somit sehr wohl ein Bezug zur Aufrechterhaltung der für die Allgemeinheit bedeutenden Versorgung. Wenngleich das betriebsinterne Element im Vordergrund stehen mag, erscheint die Annahme nicht zwingend, der Einsatz Digitaler Zwillinge zu Überwachungszwecken erfolge ausschließlich zu betriebsinternen Zwecken. Zwar würde der Ausfall des Digitalen Zwillings, der zu Überwachungszwecken genutzt wird, die Erbringung kritischer Dienstleistungen nicht per se beeinträchtigen. Die Überwachung der realen Prozesse ist nicht unmittelbar Teil der konkreten Leistungserbringung, sondern soll im Fall gegenwärtiger oder künftiger Beeinträchtigungen lediglich ein zeitnahes Gegensteuern ermöglichen. Diese Erwägungen sprechen tendenziell dagegen, den Einsatz Digitaler Zwillinge zu Überwachungszwecken als notwendig im Sinne von § 1 Abs. 1 Nr. 1 BSI-KritisV anzusehen. Dem ist jedoch entgegenzuhalten, dass Anlagen zur Überwachung schlussendlich erforderlich sind, um die Sicherheit und

49 Vgl. BT-Drs. 18/4096, S. 19.

Funktionsfähigkeit kritischer Dienstleistungen zu gewährleisten, indem sie Bedrohungen frühzeitig erkennen und Ausfälle verhindern. Sie ermöglichen eine kontinuierliche Kontrolle und sofortige Reaktion auf sicherheitsrelevante Ereignisse, was für den reibungslosen Betrieb unerlässlich ist. Dies bestätigt auch der Verordnungsgeber, indem er in den Anhängen zu den einzelnen Sektoren jedenfalls teilweise Überwachungsvorrichtungen als Anlagenkategorie festlegt.[50] Anlagen, die der Überwachung dienen, sind somit schon kraft ausdrücklicher Anordnung für die Erbringung der kritischen Dienstleistung notwendig.

Ähnliches gilt für die Nutzung Digitaler Zwillinge, welche – neben anderen Verwendungszwecken – zumindest auch der Steuerung des realen Systems bzw. der realen Prozesse dienen. Dabei kann es keine Rolle spielen, ob der Digitale Zwilling aufgrund der in ihm integrierten Anwendungen automatisch oder lediglich durch die manuelle Bedienung eines menschlichen Nutzers Einfluss auf das reale System nehmen kann. Erlangen Unbefugte Zugriff auf den Digitalen Zwilling, wäre die Erbringung der kritischen Dienstleistung in beiden genannten Konstellationen akut gefährdet. Insofern ist der Einsatz Digitaler Zwillinge von realen, kritischen Systemen notwendig zur Erbringung kritischer Dienstleistungen.

Zu einer anderen Bewertung kommt man allenfalls dann, wenn der Umfang der Steuerungsmöglichkeit gering ausfällt. Dies wäre beispielsweise denkbar, wenn sich der Steuerungsumfang des Digitalen Zwillings auf einen abgrenzbaren kleinen Teil des realen Systems beschränkt. In einem solchen Fall lässt sich möglicherweise argumentieren, dass es an der von § 2 Abs. 10 S. 1 Nr. 2 BSIG gebotenen Erheblichkeit der drohenden Versorgungsengpässe oder Gefährdungen fehlen würde. Gegen eine solche Argumentation spricht jedoch, dass die Erheblichkeit im Sinne von § 2 Abs. 10 Nr. 2 BSIG abschließend durch die in der BSI-KritisV erfolgende Festsetzung der Schwellenwerte geregelt ist.[51] Außerdem würde durch das Abstellen auf das konkret drohende Schadenspotenzial einiges an Rechtssicherheit eingebüßt werden, was mit der ausschließlichen Maßgeblichkeit des Versorgungsgrads einhergeht.

