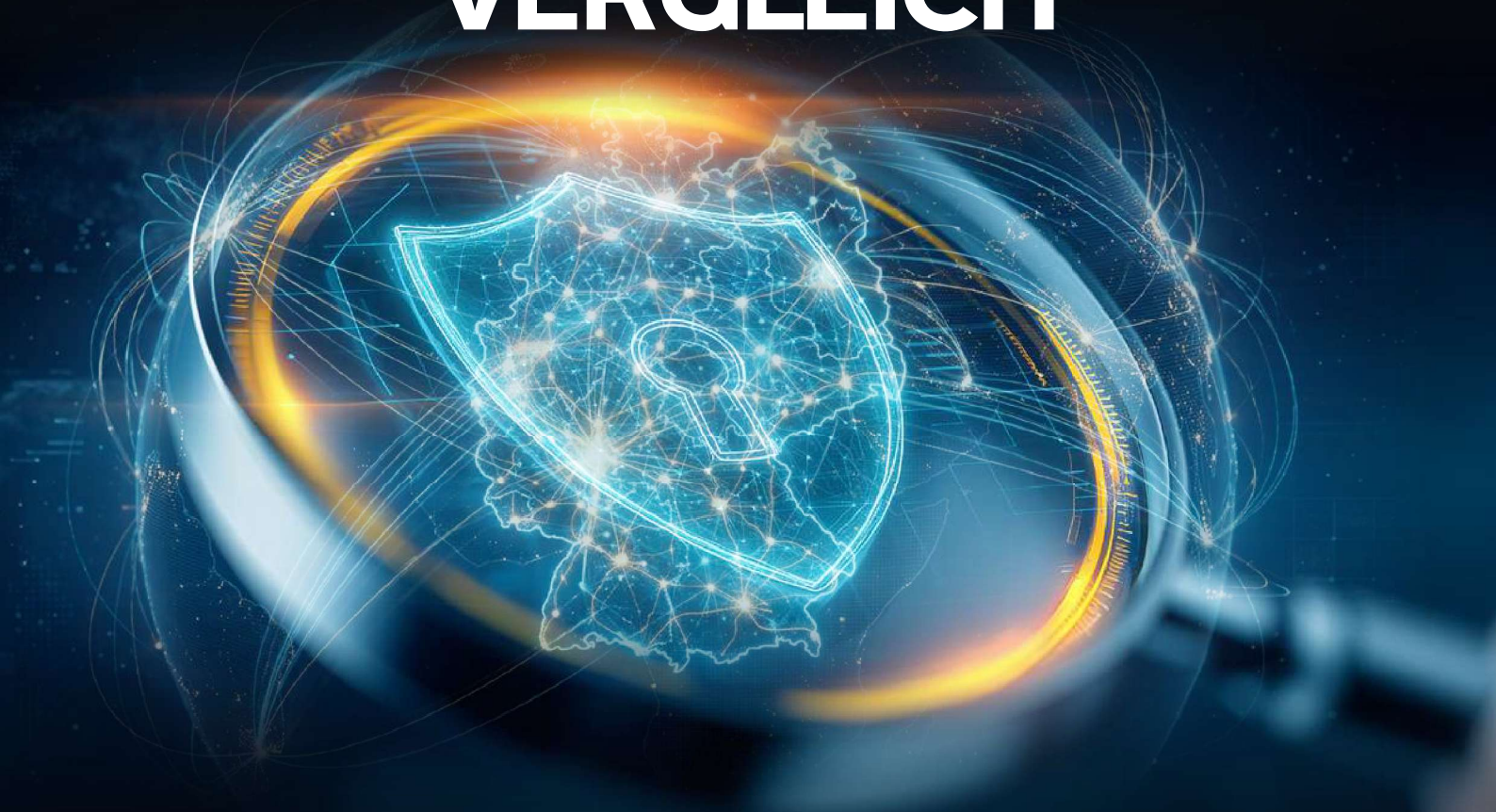
Ein Drittel aller öffentlich erreichbaren IT-Systeme weist Schwachstellen auf

# DIE LAGE DER CYBERSICHERHEIT IN DEUTSCHLAND IM INTERNATIONALEN VERGLEICH



Eine Analyse von über 15 Millionen öffentlich erreichbaren IT-Systemen in 195 Ländern zeigt: Deutschland liegt beim Schutz seiner IT-Infrastruktur im besseren Drittel, doch jedes dritte erfasste System trägt mindestens eine Schwachstelle. Bei Betreibern kritischer Infrastrukturen ist die Lage teils deutlich schlechter – und rund jedes fünfte deutsche IT-Asset wird auf US-Infrastruktur betrieben.

