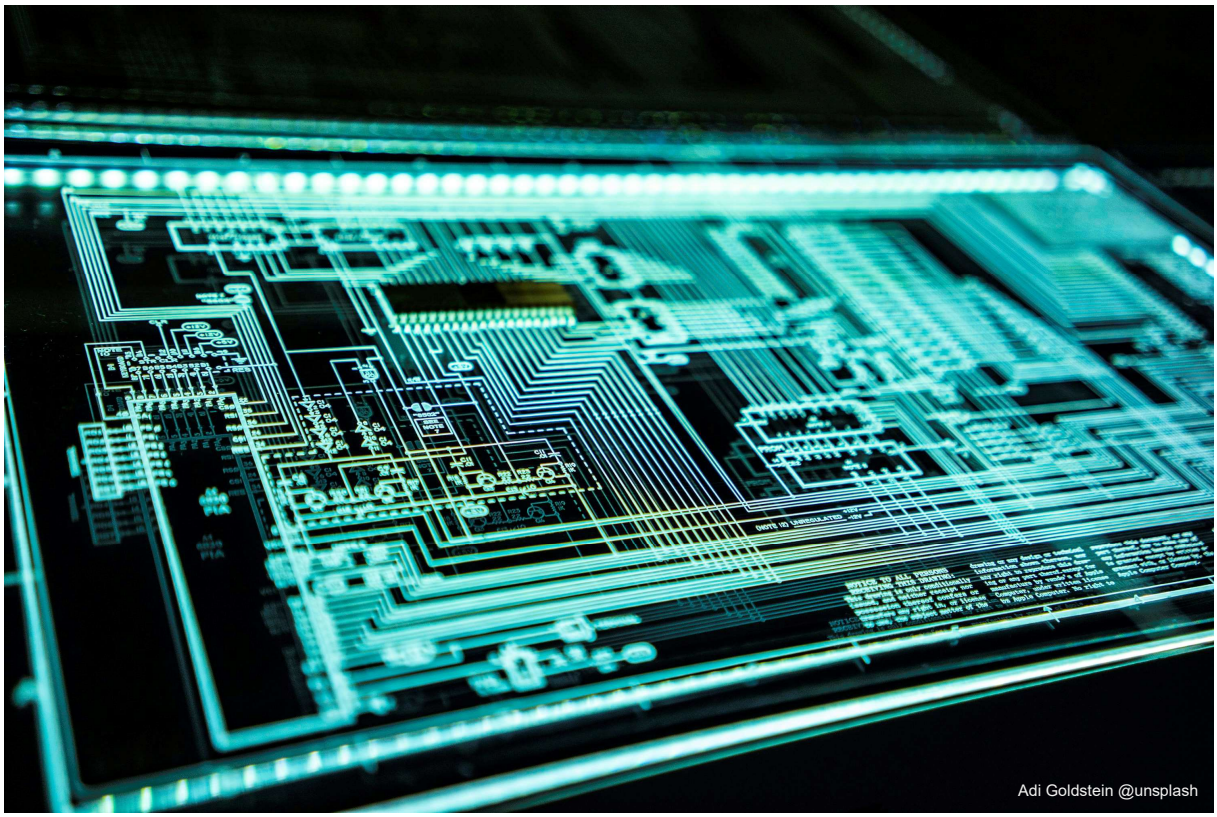
Mittelstand-Digital
Zentrum
Fokus Mensch

Vom „Bouncing Back“ zum „Bouncing Forward”?

CASESTUDY | RESILIENZ


Adi Goldstein @unsplash

Wie reagiert ein Anbieter sicherheitskritischer Software, wenn er selbst Ziel einer Ransomware-Attacke wird? Der Fall der PSI Software SE, Marktführer für Energieleitsysteme in Europa und tief in die deutsche KRITIS-Landschaft eingebunden, verdeutlicht, dass organisationale Resilienz weniger ein technisches als ein strategisches, kulturelles und beziehungsbasiertes Konstrukt ist. Diese Fallstudie fokussiert sich auf das SDG 9 (resiliente Infrastruktur) und differenziert dabei drei analytische Resilienzebenen, deren Zusammenspiel über die Verwundbarkeit eines mittelständischen Brückenbauers entscheidet.

