

Modellrechnung sieht auch im konservativen
Szenario milliardenschweren Nutzen

„RETURN ON SECURITY INVESTMENT“-ANALYSE DES CYBERDOMES



Eine Modellrechnung der Westfälischen Hochschule Gelsenkirchen schätzt den wirtschaftlichen Ertrag eines nationalen Cyberabwehrsystems ab. Ergebnis: Die politisch diskutierten Investitionskosten von ein bis zwei Milliarden Euro fallen gegenüber den vermeidbaren Schäden gering aus.

Cyberangriffe verursachen in Deutschland inzwischen Schäden in dreistelliger Milliardenhöhe. Laut der Bitkom-Studie „Wirtschaftsschutz 2025“ summierte sich der Gesamtschaden durch Wirtschaftsspionage, Sabotage und Cyberkriminalität zuletzt auf 289,2 Milliarden Euro, wobei rund 70 Prozent davon auf Cyberangriffe im engeren Sinne entfielen.^[1] Gleichzeitig hält laut Bitkom nur eine Minderheit von 40 Prozent der Unternehmen Deutschland für gut auf großflächige Cyberangriffe vorbereitet, und 39 Prozent verfügen über kein eigenes Notfallmanagement.

Vor diesem Hintergrund arbeiten das Bundesinnenministerium und das Bundesamt für Sicherheit in der Informationstechnik (BSI) an einem Konzept für einen sogenannten Cyberdome – ein zentrales, organisationsübergreifendes Verteidigungssystem gegen Cyberangriffe. Im politischen Umfeld wird dafür ein Kostenrahmen von ein bis zwei Milliarden Euro genannt. Ob sich diese Investition wirtschaftlich begründen lässt, prüft die folgende Modellrechnung nach dem Return on Security Investment (RoSI).

WAS EIN CYBERDOME LEISTEN SOLL

Ein Cyberdome ist ein umfassendes Verteidigungssystem, dessen Ziel es ist, die digitalen Infrastrukturen eines Landes zentral zu schützen. Es bündelt präventive, detektive und reaktive IT-Sicherheitsmechanismen in einer zentral koordinierten Plattform (siehe Abbildung 1).^[4]

Vier Funktionen bilden dabei das Rückgrat: Der präventive Schutz erfasst kontinuierlich Bedrohungsdaten und tauscht sie zwischen den beteiligten Organisationen aus. Die Erkennung und Analyse überwachen angeschlossene IT-Systeme in Echtzeit und identifiziert Angriffsmuster. Reaktion und Wiederherstellung leiten automatisierte oder halbautomatisierte Gegenmaßnahmen ein, etwa das Blockieren kompromittierter IP-Adressen. Die kontinuierliche Verbesserung speist jeden bearbeiteten Vorfall in neue Filterlisten, Signaturen und Reaktionspläne ein.

Technisch stützt sich das Konzept auf Sensoren in IT-Systemen, ein gemeinsames Security-Information-and-Event-Management-(SIEM)-System zum Abgleich mit bekannten Angriffs-

mustern sowie ein „Security Orchestration, Automation and Response“- (SOAR)-System für automatisierte Gegenmaßnahmen. Organisatorisch eingebettet sind diese Bausteine in Security Operations Center (SOC), die untereinander Informationen austauschen. Ein SOC ist kein neues Konzept: ein Team von IT-Sicherheitsexperten, das die IT-Infrastruktur einer Organisation überwacht und auf Vorfälle reagiert, oft ergänzt durch einen externen Managed Security Service Provider.^[5] Neu am Cyberdome ist nicht das einzelne SOC, sondern dessen Vernetzung über Organisations- und Unternehmensgrenzen hinweg. Der wirtschaftliche Mehrwert soll dabei weniger durch einzelne Technologien als durch die kollektive Koordination und gemeinsame Lagebilder entstehen.

