Zeitschrift für die gesamte Versicherungswissenschaft, 112 (2023) 3: 225 – 236
https://doi.org/10.3790/zverswiss.2023.1428301

IT-Schwachstellenmanagement in der Cyberversicherung

Roman Dickmann

Zusammenfassung

Der Beitrag befasst sich eingangs mit dem Begriff der IT-Sicherheit im Allgemeinen und in den Musterbedingungen der Cyberversicherung. Da absolute Sicherheit nicht zu erreichen ist, bedarf es der Definition eines (Mindest-)Sicherheitsniveaus, dem es sich kontinuierlich anzunähern gilt. Gesetzlich ist ein solches noch nicht festgelegt. Vielmehr haben unsichere Grundlagentechnologien und schlechte Quellcode-Qualität zum aktuellen Stand an IT-Unsicherheit geführt. Daran könnte sich nun durch neue Impulse aus dem Produktsicherheitsrecht mit dem Erfordernis eines Schwachstellenmanagements zum Anbringen des CE-Kennzeichens etwas ändern. Kernelement ist dabei der Umgang mit gemeldeten Schwachstellen und deren Beseitigung. Hierdurch könnte sich ein Sockel an IT-Sicherheit insbesondere im Internet der Dinge ergeben, was auch der Stabilisierung des Produkts Cyberversicherung dienen würde.

Abstract

This article begins by looking at the concept of IT security in general and in the standard terms and conditions of cyber insurance. As absolute security cannot be achieved, it is necessary to define a (minimum) security level that must be continuously approached. This has not yet been legally defined. Rather, insecure basic technologies and poor source code quality have led to the current level of IT insecurity. This could now change as a result of new impetus from product safety regulation with the requirement for vulnerability management in order to affix the CE mark. The core element here is the handling of reported vulnerabilities and their elimination. This could provide a baseline of IT security, particularly in the Internet of Things, which would also serve to stabilise the cyber insurance product.

Roman Dickmann, Rechtsanwalt und Fachanwalt für Versicherungsrecht, Europajurist (Univ. Würzburg), LL.M. (VersR, Univ. Münster)
Der Beitrag ist die schriftliche, ausführlichere Fassung eines halbstündigen Vortrags, den der Autor am 12.10.2023 auf dem 5. Cyberversicherungstag des DVfVW in Kooperation mit der Freien Universität Berlin dort gehalten hat. Dieser Beitrag gibt allein die Meinung des Autors wieder und nicht die seines Arbeitgebers.

Duncker & Humblot · Berlin

IT-Sicherheit ist ein zentraler Begriff in der Cyberversicherung.[1] Doch eine Definition findet sich in den Bedingungswerken nicht. Es handelt sich um einen technisch auszufüllenden Begriff.

Allgemein bezeichnet Sicherheit einen Zustand frei von unvertretbaren Risiken, wobei es absolute Sicherheit nicht gibt.[2] Im Englischen als dominanter Fach- und Brückensprache der IT wird zwischen „Safety" und „Security" unterschieden.[3] Ersteres meint die physikalische Sicherheit also etwa den Schutz vor mechanischen Gefahren, Brand, Explosion oder einem Stromschlag. Security betrifft die Protektion vor vom Hersteller bzw. Betreiber nicht beabsichtigten An- bzw. Eingriffen und deren Folgen. Zu den zum Schutz vor letzteren eingesetzten Technologien in Hard- und Software besteht kein einheitliches Verständnis.[4] Definitionen technischer Begriffe beinhalten bestenfalls einen Minimalkonsens, schlimmstenfalls eine Verkettung interpretationsbedürftiger Marketingausdrücke. Die Diskussion darüber, was etwa unter „Military Grade Encryption" zu verstehen sein soll, führt am Ende zur Feststellung einer nicht auflösbaren Unklarheit.[5] Jedenfalls wäre sich nachgehend bewusst zu machen, was man überhaupt schützen will. In A1–2.1 der Musterbedingungen des GDV für die Cyberversicherung (AVB Cyber)[6] werden als Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit genannt.[7] Dieser Katalog könnte noch um Authentizität, Zuverlässigkeit und Verbindlichkeit erweitert werden.[8] Das Erreichen der Ziele kann man statisch über eine Momentaufnahme des Ist-Zustands oder dynamisch als kontinuierliche Prüfung der asymptotischen Annäherung an ein (ständig anzupassendes) Zielniveau feststellen. Wichtigste Antagonisten der IT-Sicherheit sind Schwachstellen (auch Sicherheitslücken genannt).[9]

---

[1] Vgl. *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, 2023, S. 5 ff., https://doi.org/10.25353/ubtr-xxxx-8597-6cb4.