Am 15. Februar 2024 meldet die PSI Software SE per Ad-hoc-Mitteilung einen Cyberangriff auf ihre interne IT-Infrastruktur.[1] Eine Ransomware-Attacke hat sich in das Berliner Konzernnetzwerk eingegraben. Das Unternehmen reagiert mit der proaktiven Trennung sämtlicher Systeme vom Internet, um Datenverlust und Datenmanipulation zu verhindern. Das Landeskriminalamt Berlin übernimmt die Ermittlungen; das Bundesamt für Sicherheit in der

Informationstechnik (BSI) wird eingebunden. Die Aktie verliert am folgenden Handelstag zeitweise rund 13 Prozent, der stärkste Tagesverlust seit sieben Monaten.[2] Nach unternehmenseigener Darstellung war auf Remote-Wartungszugänge zu Kundensystemen indes kein Zugriff möglich.[3]

Unternehmenshintergrund

Die Brisanz des Vorfalls erschließt sich nicht allein aus dem unmittelbaren operativen Schaden, sondern aus der Positionierung des Unternehmens. Die PSI Software SE ist ein börsennotierter Softwarehersteller mit Sitz in Berlin und Mitglied des TecDAX. Seit der Gründung im Jahr 1969 entwickelt das Unternehmen Prozesssteuerungssysteme für Energieversorger, industrielle Anwender und Infrastrukturbetreiber.[3] Als europäischer Marktführer bei Energieleitsystemen für Strom, Gas, Wärme, Öl und Wasser ist PSI tief in die operative Realität kritischer Infrastrukturen eingebettet. Zu den Kunden zählen E.ON, der zweitgrößte Aktionär des Unternehmens, sowie EWE Netz und RheinEnergie.[3] Ein erfolgreicher Angriff auf PSI-Systeme bei den Kunden könnte potenziell die Strom- oder Wasserversorgung betreffen. Damit operiert PSI im Kernbereich der KRITIS, eben jener kritischen Infrastrukturen, deren Beeinträchtigung gravierende Versorgungsengpässe nach sich ziehen kann. Das Unternehmen beschäftigt rund 2.300 Mitarbeitende und ist in 15 Ländern aktiv.[4]

UNTERNEHMENSPROFIL | PSI SOFTWARE SE

Gegründet: 1969 in Berlin • **Umsatz 2024** 260,8 Mio. € • **Mitarbeitende** ca. 2.300

Internationale Präsenz 15 Länder • **Kunden** ca. 1850 (u.a. E.ON, EWE Netz, RheinEnergie)

Internationaler Umsatzanteil ca. 48%

Quelle: PSI Software SE Geschäftsbericht 2024 sowie Q1/2025 Bericht

Mit Transparenz und Vertrauen durch die Krise

PSI entschied früh, die wichtigsten Kunden nicht erst nach der Aufklärung, sondern unmittelbar zu informieren, noch bevor Umfang und Ursache des Vorfalls feststanden. Mit externen Spezialisten errichtete das Unternehmen Notfallsysteme, begann die forensische Aufarbeitung und hielt Kunden wie Behörden über den Fortgang der Wiederherstellung laufend auf dem Stand. Da der Produktivbetrieb erst im Mai 2024 größtenteils wiederanlief, entstanden jedoch bis in den Juli hinein signifikante operative Verluste; Gewinnwarnungen und Analystenskepsis folgten. Das Geschäftsjahr 2024 endete für PSI mit einem um 3,4 Prozent geringeren Umsatz (260,8 Mio. €) und einem negativen EBIT im oberen einstelligen Millionenbereich.[6] Die

Cyberattacke schlug mit einem Umsatzausfall und Sanierungskosten in der Größenordnung von 20 bis 30 Mio. € zu Buche.[4] Versicherungen deckten Teile dieser Belastung. Die Kundenbeziehungen überstanden die Krise weitgehend unbeschadet: Der Auftragseingang lag 2024 bei rund 13,5 Prozent unter dem Vorjahr, der Auftragsbestand blieb jedoch nahezu stabil. Insbesondere die bestehenden Kunden hätten das Unternehmen durch die Krisenzeit getragen, so CFO Gunnar Glöckle. Über die unmittelbare Bewältigung hinaus zog PSI eine strukturelle Konsequenz. An die Stelle der bisherigen Sicherheitsarchitektur traten neue Hard- und Softwarekomponenten, die die Widerstandsfähigkeit dauerhaft erhöhen sollen. „*Wir haben unsere Lektionen gelernt und sind im Unternehmen deutlich breiter aufgestellt*", so CFO Gunnar Glöckle im Interview mit dem Börsenradio.

