Kommunikation & Recht

K&R
12 | Dezember 2023
26. Jahrgang
Seiten 769 - 840

dfv Mediengruppe
Frankfurt am Main

RA Dr. Florian Deusch und Prof. Dr. Tobias Eggendorfer*

Messbarkeit von IT-Sicherheit

Kurz und Knapp

Bislang sind keine technischen Verfahren bekannt, die die Sicherheit eines IT-Systems objektiv messen. Der Beitrag stellt dar, welche technischen und rechtlichen Probleme dies verursacht, und diskutiert, wie technische Ansätze zur Lösung dieser Probleme in rechtlicher Hinsicht umgesetzt werden könnten.

I. Verfügbare Aussagen zur IT-Sicherheit von Software

Angriffe auf IT-Systeme führen oft zu Ausfällen über den betroffenen Anwender hinaus: Sie wirken sich auch auf dessen Kommunikationspartner, auf Lieferketten oder – bei kritischen Infrastrukturen – auf die Versorgung der Bevölkerung aus.[1] Wer sich mit der Frage befasst, welche IT-Anwendung für seinen Bedarf „sicher genug" ist, findet eine bunte Mischung aus Werbeaussagen von Anbietern, verschiedenen Standards und Zertifizierungen vor. Worauf soll sich der Anwender verlassen?

1. Herstellerangaben

Ursächlich für die meisten IT-Angriffe sind Sicherheitslücken durch fehlerhafte oder unsorgfältige Programmierung oder Parametrisierung von Software. Für den Gesundheitssektor hat die ENISA z. B. festgestellt, dass die meisten IT-Sicherheitsvorfälle auf Schwachstellen in Software beruhen. Im „worst case" war die Folge, dass medizinische Behandlungen (auch in Krankenhäusern) gestört waren oder abgebrochen werden mussten.[2] Diese Fehler kann der Anwender aber nicht prüfen, denn selten ist der Quellcode offen, zudem fehlen den Anwendern die fachlichen und zeitlichen Prüfungsressourcen. Auch sind Herstelleraussagen, aus denen der Anwender ableiten könnte, ob und wie „sicher" die betreffende Software ist, oft vage.

Ein Beispiel: Die Microsoft-Produkt-Webseite von „Exchange Online"[3] verspricht „Anti-Schadsoftware" und „Antispam-Filter". „Exchange Online Protection" sichert dabei Schutz vor „Spam und Schadsoftware" zu sowie Schutz vor „100 % aller bekannten Viren" und vor „99 % aller Junk-E-Mails". Diese Zusicherungen sind kaum prüfbar und somit wenig hilfreich.[4] Aussagen über die Qualität des Programmcodes von „Exchange" sind damit nicht verbunden. Sicherheitslücken u. a. von Exchange finden sich z. B. in der CVE-Datenbank des US Department of Homeland Security:[5] Für „Exchange" finden sich im Frühjahr 2023 mehrere Remote Code Execution Angriffe (Einschleusen und Ausführen von schädlichen Programmcodes durch Angreifer aus der Ferne) und Privilege Escalation Angriffe (Angreifer verschaffen sich erweiterte Rechte). Ursächlich für diese Sicherheitslücken sind typischerweise Fehler im Programmcode, zum Beispiel durch fehlerhafte Eingabekontrolle.[6] Microsoft selbst informiert darüber auf den vorgenannten Webseiten nicht.[7]

2. Zertifikate, Standards und Normen

Neben den Herstellerangaben gibt es zahlreiche Zertifizierungen, Standards und Normen zur IT-Sicherheit. Bei einer Zertifizierung zur IT-Sicherheit prüft eine maßgebliche Stelle, ob das Prüfobjekt (z. B. ein Produkt oder IT-Dienst) bestimmte Anforderungen erfüllt, die überwiegend in Normen und Standards definiert sind.[8] Diese technischen Regelwerke beschreiben für ihren Anwendungsbereich den Stand der Technik.[9]

---

* Der Beitrag geht auf einen Vortrag der Autoren bei der DSRI-Herbstakademie 2023 zurück, der veröffentlicht wurde im Tagungsband von *Bernzen/Fritzsche/Heinze/Thomsen* (Hrsg.), Das IT-Recht vor der (europäischen) Zeitenwende? Tagungsband DSRI-Herbstakademie 2023, 2023, S. 323 ff. Er ist überarbeitet und aktualisiert zum Stand Oktober 2023. Mehr über die Autoren erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 31. 10. 2023.

1 Zur Gefährdungslage in Gesellschaft, Wirtschaft und kritischer Infrastruktur (KRITIS) siehe den Bericht des BSI Die Lage der IT-Sicherheit in Deutschland 2022, S. 57, 67 https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html). Ebenso verhält sich die erst kürzlich veröffentlichte Nationale Sicherheitsstrategie zur Cyber-Sicherheit, https://www.nationalesicherheitsstrategie.de/Sicherheitsstrategie-DE.pdf).

2 Zu typischen Sicherheitsproblemen siehe *Deusch/Eggendorfer*, in: Taeger/Pohle, Computerrechts-Handbuch, 37. EL Mai 2022, Kap. 50.1 Rn. 31 ff.; zur Relevanz von Softwareschwachstellen für den Gesundheitssektor siehe die Untersuchung „ENISA Threat Landscape: Health Sector", Juli 2023 (https://www.enisa.europa.eu/publications/health-threat-landscape, dort S. 4 u. 30). Die ENISA (European Network and Information Security Agency) ist die Behörde der Europäischen Union für Cybersicherheit.