Zusammengefasst sind Digitale Zwillinge realer, kritischer Systeme mithin regelmäßig dann als notwendig für die Erbringung kritischer Dienstleistungen einzustufen, wenn sie (zumindest auch) die Beeinflussung des realen Systems ermöglichen. Ihr Einsatz (lediglich) zu Entwicklungs- und

50 Etwa Anhang 1 Teil 1 Nr. 2.7 iVm Teil 3 Nr. 3.1.3.

51 In diese Richtung wohl *Ritter* (Fn. 38), BSIG § 2 Rn. 31.

Analysezwecken ist demgegenüber als nicht notwendig zur Erbringung kritischer Dienstleistungen zu bewerten. Schwieriger ist die Beurteilung des Einsatzes zu Überwachungszwecken, wenngleich auch hier die besseren Argumente gegen die Bejahung des Notwendigkeitskriteriums sprechen.

Kommt man zu dem Schluss, dass der Digitale Zwilling eine Anlage i. S. d. § 1 Abs. 1 Nr. 1 BSI-KritisV darstellt, muss er jedoch auch einer in den Anhängen der BSI-KritisV festgelegten Anlagenkategorie zugeordnet werden können. Auch diese Frage kann nur im konkreten Einzelfall und in Abhängigkeit von der Funktions- und Verwendungsweise des Digitalen Zwillings beurteilt werden. Um an das oben genannte Beispiel im Energiesektor anzuknüpfen, wäre aber beispielsweise die Einstufung eines Digitalen Zwillings als eigenständige Anlage im Sinne von § 2 Abs. 10 S. 1 Var. 2 BSIG i.V.m. § 2 Abs. 6 BSI-KritisV[52] denkbar, wenn der Digitale Zwilling gemäß dem Anhang 1 der BSI-KritisV eine Anlage bzw. ein System zur Überwachung und/oder Steuerung und damit eine eigene Anlagenkategorie darstellt. Dies trifft etwa auf Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung zu (Anhang 1 Teil 1 Nr. 2.2, Teil 3 Nr. 1.1.2 BSI-KritisV).

Lässt sich der Digitale Zwilling hingegen keiner der in den Anhängen der BSI-KritisV festgelegten Anlagenkategorien zuordnen, führt dies jedoch nicht zwangsläufig dazu, dass er nicht zu KRITIS zählt. Vielmehr kann er auch als Teil einer Anlage KRITIS i. S. v. § 2 Abs. 10 BSIG sein („*oder Teile davon*"). Insoweit erfolgt unter Umständen die Zurechnung des Digitalen Zwillings zu einer (übergeordneten) Anlage, also dem realen System, nach § 1 Abs. 2 S. 1 Hs. 1 BSI-KritisV. Anlagenteile sind insoweit selbstständig beurteilbare und abgrenzbare Teile einer Anlage, die auch für sich genommen Anlagen nach § 1 Abs. 1 Nr. 1 BSI-KritisV darstellen können, aber für den Betrieb in einer übergeordneten Anlage vorgesehen bzw. eingebunden sind.[53] Zwingende Voraussetzung ist jedoch auch hier, dass der Digitale Zwilling für den Betrieb der (übergeordneten) Anlage und damit zumindest mittelbar auch zur Erbringung der kritischen Dienstleistung notwendig ist.

Ein konkretes Beispiel für die Einordnung als Anlagenteil wäre, wenn der Digitale Zwilling der Überwachung eines Stromübertragungsnetzes dient. So fällt das Stromübertragungsnetz zwar in eine der Anlagekategorien (Anhang 1 Teil 1 Nr. 2.3, Teil 3 Nr. 1.2.1 BSI-KritisV). Eine Anlagenkategorie

52 In den anderen Sektoren richtet sich die Qualifizierung als Anlage nach § 3 Abs. 4, § 4 Abs. 3, § 5 Abs. 4, § 6 Abs. 4, § 7 Abs. 7, § 8 Abs. 3 BSI-KritisV.