[2] Vgl. etwa *Krcmar*, Einführung in das Informationsmanagement, 2. Aufl. 2014, S. 159; Schnieder/Schnieder, in: Winzer/Schnieder/Bach, Sicherheitsforschung, 2010, S. 102.

[3] Vgl. *Eckert*, IT-Sicherheit, 10. Aufl. 2018, S. 6 f.

[4] Vgl. zu den Missverständnissen bzgl. grundlegender Begriffe der IT-Sicherheit *Spafford/Metcalf/Dykstra*, Cybersecurity – Myths and Misconceptions, 2023, S. 2 ff.

[5] Vgl. *Akgul/Abu-Salma/Bai/Redmiles/Mazurek/Ur*, From „Secure" to „Military-Grade": Exploring the Effect of App Descriptions on User Perceptions of Secure Messaging, in: Workshop on Privacy in the Electronic Society (WPES) ACM 2021, S. 119, https://doi.org/10.1145/3463676.3485602.

[6] Vom GDV als Cyberrisikoversicherung bezeichnet. Allgemeine Versicherungsbedingungen mit Stand April 2017, abrufbar unter https://gdv.de.

[7] Vgl. *Bruck/Möller*, VVG, 10. Aufl. 2023, Band 5, Vorb. AVB Cyber, S. 1475 ff.; *Lesser*, Haftungsprobleme und Versicherungslösungen bei Cyber-Risiken, Diss. 2021, S. 209 ff.

[8] Zu Definitionen siehe *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, 2023, S. 5 f., https://doi.org/10.25353/ubtr-xxxx-8597-6cb4.

[9] Zum technischen Hintergrund von Schwachstellen *Dickmann/Vettermann*, MMR 2022, 740; *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicher-

In der Cyberversicherung wird die Informationssicherheitsverletzung über die Nichterreichung der Schutzziele definiert. Es handelt sich also um eine Negativabgrenzung zum nicht definierten Idealzustand. Was aber sollen Informationssicherheit und (weiter gefasst) IT-Sicherheit positiv im versicherungsvertraglichen Zusammenhang bedeuten? Da absolute Sicherheit in der Praxis nicht zu erlangen ist, bleibt nur das Erreichen eines zu vereinbarenden (Mindest-)IT-Sicherheitsniveaus und ggf. die Verpflichtung zu dessen Einhaltung über die Vertragslaufzeit.[10] Ein solches Zielniveau ist als Vorgabe des Versicherers von diesem zu erarbeiten und im Rahmen von Verhandlungen mit potenziellen Kunden vorzustellen.[11] Differenziert werden kann etwa nach Branchen, bestimmten Unternehmensgrößen oder der Datengetriebenheit des Geschäftsmodells.[12]

Ein gesetzlich fixiertes und in der Praxis etabliertes Mindest-IT-Sicherheitsniveau bei Betrieb bzw. Benutzung durch Unternehmen und Verbraucher, aber auch für Gestaltung von Produkten mit IT-Funktionalitäten gibt es bislang nicht.[13] Eine Festlegung kann deshalb nur im Rahmen der vertraglichen Disposition der Parteien erfolgen. Risikofragen des Versicherers erfassen nur den Stand zum Zeitpunkt der Beantwortung.[14] Sie laufen damit auf die Beschreibung eines statischen Zustands hinaus. Mittels vertraglicher Obliegenheiten kann eine Dynamisierung während der Laufzeit des Versicherungsvertrags erreicht werden. Dabei kommt es jedoch, wie bei den Risikofragen, auf eine technisch präzise Formulierung an. Eine „Software auf dem aktuellen Stand" kann auch eine solche mit dem Stand der letzten vom Hersteller herausgegebenen Version sein, auch wenn diese Jahre alt ist und nicht (mehr) mit Sicherheitsupdates versorgt wird. Anders sieht es hingegen für eine „vom Hersteller derzeit sicherheitstechnisch unterstützte Software auf dem aktuellen Stand" aus, also eine solche, die gegenwärtig mit Sicherheitsupdates versorgt wird.