3 https://www.microsoft.com/de-de/microsoft-365/exchange/compare-microsoft-exchange-online-plans?market=de, dort: „mehr erfahren", dann „Erweiterte Sicherheitsfunktionen" sowie „Exchange Online Protection".

4 „100 % aller bekannten Schadsoftware" ist schwer zu bestimmen. Bereits die Frage, ob die Schadsoftware nur „bekannt" ist oder auch „in the wild" (also bei IT-Nutzern und nicht nur im Labor) auch dann noch auftritt, wenn sie bereits als „ausgestorben" gilt und deshalb von vielen Virenscannern nicht mehr erfasst wird, bleibt dabei offen. Ebenso wenig ist definiert, wessen Kenntnis maßgeblich ist: Die Kenntnis des Herstellers Microsoft, „der Community" vernetzter Sicherheitsexperten oder reicht die Verfügbarkeit der Malware z. B. im Darknet aus? Ebenso fragwürdig ist „99 % aller Junk-E-Mails", weil die ausgesonderten Mails dem Nutzer i. d. R. nicht zur Prüfung vorliegen und die Definition von Junk nicht einheitlich ist. Es fehlt weiterhin der hoch relevante Messwert der False Positives, also der Mails, die fälschlich als Spam eingestuft wurden. Eine hohe Erkennungsrate korreliert häufig mit einer hohen Rate an False Positives. Dem technisch Verständigen fallen diese Aussagen daher sofort als wenig belastbar und nutzlos auf.

5 Zur CVE („Common Vulnerabilities and Exposures")-Datenbank generell: *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 34, dort Fn. 1; für das Microsoftprodukt „Exchange" finden sich zum Beispiel bis 10. 4. 2023 folgende neun CVE-Nummern, die dem Jahr 2023 zugeordnet sind: CVE-2023-21764, CVE-2023-21763, CVE-2023-21762, CVE-2023-21761, CVE-2023-21745, CVE-2023-21710, CVE-2023-21707, CVE-2023-21706, CVE-2023-21529. CVE-Nummern werden für kritische Softwaresicherheitslücken vergeben, die bekannt gegeben wurden und für die ein Patch existiert. Es bleibt damit ein Dunkelfeld von in diesem Zeitraum entdeckten, aber nicht bekanntgegebenen Lücken.

6 Generell zu Remote Code Execution: *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 52; verglichen mit Kraftfahrzeugen hätte jede dieser Lücken wohl einen Rückruf des Kraftfahrtbundesamts ausgelöst.

7 Es gibt allerdings Kommentierungen des Herstellers zu den CVE-Einträgen auf der Spezial-Webseite „Microsoft Security Response Center", zum Beispiel https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21529. Das unterscheidet häufig OpenSource-Projekte von kommerziellen Angeboten: Erstere listen bekannte Fehler aller Art und deren Behebungszustand auf deren Webseite, z. B. https://bugzilla.mozilla.org/describecomponents.cgi?product=Firefox, letztere betonen, s. o. Fn. 4, die (vorgeblichen) Leistungen ihres Produkts.

8 § 2 Abs. 7 BISG definiert die Zertifizierung in diesem Sinn. *Kipker* widmet Zertifizierungen in der 2. Aufl. seines Rechtshandbuchs Cybersecurity (2023) das gesamte Kapitel 5.

9 Art. 3 Nr. 9 - 11, 46 ff. VO (EU) 2019/881 regelt Zertifizierungen nach dem Cyber Security Act; zur Definition des Stands der Technik durch Normen und Standards *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 489.

Die Zertifizierungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß den §§ 2 Abs. 7, 9 Abs. 1 BSIG richten sich z. B. nach den „Technischen Richtlinien des BSI und den Common Criteria".

Die „Common Criteria for Information Technology Security Evaluation" basieren auf dem Standard ISO 15408 und definieren ein Vorgehen zur Evaluierung von IT-Sicherheit. Durch eine zwischenstaatliche Vereinbarung[10] haben sich die beteiligten Regierungen, darunter Deutschland, verpflichtet, diese „Common Criteria" (aktuell CC:2022) gegenseitig anzuerkennen.[11] Die CC:2022 sind Gegenstand zahlreicher Zertifizierungsprogramme (u. a. des Cyber Security Act, siehe auch Abschnitt IV). Vorab: Die CC:2022 machen viele Vorgaben zur Dokumentation und der Herangehensweise an Softwareentwicklung, enthalten aber keine Vorgaben zu den Eigenschaften eines Programmcodes.

Der Standard „Software Reviews and Audits IEEE 1028" (aktuelle Fassung aus 2008) definiert, wie Softwareüberprüfungen zur Ermittlung von Fehlern (Reviews) zu gestalten sind. Als Fehler definiert der Standard „das Abweichen von Erwartungen".[12] Die Erwartungen, die überprüft werden, sind allerdings in der IEEE 1028 nicht definiert. Folglich ergeben sich aus einem Review IEEE 1028 keine zwingenden Aussagen zur IT-Sicherheit des geprüften Produkts.