Weltweit sind mehr als 347.000 Schwachstellen dokumentiert[1], von denen rund 1.700 nachweislich aktiv ausgenutzt werden[2] und Millionen IT-Systeme betreffen. Die Bedrohung wächst zudem weiter, beschleunigt durch den Einsatz von KI. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verzeichnet inzwischen 119 neue Schwachstellen pro Tag – ein Viertel mehr als im Vorjahr und drei Viertel mehr als noch 2022.[3] Die Angriffsfläche von Organisationen wächst damit schneller, als sie sich absichern lässt. Für einen erfolgreichen Angriff braucht es dabei selten ausgefeilte Methoden. Als Einstieg genügt häufig ein einziges IT-System, das ohnehin aus dem Internet erreichbar ist, etwa ein veraltetes Content-Management-System, eine offen zugängliche Datenbank oder ein exponiertes Administrations-Panel.

Wie schwer die Folgen sein können, zeigte der Angriff auf die Südwestfalen IT im Oktober 2023. Die Gruppe Akira gelangte über einen aus dem Netz erreichbaren VPN-Zugang ohne Mehr-Faktor-Authentisierung in das Netz des kommunalen Dienstleisters. Betroffen waren in der Folge über 70 Kommunen. Bürgerbüros, Kfz-Zulassung und Meldewesen standen wochenlang still, Steuern und Gebühren ließen sich nicht einziehen. Ein einzelnes exponiertes IT-System im Internet reichte, um die Verwaltung einer ganzen Region lahmzulegen.

Von außen erreichbare IT-Systeme sind damit der Teil der IT-Infrastruktur, der die größte Aufmerksamkeit verlangt. Für Angreifer sind sie zugleich der erste Ansatzpunkt, weil sie den direkten Erstkontakt mit dem Ziel ermöglichen. Genau diese Außensicht nimmt die folgende Auswertung ein: Sie stützt sich allein auf öffentlich verfügbare Informationen und bewertet IT-Systeme so, wie sie auch einem Angreifer offenstehen.

## WAS DIE ANALYSE MISST

Datenbasis dieses Beitrags ist die Threat-Intelligence-Plattform der SecuSeek GmbH.[4] Die dort eingesetzten Prüfverfahren stammen aus der Forschung zur internetweiten Sicherheitsmessung, entstanden in Zusammenarbeit mit dem Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule sowie mit Wissenschaftlern der Stanford University, der UC Davis und der Washington University in St. Louis.


*Abbildung 1: Datenbasis der Auswertung*

Untersucht werden die tatsächlich eingesetzten IT-Systeme und Anwendungen, etwa Web- und Mailserver, VPN-Zugänge, Datenbanken und die dahinterliegende Server- und DNS-Infrastruktur. Im Zentrum steht die Frage, ob ein IT-System bekannte Schwachstellen aufweist, wie schwer diese wiegen und ob sie bereits aktiv ausgenutzt werden. Dafür werden die eingesetzten Technologien samt Versionsstand mit den etablierten Kennungen CVE, CWE und CVSS abgeglichen. Darüber hinaus erfasst die Plattform Fehlkonfigurationen, aus dem Netz exponierte Dienste und Ports, eine unzureichend abgesicherte Mail- und DNS-Infrastruktur sowie öffentlich auffindbare Zugangsdaten. Aus den Einzelbefunden berechnet sie zusätzlich einen zusammenfassenden Resilienzwert je Ziel.

Erfasst sind auf diese Weise mehr als 250 Millionen IT-Assets. Jeder Fund wird einem Zielsystem, einer Region und, soweit die Daten es zulassen, einer Organisation zugeordnet. Für diesen Beitrag ausgewertet wurden über 15 Millionen der wichtigsten öffentlich erreichbaren IT-Systeme weltweit, darunter rund 600.000 in Deutschland, aggregiert auf Länder, Sektoren und Bundesländer.

## DEUTSCHLAND IM BESSEREN DRITTEL

Um die Lage vergleichbar zu machen, verdichtet die Plattform die Schwachstellenfunde eines Landes zu einer Risikodichte. Sie beschreibt, wie verbreitet angreifbare IT-Systeme in einem Land sind, und gibt an, welcher Anteil der erfassten IT-Assets Schwachstellen aufweist. Daneben weist sie den Anteil mit Schwachstellen hoher Schwere aus und den Anteil, der von aktiv ausgenutzten Schwachstellen betroffen ist.

