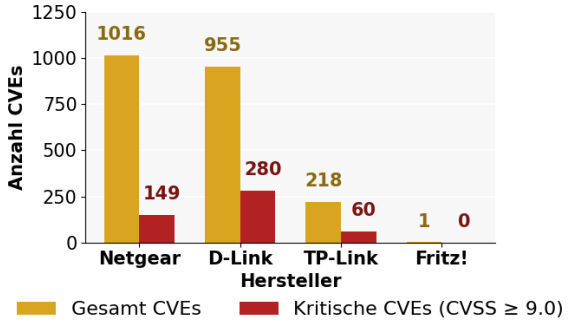
GESELLSCHAFT
FÜR INFORMATIK

POLICY BRIEF // № 6
September 2026

Router-Sicherheit und digitale Souveränität

Niklas Sax[1], Dr. Monina Schwarz[2], Marieke Petersen[1], Eva Mattes[1], Nikolas Becker[1]

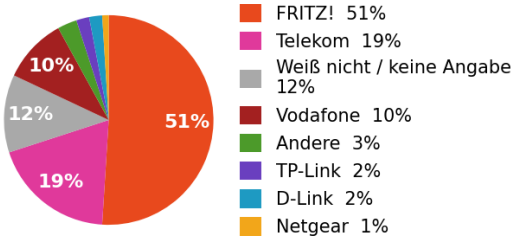
Router sind zentrale Komponenten der Netzwerkinfrastruktur. Ihre exponierte Position und zentrale Funktion machen insbesondere Heimnetzrouter zu beliebten Zielen für Cyberkriminalität. Schwachstellen in der Firmware sind ein zunehmend probates Mittel, über die Angreifer Zugriff erhalten können. Die Schwachstellenanalyse einer GI-Studie zeigt, dass die Bedrohungslage stark herstellerabhängig ist. Auffällig ist eine starke Häufung gemeldeter Schwachstellen bei außereuropäischen Herstellern. Insbesondere beim Blick auf „kritisch“ eingestufte Schwachstellen fällt FRITZ! als einziger deutscher Hersteller positiv auf.



Grafik 1: Gesamt-CVEs vs. Kritische CVEs führender Hersteller, (2020-2025). Eigene Darstellung aus Sax et al. 2026, 20

Ob Schwachstellen auf Fahrlässigkeit oder bewusst eingebaute Fehler zurückgehen, ist von außen nicht gänzlich unterscheidbar. Ein Umstand, der die Debatte um Backdoors und „Kill-Switch“-Funktionen bei Produkten aus nicht vertrauenswürdigen Ländern verschärft.

Mit 51 Prozent entfällt über die Hälfte des deutschen Routermarktes auf FRITZ! als inländischen Hersteller. Die außereuropäischen Anbieter wie TP-Link, D-Link und Netgear kommen zusammen auf lediglich fünf Prozent. Diese Verteilung ist im internationalen Vergleich ungewöhnlich souverän.



Grafik 2: Marktanteil Routerhersteller in Deutschland. Eigene Darstellung nach Daten aus Statista 2025c

[1] Gesellschaft für Informatik – Geschäftsstelle Politik und Wissenschaft
[2] Gesellschaft für Informatik – Sprecherin Fachgruppe Netzwerksicherheit

→

Aktives Preisdumping chinesischer Produkte am europäischen Markt erzeugt jedoch Handlungsbedarf. Das Beispiel der USA zeigt, wie schnell sich Marktverhältnisse verschieben können. Der Marktanteil im Bereich der Small Office/Home Office Router von TP-Link wuchs in den USA innerhalb von fünf Jahren von rund 10 Prozent auf über 60 Prozent. Seit April 2025 untersucht daher das US-Justizministerium, ob dahinter systematische Niedrigpreise standen. Parallel häuften sich staatlichen Akteuren zugerechnete Cyberangriffe über kompromittierte Router. Seit März 2026 erhalten neue, im Ausland produzierte Consumer-Router keine Zulassung der amerikanischen Zulassungsbehörde FCC mehr. Ein einzelner Produktionsschritt im Ausland genügt. Da kaum ein Anbieter die Anforderungen erfüllen kann, entscheidet faktisch ein behördliches Ausnahmeverfahren über den Marktzugang. Bisher wurden so 17 Freigaben erteilt. Aus dem Herkunftsverbot ist so ein Zertifizierungsprozess mit erheblicher Ermessensmacht geworden. Die Lehre für Europa liegt nicht in dessen Nachahmung, sondern in der rechtzeitigen Prävention.