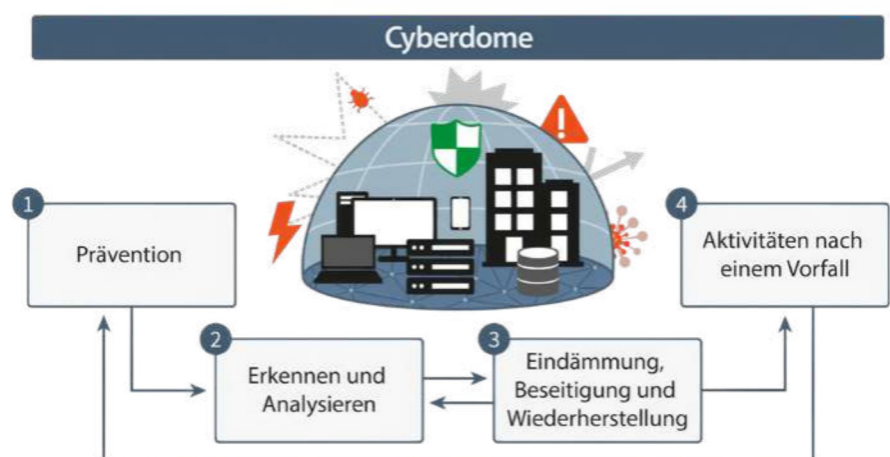


Abbildung 1: Cyberdome-Architektur (Bild: if(is))

Einen funktionierenden Cyberdome im Wirkbetrieb gibt es bereits in Israel, auf den sich der deutsche Sicherheitspakt beruft. Allerdings lässt sich das Modell nicht direkt übertragen, da rechtliche Rahmenbedingungen wie das Trennungsgebot zwischen Polizei und Nachrichtendiensten sowie der deutsche Föderalismus hierzulande andere Voraussetzungen schaffen.^[9]

GRÜNDE FÜR DIE KOLLEKTIVE BETRACHTUNG

Die RoSI-Analyse betrachtet nicht einzelne Unternehmen und Organisationen, sondern alle Beteiligten gemeinsam. Dafür sprechen vier Gründe:

- **Wirtschaftlicher Schaden:** Der Schaden aus Cyberkriminalität trifft die Volkswirtschaft als Ganzes. Er lässt sich daher nur senken, wenn alle Organisationen in Deutschland gemeinsam daran arbeiten.
- **Hybride Kriegsführung:** Die hybride Kriegsführung richtet sich gegen Staat und Gesellschaft. Einzelne Unternehmen verfügen weder über die rechtlichen noch über die technischen Mittel, um koordinierten, staatlich gelenkten Angriffen wirksam zu begegnen. Der Schutz liegt damit primär in staatlicher Zuständigkeit und lässt sich nicht auf eine einzelbetriebliche RoSI-Betrachtung übertragen. Ein gemeinsames Verteidigungssystem soll hier ansetzen.
- **Vertrauen in die Digitalisierung:** Der Staat setzt auf Digitalisierung, um die wirtschaftliche Leistungsfähigkeit und die Effizienz öffentlicher Dienstleistungen zu steigern. Das setzt voraus, dass Bürger und Unternehmen den digitalen Angeboten vertrauen. Ein gemeinsames Verteidigungssystem soll dieses Vertrauen stützen.
- **Notwendige Stakeholder des Cyberdomes:** Beteiligt wären Organisationen des Bundes, der Länder und der Kommunen sowie alle Unternehmen in Deutschland. Nach Größenklassen^[10]: Rund 2,5 Millionen Kleinstunternehmen mit weniger als zehn Beschäftigten und einem Umsatz von bis zu zwei Millionen Euro, etwa 470.000 kleine Unternehmen mit weniger als 50 Beschäftigten und einem Umsatz von bis zu zehn Millionen Euro, rund 78.000 mittlere Unternehmen mit weniger als 250 Be-

schäftigten und einem Umsatz von bis zu 50 Millionen Euro sowie etwa 21.000 große Unternehmen mit mehr als 250 Beschäftigten oder einem Umsatz von mehr als 50 Millionen Euro. Hinzu kommen Provider von Kommunikation und Diensten, Betreiber kritischer Infrastrukturen (KRITIS) sowie die Strafverfolgungsbehörden.

WIE SICH DER NUTZEN EINES CYBERDOMES BERECHNEN LÄSST

Für die wirtschaftliche Bewertung des Cyberdomes dient das RoSI-Modell (siehe Abbildung 2). Die Grundformel lautet: $RoSI = S - T$, wobei S die durch die Maßnahme vermiedenen Schäden bezeichnet und T die Kosten der Maßnahme, die Tool Costs.^[6] Solange S größer als T ausfällt, ist die Investition wirtschaftlich sinnvoll.

