Cyberversicherung

Dickmann

2025
ISBN 978-3-406-73624-7
C.H.BECK

in der Logistikkette bewusst eingetragen werden können.[580] Spezifikationen, Standards sowie Test- und Dokumentationsvorgaben suggerieren eine Scheinsicherheit, denn gerade in der Mikroelektronik werden aus Kostengründen die eigentliche Herstellung an hoch spezialisierte Unternehmen ausgelagert und meist nur Post-Produktionsprüfungen[581] durchgeführt, die nicht den nötigen Tiefgang aufweisen und nicht schnell genug an die Anforderungen neuer Bedrohungen angepasst werden. Mittels Reverse Engineering sind viele Schwachstellen jedoch nur von hoch spezialisierten Fachleuten und mit großem technischen und zeitlichen Aufwand zu entdecken.[582] Es bleiben (blindes) Vertrauen und vor allem schwierige Beweisfragen,[583] da es sich um systemische Probleme ganzer Branchen handelt.[584] Bei Monokultur in der Lieferkette und der Tendenz, bestehende Software-Module möglichst häufig wiederzuverwenden, verstärkt sich zudem die Gefahr der Mangelhaftigkeit ganzer Klassen von Geräten.[585] Mangelnde Software-Qualität insbes. bezüglich Sicherheitsaspekten stellt dabei ein allgemeines Phänomen dar.[586]

---

[580] Für Software etwa bewusstes Eintragen von böswilligem Code im Kompilierungsvorgang, vgl. Thompson, Communications of the ACM 27 Nr. 8 (Aug. 1984), 761 (763); Boucher/Anderson, Trojan Source: Invisible Vulnerabilities, 2021 (abrufbar unter arxiv.org/abs/2111.00169; abgerufen am 17.11.2023). Auch mittels gefälschter, untergeschobener modifizierter oder nachträglich ausgetauschter bzw. hinzugefügter Bauteile (etwa Implementierung von Hardware-Trojanern und Abschaltvorrichtungen (Kill-Switches) in Produkte abgefangener Lieferungen). Vgl. Kurz/Rieger, Cyberwar, 2018, S. 92 ff.; Speith/Becker/Ender/Puschner/Paar DuD 2020, 446.

[581] Tracking von Änderungen am Platinenlayout (optische oder radiologische Referenzprüfung); Überprüfung von Bauteilkennzeichen und Seriennummern sowie Durchmessen von Bauteilen.

[582] Für den Markt integrierter Schaltkreise Mavroudis/Cerulli/Svenda/Cvrcek/Klinec/Danezis, 24th ACM Conference on Computer and Communications Security (CCS'2017), ACM, 2017, 1583; für Software Gebeshuber/Teiniker/Zugaj, Exploit!, 2019, S. 97 ff.

[583] Für die Automobilindustrie Kessel PHi 2018, 62 (64 f).

[584] Vgl. den Vortrag von Hudson, Modchips of the State, Vortrag auf dem 35C3 vom 27.12.2018 (abrufbar unter media.ccc.de/; abgerufen am 17.11.2023).

[585] „Class break" vgl. Schneier, Click here to kill everybody, 2018, S. 31 f. und 87 ff.

[586] Whittaker/Voas, IT Pro Nov./Dec. 2002, 28 ff.; Schneier, Click here to kill everybody, 2018, S. 107 ff.; Paulus, Basiswissen Sichere Software, 2011, S. 4 ff. Pohlmann, Cyber-Sicherheit, 2019, S. 3 f. Ursprung der Probleme war bzw. ist schon die Aus- und Fortbildung von Informatikern/Programmierern in Schule, Betrieb und Studium, bei der sicheres Programmieren zB durch Programmiersprachenwahl, Risikoermittlung, Minimierung der Angriffsoberfläche, Sicherstellung von Verlässlichkeit/Vertrauenswürdigkeit/Fehlertoleranz, Kryptografie-Einsatz, Schwachstellenvermeidung, Quellcode-Prüfung und nachgelagerte Tests unter Sicherheitsaspekten bis in die 2010er Jahre (wenn überhaupt) nur eine untergeordnete Rolle spielten. Vgl. Naiakshina/Danilova/Gerlitz/v. Zezschwitz/Smith, CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; S. 311; Empfehlung der Gesellschaft für Informatik e.V. zur Berücksichtigung der IT-Sicherheit in der schulischen und akademischen Ausbildung vom 3.10.2016 (abrufbar unter dl.gi.de; abgerufen am 17.11.2023). Studiengänge mit dem Schwerpunkt IT-Sicherheit wurden in Deutschland überwiegend erst in den 2010er Jahren ins Leben gerufen. Kritisch zur Ausbildung zum Fachinformatiker Schumacher, Magdeburger Journal zur Sicherheitsforschung 2014, 457. Die IT-FortbV sieht in Anlage 5 Nr. 14 erst seit 2010 einen „Security Technician" vor. 2018 wurden „IT-Sicherheit" und „Datenschutz" in verschiedenen (dualen) Ausbildungsordnungen als Inhalte aufgenommen, aber erst für Ausbildungsverhältnisse ab Mitte 2020 fand eine umfassende Aktualisierung statt, vgl. Wiegand, heise news vom 6.3.2020 (abrufbar unter heise.de; abgerufen am 17.11.2023).