53 So auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 14.

für ein System zur Überwachung des Stromübertragungsnetzes sieht die BSI-KritisV jedoch nicht vor. In diesem Fall würde der Digitale Zwilling als betriebsnotwendiges Teil des Stromübertragungsnetzes diesem über § 1 Abs. 2 S. 1 BSI-KritisV zugerechnet und damit als Anlagenteil selbst zu KRITIS.

c) Erreichen des Schwellenwertes

Ist der Digitale Zwilling einer Anlagenkategorie zuzurechnen, muss er des Weiteren die in der BSI-KritisV festgelegten Schwellenwerte erreichen. Sofern der Digitale Zwilling einer übergeordneten Anlage als Anlagenteil zuzurechnen, ist, muss hingegen die Anlage den Schwellenwert erreichen.

Schwellenwerte sind nach § 1 Abs. 1 Nr. 5 BSI-KritisV Werte, bei deren Erreichen oder Überschreiten der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Abs. 1 S. 1 BSIG anzusehen ist. Die BSI-KritisV enthält tabellarische Anlagen, die verbindliche Schwellenwerte festlegen, die sich an den in den sektorspezifischen Normen weiter unterteilten Dienstleistungen orientieren. Die genaue Berechnung der Schwellenwerte wird im jeweiligen Teil 2 der Anlage zur BSI-KritisV näher festgelegt, wo für einen bedeutenden Versorgungsgrad von einem Regelschwellenwert von 500.000 zu versorgenden Personen ausgegangen wird.

Bei der Berechnung der Schwellenwerte ist zu beachten, dass die Schwellenwerte der BSI-KritisV jeweils pro Anlage gelten. Es gilt der strikte Anlagenbezug.[54] Insoweit ist nicht auf ein Unternehmen oder einen Betrieb in seiner Gesamtheit abzustellen. Vielmehr kommt es auf die Anlage im Einzelnen an. Das heißt, wenn keine Anlage für sich genommen den Schwellenwert überschreitet, liegt auch keine KRITIS vor.

Eine Ausnahme hiervon bildet allerdings die sogenannte "gemeinsame Anlage". Dabei handelt es sich um mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind. Sie gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind (§ 1 Abs. 2 S. 2 KritisV). In

54 Vgl. Bundesamt für Sicherheit in der Informationstechnik, Fragen und Antworten zur BSI-Kritisverordnung, abrufbar unter: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-BSI-KritisV/faq_kritisv_node.html.

diesem Fall werden die Versorgungsleistungen zur Berechnung der Schwellenwerte addiert.

2. Betreibereigenschaft

Ist der Digitale Zwilling als KRITIS einzuordnen, ist weiter festzustellen, wer als dessen Betreiber gilt und damit Adressat des gesetzlichen Pflichtenprogramms ist. In Betracht kommen sowohl der Nutzer, also der Betreiber des zugrundeliegenden realen Systems als auch der externe IT-Dienstleister, welcher häufig zur Bereitstellung der Software des Digitalen Zwillings und der erforderlichen Rechenkapazitäten hinzugezogen wird.

a) Definition und Begriffsmerkmale

Das BSIG selbst enthält keine Legaldefinition des Betreibers. Er wird jedoch in § 1 Abs. 1 Nr. 2 BSI-KritisV definiert als eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt.[55] Zur Bestimmung der Betreibereigenschaft ist demnach maßgeblich darauf abzustellen, wer die Verfügungsgewalt in eigener Verantwortung, also die tatsächliche Sachherrschaft über die Anlage oder Teile davon, ausübt.[56]

Damit weist die Betreibereigenschaft auf den ersten Blick eine gewisse Nähe zum zivilrechtlichen Besitz- und strafrechtlichen Gewahrsamsbegriff auf.[57] Ähnlich wie bei der Legaldefinition zum Anlagenbegriff in § 1 Abs. 1 Nr. 1 BSI-KritisV ist dem Betreiberbegriff jedoch ein immissionsschutzrechtliches Verständnis zugrunde zu legen.[58] Insoweit sind die für den immissionsschutzrechtlichen Betreiberbegriff entwickelten Grundsätze

55 Eine Ausnahme hiervon sieht die BSI-KritisV nur für den Sektor Finanzen vor: Nach § 7 Abs. 8 BSI-KritisV hat derjenige bestimmenden Einfluss auf eine Anlage, der die tatsächliche Sachherrschaft ausübt, unabhängig von den rechtlichen und wirtschaftlichen Umständen. Hieraus folgt, dass teilweise auch die Outsourcing-Unternehmen von Finanzunternehmen als Betreiber Kritischer Infrastruktur eingestuft werden können, vgl. *Ritter* (Fn. 38), BSI-KritisV § 7 Rn. 19.