Von der Krise zur Neuausrichtung

Kaum war der operative Betrieb wiederhergestellt, richtete PSI den Blick nach vorn. Am 1. Dezember 2024 nahm das Unternehmen mit „PSI reloaded" eine neue Organisationsstruktur in Betrieb und vollzog damit einen wesentlichen Schritt zum integrierten, cloud-first ausgerichteten Softwareunternehmen mit KI-gestützten SaaS-Lösungen. Die Konzernstruktur gliedert sich seither in fünf statt der bisher drei Säulen: Netz & Energie Management, Prozessindustrie & Metals, Diskrete Fertigung, sowie Logistik und Mobilität. Quer dazu hat industrielle Künstliche Intelligenz an Bedeutung gewonnen und fließt zunehmend in sämtliche Produktlinien ein.[6] Im März 2025 kam mit Google Cloud ein strategischer Partner für die SaaS-Transformation dazu. Diese Neuausrichtung stärkt ein Geschäftsmodell, dessen Wurzeln auch in der Tiefe der Kundenbeziehung liegen. PSI-Lösungen sind damit langfristig in die Prozesslandschaft der Kunden eingebettet; für die Kunden entstehen daraus hohe Wechselkosten, für PSI eine entsprechend hohe Bindung mit einem stabilen Sockel wiederkehrender Erlöse. Allein Wartung, Upgrades und SaaS-Verträge trugen im Geschäftsjahr 2024 bereits 106 Mio. € zum Umsatz bei[6].

Back to normal?

„*Wir sind wieder da. Back to normal*" - mit diesen Worten kommentierte Karsten Pierschke, Leiter Investor Relations der PSI Software SE, im Frühjahr 2025 auf dem Equity Forum in Frankfurt rückblickend das Krisenjahr 2024.[5] Doch die Rückkehr zur Normalität währte nur kurz. Mit dem Übernahmeangebot des US-Finanzinvestors Warburg Pincus vom 12./13. Oktober 2025 verschob sich die Resilienzfrage bei PSI auf eine neue analytische Ebene – von der Bewältigung eines externen Schocks hin zur Kontrolle über das Unternehmen selbst. Warburg Pincus will den Wandel zum reinen SaaS-Anbieter beschleunigen und stark in die Cloud-Plattform investieren. Die zuvor gedrückte Börsenbewertung – belastet durch operative

Schwierigkeiten, auch infolge des Cyberangriffs – erklären die hohe Übernahmeprämie (vgl. Abb. 1). Über die deutsche Akquisitionsgesellschaft Zest Bidco GmbH wurden 45 Euro je Aktie geboten, was einer Unternehmensbewertung von rund 702 Mio. € und einem Aufschlag von etwa 80 Prozent gegenüber dem Kursdurchschnitt der vorangegangenen Monate entspricht.[23] Nach Ablauf der verlängerten Annahmefrist am 2. Januar 2026 kontrolliert Warburg Pincus 83,24 Prozent der Anteile; E.ON bleibt mit 17,77 Prozent als strategischer Investor und zugleich größter Kunde an Bord. Das Delisting war vorbereitet, das Closing stand jedoch unter dem Vorbehalt der ausstehenden investitionskontrollrechtlichen Freigabe in Deutschland.[24]



Abbildung 1: Kursverlauf der PSI-Aktie im TecDax (2023-2026). Quelle: finanzen.net

Die Übernahme löste nämlich eine bemerkenswerte politische Reaktion aus. Das Bundeswirtschaftsministerium hatte im Januar 2026 eine Investitionsprüfung nach der Außenwirtschaftsverordnung (AWV) eingeleitet.[25] Sicherheitspolitiker bezeichneten die Transaktion öffentlich als „strategisches Risiko"; auch der Verfassungsschutz und der Verband kommunaler Unternehmen äußerten sich zurückhaltend.[26] Die Sorge wurde ebenso in einer internen Bewertung eines Energieunternehmens präzisiert: Durch den beherrschenden Einfluss eines US-Investors würde PSI potenziell dem Zugriff von US-Behörden, etwa über den CLOUD Act oder FISA Section 702, unterliegen.[27] Warburg Pincus und PSI wiesen diese Lesart unter Verweis darauf zurück, dass der operative Betrieb der KRITIS vollständig bei den Kunden liege und PSI keine eigenen Zugriffe auf deren Systeme habe.[27] Am 1. Juli 2026 erteilte die Bundesregierung schließlich die Freigabe.