Am oberen Ende der Skala stehen osteuropäische und asiatische Staaten. Belarus führt mit einer Risikodichte von 72 Prozent, gefolgt von Russland mit 71 und Südkorea mit 67 Prozent. Deutschland liegt mit 34 Prozent im besseren Drittel der 195 ausgewerteten Länder; rund 140 Länder weisen eine höhere Risikodichte auf. Gut ein Drittel der öffentlich erreichbaren Assets trägt damit mindestens eine Schwachstelle. Abbildung 2 zeigt die weltweite Risikodichte, mit Deutschland hervorgehoben.

Innerhalb Europas gehört Deutschland zum besseren, aber nicht zum führenden Feld. Sicherer aufgestellt sind mehrere andere europäische

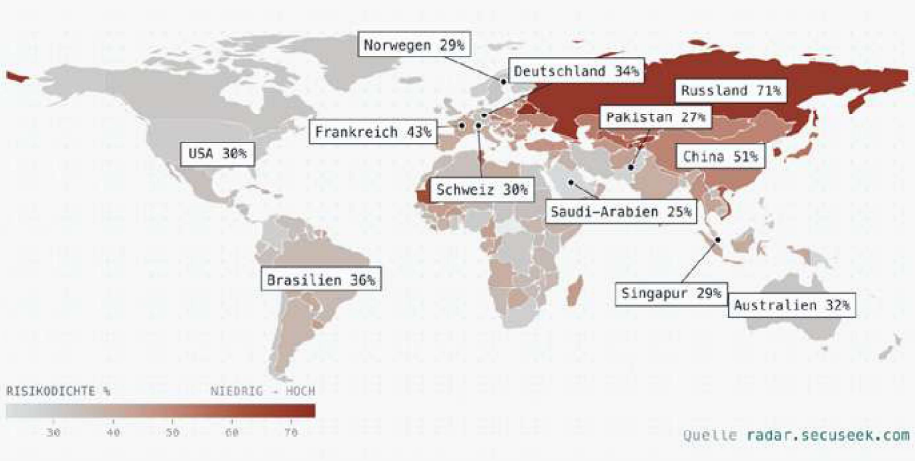



*Abbildung 2: Risikodichte je Land, niedriger ist besser*

Staaten, darunter Finnland (29 %), die Schweiz (30 %), Schweden (32 %) sowie Dänemark und Irland (je 33 %). Höhere und damit schlechtere Werte weisen die Niederlande (37 %), Italien und Spanien (je 40 %), Frankreich (43 %) und Polen (47 %) auf. Unter den 27 EU-Staaten rangiert Deutschland damit etwa auf Rang sieben, klar sicherer als die großen Nachbarn Frankreich und Polen. Bemerkenswert sind die USA: Sie führen mit über 1,5 Millionen erfassten Assets den mit Abstand größten Bestand und liegen mit 30 Prozent dennoch niedriger als Deutschland. Das zeigt, dass hier noch Verbesserungspotenzial vorhanden ist.

Der Anteil hoch-schwerer Schwachstellen trennt die Länder deutlicher als der Gesamtwert. Deutschland liegt hier mit 7 Prozent niedrig, ähnlich wie das Vereinigte Königreich (5 %) und die USA (4 %). Innerhalb der EU fällt der Wert bei den großen Staaten höher aus, bei Spanien (10 %), Italien (11 %), den Niederlanden (12 %), Frankreich (14 %) und Polen (16 %). Russland erreicht 18 Prozent. Ein hoher Gesamtwert und viele schwere Lücken gehen also nicht zwangsläufig zusammen.

## BUNDESLÄNDER: KEIN KLARES OST-WEST-GEFÄLLE

Die Analyse auf Ebene der Bundesländer in Deutschland deckt auf, dass zwischen den einzelnen Ländern deutliche Unterschiede bestehen, von 30 Prozent im Norden bis 40 Prozent in Thüringen (Abbildung 3).

An der Spitze stehen Thüringen mit 40 Prozent und Mecklenburg-Vorpommern mit 39 Prozent.

