SWP

SWP-Aktuell

NR. 27 JUNI 2026

Cybersicherheit braucht sichere Software

Wie die Politik Softwarehersteller in die Pflicht nehmen kann und weshalb sie es sollte

Alexandra Paulus

Cybersicherheitsvorfälle verursachen Schäden – etwa, wenn gegnerische Staaten kritische Infrastrukturen lahmlegen oder sensible Daten erbeuten. Viele solcher Vorfälle sind nur deshalb möglich, weil zahlreiche Softwareprodukte bekannte Schwachstellen haben. Softwarehersteller könnten diese schließen, haben jedoch kaum Anreize, in die Sicherheit ihrer Produkte zu investieren. Mit Cybersicherheitspolitik und Schutzmaßnahmen werden bisher vor allem die Symptome unsicherer Software bekämpft, nicht aber die Grundursache, nämlich deren Unsicherheit. Daher besteht politischer Regelungsbedarf – konkret in den Bereichen des Produktsicherheitsrechts, der Produkthaftungsregelungen und der Cybersicherheitsanforderungen für die Anbieter von Software-Dienstleistungen. Die EU hat bereits erste Vorschriften erlassen, allerdings bestehen Regelungslücken und Zweifel an der konsequenten Durchsetzung. Daher sollte sich die Bundesregierung jetzt für eine umfassende europäische Produkthaftungsregelung für Software einsetzen und das Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte Unternehmen, die gegen bestehende Regeln verstoßen, konsequent mit Bußgeldern belegen.

Cybersicherheitsvorfälle verursachen großen Schaden. Im Jahr 2025 kosteten Cyberangriffe deutsche Unternehmen mehr als 200 Milliarden Euro, was 4,5 Prozent des Bruttoinlandsprodukts (BIP) entsprach. Besonders schwerwiegend sind Attacken auf kritische Infrastrukturen: Im Dezember 2025 wurde nur knapp verhindert, dass eine russische Cyberoperation Teile der polnischen Energieinfrastruktur lahmlegte, und im Frühling 2026 wurde bekannt, dass iranische Akteure Angriffe auf Wasserwerke und andere kritische Infrastrukturen in den USA vorbereiten; die Volksrepublik China hatte 2024 ähnliche Operationen gegen US-Ziele durchgeführt. Zudem haben chinesische und russische Akteure über Cyberoperationen westliche Streitkräfte und deren Zulieferer und Dienstleister ausspioniert, sabotiert oder die Verfügbarkeit von Diensten eingeschränkt. Russische Nachrichtendienste nutzen auch regelmäßig Cyberoperationen, um sensible Informationen ziviler Ziele abzugreifen. Und nicht zuletzt bedrohen Cyberkriminelle die deutsche Wirtschaft, besonders den Mittelstand, und die öffentliche Verwaltung. Kurzum: In digitalisierten Gesellschaften ist

Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Cybersicherheit notwendige Bedingung für den Dreiklang aus »Sicherheit, Freiheit und Wohlstand«, den die aktuelle Bundesregierung zum Leitbild ihrer Politik erklärt hat.

Viele Cybersicherheitsvorfälle sind überhaupt erst möglich, weil Softwareprodukte bekannte Schwachstellen enthalten. Eine Hauptursache dafür ist, dass Softwarehersteller aktuell schlicht wenig Anreiz haben, Zeit und Geld zu investieren, um ihre Produkte sicher zu machen. In dieser Hinsicht liegt ein Marktversagen vor.

Cybersicherheitspolitik bekämpft bisher vor allem Symptome

Der Markt für kommerzielle Softwareprodukte unterscheidet sich in einem wesentlichen Punkt von anderen Produktmärkten: Softwarehersteller haben in der Regel keine umfassenden Konsequenzen zu befürchten, wenn ihre Produkte Schäden verursachen. Stattdessen nimmt der Großteil der bis dato eingeführten Regulierung die Betreiber, etwa von kritischen Infrastrukturen, und weitere wichtige Stellen in den Blick. Ebenso setzen viele verbreitete Cybersicherheitsmaßnahmen bei den Anwender:innen an, etwa in der Form von Warnungen, Awareness-Kampagnen oder Trainings.