Davon ist auch Hard- und Software betroffen, die eigentlich die IT-Administration vereinfachen oder IT-Sicherheit erhöhen soll.[587]

315 **(6) Ausfallsicherheit.** Werden Dienste oder Produkte zB in der Alten- und Krankenpflege mit entsprechendem Personenschadenrisiko verwendet,[588] für die sie aber nie konzipiert wurden, folglich mit keinem adäquaten Schutzniveau und der nötigen Ausfallsicherheit versehen sind, ist eine Haftung dem Grunde und der Höhe für Schäden aus einer Sicherheitslücke ohne Verwendungsausschlüsse problematisch. Darf man sich auf die **Ausfallsicherheit von Hard- und Software** verlassen, wenn von ihnen (allein) Gesundheit und Leben abhängen? Für die Antwort im konkreten Fall kommt es auf die Erkennbarkeit der (Un-)Geeignetheit des Dienstes bzw. Produkts an. Zur Einschätzung können die Beschreibung eines Sicherheitsniveaus des Dienstes oder Produkts samt entsprechender Dokumentation sowie eigene Analysen des (potenziellen) Nutzers nach dem eigenen Anforderungskatalog herangezogen werden. Im Zweifel bedarf es Nachfragen, weiterer Aufklärung, Vorab-Tests und (wohl immer) einer Absicherung über redundante oder alternative Systeme samt (Echtzeit-)Überwachung sowie durch Kontinuitätsplanung für den Notfall.[589] Das Betreiber- bzw. Nutzerrisiko kann ausnahmsweise zB bei gänzlich fehlendem Problembewusstsein dergestalt überwiegen, dass das Risiko von Hersteller und Verkäufer (voll umfänglich) zurücktritt.

316 **(7) Beschaffenheitsvereinbarung.** Primär kommt es zur Ermittlung des vertraglichen Soll-Zustands auf eine etwaige **Beschaffenheitsvereinbarung** der Parteien an. Die Beschreibung eines Produkts als **„sicher"**[590] im Sinne der IT[591] ist sehr vage und wird beispielsweise ohne ein Pflichtenheft, in Bezug genommene Vergleichsprodukte, explizite Nutzungsausschlüsse, Kompatibilitätsanforderungen oder Standards[592] schwerlich unstreitig einzugrenzen sein. Dies gilt vergleichbar für den **bloßen Verweis auf den Stand der Technik** ohne etwa die Festlegung der Methodik zur Ermittlung oder kontinuierlich aktualisierte Referenzen.[593] IT-Sicherheit auf einem zu beschreibenden Sicherheitsniveau als Momentaufnahme bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informations-

[587] Vgl. hierzu den Fall von SolarWinds und die Angriffe vor allem auf US-staatliche Einrichtungen mittels eingeschleusten Schadcodes Nakashima/Timberg, Washington Post online vom 14.12.2020 (abrufbar unter washingtonpost.com; abgerufen am 17.11.2023).

[588] Vgl. das Beispiel bei Kurz/Rieger, Cyberwar, 2018, S. 48 ff. (allerdings für einen Dienst, der explizit für die häusliche Krankenpflege ausgelegt ist).

[589] Gegebenenfalls mit analoger Rückfallebene.

[590] Im englischen Sprachraum findet sich auch der Verweis auf „military grade security" meist ohne nähere Referenz. Zum Vorgehen der FTC gegen fälschlicherweise zugesicherte Eigenschaften insbes. bzgl. sicherer Verschlüsselung Kosseff, Cybersecurity Law, 2. Aufl. 2019, S. 40 ff.

[591] Vgl. etwa Pohlmann, Cyber-Sicherheit, 2019, S. 575 f.; zum Fehlerbegriff Marly SoftwareR-HdB Rn. 1437; zur Differenzierung im Englischen zwischen „Security" und „Safety" Kriha/Schmitz, Sichere Systeme, 2009, S. 3, 615 ff. „Sicherheit" soll vorliegend beides umfassen.