Ob das anvisierte Sicherheitsniveau tatsächlich erreicht wird, ist schwierig nachzuweisen. Oft bleibt es bei einem Bemühen mit teilweiser Umsetzung erforderlicher Maßnahmen. Zertifizierungen weisen meist nur das Einhalten von

---

heitslücken, 2023, S. 1 ff., https://doi.org/10.25353/ubtr-xxxx-8597-6cb4. Zur rechtlichen Auslegung in § 7 BSIG *Kipker*, MMR 2023, 93.

[10] Vgl. *Andress*, Foundations of Information Security, 2019, S. 2 ff. Vgl. zur Definition in § 2 Abs. 2 BSIG *Ritter*, in: Kipker/Reusch/Ritter, Recht der Informationssicherheit, 2023, BSIG § 2 Rn. 5 ff.

[11] Nur bei Großrisiken kann es ggf. so sein, dass der mögliche VN sein aktuelles Sicherheitsniveau präsentiert und darauf Angebote von VR abgegeben werden.

[12] Vgl. aus US-Sicht die Beiträge zu den verschiedenen Branchen, in: Godfrey/Menapace/Reed/Schiffer, A practical Guide to Cyber Insurance for Businesses, 2022, S. 183 ff.

[13] Siehe aber sogleich zur neueren EU-Gesetzgebung.

[14] Vgl. LG Tübingen, r+s 2023, 652 m. Anm. Fortmann. Zur grob fahrlässigen Herbeiführung des Versicherungsfalls Höld VersR 2023, 353.

Prozessvorgaben zum Auditzeitpunkt aus. Ob diese fehlerfrei und wirksam umgesetzt sind und damit ein entsprechend sicherer IT-Betrieb im konkreten Einzelfall besteht, bleibt unbeleuchtet. Hier könnten (zukünftig) kontinuierliche Audits zur Umsetzung und aussagekräftige Kennzahlen helfen. Zu ersterem fehlt aktuell häufig die Bereitschaft auf Seiten der Versicherungsnehmerinnen und letztere wurden noch keine entwickelt, die sich in der Praxis bewährt haben. Die Historie der Cyberversicherung spiegelt die zunehmende IT-Unsicherheit bei vermehrten technischen Abhängigkeiten.[15]

Als die IT auf breiterer Front ab den späten 1960er-Jahren verstärkt Eingang in (damals) weniger IT-affine Branchen fand, sprach man auf Seiten der etablierten Nutzer von einer „Softwarekrise", weil es sich bei zunehmender Komplexität als immer schwerer herausstellte benutzbare und verlässlich lauffähige Versionen zu erstellen.[16] Die Krise besteht bis heute fort und hat sich insbesondere durch immer kürzere Entwicklungsintervalle und das Aufsetzen auf bzw. Inkorporieren von Softwarebibliotheken Dritter noch verschärft.[17] Das resultierende niedrige Qualitätsniveau blieb in der pre-Internet-Zeit ein eher isoliertes Problem konkreter Nutzerkreise. Für Außenstehende waren die Implikationen wenig greifbar. Kein Wunder ist es daher, dass für die Versicherungswirtschaft der Schutz der Hardware als Sachwert, die man leaste oder für deren Nutzung man die Rechenzeit (Time Sharing) bezahlte, im Fokus stand. In Deutschland wurden in der Sparte der technischen Versicherungen Nischenprodukte auch für den aufkommenden Datenschutz entwickelt.[18] Diese setzten sich in der Wirtschaft nicht durch. Bis Ende der 1980er-Jahre blieben hinsichtlich der Gefahren der Nutzung der IT Innentäter aus dem nutzenden Unternehmen das wahrgenommene Hauptrisiko.[19] Abgedeckt wurde letzteres über Vertrauensschadenversicherungen mit Zusatzbausteinen.[20] In den USA gab es ab den 1990er-Jahren mit dem Aufkommen des Internets und dortiger Verkaufsaktivi-

---

[15] Zur Geschichte aus deutscher Sicht rudimentär *Koch*, in: Bruck/Möller, VVG, 10. Aufl. 2023, Band 5, Vorb. AVB Cyber, S. 1463 ff.