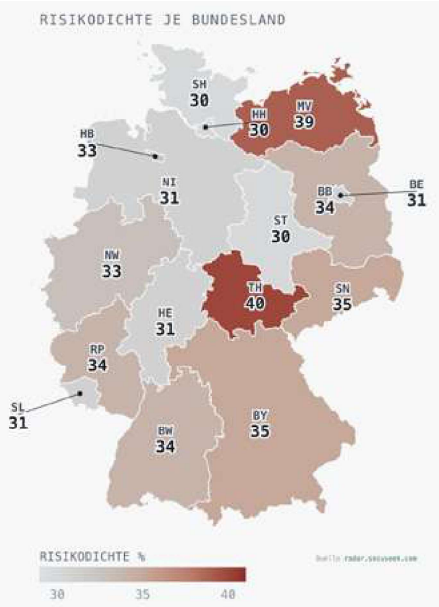



*Abbildung 3: Risikodichte je Bundesland*

Am unteren Ende liegen Schleswig-Holstein, Sachsen-Anhalt und Hamburg mit je 30 Prozent, deren IT-Assets im Schnitt sicherer aufgestellt sind als die in den übrigen Bundesländern.

Ein durchgängiges Ost-West-Gefälle zeigen die Zahlen nicht. Zwar führen mit Thüringen und Mecklenburg-Vorpommern zwei ostdeutsche Länder die Liste an, doch Sachsen-Anhalt und Brandenburg finden sich im unteren Feld, während das westliche Bayern mit 35 Prozent oben mitspielt.

Beim Anteil hoch-schwerer Schwachstellen ergibt sich ein anderes Bild. Hier liegt Nordrhein-Westfalen mit 9 Prozent vorn, gefolgt von Sachsen und Sachsen-Anhalt mit je 8 Prozent. Rheinland-Pfalz, Hessen und Schleswig-Holstein bleiben mit 5 Prozent am niedrigsten.

Aus den regionalen Werten lässt sich damit keine Landkarte der Sicherheit ableiten. Wie hoch die Risikodichte eines Landes ausfällt, hängt weniger am Standort als daran, welche Betreiber mit welcher Software den erfassten Bestand dort prägen. Ein einzelner großer Betreiber mit veralteten IT-Systemen kann den Wert eines Landes bereits spürbar heben. Für die Praxis heißt das, Maßnahmen und Aufsicht dort zu bündeln, wo sich verwundbare Betreiber und veraltete Software häufen, statt entlang der Landesgrenzen.

## KRITIS: FORSCHUNG UND GESUNDHEIT AM STÄRKSTEN BETROFFEN

Äußerst relevant sind – im Sinne der Cybersicherheit – auch die Forschungsergebnisse zu den von NIS-2 erfassten kritischen Organisationen (KRITIS-Betreiber) Deutschlands. Die Plattform verknüpft die gescannten IT-Assets mit den Betreibern aus den aufgeführten Sektoren der Richtlinie. Anders als bei den Länderwerten bezieht sich der Prozentwert hier auf die Betreiber. Als verwundbar gilt ein Betreiber, sobald mindestens eines seiner Assets eine Schwachstelle enthält.

Am stärksten betroffen sind Forschungseinrichtungen und der Gesundheitssektor. Bei den Forschungseinrichtungen weisen 57 Prozent der Betreiber mindestens eine Schwachstelle auf, im Gesundheitssektor sind es 50 Prozent. Bei Ersteren ist zudem gut die Hälfte von einer aktiv ausgenutzten Schwachstelle betroffen. Am Ende steht der Finanzsektor. Im Bankwesen trifft es 10 Prozent der Betreiber, bei den Finanzmarktinfrastrukturen 19 Prozent – beides seit Langem streng regulierte Bereiche.

Der Anteil verwundbarer Betreiber sagt wenig über die Schwere der Funde. Bei den hochschweren Schwachstellen wechselt die Reihenfolge. Vorn liegen Abwasser mit 18 Prozent, Transport mit 16 und Digitale Infrastruktur mit 15 Prozent, obwohl ihr Gesamtanteil im Mittelfeld liegt. Der Gesundheitssektor ist umgekehrt breit betroffen, trägt mit knapp 7 Prozent aber vergleichsweise wenige schwere Lücken.