Abzugrenzen sind zudem Normen und Standards, die das Management von Informationssicherheit in einer Organisation beschreiben, zum Beispiel die Normenreihe ISO 27000 und der BSI-Grundschutz. Diese regeln z. B. Maßnahmen zur Prävention und Behandlung von Sicherheitsvorfällen.[13] Sie ermöglichen aber keine Bewertung dazu, ob ein Programmcode so geschrieben wurde, dass bekannte Sicherheitsprobleme vermieden werden. Für die Messung, ob ein IT-Produkt oder -Dienst frei ist von Sicherheitslücken („Vulnerabilities"), legen die aktuellen Standards keine Anforderungen fest (siehe unten Abschnitt IV).

II. Rechtliche Folgen der fehlenden Messbarkeit von IT-Sicherheit

Rechtliche Auswirkungen aus der fehlenden Messbarkeit von IT-Sicherheit zeigen sich auf verschiedenen Ebenen:

- Aufgrund § 434 Abs. 3 S. 2 BGB (in Kraft seit 1. 1. 2022) müssen sich Softwareanbieter fragen lassen, welche Maßstäbe sie für ein mangelfreies Produkt heranziehen. Hiernach gehören zu den objektiven Anforderungen der Kaufsache „sonstige Merkmale einschließlich ihrer (…) Sicherheit"; dies umfasst auch die IT-Sicherheit. Außerhalb der Sachmangelhaftung ergeben sich zudem deliktische Verkehrssicherungspflichten, Schäden durch unsichere IT-Produkte zu vermeiden.[14]
- Zur Pflicht zur sorgfältigen Geschäftsführung von Unternehmen gehört es, Schäden fernzuhalten und dessen Bestand zu sichern, also auch die Organisation einer sicheren IT. Dafür haftet der Geschäftsführer persönlich.[15] Dabei stützen sich zahlreiche Unternehmen auf „IT-Security-Features" von Herstellern, Zertifizierungen und Standards. Oftmals sind diese werbenden Aussagen nicht prüfbar oder sogar irreführend.[16] Dabei werden erhebliche Aufwendungen für Gegenmaßnahmen getroffen, die identifizierte Bedrohungen („threats") herabsetzen sollen. Zahlreiche „threats" wären aber vermeidbar, wenn der Programmcode keine Sicherheitslücken hätte. So enthalten Softwareanleitungen zwar regelmäßig die Empfehlung zu Anti-Malware und Firewalls nebst Anwenderschulungen, doch sollen alle diese Zusatzaufwendungen nur schlecht programmierte Software kaschieren: Wer würde akzeptieren, zum Backofen noch ein zusätzliches Thermometer zu kaufen, das an minütliche Temperaturmessungen erinnert, nur weil der Temperaturfühler im Ofen unzureichend ist? Bei Software dagegen verlangen Anbieter, dass Nutzer prüfen, welche Anhänge einer E-Mail sie öffnen.
  In gleicher Weise ist die Installation von Anti-Malware zu diskutieren: Aktuell zwar nötig, doch letztlich sollte ein Betriebssystem so resilient und sicher sein, dass die Installation von Malware unmöglich ist. Dass Systeme ohne nennenswerte Sicherheitslücken möglich sind, demonstriert OpenBSD.[17]
- Auch IT-Sicherheitsbeauftragte und Datenschutzbeauftragte haben die Aufgabe, die IT-Sicherheit in ihrem Verantwortungsbereich zu prüfen.[18]
- Versicherungen, die in Anspruch genommen werden, prüfen, ob sie ihre Einstandspflicht aufgrund Fahrlässigkeit durch Einsatz unsicherer IT kürzen können.[19]
- Art. 5 Abs. 2 und Art. 24 Abs. 1 DSGVO verlangen bei der Verarbeitung personenbezogener Daten den Nachweis, welche Maßnahmen ergriffen wurden, um die Sicherheitsanforderungen des Art. 32 DSGVO zu erfüllen. Verstöße hiergegen sind bußgeldbewehrt (Art. 83 Abs. 4 DSGVO).
- Bestimmte Branchen unterliegen Spezialgesetzen zum Softwareeinsatz. KRITIS-Unternehmen dürfen kritische

10 Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/International/cc_mra_2014_pdf.pdf?__blob=publicationFile&v=1).

11 So Page vi des Teils 1 der CC:2022 (https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf), referenzierend auf die aktuelle Version der ISO 15408:2022. Die CC haben zwischenzeitlich den weiteren Standard TSEC (Information Technology Security Evaluation Criteria) aufgenommen, https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/CC-und-ITSEC/cc-und-itsec.html.

12 *Rösler/Schilch/Kneuper*, Reviews in der System- und Softwareentwicklung, 2013 Seite 7.

13 Z. B. Ziffer 4.1 ISO/IEC 27000:2018: „(…) each organization needs to establish its policy and objectives (…) and achieve those objectives by using a management system."; ebenso Seite 2 des IT-Grundschutz-Kompendiums: „standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen, IT-Systeme, Kommunikationsverbindungen, Gebäude und Räume.", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.

14 Dazu bereits *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 225 ff.; *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 451 - 463.

15 *Voigt*, IT-Sicherheitsrecht, 2. Aufl. 2022, Kapitel A Rn. 32 ff.; *Schmidl/Thannen*, in: Kipker (Fn. 8), Kap. 8 S. 318; neuerdings jedoch OLG Zweibrücken, 27. 10. 2022 – 4 U 198/21, NJW 2023, 1589 (dazu *Versteyl/El-Taki*, NJW 2023, 1548 - 1550), welches im konkreten Fall eine finanzielle Geschäftsführerhaftung aufgrund des innerbetrieblichen Schadensausgleichs abgelehnt hat. Für die Leitung von Behörden ergeben sich entsprechende Verpflichtungen aus den gesetzlichen Aufgabenzuweisungen.