Als Ausgangswert für den vermeidbaren Schaden dient der Bitkom-Gesamtschaden von 289,2 Milliarden Euro, gewichtet mit dem von Bitkom ausgewiesenen Cyberanteil von 70 Prozent. Daraus ergibt sich eine Recovery Cost von 202,44 Milliarden Euro als gesamtwirtschaftlicher Ausgangswert.^[1] Dieser wird anschließend auf die fünf wichtigsten Angriffstypen verteilt: Ransomware, Distributed Denial of Service (DDoS), Phishing, Malware und Passwort-Angriffe.

Da Bitkom selbst keine Schadenswerte je Angriffstyp ausweist, wird jeder Typ mit einem Gewichtungsfaktor versehen, der sich aus der Betroffenheitsquote der Unternehmen und den durchschnittlichen Vorfallkosten aus dem IBM Cost of a Data Breach Report 2025 zusammensetzt.^[7] Zu beachten ist dabei, dass IBM die Kosten der Bewältigung eines Datenschutzvorfalls misst, etwa Erkennung, Benachrichtigung und Geschäftsausfall. Bitkom hingegen erfasst den volkswirtschaftlichen Gesamtschaden eines Angriffs – das ist nicht dasselbe. Zudem stammt der Ransomware-Wert aus einem separaten Berichtsteil zu Erpressungsvorfällen, denn IBM führt Ransomware nicht als eigenen Angriffsvektor.

Die daraus berechneten Anteile sind daher als grobe Näherung zu verstehen, nicht als exakte Abbildung der IBM-Kategorien. Hinzu kommt, dass die IBM-Kostenwerte einem globalen Durchschnitt aus 16 Ländern entstammen. Eine länderspezifische Aufschlüsselung nach Angriffstyp liegt nicht vor.^[7] Auch die Bitkom-Zahlen beruhen auf einer Unternehmensbefragung, also auf Selbstauskünften, nicht auf verifizierten Meldedaten. Beide Modellbausteine sind damit als plausible Näherungen zu verstehen, nicht als exakte Messwerte.

Da belastbare empirische Werte zur tatsächlichen Wirksamkeit eines Cyberdomes fehlen, wurden drei Abwehrraten-Szenarien definiert,

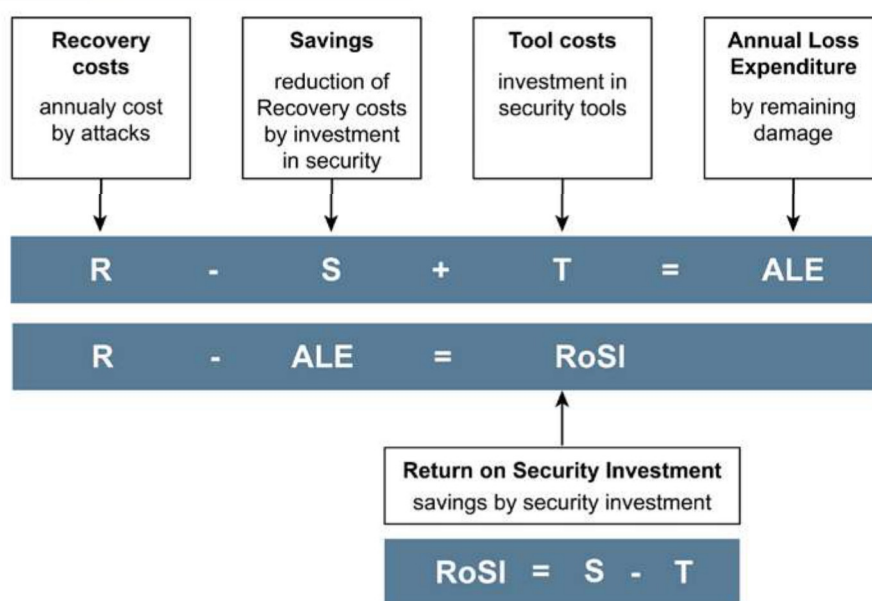


Abbildung 2: Return on Security Investment (RoSI) (Bild: if(is))

die jeweils auf einer eigenen Argumentationslinie beruhen:

- **Konservatives Szenario:** Das konservative Szenario setzt die Abwehrquote bei zehn Prozent an. Es bildet die Anlaufschwierigkeiten geteilter Bedrohungsdaten ab, wie sie in einer Untersuchung zu Cyber-Threat-Intelligence-Systemen dokumentiert sind. Dort waren geteilte Indikatoren häufig lückenhaft, verzögert und nur zu 0,09 Prozent überhaupt mit maschinenlesbaren Erkennungsregeln versehen.^[8] Im konservativen Szenario muss zum Beispiel sichergestellt werden, dass die Bedrohungsdaten standardisiert, vollständig und zeitnah ausgetauscht werden.
- **Basisszenario:** Das Basisszenario setzt 25 Prozent an, gestützt auf Befunde des IBM-Reports, wonach der Einsatz KI-gestützter Sicherheitsmechanismen und Automatisierung mit schnellerer Erkennung und effizienteren Reaktionsprozessen einhergeht.^[7] Im Basisszenario muss beispielsweise sichergestellt werden, dass die Automatisierungseffekte durch Standardisierungen, Vollständigkeit der Angriffsinformationen, intelligente Auswertung und strukturierte Reaktionsprozesse optimale Ergebnisse erzielen.
- **Optimistisches Szenario:** Das optimistische Szenario setzt 40 Prozent an, motiviert durch den im ENISA-NIS360-Bericht beschriebenen Zusammenhang zwischen Reifegrad, Koordination und Resilienz. Ein hoher Reifegrad kann demnach Unternehmen und Organisationen sogar aus der Risikozone herausführen, also aus der Gruppe der Sektoren mit besonders niedriger Widerstandsfähigkeit gegen Cyberangriffe.^[9] Im optimistischen Szenario muss zum Beispiel sichergestellt werden, dass alle Stakeholder effektiv und offen zusammenarbeiten, um gemeinsam dafür zu sorgen, dass das Risiko deutlich reduziert wird.

ERGEBNISSE DER ANALYSE

Auf Basis des beschriebenen Gewichtungsfaktors entfällt der größte Schadensanteil auf Ransomware, rund 59 Milliarden Euro. Es folgen DDoS mit 38 Milliarden Euro, Phishing mit 36 Milliarden Euro, Malware mit 35 Milliarden Euro und Passwort-Angriffe mit 34 Milliarden

Euro. Die übrigen vier Angriffstypen liegen damit vergleichsweise nah beieinander und machen zusammen rund 70 Prozent des Schadens aus. Ein wirksames Abwehrsystem müsste also breit über verschiedene Angriffsvektoren ansetzen, statt sich auf Ransomware zu konzentrieren.

Werden die drei Abwehrquoten auf den Gesamtschaden angewendet, ergeben sich im konservativen Szenario vermiedene Schäden von 20,24 Milliarden Euro, im Basisszenario 50,61 Milliarden Euro und im optimistischen Szenario 80,98 Milliarden Euro. Selbst im konservativsten Fall liegt der Wert etwa beim Zehnfachen der oberen Investitionsgrenze von zwei Milliarden Euro. Auch bei den höchsten angenommenen Tool-Kosten von zwei Milliarden Euro übersteigt der Nutzen im ungünstigsten Szenario die Investition um mehr als 18 Milliarden Euro, im Basisszenario um knapp 49 Milliarden Euro und im optimistischen Szenario um rund 79 Milliarden Euro.

Da die Tool-Kosten als einmalige Investition modelliert sind, die Einsparungen dagegen als jährlich wiederkehrender vermiedener Schaden, zahlt sich die Investition rechnerisch bereits im ersten Jahr aus. Bemerkenswert ist zudem, wie wenig die genaue Höhe der Tool-Kosten das Gesamtbild ändert. Ob ein oder zwei Milliarden Euro angesetzt werden, verschiebt den RoSI im Basisszenario lediglich zwischen 49,61 und 48,61 Milliarden Euro. Die Aussagekraft der Analyse hängt damit weit stärker von der angenommenen Abwehrquote ab als von der genauen Investitionssumme.

Für den Cyberdome setzt die Modellrechnung daher eine breite Beteiligung von Organisationen in Deutschland voraus. Sie müssten standardisierte Bedrohungsdaten teilen und abgestimmte Reaktionen ermöglichen. Für die angenommene Abwehrquote sind zudem die Auswertung der Daten und die Automatisierung von Reaktionsprozessen relevant. KI-Verfahren könnten dabei unterstützen, sofern sie belastbare Ergebnisse liefern und in geeignete Abläufe eingebunden sind. Die aus dem Betrieb gewonnenen Erkenntnisse müssten außerdem fortlaufend in die Weiterentwicklung der IT-Sicherheit und der eingesetzten IT-Systeme einfließen.