Eine dritte Größe erfasst die aus dem Netz erreichbaren sensiblen Dienste, etwa offene Fern-


*Abbildung 4: KRITIS-Betreiber nach Sektor. Anteil verwundbarer Betreiber sowie aktiv ausgenutzte und hoch-schwere Schwachstellen*

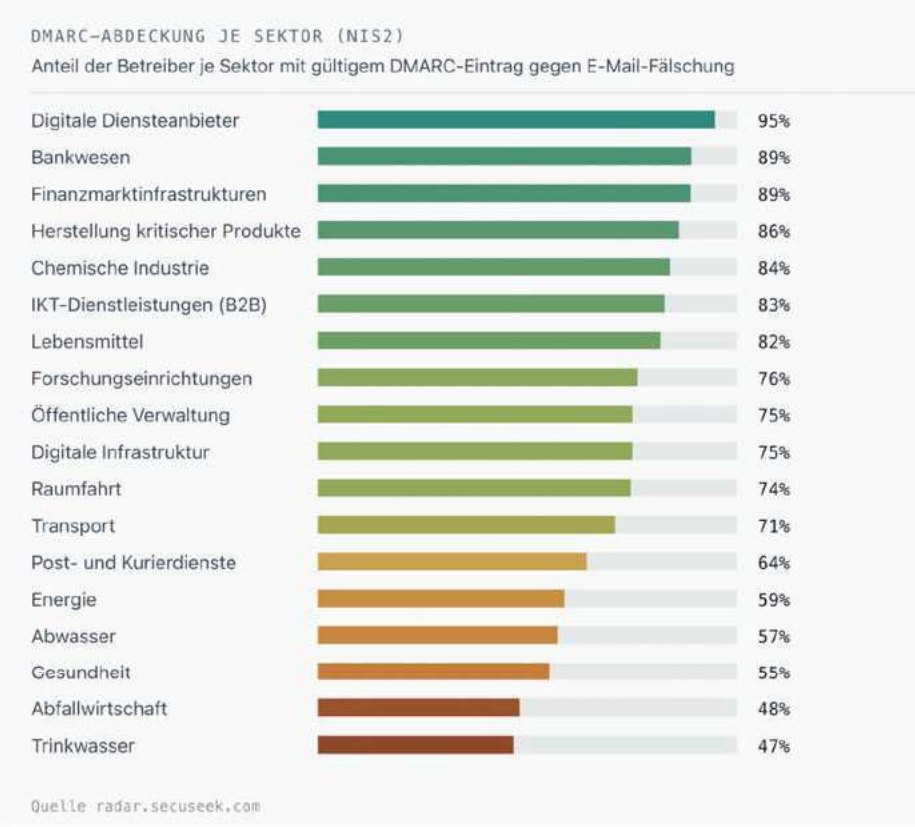



*Abbildung 5: DMARC-Abdeckung je Sektor*

wartungszugänge. Hier verschiebt sich das Feld erneut. Raumfahrt mit 70 Prozent, Herstellung kritischer Produkte mit 69 Prozent und Lebensmittel mit 67 Prozent exponieren die meisten Betreiber, während der Finanzsektor mit rund 30 Prozent am wenigsten Dienste offen ins Netz stellt. Softwarepflege und Erreichbarkeit aus dem Netz sind damit zwei verschiedene Dinge: Ein Sektor kann seine IT-Systeme aktuell halten und trotzdem viele Zugänge offen im Internet betreiben, oder umgekehrt gut abgeschottet sein und dennoch veraltete Software einsetzen.

## FALLSTUDIE: E-MAIL- UND DNS-ABSICHERUNG

Ein einzelner Kontrollbereich zeigt beispielhaft, wie ungleich der Grundschutz verteilt ist. Neben den Software-Schwachstellen erfasst die Plattform, wie gut die Betreiber ihre Mail- und DNS-Infrastruktur absichern, also die Einträge, über die E-Mail-Versand und die Namensauflösung einer Domain gesteuert werden. Die entsprechenden Einträge im DNS entscheiden mit darüber, ob sich E-Mails im Namen einer Organisation fälschen lassen oder ob Zertifikate unbemerkt für eine Domain ausgestellt werden. Sie kosten wenig und lassen sich ohne Eingriff in laufende IT-Systeme setzen.

Die grundlegenden Schutzeinträge sind weit verbreitet, die weiterführenden dagegen selten. Der SPF-Eintrag, der festlegt, welche Server im Namen einer Domain versenden dürfen, liegt bei durchschnittlich 87 Prozent der Betreiber vor. DMARC, das auf SPF aufbaut und den Umgang mit gefälschten Mails regelt, erreicht 68 Prozent. Die weiterführenden Einträge bleiben die Ausnahme. CAA, das die Ausstellung von Zertifikaten auf benannte Stellen beschränkt, kommt auf 9 Prozent, MTA-STS und TLS-RPT zur Absicherung des Mailtransports auf je rund 8 Prozent.

Wie stark der Schutz zwischen den Sektoren auseinanderfällt, zeigt Abbildung 5 am Beispiel von DMARC.