56 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 29; *M. Fischer* in G. Hornung/M. Schallbruch (Hrsg), IT-Sicherheitsrecht, 2. Aufl., Baden-Baden 2024, Teil 2 § 13 Rn. 51.

57 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 29.

58 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

anzuwenden.[59] In Übereinstimmung mit der immissionsschutzrechtlichen Rechtsprechung[60] heißt es in der Verordnungsbegründung, Betreiber sei, „wer weisungsfrei und selbstständig über die Anlage oder Teile davon verfügen kann."[61]

Zunächst ist also zu prüfen, wer den bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt. Unter „Betrieb" ist in diesem Zusammenhang die Aufrechterhaltung der organisatorisch-technischen Funktionsfähigkeit zu verstehen.[62] Einfluss auf die Beschaffenheit der Anlage hat hingegen, wer auf die zur Anlage gehörenden betriebsnotwendigen Gegenstände physisch einwirken kann.[63] Bei dieser Prüfung sind sodann die rechtlichen, wirtschaftlichen und tatsächlichen Umstände im Rahmen der Gesamtbetrachtung zu berücksichtigen. Das Erfordernis der rechtlichen und tatsächlichen Verfügungsmacht beruht auf dem Gedanken, dass derjenige verpflichtet werden soll, der im Bedarfsfall am effektivsten die erforderlichen Maßnahmen ergreifen kann.[64] Wirtschaftliche Umstände sind deshalb zu berücksichtigen, um zumindest eine weitgehende Synchronität zwischen den wirtschaftlichen Nutzungen der Anlage bzw. dem wirtschaftlichen Risiko und den mit der Erfüllung des gesetzlichen Pflichtenprogramms verbundenen Kosten herzustellen.[65] Den wirtschaftlichen Umständen wird jedoch teils nur eine untergeordnete Bedeutung zugemessen.[66] Zur Beurteilung der rechtlichen Umstände, aus denen sich ein bestimmender Einfluss auf die Beschaffenheit oder den

59 *Fischer* (Fn. 56), Teil 2 § 13 Rn. 52.

60 Die immissionsschutzrechtliche Rechtsprechung verwendet diese Formulierung gleichwohl nicht als Definition, sondern versteht die Weisungsunabhängigkeit und Selbstständigkeit als starkes Indiz, vgl. OVG Münster NVwZ-RR 2009, 462 (463); OVG Lüneburg NVwZ 2009, 991 (992); der Sache nach auch VGH Mannheim NVwZ 1988, 562 (563).

61 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.

62 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 32.

63 Auf die physische Einwirkungsmöglichkeit abstellend auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 32, jedoch ohne auf die Betriebsnotwendigkeit der Gegenstände einzugehen.

64 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); auf den Effektivitätsgedanken verweisend auch *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 30; *S. Silberg* in M. Dreher (Hrsg.), Versicherungsaufsichtsgesetz, 14. Auflage 2024, BSI-KritisV § 7, Rn. 24.

65 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); OVG Münster NVwZ-RR 2009, 462 (463).

66 Zum Immissionsschutzrecht *T. Schmidt-Kötters* in: L. Giesberts/M. Reinhardt (Hrsg.), BeckOK Umweltrecht, 71. Ed., Stand 01.01.2024, BImSchG § 4 Rn. 115.