16 Ein gängiges Beispiel ist das Versprechen einer durchgängigen Verschlüsselung, die in Realität aus der Kombination von TLS, Plattenverschlüsselung und erneuter Transportverschlüsselung besteht. Dazu kritisch *Deusch/Eggendorfer*, K&R 2022, 577, 579 f.

17 Siehe www.openbsd.org, nur zwei entfernt ausnutzbare Sicherheitslücken in über 25 Jahren. Hier sind vor allem das stringente Qualitätsmanagement in der Softwareentwicklung bei OpenBSD ursächlich, die unter anderem Coding Standards, Code Reviews und gründliche Tests vorsehen.

18 Für IT-Sicherheitsbeauftragte: § 166 TKG bzw. der zugrundeliegende vertragliche Auftrag i. V. m. den einschlägigen Normen wie z. B. Normabschnitt 4.1 ISO 27001; für Datenschutzbeauftragte: Art. 39 i. V. m. Art. 32 DSGVO.

19 *Gabel/Heinrich/Kiefner*, Rechtshandbuch Cyber-Security, 2019, Kapitel 12 Rn. 102 - 109.

Komponenten gemäß § 9b Abs. 1 BSIG nur nach vorheriger Anzeige beim BSI einsetzen; Telekommunikationsunternehmen müssen Zertifizierungen vorweisen (§ 165 Abs. 4 TKG). Außerdem verlangt der Gesetzgeber von verschiedenen Unternehmen schriftliche Konzepte zum Schutz ihrer Systeme (z. B. §§ 8a, 8c, 8f BSIG, §§ 165, 166 TKG, § 11 EnWG). Auch hierzu wird auf Standards zurückgegriffen.

- Fehlende Transparenz zur IT-Sicherheit beeinflusst auch Entscheidungen der Legislative und Judikative. In der Gesetzesbegründung zu § 129 BetrVG ist z. B. zu lesen, dass virtuelle Betriebsversammlungen via „WebEx Meetings oder Skype" ermöglicht würden. Hierauf referenzierend führt das LAG Köln aus, „alle heutigen marktgängigen Konferenzsysteme" böten „durchweg die Möglichkeit hinreichend sicherer und verschlüsselter Kommunikation." Es existiert indes der technische Gegenbeweis durch Fälle, in denen Bild- und Tonaufnahmen aktiviert waren, obwohl der Nutzer sie ausgestellt hatte.[20]

III. Technische Lösungsansätze zur IT-Sicherheitsmetrik

Das Ziel, eine verlässliche, objektive, vergleichbare und belastbare Bewertung von Sicherheit zu schaffen, erfordert eine einheitliche Sicherheitsmetrik. Dazu finden sich in der Informatik-Literatur zwei Kernbereiche: Software-Qualitätsmetriken und verwandte Ansätze einerseits und Überlegungen zur Messung von Software-Sicherheit andererseits.[21]

1. Software-Qualitätsmetriken

Schon in den 80er Jahren fragte sich die Forschung, ob sich bereits während der Software-Entwicklung Komponenten mit einer hohen Fehlerwahrscheinlichkeit identifizieren lassen.[22] Allerdings war dieser erste Ansatz noch verkürzt: Wenn die empfohlenen Unit-Tests (überhaupt) durchgeführt wurden, waren dort entdeckte Fehler unbeachtlich. Außerdem beschränkten sich die Autoren in der Auswertung auf funktionale Einschränkungen, die aber sind meist unabhängig von Sicherheitslücken. Damit ist dieses Verfahren für eine vergleichende Bestimmung von Softwarequalität ungeeignet. Konzepte für Software-Qualitätsmetriken scheitern regelmäßig auch daran, dass sich die Autoren nicht auf eine Definition von Softwarequalität einigen können.[23]

2. Ideen für Software-Sicherheitsmetriken

Einige Forscher schlagen vor, Sicherheitsmetriken zur Verbesserung des Entwicklungsprozesses und für den Vergleich von Software zu entwickeln, allerdings ohne konkrete Umsetzung.[24]

Andere Arbeiten scheitern an der Messung von IT-Sicherheit, obwohl sie umfangreiche Berechnungsverfahren zur Verknüpfung gemessener Sicherheit vorschlagen. Als Lösung ziehen sie Schätzverfahren für die IT-Sicherheit heran, die jedoch außerhalb der IT entwickelt wurden und so keine Aussagekraft haben.[25]

Andere Metriken versuchen externe Größen, wie z. B. die Komplexität von Passwörtern zu bewerten, das allerdings liefert keine Aussage zur Softwarequalität.[26]

3. Zwischenfazit

Es zeigt sich – auch mit Blick auf weitere Empfehlungen wie die Common Criteria etc. –, dass es noch an einer verlässlichen Metrik für Sicherheit fehlt. Eine solche Metrik ist Gegenstand grundlegender Forschung in der Informatik und dringend notwendig. Denn erst durch eine Metrik lassen sich die nötigen Vergleichswerte erkennen. Es fehlen Messkriterien, um Programmcode auf Inhalte zu prüfen, die eine Schwachstelle verursachen. Technische Normen und Standards müssten derartige Schwachstellen als Fehler definieren und die Fehlerfreiheit als Vorgabe festsetzen. Daraus ließen sich sodann Kriterien einer Messung festlegen. Ein solches Vorgehen könnte zur Folge haben, dass Softwarehersteller ihre Programmcodes zumindest gegenüber einer Prüfinstanz offenlegen. Geheimhaltungsinteressen wären in diesem Fall durch Schweigepflichten und technische Vorkehrungen zu schützen. Um eine belastbare Metrik zur IT-Sicherheit zu schaffen, ist ein Zusammenwirken von Informatik und Rechtswissenschaft sinnvoll.