Tatsächlich können Nutzer:innen und Betreiber dafür sorgen, dass ihre Software auf dem neuesten Stand und sicher konfiguriert ist; außerdem können sie ihre IT-Systeme so aufsetzen, dass Risiken begrenzt werden. Aber gegen unsichere Software können die genannten Maßnahmen wenig ausrichten. Die deutsche und europäische Cybersicherheitspolitik sollte sich daher darauf konzentrieren, kommerzielle Softwarehersteller dazu zu bringen, sichere Produkte zu entwickeln.

Fallbeispiel: Wie unsichere Software für Cybersicherheitsprobleme sorgt

Ein Vorfall zeigt exemplarisch, welche Verantwortung Softwarehersteller für Cybersicherheitsvorfälle tragen — und dass nicht einmal ein Angriff stattfinden muss, um Schaden zu verursachen. Im Juli 2024 veröffentlichte der US-amerikanische Softwarehersteller CrowdStrike ein fehlerhaftes Update für seine Cybersicherheitsanwendung »Falcon«. Das Update wurde automatisch bei allen CrowdStrike-Kund:innen weltweit, die die Windows-Version der Software nutzten, installiert. Da CrowdStrike einen großen Marktanteil hat, waren die Auswirkungen enorm: Die 8,5 Millionen betroffenen Geräte weltweit erlitten einen Systemabsturz, waren vorübergehend nicht mehr funktionsfähig und mussten aufwendig zurückgesetzt werden. Der entstandene Schaden wird auf mehr als 5,4 Milliarden US-Dollar geschätzt.

Der Vorfall war auf eine Verkettung mehrerer Fehler des Softwareherstellers zurückzuführen. An erster Stelle stand ein Programmierfehler. Dass einzelne Entwickler:innen Fehler machen, ist nicht ungewöhnlich, und es kann vorkommen, dass diese Fehler in internen Testläufen nicht auffallen. Dieser Fehler ließ die betroffenen Geräte abstürzen, weil das Programm keine — eigentlich üblichen — Überprüfungsmechanismen enthielt, die den Fehler festgestellt und einen Systemabsturz verhindert hätten. Außerdem wurde das Update allen Kund:innen weltweit gleichzeitig bereitgestellt; gute Praxis wäre jedoch gewesen, das Update nacheinander an einzelne Kund:innen-Segmente auszurollen und dabei zu überprüfen, ob es zu Problemen kommt. Kurzum: Der Softwarehersteller hätte die enormen Schäden für seine Kund:innen mit relativ einfachen Mitteln verhindern können.

Herstellern fehlen Anreize für die Entwicklung sicherer Software

Seit Jahren gehen die meisten entdeckten Software-Schwachstellen auf dieselben, lange bekannten und häufig leicht vermeidbaren Fehler von Softwareherstellern zurück. Dabei liegen hinreichende Erkenntnisse vor, wie Entwicklungsprozesse und Produkte sicher gestaltet werden können, gibt es doch eine Vielzahl praktischer Handreichungen zum Thema. So sollten Hersteller beispielsweise Schwachstellen in Open-Source-Komponenten, die sie in ihre Produkte integrieren, beobachten und bei Bedarf schließen. Dabei können sie heutzutage auf KI-Anwendungen zurückgreifen. Zudem sollten sie nur solche Open-Source-Komponenten integrieren, die aktiv weiterentwickelt werden. Ebenso sollten sie speichersichere Programmiersprachen verwenden, um eine häufige Art von Schwachstellen zu vermeiden.

Warum setzen die Hersteller kommerzieller Software diese guten Praktiken dann nicht einfach um? Das hat vier miteinander verwandte Gründe: Erstens streben Softwarehersteller häufig danach, ihre Produkte möglichst schnell auf den Markt zu bringen. Schwachstellen lassen sich schließlich immer noch durch ein Sicherheitsupdate schließen. Zweitens: Nutzer:innen können die Sicherheit von Softwareprodukten nur schwer beurteilen, da es für Software kein weit verbreitetes IT-Sicherheitskennzeichen gibt. Außerdem spielt bei der Kaufentscheidung von Nutzer:innen — einschließlich Unternehmenskunden — die Sicherheit von Software häufig nur eine geringe Rolle im Vergleich zur Funktionalität und zum Preis. Drittens wirken sich Cybersicherheitsvorfälle langfristig kaum auf die Reputation oder die Börsennotierung von Unternehmen aus. Und viertens haben Hersteller auch keine juristischen oder finanziellen Konsequenzen für unsichere Produkte zu befürchten. An diesem letzten Punkt sollte die Politik ansetzen.