[16] Vgl. *Dykstra*, Communications of the ACM, Band 15, Nr. 10, 1972, S. 859; *Ensmenger/Aspray*, in: Hashagen/Kell-Slawik/Norberg, History of Computing: Software Issues, Int. Conference from 05.–07.04.2000, 2013, S. 139 ff.

[17] Vgl. *Schneier*, Secret & Lies, 15th Anniversary Edition 2015, S. 161 f.; *Fretheim/Deschene*, Secure Software Systems, 2023, S. 230; zu Angriffen auf die Softwarelieferkette *Plate/Fischer*, iX 10/2022, 44; Kaps iX 3/2023, 90.

[18] Etwa eine Datenschutzhaftpflichtversicherung ab den 1970er-Jahren, vgl. *Breuer*, VW 1988, 356. Zur Geschichte des Datenschutzes *Pohle*, Datenschutz und Technikgestaltung, Diss. 2018, S. 31 ff., abrufbar unter https://edoc.hu-berlin.de/.

[19] Begrenzten Schutz gewährte die Computer-Missbrauch-Versicherung, vgl. *Heidinger*, Die Computer-Missbrauch-Versicherung, 1986; *v. Heyden*, in: Seuß, Richtig versichern, 1980, S. 201; *Ihlas*, VersR 1994, 898.

[20] Vgl. *Meyer-Rassow/Schildmann*, Technische Versicherungen, 1990, S. 47 ff.; *Mikosch*, Industrie-Versicherungen, 1991, S. 109 ff.

täten (E-Commerce) erste Versicherungslösungen, die auch Eigenkosten der Versicherungsnehmer etwa für das Wiederherstellen von Systemen oder die Abwehr von Bußgeldern einschlossen. In Europa fand dies wenig Echo.[21] In Deutschland boten einige internationale Versicherer entsprechende Policen an. In den Bedingungen zur Betriebshaftpflichtversicherung fand der wenig praxisrelevante Einschluss des IT-Nutzer-Haftpflicht-Risikos vor allem akademische Beachtung.[22] Erst mit der zunehmenden Digitalisierung von Kernarbeitsprozessen auch in Deutschland ab den 2010er-Jahren und vor allem des Aufkommens von Erpressung mittels Ransomware änderte sich dies.[23] Cyberversicherungen mit sehr unterschiedlichen Deckungsumfängen nahmen sich vor allem der Kreise Forensik-Kosten und Betriebsunterbrechungsschäden an. Mit der DS-GVO[24] und der vor allem europarechtlich verstärkten Regulierung zur IT-Sicherheit wird sich der Fokus bald wohl auch auf Haftpflichtrisiken und den entsprechenden Baustein in der Cyberversicherung erstrecken. Eine flächendeckende Verbreitung als essenzielle Deckung wie Sach- und Betriebshaftpflichtpolicen für Unternehmen, die allesamt der Digitalisierung nicht entgehen können, hat die Cyberversicherung bislang nicht gefunden. Neben sparten- und produktimmanenten Problemen und Unsicherheiten etwa zu Deckungsumfängen, belastbaren Schadenzahlen oder Marktkapazitäten führt eine nicht mehr nur von Fachleuten angeprangerte flächendeckende IT-Unsicherheit zu einem immer bedrohlicher wirkenden Ist-Zustand für alle Betreiber und Nutzer.