IV. Rechtliche Auswirkungen einer IT-Sicherheitsmetrik

Belastbare Aussagen zur IT-Sicherheit könnten Anbieter und Anwender unterstützen, ihre rechtlichen Pflichten zur Cybersecurity nachweislich zu erfüllen. Fraglich ist, ob Informationen zur Messbarkeit von IT-Sicherheit in den existierenden Zertifizierungsverfahren oder für den geplanten Cyber Resilience Act Relevanz erhalten können.

1. Aktuelle Zertifizierungen zur IT-Sicherheit

Zertifizierungen dienen in der IT-Sicherheit als Nachweis, bestimmte Anforderungen zu erfüllen; eine IT-Sicherheitskennzahl könnte so einem Zertifikat entsprechen.

Zu unterscheiden sind gesetzlich geregelte Zertifizierungen (wie unten behandelt) und Zertifizierungen, die außergesetzlichen Regelungen folgen, meist branchen- oder berufsspezifische Standards.[27] Gesetzliche Zertifizierungen sind durch § 9 BSIG bzw. durch die VO (EU) 2019/881 (Cyber Security Act) geregelt, siehe unten lit. a. Beispielhaft diskutieren dazu lit. b

20 *Deusch/Eggendorfer*, in: Heinze (Hrsg.), Daten, Plattformen und KI als Dreiklang unserer Zeit, 2022, S. 803, 822; eine weitere fatalistische Fehlbeurteilung liegt der falschen Aussage des OLG Köln zugrunde, wonach Sicherheitslücken die Verkehrsfähigkeit eines Smartphones nicht beeinträchtigen, weil jedes Betriebssystem Sicherheitslücken aufweise (OLG Köln, 30. 10. 2019 – 6 U 100/19, K&R 2019, 796 ff., Rn. 60 f., dazu *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 456. Derartige Prämissen unterstellen hinreichend sichere IT als unerreichbare Utopie, was technisch falsch ist.

21 Frühe Ansätze dazu liefern zum Beispiel *Shen/Yu/Thebaut*, IEEE Transactions on Software Engineering, Vol. SE-11, No. 4, April 1985; *Khoshgoftaar/Munson/Bhattacharya/Richardson*, IEEE Transactions on Software Engineering, Vol. 18, No. 11, November 1992; *Savola*, IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No. 1, January 2010; *Savola*, Strategies for Security Measurement Objective Decomposition, 2012.

22 *Shen/Yu/Thebaut*, IEEE Transactions on Software Engineering, Vol. SE-11, No. 4, April 1985.

23 *Khoshgoftaar/Munson/Bhattacharya/Richardson*, IEEE Transactions on Software Engineering, Vol. 18, No. 11, November 1992; *Cavano/McCall*, A Framework for the measurement of software quality, ACM SIGSOFT, Software Engineering Notes, Volume 3, Issue 5, November 1978, pp 133 - 139.

24 *Savola*, IJCSNS International Journal of Computer Science and Network Security, Vol. 10 No. 1, January 2010.

25 *Wang/Wulf*, in: NIST, Proceedings of the 20th NISSC, 1997, S. 522; *Evesti/Savola/Ovaska/Kuusijärvi*, in: MOPAS 2011: The Second International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, 2011, S. 1.

26 *Islam/Falcarin*, Proceedings of the 2011 10th IEEE International Conference On Cybernetic Intelligent Systems, September 1 - 2, S. 70.

27 Außergesetzliche Zertifikate sind oft in Cloud-Angeboten vorzufinden, die bezwecken, die Anforderungen des Art. 28 DSGVO nachzuweisen; hier ist zwar die Anforderung der IT-Sicherheit gesetzlich geregelt, aber nicht der Inhalt des Zertifikats, siehe dazu *Stutz/Münzberg*, in: Schläger/Thode, Handbuch Datenschutz- und IT-Sicherheit, 2. Aufl. 2022, Kapitel B 7.5 Rn. 191.

das EUCC Scheme und lit. c das IT-Sicherheitskennzeichen gemäß § 9a BSIG.

a) § 9 BSIG und Cyber Security Act

Für bestimmte Produkte oder Leistungen kann beim BSI das „Deutsche IT-Sicherheitszertifikat" beantragt werden.[28] Die Vorgaben und das Verfahren regeln § 9 BSIG und die BSI-Zertifizierungs- und Anerkennungsverordnung (BSI-ZertV). Das Zertifikat bestätigt die Erfüllung der vom BSI festgelegten Kriterien (§ 9 Abs. 4 BSIG).