Wie die Politik die richtigen Anreize setzen kann

Aktuell tragen die Kosten für Cybersicherheitsvorfälle, die durch unsichere Software verursacht werden, in der Regel die Anwender:innen. Regulierungsmaßnahmen können jedoch, wie die Verankerung des Verursacherprinzips im Umweltrecht zeigt, dafür sorgen, dass die Hersteller zur Verantwortung gezogen werden. Allerdings können neben den Herstellern auch die Anwender:innen eine Teilverantwortung für Cybersicherheitsvorfälle haben — etwa, wenn sie keine Sicherheitsupdates installiert haben. Nichtsdestotrotz gibt es mehrere regulatorische Ansatzpunkte.

Bisher können Geschädigte bei mangelhafter Software grundsätzlich über das Gewährleistungsrecht Ansprüche geltend machen. Dafür müssen sie jedoch einen Vertrag mit dem Anbieter haben. Bei Cybersicherheitsvorfällen mit hohen Folgeschäden ist allerdings etwa eine Rückerstattung des Kaufpreises nur ein geringer Trost. Für weitergehende Ansprüche muss bisher meistens belegt werden, dass die Software nicht den erforderlichen Sicherheitsanforderungen entsprach und gerade dieser Umstand den Schaden verursacht hat. Doch dieser Nachweis ist in der Praxis oft schwer zu erbringen, weil Sicherheitsvorfälle häufig auf mehrere Faktoren zurückzuführen sind. Ohne weitergehende Vorschriften bestehen also hohe Hürden, um Hersteller für unsichere Software in die Pflicht zu nehmen.

Doch der Politik stehen für dieses Ziel drei Regulierungsmöglichkeiten zur Verfügung. Erstens kann der Gesetzgeber im Produktsicherheitsrecht Anforderungen formulieren, die Hersteller erfüllen müssen, um ihre Produkte überhaupt auf den Markt bringen zu dürfen. Marktaufsichtsbehörden überwachen die Einhaltung der Vorgaben und verhängen bei Verstößen Bußgelder. So soll verhindert werden, dass Hersteller unsichere Produkte überhaupt anbieten.

Das zweite Instrument ist das Produkthaftungsrecht. Entsprechende Regulierung erlaubt es Geschädigten, sofern sich der Schaden aus einem fehlerhaften Produkt er-

gibt, gegenüber dem Hersteller des Produkts Ansprüche wie Schadensersatz geltend zu machen. Produkthaftungsbestimmungen können also nicht nur die rechtliche Grundlage dafür darstellen, individuellen Schaden wiedergutzumachen, sondern auch — da großer finanzieller Schaden droht — für Hersteller Anreize setzen, mehr in die Sicherheit ihrer Produkte zu investieren. Erfahrungen aus der Automobil- und der Pharmabranche zeigen, dass die Einführung von Produkthaftung tendenziell mit sichereren Produkten korreliert. Bei Produkthaftungsrecht braucht es kein Vertragsverhältnis zwischen Hersteller und Geschädigten, und auch Folgeschäden können geltend gemacht werden.

Doch Software-Schwachstellen können nicht nur ausgenutzt werden, wenn die Software erworben und auf eigenen Systemen installiert wird (»On-Premises«). Das Gleiche gilt, wenn sie als Dienstleistung — üblicherweise als Cloud-Lösung — bezogen wird (»Software-as-a-Service«, kurz SaaS). Für solche Nutzungsmodelle greifen das Produkthaftungs- oder Produktsicherheitsrecht häufig nicht. Deshalb kann der Gesetzgeber ergänzend eigenständige Cybersicherheitsanforderungen für diese Anbieter festlegen.