Eine durchdringende Ungewissheit ergibt sich aus lange fehlenden Standards bei der Ausbildung von Programmiererinnen und dem Schreiben von Quellcode.[25] Zwar ist unstreitig, dass für Quellcode Fehlerfreiheit nicht garantiert werden kann. Dies rechtfertigt aber nicht das mithin sehr niedrige Qualitäts-

---

21 Vgl. *Grzebiela*, Internet-Risiken, 2002, S. 102 ff.

22 Vgl. etwa *Koch*, r+s 2005, 182.

23 Vgl. *Pache*, Kompass Cyberversicherung, 2023, S. 45, der die Marktentstehung in der BRD ohne weitere Nachweise auf 2015 datiert; sowie *Choudhry*, Der Cyber-Versicherungsmarkt in Deutschland, 2014, S. 5 ff.; *Heidemann/Flagmeier*, Sonderheft: Cyberversicherungen, 5. Aufl. 2020, S. 1 ff.; *Baban/Barker/Gruchmann/Paun/Peters/Stuchtey*, Cyberversicherungen als Beitrag zum IT-Risikomanagement, Studie 2017, S. 17 ff., abrufbar unter https://bigs-potsdam.org. Für den ggf. im Entstehen befindlichen Markt im Verbraucherbereich *Fortmann*, Verbraucher-Cyberversicherung, 2022, S. 140, 301 ff.

24 Zur Entstehung sei der Dokumentarfilm *Bernet*, Democracy – Im Rausch der Daten, 2015, abrufbar unter https://bpb.de empfohlen.

25 Vgl. *Schumacher*, Magdeburger Journal zur Sicherheitsforschung 2014, 457. Zu den IT-Sicherheits-Inhalten der Ausbildung zur Fachinformatikerin Kersken, IT-Handbuch für Fachinformatiker*innen, 11. Aufl. 2023, S. 1293 ff. (letztes Kapitel) mit gesetzlicher Grundlage in der FIAusbV v. 28.02.2020, BGBl. I S. 250. Bei Einführung des Berufsbilds mit der ITKTAusbV v. 10.07.1997, BGBl. I S. 1741, war IT-Sicherheit noch kein explizit genannter Ausbildungsinhalt.

niveau bei der Erstellung und Pflege von Software.[26] Gründe sind neben fehlender bzw. unzureichender sicherheitstechnischer Aus- und Fortbildung etwa unsichere Grundlagentechnik, Design- und Implementierungsdefizite, ausbleibende oder zu geringe Testumfänge, unsichere Grundkonfigurationen im Auslieferzustand sowie fehlende Updatemöglichkeiten und Produktpflege. Auch voraus- bzw. nachgehende Faktoren wie unzureichende Fehler-/Sicherheitskultur, überfordernde Überkomplexität von Projekten, unangemessener Zeitdruck in der Entwicklung und fehlende IT-Sicherheits-Hygiene tragen zum Verbleib auf niedrigem Niveau bei.

An der Wurzel werden die Probleme nicht angepackt.[27] Vielmehr wurde auf nachgehende Korrekturen gesetzt. Als Beispiele sind etwa Audits zu nennen, die aber Code (soweit er überhaupt zugänglich ist) nur punktuell zum aktuellen Entwicklungsstand und mit ggf. eingeschränkten Prüfumfängen inspizieren. Häufig kann dabei nicht auf eine umfassende Dokumentation zurückgegriffen werden, die etwa Designentscheidungen der Programmiererinnen transparent macht.[28] Schließlich stellt sich noch die Frage, ob hinsichtlich der IT-Sicherheit von den Beteiligten mit der richtigen Einstellung und realistischen Erwartungen in das Audit gegangen wird. Wie ein Angreifer zu denken, ohne sich an Nutzungskonventionen zu halten, ist keine leichte Aufgabe, insbesondere, wenn man auf der Herstellerseite steht. Es geht schließlich im Kern um die Detektion von Schwachstellen, also die Ausnutzung von Funktionen, aber vor allem von Programmierfehlern entgegen der Intention der Ersteller. Ziel der An- bzw. Eingreifenden ist es vornehmlich Nutzerrechte zu erhöhen oder unberechtigten Zugriff auf Daten zu erlangen. IT-Unsicherheit speist sich vor allem aus Schwachstellen.[29] Für den Handel mit ihnen ist ein globaler Markt entstanden. Dieser reicht von Informationen über schon jahrelang bekannte Lücken in (nicht mehr) gepflegter Software, die teilweise schon bei Inverkehrbringen irreparabel bestanden, bis zu solchen in aktuell vom Hersteller unterstützten Titeln, die ihm und der Öffentlichkeit bislang nicht bekannt geworden sind (Zero Days).[30]

---

[26] Vgl. *Schneier*, Blogeintrag vom 18.01.2007, abrufbar unter https://schneier.com; *Vaughan-Nichols*, ZDNET Tech/Security vom 18.07.2019, abrufbar unter https://zdnet.com.