Die Grenzen einer rein technischen Erklärung

Der Cyberangriff und die Übernahme durch einen US-Investor forderten die Widerstandsfähigkeit von PSI auf je eigene Weise, und in beiden Fällen greift eine rein technische Betrachtung zu kurz. Sie erklärt zwar, warum der Schaden des Cyberangriffs auf die internen Systeme begrenzt blieb. Warum PSI die Krise aber als Unternehmen überstand, erklärt sie nicht. Denn der operative Einbruch war erheblich, mit sinkendem Umsatz, einem negativen Betriebsergebnis und Gewinnwarnungen, und dennoch blieb der Auftragsbestand nahezu unverändert. Der Eigentümerwechsel verändert die Sicherheitsfrage grundlegender,

als es zunächst scheint. Es geht nicht mehr um die Abwehr eines externen Angreifers, sondern um die Vertrauenswürdigkeit des Zulieferers selbst: Wer ein Softwarehaus kontrolliert, kontrolliert potenziell auch dessen Wartungs- und Update-Zugänge in die Systeme der Kunden. Beide Herausforderungen verweisen damit auf dieselbe Größe: Vertrauen. Beim Eigentümerwechsel geht es um das Vertrauen in die Kontrolle über den Zulieferer, beim Cyberangriff um das Vertrauen der Kunden in ein angeschlagenes Unternehmen. Aufschlussreich ist daher weniger, wie gut PSI seine Systeme schützte, als vielmehr, wer in der Krise zum Unternehmen hielt und warum.

Soziales Kapital als unterschätzte Resilienzressource

Bemerkenswert ist, was PSI nach eigenen Angaben in der Krise nicht verlor: langfristige Kundenbeziehungen. „*Keine langfristige Partnerschaft ging verloren*", so Pierschke.[5] Dies verweist auf das Konstrukt der „relational resilience" nach Weick und Sutcliffe (2007):[12] Das Vertrauen in eine Organisation überdauert eine Krise dann, wenn die Krisenreaktion transparent, proaktiv und konsistent erfolgt. Die Glaubwürdigkeit eines Anbieters konstituiert sich nicht durch die Abwesenheit von Krisen, sondern durch deren proaktive Bearbeitung. Der Fall PSI legt nahe, dass organisationale Resilienz weniger eine technische als eine kulturelle und strategische Kapazität ist, deren technische Komponenten notwendige, aber nicht hinreichende Bedingungen darstellen. Eine entscheidende Ressource im vorliegenden Fall war weniger ein Backup-System, sondern das über lange Zeit aufgebaute Vertrauenskapital bei Kunden, Behörden und Investoren, ein Befund, der mit Annahmen zur relationalen Resilienz (Weick & Sutcliffe, 2007)[12] und zum sozialen Kapital in Krisen (Adler & Kwon, 2002)[16] konvergiert. Der Blick verschiebt sich damit von der IT-Architektur zum Beziehungsgefüge aus Kunden, Behörden und Investoren. Resilienz zeigt sich hier nicht als fester Zustand eines technischen Systems, sondern vielmehr als Fähigkeit, die aus den Beziehungen des Unternehmens erwächst. Zentral dabei ist die Position, die PSI in diesem Gefüge einnimmt.

Drei analytische Ebenen der Resilienz

PSI nimmt in der digitalwirtschaftlichen Infrastruktur eine spezifische Stellung ein. Das Unternehmen ist kein für Endkunden sichtbarer Anbieter, aber strukturell relevant für die unsichtbare Funktionsfähigkeit moderner Versorgungs- und Mobilitätssysteme. Martin und Sunley (2015) charakterisieren solche Akteure in der ökonomischen Resilienzforschung als sogenannte „Brückenbauer" - Organisationen, die zwischen Technologieentwicklung, operativer Steuerung und institutioneller Regulierung vermitteln und deren Ausfall

kaskadierende Effekte in nachgelagerten Systemen auslösen kann.[10] Gerade diese Stellung erzeugt eine strukturelle Doppelzumutung: PSI produziert Resilienz für andere und muss zugleich selbst resilient sein, um diese Leistung erbringen zu können. Eben diese Position macht sichtbar, dass sich Resilienz im Fall PSI nicht auf eine einzelne Ebene reduzieren lässt. In Anlehnung an die Differenzierungen der Organisationsforschung (Linnenluecke, 2017; Hernes et al., 2024)[8],[9] und an die Systemlogik kritischer Infrastrukturen sind drei Ebenen zu unterscheiden:

1. Organisationale Resilienz

PSI muss als Unternehmen widerstandsfähig gegenüber Cyberangriffen, regulatorischen Verschiebungen und Marktveränderungen sein. Diese Ebene umfasst die IT-Sicherheitsarchitektur, Krisenkommunikation, Lieferkettenstabilität und finanzielle Tragfähigkeit. Sie betrifft die Frage, ob das Unternehmen einen Schock absorbieren und sich rekonstituieren kann. Im Februar 2024 wurde genau diese Ebene getroffen. PSI absorbierte den Angriff durch die sofortige Isolierung der Systeme und die transparente Kommunikation nach außen und rekonstituierte sich anschließend über eine erneuerte Sicherheitsarchitektur.

2. Kundenseitige Resilienz

PSI-Produkte, so unter anderem Leitsysteme, Echtzeit-Monitoring und prädiktive Wartungssoftware, sollen die Resilienz der Kunden erhöhen. Die Software erkennt Netzschwankungen, optimiert Lastflüsse und ermöglicht im Idealfall den teilautonomen Weiterbetrieb auch bei Ausfällen einzelner Komponenten. Resilienz ist hier nicht Eigenschaft des Anbieters, sondern Leistung, die der Anbieter seinen Kunden ermöglicht. Im Angriffsfall bewährte sich diese Ebene. Weil die Kundeninstallationen über ein doppeltes Schleusenprinzip von PSIs interner IT getrennt waren – ein Zugang ließ sich nur beidseitig freigeben –, blieb nach Unternehmensangaben kein Kunde vom Vorfall betroffen.

3. Systemische Resilienz

Da PSI als zentraler Lieferant in mehreren KRITIS-Sektoren operiert, wirken die Lösungen des Unternehmens über das einzelne Kundenunternehmen hinaus auf die Stabilität ganzer Wertschöpfungssysteme, etwa die europäische Stromversorgung oder urbane Logistikketten. Die Resilienz eines Brückenbauers wird damit zur Systemfrage, die die einzelwirtschaftliche Optimierungslogik übersteigt. Im Fall PSI trat diese Ebene weniger beim Angriff selbst zutage als beim Eigentümerwechsel. Da rund 90 Prozent der großen deutschen Netzbetreiber PSI-Software nutzen, wurde die Kontrolle über das Unternehmen zur Frage der

Versorgungssicherheit und rief mit der staatlichen Investitionsprüfung eine systemische Schutzinstanz auf den Plan.

„Bouncing forward“ auf Kosten der Souveränität

Hernes, Blagoev, Kunisch und Schultz (2024) erweitern die Resilienzdebatte neben einer relationalen um eine zeitliche Dimension. Organisationen reagieren auf disruptive Ereignisse nicht nur dadurch, dass sie zum Vorzustand zurückkehren („bouncing back"), sondern indem sie daraus eine zukunftsgerichtete Entwicklung ableiten („bouncing forward").[8] Resilienz ist damit keine feste Eigenschaft, sondern entfaltet sich über die Zeit. Ein Unternehmen entwirft mögliche Reaktionswege bereits vor einer Krise, aktualisiert sie im Ernstfall und richtet sie anschließend an den veränderten Bedingungen neu aus. Auf das Absorbieren des Schocks folgte bei PSI kein Zurück zum Ausgangszustand, sondern eine Neuausrichtung: die Erneuerung der Sicherheitsarchitektur und der beschleunigte Übergang zum SaaS-Modell. PSI kehrte nicht zum Vorzustand zurück, sondern nutzte die Krise zunächst zur Transformation – eine Bewegung, die dem Dreischritt „Absorb – Adapt – Transform" entspricht (Walker et al., 2004).[11] Diese Transformation hat jedoch ihren Preis, und er liegt nicht allein im Technischen. Die Neuausrichtung auf Cloud und SaaS ist kapitalintensiv, und ihre Finanzierung sicherte PSI über den Einstieg des US-Investors Warburg Pincus. Das schafft jedoch eine paradoxe Lage: PSI gewinnt zwar potenziell an Widerstandsfähigkeit (z.B. Kapital, ein stabiler Eigentümer, Unabhängigkeit vom Quartalsdruck), gibt dafür aber die Kontrolle an einen Investor in fremder Jurisdiktion ab. Weil PSIs Software kritische Infrastruktur steuert, berührt der Eigentümerwechsel die digitale Souveränität. Es geht nicht mehr nur darum, ob die Netze zuverlässig laufen, sondern wer im Ernstfall auf die Systeme zugreifen, sie steuern oder gar Daten einsehen kann und welchem Recht dieser Zugriff untersteht. PSI und Warburg Pincus haben zwar zugesichert, dass die Verantwortung für sensible Kunden- und Infrastrukturdaten allein bei PSI verbleibt und alle Datenschutz- und Vertraulichkeitspflichten fortgelten. Solche Zusagen wirken jedoch auf privatrechtlicher Ebene; ob sie einem extraterritorialen Zugriff nach CLOUD Act oder FISA standhalten, ist offen, da diese Gesetze an der Kontrolle des Eigentümers ansetzen und private Vertraulichkeitszusagen überlagern können.