Zertifizierungen gemäß § 9 BSIG sind z. B. erforderlich für

- den Einsatz Kritischer Komponenten durch Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotential (§ 165 Abs. 4 TKG, derzeit für von der Bundesnetzagentur festgelegte Funktionen im 5G-Mobilfunk) und
- Smart-Meter-Gateways gemäß § 24 Messstellenbetriebsgesetz (intelligente Messsysteme, z. B. für den Stromverbrauch).
- Überdies können Betreiber kritischer Infrastrukturen ihre IT-Sicherheitsmaßnahmen gemäß § 8a Abs. 3 BSIG durch ein Zertifikat gemäß § 9 BSIG nachweisen.[29] Auch freiwillige Zertifizierungen sind möglich.

Das BSI muss die Zertifizierung erteilen, wenn der Antragsteller die Kriterien gemäß § 9 Abs. 4 BSIG erfüllt. Diese legt das BSI fest und veröffentlicht sie auf seiner Internetseite (§ 4 BSI-ZertV). Derzeit sind Zertifizierungen nach den Technischen Richtlinien (TR) des BSI und nach den „Common Criteria" möglich; bei einer belastbaren Metrik zur IT-Sicherheit könnten bestimmte Messergebnisse Zertifizierungskriterien sein (siehe dazu unten Punkt b).[30]

Ob und wie lange das bisherige „Deutsche IT-Sicherheitszertifikat" relevant bleibt, hängt vom Ausbau der Zertifizierungen gemäß dem Cyber Security Act ab (CSA – VO (EU) 2019/881). Die Art. 46 ff. CSA schaffen einen Rahmen für Zertifizierungen, die in allen EU-Staaten gelten und das BSI-Zertifikat ablösen werden.[31]

b) EUCC Scheme Zertifizierungen (Common Criteria/ISO 15408)

Das EUCC Scheme[32] definiert auf Grundlage der CC:2022 (identisch ISO 15408) Kriterien zur Zertifizierung von „ICT-Products" i. S. d. Art. 2 Nr. 12 CSA (Elemente von Netz- und Informationssystemen).[33]

Allerdings fehlt es im EUCC Scheme bislang an Vorgaben zu einer messbaren IT-Sicherheit. Das EUCC Scheme setzt nicht einmal den Nachweis einer statischen Code-Analyse voraus, die z. B. Kopierfunktionen mit Längenbeschränkung zur Verhinderung sogenannter Pufferüberläufe erzwingen könnte. Diese sind für die Programmiersprache C in der Norm ISO/IEC 9899 (Annex K) seit Jahrzehnten definiert und somit Stand der Technik.[34] Im EUCC Scheme wäre eine solche Vorgabe im Annex 4 zu verorten („Minimum Site Security Requirements"). Denn unter dem Titel „Purpose" ist der Zweck festgelegt, einen Mindeststand an Sicherheitsanforderungen zu definieren, der bei der Programmierung zu erfüllen ist. Annex 4 legt aber keine Standards zur Qualität des zu programmierenden Codes fest, sondern schreibt in Ziffer 4 eine „Development Security Documentation (DSD)" vor. Die DSD soll die Maßnahmen beschreiben, welche in der Entwicklung ergriffen wurden, um die Sicherheit des betreffenden IKT-Produkts zu gewährleisten. Die Bedrohung von Pufferüberläufen ist zwar in Annex 7 des EUCC Scheme erkannt und es werden Tests dazu vorgeschlagen (dort S. 212, 215, 217). Ein Bezug zu den Gegenmaßnahmen nach dem Stand der Technik gemäß ISO/IEC 9899 fehlt indes.[35]

Die Erwägungsgrund 77 zum CSA untermauert diesen Befund. Er lautet:

„Die Konformitätsbewertung und die Zertifizierung an sich können nicht garantieren, dass die zertifizierten IKT-Produkte, -Dienste und -Prozesse cybersicher sind. Es handelt sich vielmehr um Verfahren und technische Methoden, um zu bescheinigen, dass die IKT-Produkte, -Dienste und -Prozesse geprüft wurden und bestimmte Anforderungen an die Cybersicherheit erfüllen, wie sie anderweitig, beispielsweise in technischen Normen, festgelegt sind."

Kriterien für eine messbare IT-Sicherheit wären daher in die Zertifizierungsschemata aufzunehmen und gegebenenfalls auch der CSA zu ändern. Die internationale Anerkennung durch eine Ergänzung der CC:2022 um diese Kriterien würde der IT-Sicherheitsmetrik die notwendige Durchsetzungskraft verleihen.

c) Freiwilliges Sicherheitskennzeichen gemäß § 9c BSIG

Das freiwillige IT-Sicherheitskennzeichen gemäß § 9c BSIG bescheinigt (i) die Zusicherung des Herstellers, wonach das Produkt den IT-Sicherheitsanforderungen des BSI entspricht und (ii) eine Plausibilitätskontrolle dieser Angaben durch das BSI (§§ 9c Abs. 4 BSIG und 5 i. V. m. § 7 BSI-IT-Sicherheitskennzeichenverordnung – ITSiKV).[36] Nach der Freigabe *muss* der Hersteller/Diensteanbieter das Etikett des IT-Sicherheits-

28 Liste erteilter Zertifikate: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Listen/listen_node.html.

29 Die Pflicht des § 165 Abs. 4 TKG war bis zum 30. 11. 2021 als § 109 TKG (a. F.) formuliert. § 9 BSIG ist zwar nicht im Gesetzestext (§ 109 TKF a. F. bzw. § 164 TKG) genannt, jedoch in der Gesetzesbegründung, dazu *Keppeler*, in: Ritter (Hrsg.), Die Weiterentwicklung des IT-Sicherheitsgesetzes, 2021, Art. 2, § 109 TKG, Rn. 767. Zur Festlegung Kritischer Komponenten durch die Bundesnetzagentur: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/ListekritischeFunktionen.pdf?__blob=publicationFile&v=3. Zum Nachweis gemäß § 8a BSIG: *Schneider*, in: Schneider (Hrsg.), Handbuch EDV-Recht, 5. Aufl., Kap. A Rn. 1448.