WAS DER STAAT SPART

Für ein Unternehmen bemisst sich der Nutzen einer Sicherheitsinvestition an den eigenen ver-

miedenen Kosten. Für den Staat stellt sich die Rechnung anders dar, denn der volkswirtschaftliche Schaden von rund 202 Milliarden Euro entspricht bei einem deutschen Bruttoinlandsprodukt von etwa 4.469,8 Milliarden Euro im Jahr 2025 einem Anteil von rund 4,5 Prozent.^[10]

Jeder vermiedene Euro verbleibt damit unmittelbar in der gesamtwirtschaftlichen Wertschöpfung, etwa als erhaltene Produktion, gesicherte Arbeitsplätze oder ausbleibende Wiederherstellungskosten. Die Investition ist aus staatlicher Sicht damit keine klassische Ausgabenposition, sondern eine Maßnahme zum Erhalt eines spürbaren Anteils der gesamtwirtschaftlichen Leistung. Aber auch das dadurch zu generierende Vertrauen in die digitale Zukunft sowie die gemeinsame Verteidigung gegen hybride Kriegsführung sind weitere Mehrwerte.

WER VOM CYBERDOME PROFITIERT

In absoluten Zahlen entsteht der größte Nutzen im Mittelstand, schlicht weil hier die meisten Unternehmen und Beschäftigten angesiedelt sind. Bei Ransomware etwa stehen im Mittelstand 9,19 Milliarden Euro vermiedener Schaden 5,66 Milliarden Euro bei Großunternehmen gegenüber. Pro Firma gerechnet kehrt sich das Bild um, Großunternehmen profitieren mit rund 326.700 Euro deutlich stärker als der Mittelstand mit rund 21.000 Euro, was an ihren höheren Schadenspotenzialen liegt. Wird stattdessen pro Beschäftigten gerechnet, kehrt sich das Verhältnis erneut um. Bei Ransomware ergeben sich rund 615 Euro Nutzen pro Kopf im Mittelstand gegenüber 358 Euro bei Großunternehmen, bei DDoS und Phishing fällt der Abstand noch größer aus.^[12, 11] Grund dafür ist, dass Großunternehmen meist schon über eigene SOC- und SIEM-Infrastruktur verfügen, wodurch der zusätzliche Nutzen eines Cyberdomes für sie geringer ausfällt als für Unternehmen, denen diese Strukturen fehlen.

Damit stellt sich die Frage, ob ausgerechnet der Mittelstand technisch überhaupt in der Lage ist, von einem hochautomatisierten Verteidigungssystem zu profitieren. Ein Teil der Arbeit beschreibt die heterogene, historisch gewachsene IT-Landschaft in Deutschland als Hindernis für automatisierte Reaktionsprozesse, ein anderer Teil erwartet gerade für kleine und mittlere Unternehmen den größten Nutzen.

Der scheinbare Widerspruch löst sich auf, sobald Automatisierung nicht nur auf Ebene des einzelnen Unternehmens gedacht wird. Sie kann bereits bei vorgelagerten Infrastrukturanbietern ansetzen. Die Deutsche Telekom bietet mit Security OnNet Basic bereits ein Produkt an, das betrügerische Webseiten und Phishing-Links unmittelbar auf Netzebene blockiert, ohne dass Kunden dafür eigene Hardware oder Fachpersonal benötigen, ergänzt um eine automatisierte Botnet-Erkennung.^[11]

Für den Mittelstand ergibt sich der Nutzen eines Cyberdomes damit weniger aus einer eigenen

Ergänzend zeigt sich bei Betreibern kritischer Infrastrukturen ein uneinheitliches Bild. Sie sind bei Ransomware, Phishing und Passwort-Angriffen häufiger betroffen als der Rest der Wirtschaft, bei DDoS-Angriffen seltener, vermutlich weil ihre gesetzliche Notfallvorsorge hier schon besonders greift.^[12] Eine pauschale Priorisierung von KRITIS-Betreibern lässt sich daraus nicht ableiten.

lauschwierigkeiten geteilter Bedrohungsdaten abbildet. Wie oben beschrieben, enthielten nur 0,09 Prozent der geteilten Indikatoren überhaupt maschinenlesbare Erkennungsregeln.^[8] Das ist zunächst ein Standardisierungsproblem, kein Automatisierungsproblem. Erst einheitliche Datenformate, etwa über Standards wie STIX und TAXII, schaffen die Grundlage für Automatisierung.