[27] Zu den diesbezüglichen Missverständnissen *Spafford/Metcalf/Dykstra*, Cybersecurity – Myths and Misconceptions, 2023, S. 214 ff.; *v. Leitner*, Antipatterns und Missverständnisse in der Softwareentwicklung, Vortrag auf dem 34C3 am 29.12.2017, abrufbar unter https://media.ccc.de.

[28] Vgl. den Vortrag von v. Leitner, Das nützlich-unbedenklich Spektrum, Vortrag auf dem 36C3 am 28.12.2019, abrufbar unter https://media.ccc.de.

[29] Zu diesen *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, 2023, S. 1 ff., https://doi.org/10.25353/ubtr-xxxx-8597-6cb4.

[30] Vgl. *Dickmann/Vettermann*, MMR 2022, 740.

Auch Software, die vermeintlich die Sicherheit erhöhen soll, ist vor diesen Fehlern nicht gefeit.

Der Markt für IT-Unsicherheit floriert mit einem Wachstum an nachgewiesener Schadsoftware.[31] Insbesondere im Bereich der Ransomware hat das organisierte Verbrechen Affiliate-Strukturen errichtet.[32] Arbeitsteilung findet von der Softwareentwicklung über die Infektion der Opfer bis zur Abwicklung der Erpressung mehrstufig statt.[33] Die teilweise wie mittelständische Unternehmen organisierten Zusammenschlüsse der Täter suchen selbst nach Schwachstellen und nutzen diese (meist verkettet mit weiteren) zum Eindringen in fremde Systeme aus. Schlimmstenfalls führt dies zum Kontrollverlust über ganze Netzwerke. Aber auch staatliche Stellen fragen Sicherheitslücken etwa zur Erstellung von Trojanern für den Einsatz bei Polizei, Militär und Nachrichtendiensten nach oder bedienen sich Dienstleistern.[34] Doch insbesondere die Verwaltung als IT-Nutzerin bzw. Betreiberin kann selbst Opfer einer Ransomware-Attacke werden.[35]

Bislang hat sich kein Sockel an IT-Sicherheit entwickelt, auf dessen Erreichen man sich bei Produkten und deren Betrieb verlassen kann. Blickt man in die Historie der Feuerversicherung, hat sich dort nach den Stadtbränden und den zunehmenden (Explosions-)Gefahren der Industrialisierung ein hohes vorbeugendes und abwehrendes Brandschutzniveau etabliert.[36] Maßnahmen zur Erreichung waren etwa Mindestanforderungen an die Feuerwiderstandskraft von Baumaterialien, Bauordnungsrecht und Brand(nach)schau. Feuerversicherungen setzten Anreize etwa über die Förderung der Anschaffung von Feuerlöschgeräten. Jedoch ging es vordringlich um die Minimierung der Risiken der nur

[31] Vgl. *Anderson*, Security Engineering, 3. Aufl. 2020, S. 293 ff.; *Perlroth*, This is how they tell me the world ends, 2021. Zu üblichen Fehleinschätzungen bzgl. Malware *Spafford/Metcalf/Dykstra*, Cybersecurity – Myths and Misconceptions, 2023, S. 244 ff.

[32] Vgl. zuletzt *Schmidt*, c't 26/2023, 80.

[33] Vgl. *Anderson*, Security Engineering, 3. Aufl. 2020, S. 41 ff.