[592] Etwa eine Zertifizierung nach den Allgemeinen Kriterien für die Bewertung der Sicherheit von Informationstechnologie (Common Criteria), die Beachtung des Federal Information Processing Standard (FIPS) für die zivilen Regierungseinrichtungen der USA oder des Mindeststandards des BSI nach § 8 Abs. 1 BSIG (abrufbar unter bsi.bund.de); zu Standards in der Informationssicherheit insgesamt Sohr/Kemmerich in Kipker Cybersecurity-HdB Kap. 2 Rn. 202 ff. Kritisch zu den CC Anderson, Security Engineering, 3. Aufl. 2021, S. 1029 ff.

[593] Vgl. etwa TeleTrust e.V., Handreichung zum „Stand der Technik", Ausgabe V 2_2023-05 DE (abrufbar unter teletrust.de; abgerufen am 17.11.2023).

technik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind. IT-Sicherheit ist folglich kein Produkt, sondern eine relative, sich verändernde Eigenschaft zu einem bestimmten Zeitpunkt.[594] In Software beginnt Sicherheit schon beim Schreiben und Kompilieren.[595] Sicherheitskritisch ist im Bereich der IoT vor allem eingebettete Software zur Steuerung externer Prozesse. Die konkrete Kritikalität kann nur im Nutzungskontext ermittelt werden.[596] Folglich bedarf es einer beschreibenden Auseinandersetzung insbes. mit dem konkret-individuell tragbaren Maß, (resultierender) konkreter Spezifikationen, der Erarbeitung eines Sicherheitsmodells, prozessualen Vorgaben zur Qualitätssicherung und zu Test-Mitteln/Methoden sowie Bewertungskriterien für die Testergebnisse.[597] Auch Negativabgrenzungen[598] zu dem, was nicht geschuldet wird, und Beschreibungen des konkret vorgesehenen Einsatzszenarios samt Schnittstellen und vorhandener Sicherungsparameter können der Annäherung dienen.

Zur Vereinbarung der Beschaffenheit von Produkten oder Produktklassen können für die IT-Sicherheit und den Datenschutz aus Nutzer- und Betreibersicht Vorarbeiten aus Wirtschaft, Wissenschaft und Gesetzgebung fruchtbar gemacht werden. Hier sei exemplarisch auf Geräte des Internets der Dinge eingegangen. Zur Erhöhung der Produktsicherheit wurde ein **(bislang) unverbindlicher Kanon von Sicherheitsmerkmalen für IoT-Geräte** erarbeitet, bei deren ordnungsgemäßer Implementierung wenigstens ein **Basisschutz**[599] der Geräte bei Netzwerkeinbindung gewährleistet ist. Im **Produktsicherheitsrecht** sind etwa Kategorien von Funkanlagen[600] in den Fokus der Regulierung gerückt (Art. 3 Abs. 3 S. 1 d–f RL (EU) 2014/53[601]). Für diese werden IT-Sicherheitsanforderungen formuliert, die die **Konformität** zur Anbringung des CE-Kennzeichens betreffen (vgl. Art. 30 VO (EG) 765/2008 sowie für Funkanlagen Erwgr. 43 ff. RL (EU) 2014/53).[602] Vereinfacht und zusammenfassend dargestellt sind die IT-Sicherheitsanforderungen:[603] **317**

[594] Mithin ist IT-Sicherheit bei nicht bloß momentaner Betrachtung als in Schleifen verlaufender dynamischer Prozess zur asymptotischen Annäherung an ein stetig anzupassendes Zielniveau zu sehen. Vgl. Anderson, Security Engineering, 3. Aufl. 2021, S. 1030.

[595] Vgl. Boucher/Anderson, Trojan Source: Invisible Vulnerabilities, 2021 (abrufbar unter arxiv.org/abs/2111.00169; abgerufen am 17.11.2023).

[596] Liggesmeyer, Software-Qualität, 2. Aufl. 2009, S. 440 ff.

[597] Vgl. den Leitfaden bei Liggesmeyer, Software-Qualität, 2. Aufl. 2009, S. 481 ff. und Anderson, Security Engineering, 2. Aufl. 2008, S. 857 ff.

[598] Hierzu Graf v. Westphalen in Foerste/Graf v. Westphalen ProdHaft-HdB § 1 Rn. 23 ff und 38 f.

[599] Für einen umfassenderen Ansatz ENISA, IoT Security Standards Gap Analysis vom 17.1.2019, S. 12 ff. (abrufbar unter enisa.europa.eu; abgerufen am 18.11.2023); Williams, Secure Software Lifecycle, Version 1.0 2019, S. 20 f. (abrufbar unter cybok.org; abgerufen am 18.11.2023).