> **Preisdumping erzeugt Handlungsbedarf. Die Lehre für Europa liegt jedoch nicht in der Nachahmung der USA, sondern in der rechtzeitigen Prävention.**

Verbraucher*innen sollte es möglich sein, beim Kauf und der Verwendung von Heimnetzroutern einfach einen Überblick über Faktoren wie Preis und Kompatibilität aber auch Langlebigkeit und Sicherheit eines Produkts zu erhalten. Sie müssen befähigt werden, relevante Sicherheitseinstellungen zu verstehen und eigenständig einzustellen. Hersteller wiederum müssen ihre Produkte so entwickeln, dass mögliche Fehlerquellen reduziert werden und Router zuverlässig mit Updates versorgt werden können. Dabei sollten die Produkte auf eine möglichst lange Lebenszeit ausgelegt entwickelt werden. Gesetzliche Vorgaben sollten nicht nur über oberflächliche Parameter entscheiden, sondern müssen konsequent über den Lebenszyklus hinweg und über alle Funktionen und Komponenten zusammen gedacht, entwickelt und umgesetzt werden. Ergebnis darf nicht die Schaffung zusätzlicher Dokumentationspflichten ohne Nutzen sein, sondern sollte schlüssige Vorgaben liefern, die Herstellern klare Wege aufzeigen um die Cybersicherheit nachhaltig zu verbessern.

Handlungsempfehlungen

→ *Gestaffelte Sicherheitsanforderungen etablieren*

Der aktuelle Regulierungsrahmen für Router behandelt alle Router weitgehend gleich, obwohl die Risiken je nach Kontext stark variieren. Dies sollte sich in einer differenzierten Sicherheitsarchitektur mit gestuften Anforderungen widerspiegeln: Während für Heimnetzrouter grundlegende Sicherheitsstandards wie die BSI TR-03148 ausreichend sein können, sollten beispielsweise für Unternehmensrouter strengere Prüfkriterien gelten. Für Router in KRITIS-Kontexten sollten höchste Sicherheitsanforderungen gelten, wie verpflichtende Penetrationstests, formale Verifikation sicherheitskritischer Komponenten und strenge Herstellerprüfungen. Federführung und Prüfung sollten beim BSI liegen, das mit TR-03148 und dem IT-Sicherheitskennzeichen bereits über die nötigen Instrumente verfügt und dessen Zuständigkeiten der Cyber Resilience Act/Cybersecurity Act 2 weiter bündelt.

→ *CSA2-Logik auf den Endgerätemarkt übertragen*

Der Cybersecurity Act 2 ermöglicht erstmals, nicht-technische Risiken in IKT-Lieferketten systematisch zu bewerten und Komponenten hochriskanter Lieferanten auszuschließen. Er zielt auf KRITIS und Telekommunikationsnetze; Heimnetzrouter fallen nicht darunter und sollten es angesichts ihres Einsatzkontextes auch nicht. In andere sicherheitsrelevante Netzwerke, beispielsweise im Unternehmenskontext, können sie dennoch als Einfallstor dienen. EU und Bundesregierung sollten daher prüfen, welche Elemente der CSA2-Logik sich auf den Endgerätemarkt übertragen lassen, etwa die Bewertung nicht-technischer Risiken und die Möglichkeit, bei wiederholt nicht behobenen Sicherheitsmängeln regulatorisch einzugreifen.

→ *Transparenz über Lieferketten gewährleisten*

Sicherheit lässt sich nur bewerten, wenn nachvollziehbar ist, woher ein Gerät und seine Komponenten stammen. Internetanbieter sollten daher verpflichtet werden, die Herstellerherkunft ihrer White Label Produkte offenzulegen. Bei kritischen Komponenten sollte die Product Bill of Material (PBOM), also das Verzeichnis aller Hardware- und Softwarekomponenten nicht nur auf Anforderung, sondern öffentlich verfügbar sein. Das ermöglicht unabhängige Prüfung und beschleunigt die Zuordnung neu bekanntwerdender Schwachstellen.