Darauf aufbauend wird der Sprung zum realistischen Szenario zur Frage des Automatisierungsgrads. KI-gestützte Mechanismen verkürzen die Erkennungs- und Reaktionszeiten erheblich.^[7] Für einen Cyberdome bedeutet



technischen Integration als aus der automatisierten Absicherung durch Provider, über deren Netze ohnehin ein Großteil des Datenverkehrs läuft. Um von diesem Effekt zu profitieren, muss die eigene, oft veraltete IT-Landschaft nicht sofort grundlegend umgebaut werden. Mittelfristig sollte sie dennoch modernisiert werden.

PRIORITÄTEN FÜR DEN AUFBAU

Ob die drei Szenarien tatsächlich erfolgreich umgesetzt werden können, hängt von konkreten Voraussetzungen ab, die sich unmittelbar aus ihrer Herleitung ergeben. Ausgangspunkt ist das konservative Szenario, das heutige An-

das den Ausbau von leistungsstarken SIEM- und SOAR-Systemen, damit Verdachtsfälle nicht mehr überwiegend manuell geprüft und priorisiert werden müssen.

Der Sprung zum optimistischen Szenario setzt einen hohen Koordinationsgrad voraus, wie ihn der ENISA-NIS360-Bericht beschreibt, eine

sektorübergreifende Zusammenarbeit, die über Informationsaustausch hinausgeht und gemeinsame Reaktionsprozesse einschließt.^[13] Im Drei-Säulen-Modell des BSI müsste der Analyseverbund über reine Informationssammlung hinausgehen und belastbare Handlungsempfehlungen ableiten.^[13]

Daraus ergibt sich eine klare Reihenfolge. Zunächst die Datenbasis vereinheitlichen, darauf aufbauend Sensorik und Automatisierung ausbauen, mittelfristig einen vollständigen Analyseverbund etablieren, an dem auch große Unternehmen verbindlich teilnehmen. Ohne die Beteiligung großer Unternehmen bliebe das gemeinsame Lagebild unvollständig, auch wenn ihr eigener Schutzgewinn vergleichsweise gering ausfällt. Aber auch die aktive und flächendeckende Teilnahme der Provider spielt für die effektive Wirkung eine wichtige Rolle.

Ein wachsender Teil der Risiken ergibt sich aus Lieferketten- und Dienstleisterabhängigkeiten, der Anteil von Sicherheitsvorfällen mit Beteiligung Dritter hat sich zwischen 2024 und 2025 laut Verizon etwa verdoppelt.^[14]

STAND DER UMSETZUNG IN DEUTSCHLAND

Konkrete Pläne wurden im Sicherheitspakt^[15] nicht genannt. Das BSI hat das Vorhaben inzwischen in drei Säulen konkretisiert: erweiterte Sensorik, ein zentraler Analyseverbund und ein offenes Ökosystem mit normierten Schnittstellen.^[13] Seit März 2026 vernetzt das BSI gemeinsam mit der Genossenschaft Govdigital Security Operations Center öffentlicher IT-Dienstleister aus zehn Bundesländern. BSI-Präsidentin Claudia Plattner formulierte dazu das Ziel einer „Industrialisierung der Cybersicherheit“.

Da die drei Szenarien auf Annahmen und nicht auf Messwerten beruhen, stellt sich die Frage, woran sich künftig ablesen lässt, welchem Szenario sich ein realer Cyberdome tatsächlich annähert. Vier Indikatoren bieten sich an: der Anteil automatisiert priorisierter Verdachtsfälle in den SOAR-Systemen, die durchschnittliche Erkennungs- und Reaktionszeit, die Anzahl der an das BSI-Sensorik-Netzwerk angebundenen Organisationen sowie der Anteil maschinenlesbarer Bedrohungsindikatoren.^[16]

Offen bleibt zudem, ab welcher Beteiligungsquote ein Cyberdome seine volle Wirkung ent-

faltet. Da IT-Sicherheitsmaßnahmen anderen Organisationen zugutekommen, ohne dass die investierende Organisation den vollen Nutzen internalisiert, besteht ein struktureller Anreiz zum Trittbrettfahren.^[16] Ein Cyberdome müsste diesem Risiko durch geeignete Teilnehmanreize begegnen, etwa durch die verbindliche Anbindung von Sensoren statt bloßer nachträglicher Meldepflichten, sonst bleiben die hier modellierten Abwehrkosten reine Annahmen, die sich in der Praxis nicht einstellen.