Diese drei Regulierungswege sollte die Bundesregierung nicht im Alleingang beschreiten. Vielmehr sollte sie sich vor allem auf EU-Ebene einbringen, um europäische Regelungen voranzutreiben. Wenn europäische Rechtsakte erlassen werden, ist wieder die Bundespolitik am Zug: EU-Richtlinien sind dann in nationales Recht umzusetzen und EU-Verordnungen häufig von Durchsetzungsgesetzen zu flankieren.

Die besondere Rolle von Open-Source-Software

Open-Source-Software (OSS) bildet das Rückgrat so gut wie aller Softwareprodukte. KI-Anwendungen wie das Sprachmodell Mythos Preview wurden erfolgreich eingesetzt, um Schwachstellen in zahlreichen OSS-Komponenten zu finden. In der vorliegenden Analyse liegt der Fokus auf kommerziellen Softwareherstellern, doch OSS sollte stets mitgedacht werden.

Die Regulierung von nicht-kommerziellen OSS-Entwickler:innen kann unbeabsichtigte Folgen haben. So könnten Hobby-Entwickler:innen aus Angst vor Haftung oder erhöhtem Sicherheitsaufwand ihre Tätigkeit aufgeben. Daher ist hier besondere Vorsicht geboten. Als ein möglicher Ausweg könnten kommerzielle Softwarehersteller, die OSS-Komponenten verwenden, in die Pflicht genommen werden, Schwachstellen darin zu beheben. Ebenso können Regierungen ein Inventar der für sie besonders kritischen OSS-Komponenten erstellen und diese dann zielgerichtet absichern (lassen).

Mehr Pflichten für Hersteller erfordern Güterabwägungen

Die Regulierung von Softwareherstellern bietet Vor- und Nachteile. Erstens ist der dynamische und relativ kostengünstige Software-Sektor die Grundlage moderner digitalisierter Gesellschaften und Volkswirtschaften geworden. Nicht alle, aber einige Maßnahmen, mit denen Hersteller ihre Softwareprodukte sicherer gestalten können, kosten Zeit und Ressourcen; zudem verursachen mögliche Sanktionen oder Haftungsrisiken Kosten. Es ist davon auszugehen, dass Hersteller diese erhöhten Ausgaben an ihre Kund:innen weitergeben würden, so dass die Preise für Software steigen dürften. Dies bedeutete letztendlich, dass sich die Cybersicherheit von Software im Preis niederschlagen würde, denn je unsicherer die Software — also je mehr Aufwand ein Hersteller betreiben müsste, um sein Produkt abzusichern, oder je größere Rückstellungen für Haftungsrisiken gebildet werden müssten — desto teurer das Produkt. Wenn Software insgesamt teurer würde, könnten sich einerseits Domino-Effekte wie Inflation einstellen. Andererseits wäre es zu begrüßen, wenn die Sicherheit von Software die Preisbildung beeinflussen würde, da sich das auf Kaufentscheidungen auswirken dürfte und langfristig das Cybersicherheitsniveau steigen sollte.

Zweitens können zusätzliche Pflichten für kommerzielle Softwarehersteller auch ungewollte Auswirkungen haben. Ein wichtiger Faktor dabei: Der Markt für Softwareprodukte ist stark von US-Unternehmen dominiert — das gilt besonders für Betriebssysteme, Office-Anwendungen, Cybersicherheitsprodukte und KI-Anwendungen. Entsprechend haben US-Hersteller einen entscheidenden Einfluss auf das Cybersicherheitsniveau in Deutschland. Wenn Regelungen im deutschen oder europäischen Alleingang etabliert würden, könnten internationale Anbieter beschließen, ihre Produkte nicht länger auf dem deutschen oder europäischen Markt anzubieten. In der Folge wären diese (mutmaßlich unsichereren) Produkte nicht mehr auf dem europäischen Markt verfügbar.