30 Zum Anspruch auf das Zertifikat: *Paschke*, in: Ritter (Fn. 29), Art. 1, § 9 BSIG Rn. 580; Internetseite des BSI mit Zertifizierungskriterien: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/zertifizierung-von-produkten_node.html.

31 Die Anerkennung nationaler Zertifizierungen wie das Deutsche IT-Sicherheitszertifikat des BSI sind abhängig von zwischenstaatlichen Anerkennungsvereinbarungen. Für Zertifizierungen nach den „Common Criteria" gibt es z. B. das Agreement on the Recognition of Common Criteria Certificates in the field of IT Security (CCRA), dazu siehe oben Abschnitt I Ziffer 2. Vertragsbeteiligte sind neben einigen EU-Staaten z. B. Indien, Israel sowie die Türkei und die USA, siehe das BSI-Dokument „Deutsche IT-Sicherheitszertifikate", S. 4 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/7148_pdf.pdf?__blob=publicationFile&v=1). Zur Ablösung des BSI-Zertifikats *Voigt* (Fn. 15), Kap. F Rn. 352. Die EU-Zertifikate dagegen setzen entsprechende Durchführungsverordnungen voraus. Bislang gibt es dazu lediglich die Entwürfe „European Cybersecurity Certification Scheme on Common Criteria – EUCC Scheme)" sowie „European Certification Scheme for Cloud Services – EUCS". Ein Schema für 5G-Technologien befindet sich bei der ENISA in Arbeit (https://certification.enisa.europa.eu/).

32 Entwurf für die Normierung einer Zertifizierung für Hard- und Software gemäß dem CSA, siehe Fn. 31.

33 Seite 9 EUCC, abrufbar unter https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme.

34 *Deusch/Eggendorfer*, in: Taeger/Pohle (Fn. 2), Kap. 50.1 Rn. 91; zu ISO/IEC 9899 (Entwurfsstand der Revision 2022): https://www.open-std.org/jtc1/sc22/wg14/www/docs/n2310.pdf, dort S. 427 ff.

35 Kritisch zum EUCC Scheme bereits *Deusch/Eggendorfer*, in: Taeger (Hrsg.), Im Fokus der Rechtsentwicklung, 2021, S. 321, 323; Der Entwurf des European Certification Scheme for Cloud Services (EUCS) fordert dagegen zumindest auf Seite 111 Pentests (https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme/@@download/fullReport).

36 Die Verfasser danken dem zuständigen Referatsleiter des BSI, Herrn Joshu Wiebe, und seinem Team für die wertvollen Informationen über das IT-Sicherheitskennzeichen.

kennzeichens am Produkt anbringen (§ 9c Abs. 6 BSIG); das Etikett enthält einen Internet-Link mit aktuellen Informationen des BSI, wie z. B. Sicherheitslücken und deren Behebung.[37] Positiv ist die Dynamik dieses Verfahrens: Die Aktualisierungen veranlassen den Hersteller, sein Produkt „auf dem aktuellen Stand" zu halten, um negative Hinweise zu vermeiden.

Zu hinterfragen sind dagegen die derzeitigen inhaltlichen Anforderungen an das IT-Sicherheitskennzeichen in „Technischen Richtlinien" des BSI (BSI TR). Für Breitbandrouter z. B. schreibt Ziffer 4.2 BSITR 03148 eine Updatefunktion vor, um Sicherheitslücken zu beheben.[38] Es fehlt allerdings eine ausdrückliche Vorgabe, Programmcode für die Firmware des Routers ohne Schwachstellen zu erstellen und z. B. Pufferüberläufe zu vermeiden. Der Hersteller muss in § 7 BSI-IT-Sicherheitskennzeichenverordnung lediglich versichern, „ihm bekannt werdende Sicherheitslücken zu beheben". Nach diesem Wortlaut muss der Hersteller nur Fehler im Nachgang beseitigen, hat aber keinen Anreiz, Software von Anfang an messbar sicher zu gestalten.

Mit Bußgeld bis zu € 500 000 kann zwar belegt werden, wer das IT-Sicherheitskennzeichen ohne Freigabe des BSI verwendet (§ 14 Abs. 2 Nr. 11, Abs. 5 S. 2 i. V. m. § 9c Abs. 4 S. 1 BSIG); für vorsätzliche oder fahrlässige Falschangaben gibt es jedoch keine ausdrückliche Straf- oder Bußgeldbewehrung. Im Gegensatz dazu schreibt Art. 65 CSA wirksame Sanktionen bei Verstößen gegen die Schemata zur Zertifizierung vor, wenngleich die Umsetzung in Deutschland noch offen ist.