Am oberen Ende sichern digitale Diensteanbieter, Banken und Finanzmarktinfrastrukturen ihre Mail-Infrastruktur mit DMARC-Quoten um 90 Prozent ab. Am Ende stehen die Wasserwirtschaft und die Entsorgung. Bei Trinkwasser tragen 68 Prozent einen SPF- und 47 Prozent einen DMARC-Eintrag, bei Abwasser sind es 66 Prozent und 57 Prozent. Gerade die Betreiber

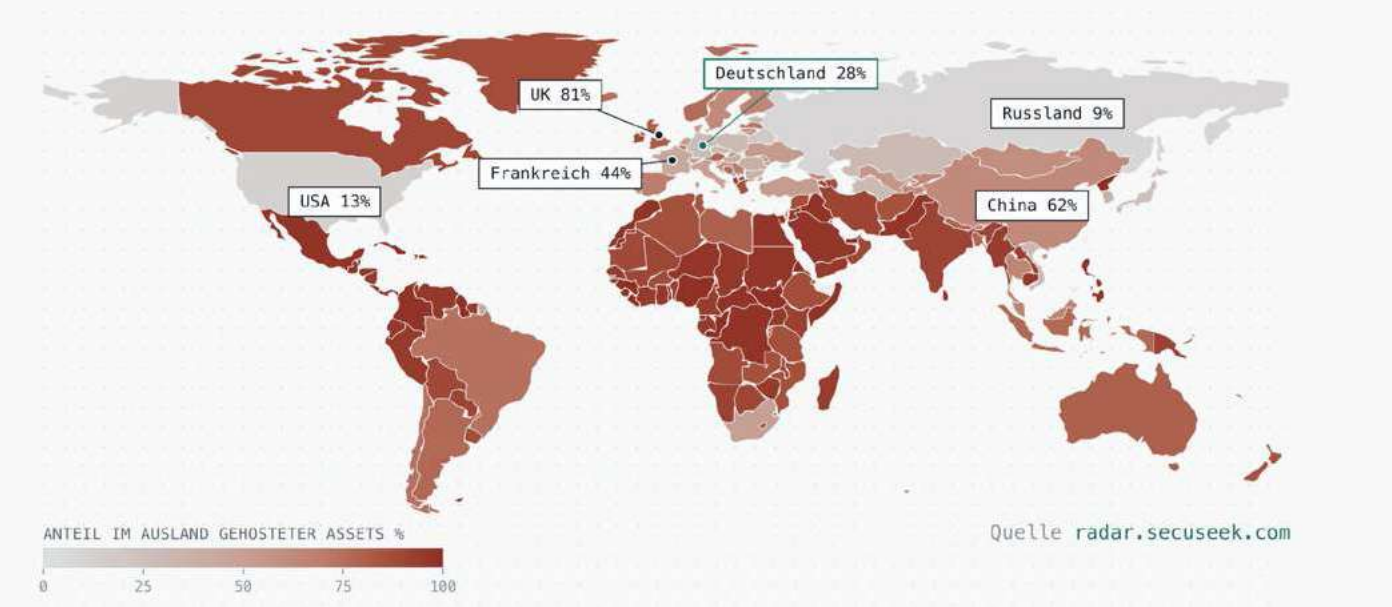



*Abbildung 6: Anteil der im Ausland gehosteten IT-Assets je Land, niedriger bedeutet mehr Hosting im eigenen Land*

der physischen Daseinsvorsorge liegen damit bei einem Schutz zurück, der sich ohne großen Aufwand nachrüsten ließe.

## JEDES FÜNFTE DEUTSCHE IT-ASSET STEHT IN DEN USA

Neben den Auswertungen zu den Bundesländern und den KRITIS-Betreibern bezieht sich die nachfolgende auf den Standort. Sie erfasst, welcher Anteil der IT-Assets eines Betreibers außerhalb Deutschlands gehostet wird. Für den Datenschutz ist das von Belang, da der Serverstandort einen Einfluss auf das anwendbare Recht hat. Daten, die auf US-Infrastruktur gespeichert werden, unterliegen dem CLOUD Act, unabhängig davon, wo das betreibende Unternehmen seinen Sitz hat.

Weltweit zeigt sich eine erhebliche Spannbreite: Es gibt Staaten, in denen nahezu alles im eigenen Land gehostet wird, aber ebenso solche, die fast vollständig auf ausländische Infrastruktur angewiesen sind. Deutschland liegt mit 28 Prozent Auslandsanteil im unteren Bereich (Abbildung 6).