Auch hier könnte dies einerseits den positiven Nebeneffekt haben, die Stellung derjenigen Anbieter zu verbessern, die die Cybersicherheit ihrer Produkte priorisieren. Andererseits ist Europa im Technologiebereich insgesamt und speziell im Bereich Cybersicherheit stark abhängig von US-amerikanischen Anbietern und es mangelt teilweise an europäischen Alternativen. Wenn sich wichtige US-Softwarehersteller vom EU-Markt zurückzögen, könnte dies — allen Bestrebungen, diese Abhängigkeiten zu reduzieren, zum Trotz — daher zu Unterbrechungen im Betriebsablauf führen. Zudem dürften strengere europäische Regeln für US-Unternehmen die transatlantischen Beziehungen strapazieren.

Drittens widerspräche zusätzliche Regulierung dem aktuellen Zeitgeist in Brüssel, wonach gerade im Digitalbereich eher der Abbau und die Verschlankung bestehender Markteingriffe anzustreben sind.

Viertens treffen Cybersicherheitsauflagen kleine und mittelständische Softwarehersteller — die gerade in Europa eine wichtige Rolle spielen — unverhältnismäßig stärker als große Technologiekonzerne, da erstere weniger Ressourcen für die Umsetzung zur Verfügung haben als letztere. Erleichterungen für kleine und mittlere Unternehmen (KMU) können diesen Effekt abfedern.

Insgesamt erfordern politische Entscheidungen über Pflichten für die Hersteller und Anbieter von Software also eine Güterabwägung zwischen Cybersicherheit auf der einen und Effizienz und Innovationskraft auf der anderen Seite. Die Frage ist, ob die Kosten von Cybersicherheitsvorfällen diese Maßnahme rechtfertigen. Mit Blick auf die Bedrohungslage ist diese Frage zu bejahen.

Bestehende Produktsicherheitsregelungen für Software

In den vergangenen Jahren hat die EU für jede der oben genannten Regulierungsoptionen — Produkthaftung, Produktsicherheitsrecht und Cybersicherheitsanforderungen für Dienstleister — Gesetze verabschiedet. Allerdings weisen sie teilweise Lücken auf und es gibt Anzeichen, dass die Bundesregierung nicht plant, die Regelungen strikt durchzusetzen.

Im Bereich Produktsicherheitsrecht gibt es bisher keine geltende umfassende Regulierung für Software, sondern nur branchenspezifische Vorgaben für Medizinprodukte, In-vitro-Diagnostika, Funkanlagen, Kraftfahrzeuge und Hochrisiko-KI-Systeme. Im Dezember 2027 treten zudem wichtige Vorschriften der neuen EU-Cyberresilienz-Verordnung (Cyber Resilience Act, CRA) in Kraft. Dieses Gesetz formuliert Pflichten für Hersteller von »Produkten mit digitalen Elementen«, also von Software und Produkten mit eingebetteter Software wie etwa Internet-of-Things(IoT)-Geräte. Das entsprechende Durchsetzungsgesetz hat die Bundesregierung bereits auf den Weg gebracht.

Wenn der CRA gilt, werden alle Hersteller, die ihre Produkte auf dem europäischen Markt anbieten möchten, die darin formulierten Cybersicherheitspflichten erfüllen müssen. Konkret werden Hersteller beispielsweise Schwachstellen in ihren Produkten, die aktiv ausgenutzt werden, während der Produktlebensdauer schließen (lassen) müssen. Für viele Produkte können Hersteller selbst bestätigen, dass sie die Vorgaben einhalten. Doch für besonders »wichtige« und »kritische« Produkte wie Firewalls

müssen unabhängige Stellen die Konformität prüfen, bevor das Produkt auf den Markt gebracht werden darf. Bei Verstößen müssen Hersteller Bußgelder zahlen und die Mängel beheben oder ihr Produkt vom Markt nehmen. Außerdem können Kund:innen gegen Hersteller, die gegen den CRA verstoßen, Ansprüche geltend machen.