[34] Mit erheblichem Missbrauchspotenzial. Vgl. zur journalistischen Recherche zum Pegasus-Komplex *Richard/Rigaud*, Die Akte Pegasus, 2023. Für eine EU-weite Analyse *Marzocchi/Mazzini*, Pegasus and surveillance spyware, PE 732.268 – Mai 2022. Zu den Empfehlungen des Europäischen Parlaments vom 15.07.2023 nach dem Pegasus-Untersuchungsausschuss Dokument P9_TA(2023)0244, jeweils abrufbar unter https://www.europarl.europa.eu/.

[35] Vgl. *Dickmann/Vettermann*, MMR 2022, 852. Praxisbeispiele sind etwa die Malware-Infektion im Landkreis Anhalt-Bitterfeld, dazu *Kannenberg*, heise online vom 09.07.2021, abrufbar unter https://heise.de, oder der Angriff auf das Kammergericht Berlin, dazu *Heidtmann/Hurtz*, Süddeutsche Zeitung Digital vom 28.01.2020, abrufbar unter https://sueddeutsche.de.

[36] Vgl. Koch, Geschichte der Versicherungswirtschaft in Deutschland, 2012, S. 7, 42 ff., 105 ff.

begrenzt kontrollierbaren Naturgewalt Feuer, wohingegen es im Bereich Cyber vor allem um den Schutz vor Ein- und Angreifern geht.

In der Cyberversicherung ergeben sich Probleme unter anderem bei der Risikoauswahl (Adverse Selection), durch fehlende Anreize zur Verbesserung der IT-Sicherheit auf Versicherungsnehmer-Seite (Moral Hazard) und der Deckungsbegrenzung mit Blick auf massenhaft auftretende gleichartige Schäden (Kumul).[37] Auf diese wurde von Seiten der Versicherer vor allem mit Risikoausschlüssen, Sublimits und Selbstbehalten reagiert. Regressmöglichkeiten gegen Organe und Arbeitnehmer der Versicherungsnehmerin bleiben (falls kein versicherungsvertraglicher Verzicht vereinbart wurde) arbeits- bzw. anstellungsvertraglich beschränkt.[38] Bei einigen Versicherern findet eine Dynamisierung dahingehend statt, dass etwa bei verzögerter Erfüllung zeitkritischer Obliegenheiten mit dem Hinausschieben automatisch Sublimits sinken bzw. sich Selbstbehalte erhöhen.

Doch dies allein wird nicht zum Erreichen eines Mindest-IT-Sicherheitsniveaus führen, auf dessen tatsächliche Einhaltung man sich ohne vertragliche Vereinbarung verlassen kann. Gesetzlich fehlte es bislang an einer Verankerung von „Security" (im Gegensatz zu „Safety"). Allein in regulatorischen Nischen wie der für kritische Infrastrukturen oder bei einzelnen Produkten finden sich Regelungsinseln.[39]

Daran könnte sich nun mit einer ganzen Welle an europäischer Regulierung etwas ändern.[40] Neben der im Anwendungsbereich erweiterten KRITIS-Gesetzgebung[41] werden als weitere Säulen das digitalisierte Schuldrecht[42], die digitalisierte Produkthaftung[43] und das digitalisierte Produktsicherheitsrecht[44] errichtet. Im Weiteren soll es um die letztgenannte Materie gehen.

---

[37] Vgl. *Anderson*, Security Engineering, 3. Aufl. 2020, S. 284; *Spafford/Metcalf/Dykstra*, Cybersecurity – Myths and Misconceptions, 2023, S. 130 ff.

[38] Vgl. *Schilbach/Becker*, r+s 2023, 289 auch zum möglichen Innenausgleichsanspruch gegen einen D&O-Versicherer. Zu Subsidiaritätsklauseln *Fortmann* r+s 2019, 429; *Prölss/Martin/Klimke*, 31. Aufl. 2021, AVB Cyber A1–12 Rn. 1 ff.

[39] Für KRITIS vgl. zu § 8a BSIG *Beucher/Ehlen/Utzerath*, in: Kipker, Cybersecurity, 2. Aufl. 2023, Kap. 14, Rn. 79 ff.

[40] Vgl. *Dickmann*, Int. Cybersecurity Law Review 4 (2023), 21, https://doi.org/10.1365/s43439-022-00064-9.