[600] Technologieoffen für Produkte mit Sende-/Empfangstechnik für Funk wie etwa Router oder Smartphones, aber auch über Bluetooth ansprechbare Armbanduhren, „smarte" Spielzeuge etwa mit online-basierender Spracherkennung oder per App steuerbare WLAN-Babyphones.

[601] Aktivierung durch VO (EU) 2022/30 zum 1.8.2024. In Deutschland umgesetzt in § 4 Abs. 3 Nr. 4–6 FuAG.

[602] Mithin handelt es sich um eine (behördlich ungeprüfte) Behauptung des Herstellers. Zur Wahrnehmung am Markt Lenz, Produkthaftung, 2. Aufl. 2022, § 8 Rn. 68 ff. Vgl. auch den Entwurf der Kommission zum Cyber Resilience Act vom 15.9.2022, COM(2022) 454

- Erreichen und Erhalten eines Risiko-basierenden angemessenen Sicherheitslevels und eines entsprechenden Umgangs mit Sicherheitslücken,
- Auslieferung ohne bekannte Sicherheitslücken,[604]
- Auslieferung mit sichereren Grundeinstellungen (secure by default) und Rücksetzmöglichkeit,[605]
- Vertraulichkeits- und Integritätsschutz von Daten während der gesamten Datenverarbeitung, -speicherung und -übermittlung,[606]
- die aussagekräftige und verständliche IT-sicherheitstechnische Dokumentation des Herstellers im Rahmen des vorgesehenen Einsatzzwecks insbesondere durch Aufzeichnung und Monitoring des Zugangs zu und der Modifikation von Daten,[607]
- Liste der verwendeten Software-Komponenten (Software Bill of Materials – SBOM) mit allen Abhängigkeiten,[608]
- Vornahme von regelmäßigen effektiven Sicherheits-Tests,
- die Implementierung einer Unternehmens-Richtlinie des Herstellers bzw. Händlers zur Meldung und zum Umgang mit Schwachstellen samt Veröffentlichung der Details nach Beseitigung (Coordinated Vulnerability Disclosure),[609]

---

final. Vgl. Dittrich/Heinelt RDi 2023, 309; Rennert ZfDR 2023, 206; Wiebe/Daelen EuZW 2023, 257; Voigt/Falk MMR 2023, 88 und kritisch Siglmüller ZfPC 2023, 221. Für die Bereichsausnahme für Open-Source-Software und Zielkonflikte beim Einsatz in kommerzieller Software Poncza/Keppeler/Lennartz ZfPC 2023, 117.

[603] Orientiert an den Anhängen 1 und 2 des Cyber Resilience Acts (CRA) in der Fassung des Vorschlags der EU-Kommission vom 15.9.2022, COM(2022) 454 final (Zustimmung des EU-Parlaments erfolgt, aber die finale Fassung liegt noch nicht vor, vgl. Meldung c't 08/2024, 46; zur Bereichsausnahme für Open Source vgl. Henning, Artikel vom 14.3.2024, abrufbar unter netzpolitik.org; abgerufen am 6.4.2024); ETSI/EN 303645 V2.1.1 (2020-06) und IT-Grundschutz-Kompendium Abschn. SYS.4.4, an Stallings in Vacca, Computer and Information Security Handbook, 2012, S. 339 ff. und am Code of Practice for Consumer IoT Security des Britischen Ministeriums für Digitales, Kultur, Medien & Sport vom Oktober 2018 (abrufbar unter gov.uk; abgerufen am 17.11.2023); ENISA, Good Practices for Security of IoT, November 2019 (abrufbar unter enisa.europa.eu; abgerufen am 17.11.2023); nicht berücksichtigt sind die Absicherung von Apps/Software etwa zur Steuerung und des nachgelagerten Backends (Cloud), zur Analyse dieser Mangel/Bicchi, Praktische Einführung ins Hardware Hacking, 2020, S. 217 ff.

[604] Vgl. Aigner/Gebeshuber/Hackner/Kania/Kloep/Kofler/Neugebauer/Widl/Zingsheim, Hacking & Security, 2018, S. 1039 ff.; Kizza S. 520 ff.; BSI, Technische Richtlinie-02102-1: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2023-01 (abrufbar unter bsi.bund.de; abgerufen am 17.11.2023).

[605] Vgl. NIST Special Publication 800-63B (abrufbar unter nist.gov; abgerufen am 17.11.2023); → Rn. 81 ff.

[606] Vornorm DIN SPEC 27072:2019-05, S. 9.

[607] Also Threat Modeling. Dabei geht es um Erwartungsmanagement bzgl. IT-Sicherheit und Datenschutz auf Verwender- und Nutzerseite und Informationspflichten des Herstellers bzgl. erwarteter Bedrohungsszenarien (Scope), des gewählten Schutzniveaus und (nicht) implementierter Schutzmaßnahmen.