Allerdings findet die Verordnung keine Anwendung auf Produkte, »die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder verändert werden, oder Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind«, da in dem Bereich keine EU-Kompetenz vorliegt (auf Dual-Use-Produkte ist die Verordnung jedoch anwendbar). In diesem Bereich sind daher entweder Initiativen im Rahmen der Gemeinsamen Sicherheits- und Verteidigungspolitik (GSVP) möglich oder nationale Maßnahmen. Mit Blick auf letztere fordert der CRA die EU-Mitgliedstaaten auf, in diesen Bereichen für ein mindestens ebenso hohes Schutzniveau wie im CRA gefordert zu sorgen. Und tatsächlich gelten für Produkte im Sicherheits- und Verteidigungsbereich häufig bereits hohe Sicherheitsanforderungen, etwa über Beschaffungsrichtlinien oder verpflichtende Zertifizierungen. Diese Vorgaben sind teilweise eingestuft und können hier daher nicht bewertet werden; von ihnen kann allerdings häufig in begründeten Fällen abgewichen werden. Deshalb ist fraglich, ob diese Instrumente geeignet sind, die Sicherheit dieser Produkte insgesamt anzuheben.

Bestehende Produkthaftungsregelungen für Software

Auch wenn der CRA nach seinem Inkrafttreten Ende 2027 entschieden durchgesetzt würde, wäre zu erwarten, dass unsichere Softwareprodukte weiter Schäden verursachen. Dann kann das Produkthaftungsrecht ins Spiel kommen. Dabei sind besondere Güterabwägungen zu treffen: Solche Regelungen tragen zum Schutz von Verbraucher:innen bei, beschneiden aber die unternehmerische Freiheit, wenn Hersteller etwa Haftungskosten und die Versicherbarkeit ihrer Geschäftsmodelle sowie Rückruf- und Prozessrisiken berücksichtigen müssen.

Das aktuell geltende deutsche Produkthaftungsgesetz findet keine Anwendung auf Software. Doch 2024 wurde eine neue Version der EU-Produkthaftungsrichtlinie verabschiedet, die dem deutschen Gesetz zugrunde liegt. Zurzeit beraten die Bundestagsabgeordneten des Ausschusses für Recht und Verbraucherschutz über einen Kabinettsentwurf der Bundesregierung, der die Richtlinie in nationales Recht umsetzt.

Die alte Richtlinie von 1985 war auf Software wegen deren Eigenschaft als immaterielles Wirtschaftsgut nicht anwendbar, die neue Version jedoch schon. Allerdings fällt die Richtlinie in den Bereich Verbraucherschutz, weshalb drei bedeutende Einschränkungen gelten: Nur natürliche Personen können Ansprüche geltend machen, und zwar nur, wenn die Software ausschließlich privat verwendet wird, und nur bei Personen-, Sach- oder Datenschäden. Dies bedeutet im Umkehrschluss, dass weder Unternehmen noch Gebietskörperschaften (wie etwa Kommunen) oder natürliche Personen, die eine Software beruflich verwenden, Ansprüche geltend machen können. Und auch reine Vermögensschäden fallen nicht in den Anwendungsbereich der Richtlinie.

Der Hintergrund dieser Einschränkungen: Die Richtlinie regelt verschuldensunabhängige Haftung, das bedeutet, dass Hersteller auch haften, wenn ihnen weder Vorsatz noch Fahrlässigkeit nachgewiesen werden können. Damit sich aus dem Gesetz keine nicht mehr versicherbaren, existenzbedrohenden Haftungsrisiken ergeben, sind der Haftung enge Grenzen gesetzt. Und Unternehmen werden als weniger schutzbedürftig betrachtet, weil sie sich üblicherweise vertraglich gegen Schäden absichern können.

Diese Einschränkungen sind jedoch mit Blick auf den Softwaremarkt wenig sinnvoll. Viele Produkte werden sowohl von privaten Verbraucher:innen als auch im beruflichen Kontext genutzt. Und die großen

Softwarehersteller verfügen häufig über so große Marktmacht, dass sie die Vertragsbedingungen bestimmen (und etwa Haftung ausschließen lassen) können. Das gilt besonders, wenn kleine und mittelständische Unternehmen Produkte von großen US-Herstellern beziehen. Zudem verursachen Cybersicherheitsvorfälle vor allem finanzielle Schäden: Wenn etwa Cyberkriminelle die Daten von Unternehmen verschlüsseln und Lösegeld erpressen, ruht häufig der Betrieb und den Firmen entgehen Gewinne. Vor diesem Hintergrund sind die Einschränkungen des EU-Produkthaftungsrechts problematisch.