Betrieb einer Anlage ergeben kann, ist die Weisungsfreiheit des potenziellen Betreibers maßgeblich.[67] Betreibereigenschaft und Eigentümerstellung können auseinanderfallen.[68] Maßgeblich ist vielmehr die rechtliche Inhaberschaft der Verfügungsgewalt, die der Eigentümer auf Dritte übertragen kann.[69] Mit den „tatsächlichen Umständen" wiederum verweist der Verordnungsgeber auf die tatsächliche Sachherrschaft bzw. Funktionsherrschaft.[70] Die Bewertung der „wirtschaftlichen Umstände" orientiert sich hingegen daran, wer das wirtschaftliche Risiko trägt und wer berechtigt ist, aus der Anlage wirtschaftlichen Nutzen zu ziehen.[71]

Schwierigkeiten kann der Betreiberbegriff somit bereiten, wenn zwei oder mehr Personen Einfluss auf Betrieb und Beschaffenheit der Anlagen oder ihrer Teile haben. Für diese Fälle sieht § 1 Abs. 2 S. 3 BSI-KritisV die Möglichkeit der gemeinsamen Betreiber vor. Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist danach – ähnlich wie bei einer gesamtschuldnerischen Haftung – jeder für die Erfüllung der Betreiberpflichten verantwortlich.[72] Zwar können sie untereinander eine Aufteilung der Pflichten vertraglich vereinbaren,[73] sie sind aber im Außenverhältnis gegenüber dem BSI gemeinsam verantwortlich.[74] Hierdurch will der Verordnungsgeber insbesondere verhindern, dass sich ein Betreiber seiner Betreibereigenschaft entledigt, indem er das operative Tagesgeschäft auf einen Dritten überträgt.[75]

Die Abgrenzung vom Betreiber zu gemeinsamen Betreiber ist jedoch mitunter schwierig.[76] Dies gilt insbesondere dann, wenn sich ein Betreiber beim Betrieb der Anlage oder der hierfür erforderlichen informationstech-

67 Vgl. *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 30.
68 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6.
69 Wohl auch Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6; *K. Beucher, T. Ehlen, J. Utzerath* in: D. Kipker (Hrsg.), Cybersecurity, 2. Aufl., München 2023, Kap. 14 Rn. 53.
70 Vgl. Bundesministerium des Innern, Begründung zur BSI-KritisV, S. 6; *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 53.
71 *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 53; zum Immissionsschutzrecht etwa OVG Münster NVwZ-RR 2009, 462 (463).
72 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.
73 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 22.
74 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.
75 *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 33.
76 Die Herausarbeitung konkreter Abgrenzungskriterien würde den Rahmen dieser Untersuchung sprengen und bleibt daher einer eigenen Untersuchung vorbehalten.

nischen Systeme eines Dritten bedient (sogenanntes *Outsourcing*). Von einer gemeinsamen Betreibereigenschaft ist in solchen Fällen jedenfalls dann auszugehen, wenn das Outsourcing relevante Anlagenteile betrifft.[77] Das Outsourcing lediglich untergeordneter Tätigkeiten bleibt hingegen außer Acht.[78] Der Unterauftragnehmer ist in diesen Fällen meist weisungsabhängig vom Auftraggeber, sodass der bestimmende Einfluss über die KRITIS-Anlage beim Betreiber verbleibt.[79]

b) Anwendung des Beurteilungsmaßstabs auf Digitale Zwillinge

Im Hinblick auf die Frage, wer als Betreiber des Digitalen Zwillings einzustufen ist, kommt es nach dem Vorstehenden darauf an, wer unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb des Digitalen Zwillings ausübt. Weil die Zuordnung der Betreibereigenschaft, wie gesehen, stets nur unter Berücksichtigung der konkreten Umstände des Einzelfalls möglich ist,[80] können auch hier nur allgemeine, auf typisierte und praktisch besonders bedeutsame Fallkonstellationen bezogene Einschätzungen getroffen werden.