Schlussüberlegung

Der Fall PSI zeigt, dass Widerstandsfähigkeit in der Softwareindustrie weniger auf technischen Schutzmaßnahmen allein beruhte als auf Kundenbeziehungen, die auch während der Krise

stabil blieben. Die entscheidende Frage ist dabei nicht nur, wie ein Unternehmen Schocks abwehrt, sondern auch welche Abhängigkeiten es eingehen kann, ohne die Quelle seiner Resilienz preiszugeben. Resilienz ist damit kein einmal erreichter Zustand, sondern ein Prozess, der sich über die Zeit fortlaufend neu bildet. Jede Bewältigung verändert die Ausgangslage für die nächste. Für PSI entscheidet sich daran, ob die neuen Abhängigkeiten, die die Transformation mit sich bringt, seine bisherige Handlungsfreiheit einschränken.

Quellen und weiterführende Literatur

1. Ad-hoc-Mitteilung der PSI Software SE vom 15.02.2024: 'Cyberangriff auf PSI'. (https://www.psi.de/unternehmen/investor-relations/ad-hoc-mitteilungen/cyberangriff-auf-psi (abgerufen 09/2025))
2. Handelsblatt (16.02.2024): 'PSI Software: Hacker legen wichtigen Dienstleister für Energieunternehmen lahm', (https://www.handelsblatt.com/unternehmen/energie/psi-software-hacker-legen-wichtigen-dienstleister-fuer-energieunternehmen-lahm/100015519.html)
3. ChannelPartner (21.02.2024): 'Cyberangriff auf PSI Software', (https://www.channelpartner.de/article/3900950/cyberangriff-auf-psi-software.html)
4. PSI Software SE: Pressemitteilung 'PSI im 1. Quartal mit Belastungen aus der Cyberattacke und stabilem Cashflow' (30.08.2024) (https://www.psi.de/unternehmen/newsroom/pressemitteilungen/psi-im-1-quartal-mit-belastungen-aus-der-cyberattacke-und-stabilem-cashflow)
5. BRN AG (27.03.2025): 'PSI nach Cyberangriff zurück auf Kurs – Back to normal'. Interview mit Karsten Pierschke, Leiter Investor Relations PSI Software SE (https://www.brn-ag.de/44288-PSI-Cyberangriff-Energie-Strategie-Digitalisierung)
6. PSI Software SE: Pressemitteilung 'PSI im 1. Quartal 2025 mit Rekordauftragseingang' (30.04.2025) (https://www.psi.de/unternehmen/newsroom/pressemitteilungen/psi-im-1-quartal-2025-mit-rekordauftragseingang)
7. Burnard, K. & Bhamra, R. (2011): Organisational resilience: development of a conceptual framework for organisational responses. International Journal of Production Research, 49(18), 5581–5599, (https://doi.org/10.1080/00207543.2011.563827)
8. Hernes, T., Blagoev, B., Kunisch, S. & Schultz, M. (2024): From Bouncing Back to Bouncing Forward: A Temporal Trajectory Model of Organizational Resilience. Academy of Management Review, 50(1), 72–92, (https://doi.org/10.5465/amr.2022.0406)
9. Linnenluecke, M.K. (2017): Resilience in Business and Management Research: A Review of Influential Publications and a Research Agenda. International Journal of Management Reviews, 19(1), 4–30, (https://doi.org/10.1111/ijmr.12076)
10. Martin, R. & Sunley, P. (2015): On the notion of regional economic resilience: conceptualization and explanation. Journal of Economic Geography, 15(1), 1–42, (https://doi.org/10.1093/jeg/lbu015)
11. Walker, B. et al. (2004): Resilience, adaptability and transformability in social-ecological systems. Ecology and Society, 9(2), 5, (https://doi.org/10.5751/ES-00650-090205)
12. Weick, K.E. & Sutcliffe, K.M. (2007): Managing the Unexpected: Resilient Performance in an Age of Uncertainty. 2. Aufl., Jossey-Bass, (https://www.researchgate.net/publication/265106124_Managing_the_Unexpected_Resilient_Performance_in_an_Age_of_Uncertainty/references)