[608] Vgl. Crossley, Software Supply Chain Security, 2024, Kap. 8.

[609] Vgl. ISO/IEC 29147:2018; IoT Security Foundation, Vulnerabilty Disclosure, Best Practice Guideline, Release 2.0, September 2021 (abrufbar unter iotsecurityfoundation.org; abgerufen am 17.11.2023); Silversten/Phillips/Paoli/Ciobanu, Economics of vulnerability disclosure, ENISA, Dezember 2018 (abrufbar unter enisa.europa.eu; abgerufen am 17.11.2023).

– die Implementierung eines Prozesses zur Meldung von Schwachstellen etwa durch Kunden und IT-Sicherheitsforscher zu deren Beseitigung bzw. zur Entwicklung und Bereitstellung (anderweitiger) Schutzmaßnahmen,[610]
– die Sicherstellung der kostenlosen Bereitstellung von Sicherheits-Updates ohne schuldhaftes Zögern bei möglichst automatischem Einspielen,[611]
– die Minimierung der Angriffsoberfläche (→ Rn. 113 ff.),[612]
– der Verzicht auf oder die Beschränkung der Erhebung von Daten auf das Nötigste (Datenminimierung),[613]
– Schutz der essenziellen Funktionen vor Angriffen, die auf den Ausfall gerichtet sind (denial of service), und Minimierung der Auswirkungen solcher auf andere Dienste und Systeme,[614]
– Mitteilung bis wann technischer Support und insbesondere Sicherheitsupdates bereitgestellt werden,
– eine einfache Möglichkeit zum sicheren Löschen der Nutzerdaten (insbesondere bei Außerbetriebnahme),[615]

Hinzu können etwa Pflichten zu **318**

– der Sicherstellung einer einfachen Installation und Konfiguration der sicherheitsrelevanten Parameter,[616]
– der Aufrechterhaltung und Dokumentation der notwendigen Umfänge der IT-sicherheitstechnischen Produktpflege,
– der Informationen über eine Mindestunterstützungsdauer mit Sicherheitsupdates,
– der rechtlichen und technischen Ermöglichung von Sicherheitsüberprüfungen durch Betreiber und Nutzer,[617]
– dem Umgang mit dem Produkt am Ende des Lebenszyklus (end of life),[618]
– der Validierung der vom Nutzer eingegebenen Daten[619] und

[610] ETSI/EN 303645 V2.1.1 (2020-06) Provision 5.2. Vgl. auch die Beiträge in Balaban et al., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, November 2021 (abrufbar unter sec4research.de; abgerufen am 17.11.2023); Kipker/Rockstroh ZRP 2022, 240; diverse, Chaos Computer Club, Hackbibel 3, 2024, S. 126.

[611] Macaulay, RIoT Control, 2016, S. 152 ff.

[612] Insbesondere die Deaktivierung von Fernwartungsschnittstellen im Auslieferzustand oder wenigstens deren erzwungene, geführte Konfiguration und Absicherung bei Erstinbetriebnahme. Vgl. für den industriellen Bereich Fallenbeck/Eckert in Vogel/Heuser/Bauernhansl/Hompel, Handbuch Industrie 4.0, Bd. 4, 2020, S. 144 ff.

[613] Insbesondere die Detektion zur Vermeidung der Entstehung von Bot-Netzen, vgl. Vacca, Computer and Information Security Handbook, 2012, S. 121 ff.

[614] Etwa gegen Stromausfall, DDoS-Attacken oder Unterbrechung der Netzwerkverbindung; vgl. Macaulay, RioT Control, 2016, S. 119 ff.

[615] Wichtig auch vor Versand zur Reparatur/Entsorgung/Verkauf/Verschenken. Zur Benutzbarkeit und Benutzerfreundlichkeit („einfach") im Sicherheitskontext vgl. Kriha/Schmitz, Sichere Systeme, 2009, S. 533 ff.

[616] Beispiel: Einrichtungsassistent/Handbuch mit Schritt-für-Schritt-Anleitung und Erklärung der Parameter. Keine Veränderung der Konfiguration anderer Geräte ohne Zustimmung des Nutzers, Vornorm DIN SPEC 27072:2019-05, S. 10 sowie zu Aspekten der Benutzerfreundlichkeit Margraf/Heinemann in Hornung/Schallbruch IT-SicherheitsR-HdB § 4 Rn. 5 ff.

[617] Vgl. Dickmann in Chaos Computer Club, Hackbibel 3, 2024, S. 102.

[618] Etwa Ermöglichung des Einspielens einer eigenen Firmware und deren Pflege durch die Community.

[619] Etwa um sicherheitsrelevante Fehlkonfigurationen oder Puffer-Überlauf-Attacken zu vermeiden.