Bevor entschieden werden kann, ob der Nutzer und/oder der Provider des Digitalen Zwillings auf dessen Betrieb und Beschaffenheit bestimmenden Einfluss ausüben kann, muss zunächst bestimmt werden, was als Betrieb des Digitalen Zwillings sowie unter dessen Beschaffenheit zu verstehen ist. Hinsichtlich des Betriebsbegriffs bestehen keine Besonderheiten; maßgeblich ist die Funktionsfähigkeit des Digitalen Zwillings. Hinsichtlich der Beschaffenheit des Digitalen Zwillings ist zu beachten, dass der Digitale Zwilling im hier zugrunde gelegten Sinne nicht lediglich die virtuelle, gar grafisch dargestellte Replikation des realen Systems umfasst. Vielmehr besteht der Digitale Zwilling aus einer Software, die diese Replikation ermöglicht, aber wiederum auf einer Hardware operiert und über eine Schnittstelle mit dem realen, abgebildeten System verbunden ist. Eine phy-

77 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41.

78 Bundesministerium des Innern, Begründung zur 2. ÄnderungsVO der BSI-KritisV, S. 41, als Beispiel nennt der Verordnungsgeber das „Gebäudemanagement".

79 *Fischer* (Fn. 56), Teil 2 § 13 Rn. 52; *Glade* (Fn. 43), BSI-KritisV § 1 Rn. 33.

80 Vgl. zum Immissionsschutzrecht VGH Mannheim NVwZ 1988, 562 (563); *Schmidt-Kötters* (Fn. 66), BImSchG § 4 Rn. 115.

sische Einwirkung kann somit nicht nur an der physischen, am oder im realen System befindlichen Schnittstelle erfolgen, sondern auch an der korrespondierenden Hardware.

In tatsächlicher Hinsicht können regelmäßig sowohl Nutzer als auch Provider Einfluss auf den Digitalen Zwilling nehmen. Der Nutzer dürfte regelmäßig auf die Schnittstelle und damit in Teilen auf die Beschaffenheit des Digitalen Zwillings physisch einwirken können. Aufgrund der essenziellen Bedeutung der Schnittstelle für die Funktionsfähigkeit des Digitalen Zwillings besteht somit auch eine Einflussmöglichkeit hinsichtlich des Betriebs des Digitalen Zwillings. Der Provider wiederum dürfte regelmäßig auf die Software sowie die korrespondierende Cloudstruktur (Hardware) Einfluss nehmen können, sei es im Wege einer Abschaltung, der Durchführung von Updates oder einer Anpassung im Rahmen des Kundenservice gegenüber dem Nutzer. Insoweit besteht regelmäßig auch seitens des Providers eine Einflussnahme auf den Betrieb und die Beschaffenheit des Digitalen Zwillings.

In rechtlicher Hinsicht ist zu beachten, dass es regelmäßig allein vom Nutzer abhängt, ob er die Dienstleistung des Providers betreffend die Bereitstellung der Komponenten des Digitalen Zwillings annimmt oder nicht. Somit wird er regelmäßig auch zur Entfernung der Schnittstelle berechtigt sein, weshalb ihm in der Regel auch rechtlich eine Einflussmöglichkeit auf den Betrieb und die Beschaffenheit des Digitalen Zwillings zusteht. Die Vertragsbeziehung zwischen Nutzer und Provider wird es demgegenüber dem Provider realistischerweise nicht erlauben, die Software oder Hardware des Digitalen Zwillings nach Gutdünken zu beeinflussen. Regelmäßig wird er allenfalls berechtigt und verpflichtet sein, Updates und ggf. auf individuellen Wunsch des Nutzers Anpassungen vorzunehmen. Insoweit ist eher von dem Fehlen der Selbstständigkeit und Weisungsunabhängigkeit des Providers auszugehen.

Das wirtschaftliche Risiko des Einsatzes des Digitalen Zwillings im konkreten Fall trägt der Nutzer. Dem mit dem Digitalen Zwilling verbundenen potenziellen Nutzen (etwa in Gestalt von Effizienzsteigerungen) stehen die mit ihm einhergehenden Kosten gegenüber (etwa Lizenz- und Betriebsgebühren). Demzufolge dürften die wirtschaftlichen Umstände regelmäßig gegen den bestimmenden Einfluss des Providers sprechen. Denn ob sich der Einsatz des Digitalen Zwillings im Kontext der Erbringung der kritischen Dienstleistung lohnt, liegt außerhalb seiner Risikosphäre.