Neben der EU hat bisher kein Land Produkthaftungsregelungen verabschiedet, die die Nutzer:innen von Softwareprodukten zu Ansprüchen berechtigen. In den USA hatte es unter der Biden-Regierung Diskussionen über die Einführung einer Produkthaftung für Software gegeben, doch die Trump-Regierung strebt im Digitalbereich nach Deregulierung. Die EU-Kommission hatte 2022 einen Vorschlag für eine eigene Produkthaftungsrichtlinie für KI-Anwendungen vorgelegt. Diesen Vorschlag zog die Kommission dann jedoch im Oktober 2025 aus verschiedenen Gründen selbst zurück.

Bestehende Anforderungen für SaaS-Anbieter

Produkthaftungsrecht ist üblicherweise nur auf On-Premises-Softwarelösungen anwendbar, nicht aber auf Software-as-a-Service (SaaS), da es sich bei Letzterer um eine Dienstleistung handelt. Der CRA ist dann auf SaaS anwendbar, wenn die Dienstleistung als »remote data processing solution« zum Produkt gehört. Zusätzlich müssen SaaS-Anbieter die Anforderungen der »Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union« (NIS-2-Richtlinie) beachten. Die Bundesregierung hat die NIS-2-Richtlinie im Dezember 2025 verspätet umgesetzt. Diese schreibt vor, dass Anbieter sichere Dienste anbieten müssen, was auch das Management von Software-Schwachstellen einschließt.

Problematisch ist bei NIS-2 nicht so sehr, dass sie Regelungslücken enthielte, denn sie hat einen weiten Anwendungsbereich und gilt für alle Anbieter, die ihre Dienste auf dem europäischen Markt anbieten. Eine Ausnahme kleiner Unternehmen ist im SaaS-Bereich kaum relevant. Problematisch ist, dass es Zweifel an der entschiedenen Durchsetzung des Gesetzes in Deutschland gibt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist zuständig für die Verhängung von Bußgeldern bei Verstößen. Die BSI-Präsidentin gab jedoch an, dass ihre Behörde Unternehmen, die gegen die Auflagen verstoßen, im Regelfall nicht mit Bußgeldern belegen werde. Doch werden Unternehmen ihre Cybersicherheitspraktiken anpassen, wenn sie keine Sanktionen zu befürchten haben? Wenn die Verpflichtungen schon gegenüber deutschen Unternehmen nicht strikt durchgesetzt werden, wie sollen sie dann dafür sorgen, dass US-SaaS-Anbieter ihre Cloud-Lösungen sicherer gestalten? Und inwiefern wird das BSI bereit sein, Verstöße gegen den CRA — für dessen nationale Durchsetzung die Cybersicherheitsbehörde ebenfalls zuständig sein wird — mit Bußgeldern zu belegen oder Produktrückrufe zu veranlassen?

Vier Aufgaben für die Bundespolitik

Wenn sich die verheerende Cybersicherheitslage bessern soll, muss Software sicherer werden. Um entsprechende Anreize zu setzen, sollte die Bundespolitik vier Dinge tun.

Erstens sollte die Bundesregierung auf nationaler Ebene die bestehenden Regeln strikt durchsetzen. Die bereits geltende NIS-2-Richtlinie ebenso wie der 2027 in Kraft tretende CRA können ihre Wirkung erst dann entfalten, wenn die Hersteller bei Verstößen Sanktionen zu befürchten haben. Das BSI sollte daher zunächst einfordern, dass sich alle von NIS-2 betroffenen Unternehmen in dem entsprechenden Portal registrieren — bisher hat das nur etwa die

Hälfte getan. Anschließend sollte das BSI bei Verstößen Bußgelder in Aussicht stellen, und zwar auch für US-Firmen. So könnte es Unternehmen dazu veranlassen, die Vorgaben prioritär umzusetzen. Die US-Administration zeigt sich seit kurzem offen für Regulierung, die die Cybersicherheitsrisiken von KI-Anwendungen begrenzen soll. Für die Durchsetzung der Vorgaben gegenüber US-Unternehmen sollte daher entsprechend zuvor politisch der Boden bereitet werden. Gleichzeitig sollte sich die Bundesregierung auch auf etwaige Abwehr- oder Vergeltungsmaßnahmen aus Washington vorbereiten.