Innerhalb der kritischen Infrastrukturen teilt sich das Feld deutlich. Die physische Daseinsvorsorge bleibt fast vollständig im Inland. Bei Trinkwasser liegen rund 4 Prozent der IT-Assets im Ausland, bei der öffentlichen Verwaltung

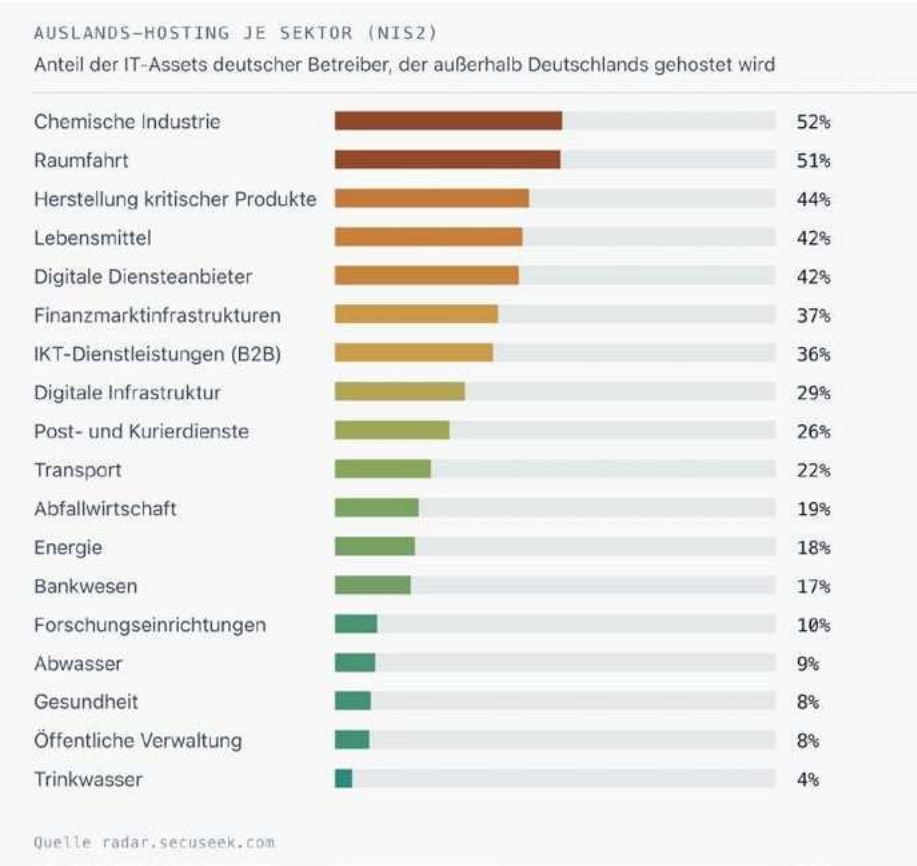



*Abbildung 7: Anteil der IT-Assets deutscher Betreiber je Sektor, der im Ausland gehostet wird*

und im Gesundheitswesen je rund 8 Prozent. Am anderen Ende hosten die chemische Industrie und die Raumfahrt mit je rund 51 Prozent die Hälfte ihrer Assets außerhalb Deutschlands, gefolgt von der Herstellung kritischer Produkte mit rund 44 Prozent.

Über die Sektoren hinaus lässt sich der Anteil der Hosting-Standorte für Deutschland insgesamt beziffern. 72 Prozent der erfassten deutschen Assets liegen im Inland, 28 Prozent im Ausland. Damit steht das Land besser da als die meisten Nachbarn. Frankreich kommt auf 44 Prozent


*Abbildung 8: Auslands-Hosting deutscher IT-Assets nach Zielländern*

Auslands-Hosting, das Vereinigte Königreich auf über 80 Prozent, während die USA mit 13 Prozent fast alles im eigenen Land betreiben.

Von den 28 Prozent deutscher Assets im Ausland liegen 72 Prozent auf US-Infrastruktur, gefolgt von Israel mit 9 Prozent und Belgien mit 4 Prozent (Abbildung 8). Rechnerisch liegt damit rund jedes fünfte erfasste deutsche Asset in den Vereinigten Staaten. Bei Frankreich zeigt sich dasselbe Muster. 54 Prozent des Auslands-Hostings entfallen auf die USA, 14 Prozent auf Deutschland.