→

→ *Marktmonitoring durch die BNetzA einführen*

Die souveräne Marktposition einheimischer Produkte ist keine Selbstverständlichkeit. Wo der Preis das entscheidende Kaufkriterium ist, können sich Marktanteile schnell verschieben. Die Bundesnetzagentur (BNetzA) sollte daher als Marktüberwachungsbehörde ein regelmäßiges Monitoring der Herstelleranteile im Endgerätemarkt übernehmen und Schwellenwerte definieren, ab denen Abhängigkeiten sicherheitspolitisch kritisch werden. So entsteht eine Frühwarnfunktion, bevor Konzentrationen erreicht werden, die sich nachträglich schwer korrigieren lassen.

→ *Security-by-Design konsequent umsetzen*

Sicherheit muss bei Herstellern von Beginn an ein integraler Bestandteil der Entwicklung sein, da Sicherheit im Nachhinein nur mit sehr hohem Aufwand lückenlos in ein Produkt eingebracht werden kann. Aus bekannten Angriffsmustern lassen sich konkrete Sicherheitsprobleme ableiten, auf die getestet werden kann. Sicherheitsexpert*innen sollten früh in die Entwicklung eingebunden werden, um mit einer Veto-Funktion die Weiterentwicklung fehlerhafter Produkte zu unterbinden. Regelmäßige externe Audits decken blinde Flecken auf.

→ *Bewusstsein für Router als Sicherheitsgerät schaffen*

Router sind sicherheitskritisch für alle angeschlossenen Geräte und müssen regelmäßig gewartet werden. Verbraucher*innen sollten bestärkt und ermächtigt werden, zentrale Schutzmaßnahmen umzusetzen: voreingestellte Passwörter sofort ändern, WPS deaktivieren, Fernzugriff restriktiv handhaben und nicht benötigte Dienste abschalten. Auto-Updates sollten standardmäßig aktiviert sein.

Mehr zum Thema

→ **GI-STUDIE** zur Lage der Router-Sicherheit in Deutschland:

Sax et al. (2026) **Router-Sicherheit und digitale Souveränität in Deutschland.** Gesellschaft für Informatik, Berlin.

https://gi.de/fileadmin/GI/Allgemein/PDF/2026-06_GI_Router-Sicherheit_und_digitale_Souveraenitaet.pdf

→ **GI-WHITEPAPER** zum verantwortungsvollen Melden von Sicherheitslücken, einem wichtigen Teil des Schwachstellenmanagements:

Petersen et al. (2026) **Reform des Computerstrafrechts.** Gesellschaft für Informatik, Berlin.

https://gi.de/fileadmin/GI/Hauptseite/Aktuelles/Meldungen_und_Blogbeitraege/2026/2026-08-24_Whitepaper.pdf

LITERATUR

[1] Bundesamt für Sicherheit in der Informationstechnik, „Tipps für ein sicheres Heimnetzwerk," 2026. [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Wegweiser_kompakt_Router_einrichten.pdf?__blob=publicationFile&v=24. [Zugriff am 23.02.2026].

[2] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2024," 2024. [Online]. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5. [Zugriff am 21.08.2026].

[3] Bundesamt für Verfassungsschutz, „Gemeinsamer Warnhinweis: Russischer Cyberangriff auf Internetrouter," 2026. [Online]. https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2026/2026-04-07-joint-cybersecurity-advisory.html. [Zugriff am 13.04.2026].

[4] S. Hill., „Everything You Need to Know About the Foreign-Made Router Ban in the US," Wired, 2026. [Online]. Verfügbar: https://www.wired.com/story/us-government-foreign-made-router-ban-explained/. [Zugriff am 13.04.2026]

[5] Young, M. et al., „European Commission Proposes Cybersecurity Act 2: New EU Supply Chain Rules and Certification Reforms" https://www.globalpolicywatch.com/2026/01/european-commission-proposes-cybersecurity-act-2-new-eu-supply-chain-rules-and-certification-reforms/ [Zugriff am 16.08.2026]

ÜBER DIE GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik.

GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Geschäftsstelle Berlin
Weydingerstraße 14-16
10178 Berlin
Tel: +49 1767 322 404 3

Ansprechpartner:
Nikolas Becker
Bereichsleitung Politik & Wissenschaft

Mail: nikolas.becker@gi.de
Tel: +49 (0)1767 322 404 3
Web: www.gi.de