13. Hillmann, J. & Guenther, E. (2021): Organizational Resilience: A Valuable Construct for Management Research? International Journal of Management Reviews, 23(1), 7–44, (https://doi.org/10.1111/ijmr.12239)

14. Vargo, S.L. & Lusch, R.F. (2008): Service-dominant logic: continuing the evolution. Journal of the Academy of Marketing Science, 36(1), 1–10, (https://doi.org/10.1007/s11747-007-0069-6)

15. Taleb, N.N. (2012): Antifragile: Things That Gain from Disorder. Random House (https://doi.org/10.1108/10595421311319852)

16. Adler, P.S. & Kwon, S.-W. (2002): Social Capital: Prospects for a New Concept. Academy of Management Review, 27(1), 17–40, (https://www.jstor.org/stable/4134367)

17. United Nations (2015): Transforming our World: The 2030 Agenda for Sustainable Development. Resolution A/RES/70/1, Targets 9.1–9.5. (https://sdgs.un.org/2030agenda)

18. UN ESCAP (2019): The Disaster Riskscape Across Asia-Pacific: Pathways for Resilience, Inclusion and Empowerment. United Nations Publication, (https://www.unescap.org/publications/asia-pacific-disaster-report-2019)

19. OECD (2019): Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. (https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html)

20. Bundesamt für Sicherheit in der Informationstechnik (BSI, 2024): Die Lage der IT-Sicherheit in Deutschland 2024, (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf)

21. Europäische Union (2022): Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, (https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555)

22. Ani, U.P.D., He, H. & Tiwari, A. (2017): Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32–74, (https://doi.org/10.1080/23742917.2016.1252211)

23. Finanztrends (15.10.2025): „PSI Software-Aktie: Unglaublich, was passiert!" (https://www.finanztrends.de/news/psi-software-aktie-unglaublich-was-passiert/)

24. Ad-hoc-News / boerse-global.de (23.01.2026): „PSI Software Aktie: KRITIS-Alarm". Warburg Pincus kontrolliert nach Ende der Annahmefrist 83,24 % der Anteile; Delisting in Vorbereitung, (https://www.ad-hoc-news.de/boerse/news/ueberblick/psi-software-aktie-kritis-alarm/68512044)

25. Handelsblatt (11.03.2026): „Software: Bundesregierung prüft Übernahme von PSI durch US-Investor". Beginn der Investitionsprüfung nach Außenwirtschaftsverordnung (AWV) im Januar 2026, (https://www.handelsblatt.com/politik/deutschland/software-bundesregierung-prueft-uebernahme-von-psi-durch-us-investor/100207431.html)

26. Handelsblatt (Frühjahr 2026): „Kritische Infrastruktur: Politiker warnen vor US-Einstieg bei Berliner Software-Firma". Aussagen Marc Henrichmann (CDU, Vorsitzender Geheimdienste-Kontrollgremium) und Konstantin von Notz (Grüne, Vize-Vorsitzender); Stellungnahmen Verfassungsschutz und Verband kommunaler Unternehmen (VKU), (https://www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-politiker-warnen-vor-us-einstieg-bei-berliner-software-firma/100217432.html)

27. Handelsblatt (17.12.2025): „Kritische Infrastruktur: Sorge vor Übernahme des Softwarehauses PSI durch US-Investor". Interne Bewertung eines Energieunternehmens; Hinweise auf CLOUD-Act- und FISA-Section-702-Risiken; Stellungnahmen Warburg Pincus und PSI, (https://www.handelsblatt.com/politik/deutschland/kritische-infrastruktur-sorge-vor-uebernahme-des-softwarehauses-psi-durch-us-investor/100184397.html)