In Anbetracht dieser Erwägungen ist zusammengefasst regelmäßig der Nutzer des Digitalen Zwillings als dessen Betreiber einzustufen. Er übt

unter Berücksichtigung tatsächlicher, rechtlicher und wirtschaftlicher Umstände bestimmenden Einfluss auf den Betrieb und die Beschaffenheit des Digitalen Zwillings aus. Ob hingegen der Provider eines Digitalen Zwillings mit dem Nutzer als gemeinsamer (§ 1 Abs. 2 S. 3 BSI-KritisV) oder gar alleiniger Betreiber des Digitalen Zwillings anzusehen ist, kann keinesfalls pauschal beantwortet werden. Große Bedeutung kommt auch hier der konkreten technischen Ausgestaltung des Digitalen Zwillings sowie den Details des Vertragsverhältnisses zwischen dem Nutzer und dem Provider zu.

II. Digitale Zwillinge als Digitale Dienste i. S. d. § 2 Abs. 11 BSIG

Sind in den Betrieb des Digitalen Zwillings externe IT-Dienstleister eingebunden – wovon regelmäßig auszugehen ist – fallen diese potenziell in die Kategorie als Anbieter eines digitalen Dienstes in den Anwendungsbereich des BSIG. Dies ist unabhängig von einer potenziellen Einstufung als KRITIS-Betreiber, beide Rechtsregime sind parallel anwendbar.[81]

1. Digitaler Dienst

§ 2 Abs. 11 BSIG unterscheidet zwischen drei verschiedenen Arten von digitalen Diensten: Erfasst sind Online-Marktplätze (Nr. 1), Online-Suchmaschinen (Nr. 2) und Cloud-Computing-Dienste (Nr. 3). Im Fall Digitaler Zwillinge kommt insbesondere letztere Variante in Betracht, da davon auszugehen ist, dass Digitale Zwillinge aufgrund des erforderlichen Rechenaufwands überwiegend in der Cloud betrieben werden.

Cloud-Computing-Dienste werden definiert als alle in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachten Dienstleistungen[82], die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden. Dazu zählt die cloudgestützte Bereitstellung von Infrastruktur (Infrastructure as a Service

81 *Ritter* (Fn. 38), BSIG § 2 Rn. 36.

82 Dieser Definitionsbestandteil ergibt sich aus dem Verweis auf Art. 1 Abs. 1 lit. b RL (EU) 2015/1535.

– IaaS), von Plattformen (Platform as a Service – PaaS) sowie von Software (Software as a Service – SaaS).[83]

In Bezug auf Digitale Zwillinge kommt nicht etwa nur SaaS in Betracht, also etwa wenn der Nutzer beim IT-Provider die Software einkauft. Denkbar sind auch IaaS, wenn der Nutzer auch Entwickler des Digitalen Zwillings ist und lediglich auf externe Rechenressourcen zurückgreift, oder PaaS, wenn für die Entwicklung eine technische Umgebung erforderlich ist. Entscheidende Bedeutung kommt auch hier den vielgestaltigen konkreten Umständen der technischen Ausgestaltung des Digitalen Zwillings zu, die nur eine Einzelfallbewertung zulassen.

2. Anbietereigenschaft

Regelungsadressaten der IT-Sicherheitspflichten sind juristische Personen, die den digitalen Dienst anbieten (§ 2 Abs. 12 BSIG). Anders als bei KRITIS nimmt das BSIG somit nur juristische Personen in die Pflicht, nicht aber natürliche Personen.