– datenschutzkonformen Grundeinstellungen mit frühestmöglicher und transparenter Information des Nutzers über die Datenerhebung und -nutzung sowie Opt-Out-Möglichkeiten (Art. 5, 6, 12, 13, 21, 25, 32 DS-GVO; → Rn. 106 ff.)

treten.

319 Für den industriellen Bereich etwa zur Anlagen- und Prozesssteuerung kommen noch weitere Parameter hinzu, die je nach erwartbarem Bedrohungsszenario bei Schutzmaßnahmen auf Hard- und Software-Ebene berücksichtigt werden müssen.[620] Die Beachtung im konkreten Produkt kann insbes. zu Konflikten mit der geforderten Vielseitigkeit, Anpassbarkeit, Benutzerfreundlichkeit, Energieeffizienz und Performanz führen. Die Konkurrenzen sind im konkreten Einzelfall aufzulösen. Die Parameter IT-Sicherheit und Datenschutz sind bereits von Beginn der Produktentwicklung an einzuplanen, um etwa ausreichende Leistungs- und Speicherressourcen im Gerät zur Verfügung zu stellen und die Software[621] entsprechend konzeptionell auszurichten.[622]

320 Der ganzheitliche Betrachtungsansatz umfasst auch die **An- und Einbindung in IT-Infrastruktur.**[623] Bei einer **Cloudanbindung** etwa zur Steuerung im Fernzugriff sind auch die Absicherung dieser selbst und der Verbindungen zum Gerät etwa über Programmierschnittstellen, Apps und Software im Blick zu behalten und vertraglich einzufordern.[624] Unsichere Produkte sind bei entsprechenden Hauptleistungspflichten (partiell) fehlerhaft oder gar untauglich[625] und daher mangelhaft. Darlegungs- und beweispflichtig hinsichtlich des Mangels ist grundsätzlich der Käufer. Sind Sicherheitsmechanismen aber nicht dokumentiert und etwa über die Bedienoberfläche bzw. Programmierschnittstelle nicht konfigurierbar, genügt der Käufer mit entsprechendem Vortrag seiner primären Darlegungspflicht insbes., wenn der Quellcode nicht offen vorliegt. Es gibt per se keine Vermutung dahingehend, dass ein Produkt verein-

[620] Beispiele: Absicherung gegen physikalische Manipulation und ungewollte Hardware-Veränderungen, Manipulation von Programmabläufen und Speichervorgängen durch Fehlereinstreuung mittels kurzer Unterbrechung der Stromversorgung (Glitching); Rückschlüsse auf Passworte/Schlüssel durch Analyse der Stromkonsumption; Ausfall bei zeitkritischen Systemen (Echtzeit-Backup/Redundanz) sowie gegen Manipulation von Datensätzen, zeitkritisches und beweissicheres Logging, Absicherung der Maschine-zu-Maschine Kommunikation, vgl. O'Flynn/van Woudenberg, The Hardware Hacking Handbook, 2021, S. 401 ff.; Fallenbeck/Eckert in Vogel/Heuser/Bauernhansl/Hompel, Handbuch Industrie 4.0, Bd. 4, 2020, S. 136 und zur Cloud-Absicherung, S. 139 ff.; zur Absicherung nach IEC 62443 Kienzle/Glemser iX 9/2019, 58.

[621] Vgl. hierzu die Auflistung unter thedigitalstandard.org (zuletzt abgerufen am 29.3.2019) aus Sicht eines Sicherheits- und Datenschutz-Tests von Software nach deren Inverkehrbringen. Es werden auch das dahinterstehende Geschäfts- und Datennutzungsmodell adressiert.

[622] Fallenbeck/Eckert in Vogel/Heuser/Bauernhansl/Hompel, Handbuch Industrie 4.0, Bd. 4, 2020, S. 138.

[623] Für Verträge mit der Öffentlichen Hand vgl. den Basisvertrag EVB-IT-Cloud (abrufbar unter cio.bund.de; abgerufen am 17.11.2023) mit Verweisen auf diverse Sicherheitsstandards in Nr. 6.2 EVB-IT Cloud-AGB und im Vertragsmuster.

[624] Macaulay, RIoT Control, 2016, S. 49 ff. Zur rechtlichen Risikoverteilung bei gemeinsamer Verantwortung Schultz/Sarre CR 2022, 281.