FAZIT

Selbst unter konservativen Annahmen übersteigt der potenzielle Nutzen eines Cyberdomes die diskutierten Investitionskosten um ein Vielfaches, und das schon bei einer einmaligen Investition ohne Berücksichtigung laufender Betriebskosten. Aus staatlicher Sicht kommt hinzu, dass jeder vermiedene Euro unmittelbar der gesamtwirtschaftlichen Wertschöpfung zugutekommt, einem Anteil von rund 4,5 Prozent des deutschen Bruttoinlandsprodukts.

Der Mehrwert entsteht dabei weniger durch einzelne IT-Sicherheitstechnologien als durch organisationsübergreifende Koordination. Davon profitiert gerade der Mittelstand, allerdings nicht durch eigene technische Aufrüstung, sondern über vorgelagerte Infrastrukturanbieter.

Entscheidend ist die richtige Reihenfolge: zunächst einheitliche Datenformate und Automatisierung, dann ein vollständiger Analyseverbund unter Einbindung aller Unternehmensgrößen. Belastbare Daten zur tatsächlichen Abwehrleistung fehlen bislang. Die verwendeten Szenarien sind plausible Annahmen, keine Prognosen. Ausschlaggebend wird sein, ob die politischen und institutionellen Weichen dafür gestellt werden. ■

Literatur

- ^[13] Bitkom e. V. (2025), Wirtschaftsschutz 2025, www.bitkom.org
- ^[14] BSI (2025), Die Lage der IT-Sicherheit in Deutschland 2025, www.bsi.bund.de
- ^[15] BMI (2026), Zusammenarbeit zur Cybersicherheit mit Israel wird vertieft
- ^[16] Pohlmann, N. (2026), Cyberdome, Glossar Cyber-Sicherheit, <https://norbert-pohlmann.com/glossar-cyber-sicherheit/cyberdome/>
- ^[17] Schulmann, H. und Waidner, M. (2026), Israels Cyber Dome ist kein Iron Dome, FAZ
- ^[18] Pohlmann, N. (2022), Return on Security Investment (RoSI), Glossar Cyber-Sicherheit, <https://norbert-pohlmann.com/glossar-cyber-sicherheit/return-on-security-investment-rosi/>

^[13] IBM Security und Ponemon Institute (2025), Cost of a Data Breach Report 2025

^[14] Jin, B. u. a. (2024), Sharing cyber threat intelligence, NDSS Symposium 2024

^[15] ENISA (2026), ENISA NIS360 2026, www.enisa.europa.eu

^[16] Statistisches Bundesamt (2026), Wichtige gesamtwirtschaftliche Größen, www.destatis.de

^[17] Deutsche Telekom (2026), Automatischer Schutz vor Cybercrime auch für Business Festnetz

^[18] Bitkom e.V. (2026), Bitkom-Dataverse: Wirtschaftsschutz

^[19] BSI (2026), Cyberdome, www.bsi.bund.de

^[20] Verizon (2025), 2025 Data Breach Investigations Report

^[21] IBM (2021), Was ist ein Security Operations Center (SOC)?, www.ibm.com

^[22] Dykstra, J. und Yurcik, W. (2026), Applying Public Health Systematic Approaches to Cybersecurity: The Economics of Collective Defense, arXiv:2602.13869

^[23] Institut für Mittelstandsforschung Bonn (2023), Sonderauswertungen des Statistischen Bundesamtes zum Unternehmensbestand und zu abhängig Beschäftigten nach Beschäftigtengrößenklassen, www.ifm-bonn.org



LAURA ZIMMERMANN

studiert den Master Informatik an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums auch mit dem Thema „Return on Security Investment-Analyse des Cyberdomes für Deutschland“.



NORBERT POHLMANN

ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrust und im Vorstand des Internetverbandes – eco.