III. IT-Sicherheitspflichten

Für Betreiber von KRITIS sieht das BSIG die strengsten IT-Sicherheitspflichten vor.[84] Diese Pflichten beinhalten insbesondere:

- angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme sicherzustellen, wobei der Stand der Technik eingehalten werden soll (§ 8a Abs. 1 BSIG);
- Systeme zur Angriffserkennung einzusetzen, die durch eine laufende Überwachung des Betriebs eine automatische Protokollierung und De-

83 EU-Kommission, Communication from the Commission to the European Parliament and the Council – Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, 4.10.2017, COM(2017) 476 final/2, Ziff. 4.4.1. Die deutsche Übersetzung spricht statt von „Software as a Service" fälschlicherweise von „Service as a Service"; *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 221; *Ritter* (Fn. 38), BSIG § 2 Rn. 35.

84 Das BSIG sieht in § 8d Ausnahmeregelungen u. a. für Kleinstunternehmer und Betreiber öffentlich zugänglicher Telekommunikationsnetze vor. Aufgrund ihrer Bedeutung für den Einzelfall wird hierauf nicht weiter eingegangen.

tektion von sowie Reaktion auf Störungen ermöglichen (§ 8a Abs. 1a BSIG);
- die Einhaltung der IT-Sicherheit gegenüber dem BSI regelmäßig durch Audits nachzuweisen (§ 8a Abs. 3 BSIG);
- gegenüber dem BSI eine rund um die Uhr erreichbare Kontaktstelle zu benennen (§ 8b Abs. 3 BSIG);
- bestimmte Störungen der IT, die Auswirkungen auf die Verfügbarkeit der kritischen Dienstleistung haben oder haben können, dem BSI zu melden (§ 8b Abs. 4 BSIG).

Das an Anbieter digitaler Dienste gerichtete Pflichtenprogramm weist große Parallelen auf. Insbesondere müssen auch hier technische und organisatorische Maßnahmen zur Gewährleistung der IT-Sicherheit ergriffen werden (§ 8c Abs. 1–2 BSIG). Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Bereitstellung eines innerhalb der EU erbrachten digitalen Dienstes haben, sind unverzüglich an das BSI zu melden (§ 8c Abs. 3 BSIG). Erleichterungen sind etwa insofern vorgesehen, als die Einhaltung der in § 8c Abs. 1–2 BSIG festgelegten Sicherheitspflichten nicht regelmäßig, sondern lediglich anlassbezogen und nur nach behördlicher Aufforderung nachzuweisen ist (vgl. § 8c Abs. 4 S. 1 Nr. 1 gegenüber § 8a Abs. 3 BSIG).[85] Außerdem kommt es bei der Bestimmung meldepflichtiger Vorfälle lediglich auf deren tatsächlich eingetretene Auswirkungen an, sodass die Bewertung potenzieller Auswirkungen nicht erforderlich ist.[86]

D. Zusammenfassung und Ausblick

Digitale Zwillinge im *Industrial Metaverse* eröffnen neue Möglichkeiten, reale Produktions- und Fertigungsprozesse in einer virtuellen Umgebung zu entwickeln, zu simulieren und zu optimieren. Für KRITIS bieten sie ein enormes Potenzial zur Steigerung von Sicherheit, Effizienz und Resilienz der IT-Systeme. Als potenzielle Schwachstelle muss aber auch die IT-Sicherheit Digitaler Zwillinge von Anfang an mitgedacht werden. Als virtuelles Abbild, das mit dem realen System in Echtzeit verbunden ist, kann er unter bestimmten Umständen selbst zu KRITIS oder seine Bereitstellung

85 *Beucher/Ehlen/Utzerath* (Fn. 69), Kap. 14 Rn. 233.
86 *A. Bussche/T. Schelinski*, in: A. Leupold/A. Wiebe/S. Glossner (Hrsg.), IT-Recht, 4. Aufl. München 2021, Teil 7.1 Rn. 44.

zu einem Digitalen Dienst werden und IT-sicherheitsrechtlichen Vorgaben unterliegen.

Abschließend ist darauf hinzuweisen, dass sich das IT-Sicherheitsrecht in Europa in einer großen Umbruchphase befindet. So ist mit Blick auf die Umsetzung der NIS2-Richtlinie nicht auszuschließen, dass künftig auch solche Digitalen Zwillinge den Vorgaben des BSIG unterliegen, die zum jetzigen Zeitpunkt nicht reguliert sind.