[625] Etwa wirkungslose Konfigurationsmöglichkeiten zum Abschalten von (unsicheren) Schnittstellen, wirkungslose Virenschutz- oder Datenverkehrsfilter.

barte[626] IT-Schutzmechanismen aufweist, solche ordnungsgemäß implementiert und im Auslieferzustand vorkonfiguriert sind. Für alle diese Punkte und ein etwaiges übergreifendes Sicherheitskonzept (→ Rn. 148 f.) ist dann der Verkäufer darlegungs- und beweispflichtig. Umfängliche Überprüfbarkeit ist nur bei Offenlegung des Quellcodes und lückenloser **transparenter Versionierung (Reproducible Builds)**[627] bei der Weiterentwicklung gegeben. Dies wäre der Idealfall, welcher aktuell (noch) sehr selten anzutreffen ist.

Die **Inbezugnahme von Technischen Normen und Zertifikaten**[628] ersetzt **321**
nicht die Auseinandersetzung mit deren konkreten Inhalten, also insbes. mit dem, was im Zertifizierungsverfahren tatsächlich[629] wie und woran getestet und bescheinigt wurde.[630] Werden allein Prozesse zB der Konstruktion, Produktion, des Qualitäts- oder Sicherheitsmanagements geprüft, bedeutet dies, wenn das konkrete Produkt in den Anwendungsbereich fällt, nicht mehr als ein Indiz.[631] Gewichtiger können Zertifizierungen der Eigenschaften eines bestimmten Produkts etwa nach technischen Richtlinien einzuschätzen sein.[632] Eine Zertifizierung gilt jedoch nur für die benannten Versionen[633] des Produkts und Prüfumfänge innerhalb der ausgewiesenen Laufzeit.[634] Dies beschränkt den Wert von Zertifizierungen insbes. im Bereich dynamischer Softwareentwicklung.[635] Speziell für die IT-Sicherheit haben sich noch keine (Quasi-)Standards ausgeprägt.[636] Angebotene Zertifizierungen sind zudem regelmä-

[626] Bezüglich der Vereinbarung und ihres Inhalts ist derjenige beweispflichtig, der sich jeweils darauf beruft.

[627] Fortlaufende Dokumentation und Reproduzierbarkeit der Veränderungen am Quellcode wie etwa für den Sprung von Version 1.0 auf 1.1.

[628] Etwa die Zertifizierung von Produkten oder Systemen nach den Common Criteria (ISO/IEC 15408). Der Hersteller definiert die gewünschte Funktionalität und Vertrauenswürdigkeit des Produkts nach einem vorgegebenen Schema (Security Target). Ob die Zielgrößen für beides eingehalten werden, wird in einem festgelegten Prozess bei ebenfalls vorab zu wählenden sieben unterschiedlichen Prüftiefen sehr formal ermittelt, vgl. Bishop, Computer Security, 2003, Kap. 21.8; Eckert, IT-Sicherheit, 10. Aufl. 2018, S. 222 ff. Die Zahl der bislang vom BSI erteilten Zertifikate ist überschaubar, wobei es sich durchweg um Spezialprodukte handelt, vgl. BSI, Zertifizierung von Produkten, Stand 18.12.2022 (abrufbar unter bsi.bund.de; abgerufen am 17.11.2023). Für industrielle Kommunikationsnetzte sei auf die IEC 62443 verwiesen, vgl. dazu Kienzle/Glemser iX 9/2019, 58. Kritisch zu Recht insgesamt Anderson, Security Engineering, 3. Aufl. 2021, S. 1032 ff.

[629] Zur Haftung von Zertifizierungsstellen und den kritikwürdigen Enthaftungstendenzen in der deutschen Rspr. Wagner in MüKoBGB BGB § 823 Rn. 803 ff.; BGH JA 2020, 545 mit kritischer Anm. Hager.

[630] Häufig werden etwa bei Software nur bestimmte Versionen zertifiziert. Neue Versionen, Updates und Patches unterliegen dann dem Zertifikat im Zweifel nicht mehr; vgl. auch Spindler, Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären (IT-Studie), 2007, Rn. 18 und Rn. 145 ff.

[631] Spindler IT-Studie Rn. 185 f.

[632] Vgl. zB die Technischen Richtlinien und die aktuellen Zertifizierungen des BSI, jeweils abrufbar unter bsi.bund.de.

[633] Meist Firmware-Versionen.

[634] Vgl. für die technischen Konsequenzen einer Common Criteria-Zertifizierung im Bereich der Medizin-Telematik hinsichtlich identifizierbarer Schwachstellen in Software-Modulen Maus c't 3/2020, 14.

[635] Skierka in Hornung/Schallbruch IT-SicherheitsR-HdB § 8 Rn. 108 S. 179.

[636] Im Überblick Skierka in Hornung/Schallbruch IT-SicherheitsR-HdB § 8 Rn. 8 ff. S. 156 ff.