Zweitens sollte die Bundesregierung der Aufforderung des CRA nachkommen und für Hersteller von Softwareprodukten im Sicherheits- und Verteidigungsbereich strenge Cybersicherheitsanforderungen definieren und diese auch ausnahmslos durchsetzen. Dies kann, gerade im militärischen Bereich, auf unterschiedlichen Wegen geschehen: So können Verteidigungsministerium und Bundeswehr gemeinsam Mustervertragsbausteine entwickeln für die vielen Stellen in der Bundeswehr, die für die Beschaffung und den Betrieb von Software zuständig sind. Zudem können entsprechende horizontale Mindestanforderungen für Beschaffungsvorhaben formuliert werden, die idealerweise gleichermaßen für die Bundeswehr und kritische zivile Bereiche gelten.

Drittens sollte sich die Bundesregierung auf europäischer Ebene für eine Produkthaftungsregelung speziell für Software einsetzen. Theoretisch könnte auch der Bundestag die oben beschriebenen Lücken im Gesetzentwurf zur nationalen Umsetzung der EU-Produkthaftungsrichtlinie schließen. Doch der Europäische Gerichtshof hat den Mitgliedstaaten enge Grenzen gesetzt für sogenanntes »Gold-Plating« — also das Aufsetzen nationaler Regelungen, die über EU-Rechtsakte hinausgehen. Zudem sind nationale Alleingänge bei der Regulierung des globalisierten Softwaremarkts wenig zielführend. Daher ist ein europäisches Gesetz die bessere Option.

Dieses Gesetz sollte es Unternehmen und Gebietskörperschaften sowie natürlichen Personen, die Software beruflich nutzen, ermöglichen, Ansprüche gegen Hersteller geltend zu machen. Außerdem sollten auch reine Vermögensschäden zu Ansprüchen berechtigen. Zudem könnte es den Sicherheits- und Verteidigungsbereich miteinschließen.

Ähnliche Produkthaftungsgesetze für spezielle Produktgruppen gibt es bereits. Als Begründung sollte die Bundesregierung auf die Besonderheiten des Softwaremarkts verweisen. Angesichts der verheerenden Cybersicherheitslage ließe sich für ein solches Vorhaben vermutlich eine Mehrheit in Brüssel finden. Um zu verhindern, dass ein solches Gesetz unversicherbare Haftungsansprüche eröffnet, könnten Höchstgrenzen für die Haftungssummen festgelegt werden. Und um mittelständische Unternehmen zu schützen, sollten diese Summen nach Unternehmensgröße gestaffelt sein. Auch bei einem solchen Vorhaben sollten die Auswirkungen auf die transatlantischen Beziehungen mitgedacht und entsprechende Vorkehrungen getroffen werden.

Und viertens sollten europäische Politiker:innen ein umfassendes Produkthaftungsrecht für Software in Angriff nehmen, bevor sie über ein Regime speziell für KI-Anwendungen nachdenken. Auch wenn Letztere besondere Herausforderungen stellen, sind sie zunächst einmal Software. Es erscheint daher sinnvoll, in einem ersten Schritt umfassende Produkthaftung für Software zu etablieren und erst in einem zweiten zu prüfen, inwiefern weiterer Regelungsbedarf für KI-Systeme besteht. Mutmaßlich würde ein umfassendes Produkthaftungsrecht für Software auch viele denkbare Schadensfälle von KI-Anwendungen abdecken. Eine entsprechende rechtliche Ausgestaltung stünde auch im Einklang mit jüngsten Bemühungen der EU-Kommission, die EU-Digitalregulierung zu verschlanken.

Dr. Alexandra Paulus ist Wissenschaftlerin in der Forschungsgruppe Sicherheitspolitik und Ko-Koordinierende Leiterin des Forschungsclusters Cybersicherheit und Digitalpolitik.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3—4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN (Print) 1611-6364
ISSN (Online) 2747-5018
DOI: 10.18449/2026A27