Die Zahlen relativieren die Vorstellung einer europäischen Hosting-Autonomie. Selbst Länder mit hohem Eigenanteil verlagern den Auslandsteil fast durchweg über den Atlantik. Für Betreiber kritischer Infrastruktur berührt das zwei Regelwerke zugleich, die Lieferkettenanforderungen der NIS-2-Richtlinie und die datenschutzrechtlichen Vorgaben nach der Datenschutz-Grundverordnung (DSGVO) und Schrems-II-Rechtsprechung.

## HANDLUNGS-EMPFEHLUNGEN

Aus den Befunden ergeben sich drei Maßnahmen:

- **Die eigene Angriffsfläche erfassen.** Wer seine aus dem Internet erreichbaren IT-Systeme nicht vollständig kennt, kann sie nicht absichern. Vergessene Subdomains, Testinstanzen und alte Administrationszugänge tauchen regelmäßig als Einfallstor auf. Grundlage ist ein vollständiges, aktuelles Inventar der extern erreichbaren Assets, zugleich Voraussetzung für die von NIS-2 geforderte Risikoanalyse.
- **Nur das Nötige öffentlich zugänglich machen.** IT-Systeme, die nicht zwingend aus dem Internet erreichbar sein müssen, gehören nicht ins offene Netz. Fernwartungszugänge, Datenbanken und Administrations-Panels lassen sich hinter ein VPN oder eine Zugriffskontrolle legen. Das Schließen nicht benötigter Dienste senkt die Angriffsfläche unmittelbar.
- **Kontinuierlich überwachen und Maßnahmen ableiten.** Die Angriffsfläche verändert sich täglich, ebenso die Lage bei aktiv ausgenutzten Schwachstellen. Ein Monitoring, das den eigenen Bestand laufend prüft, Funde nach realer Ausnutzung priorisiert, etwa anhand der CISA-KEV-Liste oder der Warnungen des BSI, und daraus konkrete Maßnahmen ableitet, greift, bevor eine Lücke ausgenutzt wird.

## FAZIT

Der externe Blick auf die deutsche IT-Landschaft zeichnet ein geteiltes Bild. Im internationalen Vergleich liegt Deutschland im besseren Drittel von 195 ausgewerteten Ländern, auf einer Höhe mit dem Vereinigten Königreich, vor Frankreich, Polen und Russland, aber hinter den USA. Ein guter Zustand ist das nicht: Auch in Deutschland hat rund ein Drittel der öffentlich erreichbaren IT-Assets mindestens eine Schwachstelle.

Innerhalb der kritischen Infrastrukturen endet dieser Vorsprung dort, wo es auf Grundlagen ankommt. Das stark regulierte Bankwesen sichert seine IT-Systeme durchgängig ab, während die Wasser- und Entsorgungswirtschaft bei Schutzmaßnahmen für Mail und DNS zurückliegt. Selbst Vorkehrungen mit geringem Aufwand bleiben dort aus.

Über die Sektoren hinweg fällt der Befund deutlich ungünstiger aus, als der Länderwert vermuten lässt. Die KRITIS-Betreiber liegen im Schnitt über dem allgemeinen Niveau: Bei Forschungseinrichtungen und im Gesundheitswesen trägt rund jeder zweite Betreiber mindestens eine Schwachstelle, ein erheblicher Teil davon bereits aktiv ausgenutzte Lücken. Gerade die Organisationen, deren Ausfall die größten Folgen hätte, sind damit überdurchschnittlich betroffen.

Die digitale Souveränität hält der Prüfung nur teilweise stand. Deutschland hostet mehr im eigenen Land als seine Nachbarn, doch von dem, was ins Ausland geht, liegt fast drei Viertel in den USA. ■

***Literatur***

[1] *National Institute of Standards and Technology (NIST): National Vulnerability Database (NVD). nvd.nist.gov (Stand: Juli 2026)*

[2] *Cybersecurity and Infrastructure Security Agency (CISA): Known Exploited Vulnerabilities Catalog. cisa.gov (Stand: Juli 2026)*

[3] *Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2025, Kapitel „Neue Schwachstellen" (Berichtszeitraum Juli 2024 bis Juni 2025). bsi.bund.de*

[4] *SecuSeek GmbH: Threat-Intelligence-Plattform. secuseek.com*

**DR. NURULLAH DEMIR**
ist Gründer und Geschäftsführer der SecuSeek GmbH. Er hat im Bereich Cybersicherheit promoviert. Er forscht seit über zehn Jahren zu systemrelevanten Risiken im Internet.

**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.