ßig nicht gesetzlich verpflichtend[637] und ihre Marktdurchdringung außerhalb regulierter Branchen daher meist (noch) gering.[638] Schließlich verbleibt das Risiko fehlerhafter Zertifizierungen und deren drittschützende Wirkung samt möglicher Haftung der Zertifizierungsstellen.[639] Bislang haben Zertifizierungen nur in Nischen Verbreitung gefunden. Zukünftig können (freiwillige und noch zu entwickelnde) Zertifizierungen von Produkten nach dem EU-Cybersecurity Act[640] und deren Referenzieren in Ausschreibungen an Gewicht gewinnen. Zudem können **Konformitätsanforderungen im Produktsicherheitsrecht** etwa zum Anbringen des CE-Kennzeichens die Erwartungen des Marktes prägen und diese zu einem Mindestschutzniveau werden lassen.[641]

322 **(8) Einbindung in Netzwerke.** Haftungsträchtig sind **Schwachstellen der Cloud-Infrastruktur von Hersteller oder Verkäufer,**[642] die für eine Inbetriebnahme[643] oder die Nutzung bestimmter Funktionen[644] des Produkts benötigt werden.[645] Fehlerrisiken birgt schon die sichere Einrichtung samt Passwortvergabe und sicherem Zugang.[646] Wird Cloud-Infrastruktur von Zulieferern gestellt und mittels konfektionierten Apps und Geräte-Firmware zum Betrieb von Produkten unter eigener Marke verwendet, ergeben sich Haftungsrisiken für den Verkäufer insbes. wegen Datenschutzverletzungen und drohendem Datenabfluss zB durch den nicht autorisierten Verkauf von Datensätzen seitens des Zulieferers.[647] Gegenüber dem Käufer tritt nämlich regelmäßig[648] allein der Verkäufer als (Daten-

[637] Vgl. die BSI TR-03148: Sichere Breitband Router, Version 1.2 vom 16.1.2023 (abrufbar unter bsi.bund.de; abgerufen am 17.11.2023) und die zu Recht kritische Stellungnahme des Chaos Computer Clubs vom 19.11.2018 (zur ursprünglichen Version der TR; abrufbar unter ccc.de; abgerufen am 17.11.2023).

[638] Zu spezifischen Regelungen Skierka in Hornung/Schallbruch IT-SicherheitsR-HdB § 8 S. 174 f.

[639] Vgl. hierzu Rott, Certification – Trust, Accountability, Liability, 2019, S. 203 ff.

[640] VO (EU) 2019/881 (CSA), vgl. insbes. Art. 8. KMU wurden nach Erwgr. 2 explizit in den Schutzbereich aufgenommen. Die Freiwilligkeit wird stark betont (vgl. Erwgr. 50, 91 und 92).

[641] Vgl. Dickmann ICLR 4 (2023), 21.

[642] Von diesen selbst oder für diese durch Dienstleister betrieben. Zur Abgrenzung der Sphären aus Sicht des Kunden Regenfus JZ 2018, 79 (81), allerdings mit problematischem Verständnis des Pflichtenkreises des Verkäufers. Zur Drittschadensliquidation Riehm VersR 2019, 714 (717).

[643] Beispiel: Aktivierungsserver.

[644] Beispiele: Server zum Synchronisieren, zur Datenspeicherung/-präsentation oder Fernbedienung eines Geräts per Web-Login oder App.

[645] Vgl. hierzu Solmecke/Vodrik MMR 2013, 755.

[646] Vgl. für den unzureichenden Schutz bei Kundenportalen Wiegenstein, ix 2018, 74 sowie bereits Mankowski in Ernst, Hacker, Cracker & Computerviren, 2004, Rn. 488 ff.; zu datenschutzwidrigen Voreinstellungen LG Berlin MMR 2018, 329 mAnm Heldt (Facebook); KG ZD 2018, 118 sowie nachfolgend EuGH NJW 2022, 1740; BGH GRUR 2023, 193.

[647] Vgl. den Vortrag von Steigerwald, Smart Home – Smart Hacks, Vortrag auf dem 35C3 vom 28.12.2018 (abrufbar unter ccc.de/; abgerufen am 17.11.2023). Besonders problematisch erscheint die erzwungene Aktivierung über die Hersteller-Cloud, wenn dies wie auch die Erfassung von personenbezogenen Daten technisch eigentlich unnötig ist und die Steuerung auch lokal via Direktverbindung der App mit dem Gerät erfolgen könnte.

[648] Bei (bloßen) Verweisen auf Dritte: Die Rolle des Verantwortlichen steht nicht zur (Partei-)Disposition, sondern richtet sich nach den Merkmalen des Art. 4 Nr. 7 DS-GVO (insbes. die Entscheidungsgewalt über Zweck und Mittel der Verarbeitung). Für gemeinsam