2. IT-Sicherheitsmetrik im Vorschlag zum Cyber Resilience Act

Nach dem Entwurf der EU-Kommission zum Cyber Resilience Act (CRA-E)[39] sollen erstmals IT-Sicherheitsanforderungen definiert werden, die nicht sektoral für spezifische Branchen gelten, sondern horizontal für alle Produkte mit digitalen Elementen und damit im Ergebnis für jegliche Hard- und Software, auch, soweit diese in anderen Produkten integriert ist.[40]

Art. 5 i. V. m. Anhang I CRA-E schreibt für Produkte mit digitalen Elementen ein angemessenes Cybersicherheitsniveau vor sowie die Abwesenheit von „bekannten ausnutzbaren Schwachstellen". Im Interesse des „effet utile"[41] ist die Norm so auszulegen, dass Sicherheitslücken bereits dann „bekannt" sind, wenn deren Auftreten und entsprechende Gegenmaßnahmen vom Stand der Technik erfasst sind. Wenn eine Schwachstelle dagegen erst dann „bekannt" ist, wenn der Hersteller weiß, dass seine Software Lücken bzw. Unzulänglichkeiten enthält, bleibt die Norm davon abhängig, ob der Hersteller einen guten oder schlechten Kenntnisstand hat.[42]

Die formelle Umsetzung der Sicherheitspflichten aus Art. 5 CRA-E erfolgt durch die Konformitätsbewertung und -erklärung gemäß den Art. 18 ff. CRA-E. Hiernach müssen Hersteller zu den Kriterien des Art. 5 CRA-E ein Konformitätsbewertungsverfahren durchführen und eine Erklärung dazu abgeben. Art. 18 Abs. 3 CRA-E vermutet die Konformität, wenn eine Zertifizierung gemäß CRA vorliegt.[43]

Die Verzahnung mit dem Zertifizierungsverfahren des CSA führt jedoch aus Sicht der Verfasser zu Widersprüchen: CSA-Zertifizierungen lassen gerade keinen Raum für eine valide Messung von IT-Sicherheit, sondern geben lediglich das Verfahren zur Produktentwicklung vor. Außerdem konzediert der Erwägungsgrund 77 CSA, dass eine Zertifizierung nicht zu einem „cybersicheren" Produkt führt, während Art. 5 i. V. m. Anhang I CRA-E zwar nicht die Utopie einer absoluten Sicherheit verlangt, dennoch aber ein „angemessenes Cybersicherheitsniveau". Aus Sicht der Autoren müssen dazu alle Qualitätssicherungen nach dem Stand der Technik ergriffen werden. Für den Entwurf des CRA ist zu fordern, dass die Defizite bei der Definition des Stands der Technik in den bisherigen Zertifizierungsschemata behoben und die Widersprüche zum CSA beseitigt werden.

V. Zusammenfassung und Fazit

Die fehlende Belastbarkeit von Herstellerangaben führt zu Unsicherheiten bei IT-Anwendern, die gesetzlich vorgegebene IT-Sicherheitspflichten erfüllen müssen, zum Beispiel TK- und KRITIS-Unternehmen im Speziellen und sonstige Unternehmen im Rahmen allgemeiner Compliance-Vorgaben.

Leider stellen auch die gesetzlichen Zertifizierungsprogramme nicht auf technische Normen ab, die Vorgaben zum Programmcode selbst treffen, sondern das Verfahren zur Softwareentwicklung regeln.

Aus technischer Sicht ist zu fordern, dass Maßstäbe zur Softwarequalität erforscht und in die technischen Normen aufgenommen werden, welche für die gesetzlichen Zertifizierungen maßgeblich sind.

Florian Deusch
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht in der Anwaltskanzlei Dr. Gretter in Ravensburg. Er ist zudem als Datenschutzbeauftragter tätig.

Tobias Eggendorfer
ist Professor für Sicherheit in verteilten Anwendungen an der TH Ingolstadt, davor war er als Abteilungsleiter „Sichere Systeme" an der Agentur für Innovation in der Cybersicherheit für die Weiterentwicklung der Forschung im Bereich der IT-Sicherheit zuständig. Er ist zudem als IT- und Datenschutzbeauftragter tätig.

37 Zudem kann das BSI im Rahmen einer „nachgelagerten Marktaufsicht" prüfen, ob die Zusicherungen des Herstellers für ein erteiltes IT-Sicherheitskennzeichen eingehalten sind, § 9c Abs. 8 BSIG.

38 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/fuer-Hersteller/Antrag/IT-SiK-Antrag_node.html.

39 COM(2022) 454 final.

40 *Pilz/Weiß/Zwersche*, CR 2023, 154, 155; *Hessel/Callewaert*, K&R 2022, 789 ff.; *Deusch/Eggendorfer*, K&R 2022, 794, 796.

41 *Heinze*, in: Handbuch des Europäischen Privatrechts (HWB-EuP), Effektivitätsgrundsatz (https://hwb-eup2009.mpipriv.de/index.php/Effektivit%C3%A4tsgrundsatz); *Grabitz/Hilf/Nettesheim*, Das Recht der EU, 78. EL, 2023, Art. 19 EUV Rn. 53.

42 *Deusch/Eggendorfer*, K&R 2022, 794, 796.

43 *Pilz/Weiß/Zwersche*, CR 2023, 154, 155; *Hessel/Callewaert*, K&R 2022, 789 ff.; *Deusch/Eggendorfer*, K&R 2022, 794, 796.