[41] Hierzu *Vettermann*, MMR 2023, 827.

[42] Vgl. §§ 327e Abs. 3 Ziff. 2; 434 Abs. 3 S. 2 BGB; insbesondere Pflicht zur Bereitstellung von Sicherheitsaktualisierungen (keine Hauptleistung, vgl. §§ 327e Abs. 3 S. 1 Ziff. 5; 327f; 475b Abs. 4 Ziff. 2; 475c Abs. 1 S. 2 BGB) trifft nur den Vertragspartner, der nicht notwendigerweise der Hersteller ist.

[43] Neufassung der Produkthaftungs-RL im Entwurf COM(2022) 495. Vgl. *Adelberg*, ZfPC 2023, 59. Einige wesentliche Änderungen: Datenverlust als ersatzfähiger Schaden

War bislang im europarechtlich geprägten Produktsicherheitsrecht der Schwerpunkt auf „Safety" gelegt, rückt nun „Security" verstärkt in den Fokus. Dabei geht es um die Regulierung bei Inverkehrbringen von Produkten. Zentral sind die Voraussetzungen für das Anbringen des CE-Kennzeichens.[45] Der Verantwortliche muss sich einer Selbstprüfung hinsichtlich der Erfüllung unterziehen. Hinsichtlich konkreter Produktkategorien erfolgt eine sehr detaillierte Regulierung über die Aufstellung technischer Normen, die über delegierte Rechtsakte verpflichtend einzuhalten sind.

Die europäischen Normgeber haben erkannt, dass statische Sicherheitsmerkmale mit dem Stand zum Zeitpunkt des Inverkehrbringens nicht ausreichend sind. Vielmehr bedarf es einer Dynamisierung möglichst für den gesamten Nutzungszeitraum insbesondere mit Pflichten zu Sicherheitsupdates und zum Schwachstellenmanagement.[46] Letzteres stellt Organisationsanforderungen an Produzenten bzw. Betreiber. Für die entsprechenden Prozesse muss das Rad nicht neu erfunden werden.[47] Coordinated Vulnerability Disclosure (CVD) stellt ein schon länger eingeführtes System zum Umgang mit Meldungen von Informationen zu Schwachstellen über deren Bewertung und Beseitigung bis zum Ausrollen von Updates oder anderweitigen Lösungen samt Kommunikation dar.[48]

Das Schwachstellenmanagement pocht auf die Organisation eines unternehmensinternen Prozesses, der nicht im Produkt verankert sein muss, anders also als die Möglichkeit zum Einspielen von Updates mit Niederschlag im Quellcode. Die Anforderungen verlangen nach einem ganzheitlichen Ansatz und wollen auf eine Fehlerkultur hinaus, bei der Sicherheitslücken als etwas Unvermeidliches, aber möglichst schnell Abzuhelfendes im Produktlebenszyklus beachtet werden. Wie lange dieser dauert, ist eine Frage des Einzelfalls. Der Ge-

---

anerkannt sowie „vernünftigerweise vorhersehbare missbräuchliche Nutzung" und „Verletzung von Cybersicherheitsanforderungen" wurden in den Fehlerkatalog aufgenommen.

[44] Vgl. § 4 Abs. 3 Nr. 4, 5 FuAG (Geräte mit Funkschnittstelle) i. V. m. ETSI/EN 303645 V2.1.1 (2020-06), dort Ziff. 5.2 sowie den Cyber Resilience Act (als Auffangtatbestand; bislang nur im Entwurf COM(2022) 454 final vorliegend). Zu letzterem *Rennert*, ZfDR 2023, 206; *Wiebe/Daelen*, EuZW 2023, 257; *Voigt/Falk*, MMR 2023, 88.

[45] Vgl. *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, 2023, S. 57, https://doi.org/10.25353/ubtr-xxxx-8597-6cb4; *Dickmann*, Int. Cybersecurity Law Review 4 (2023), 21, https://doi.org/10.1365/s43439-022-00064-9.

[46] Ausführlicher *Dickmann*, Int. Cybersecurity Law Review 4 (2023), 21, https://doi.org/10.1365/s43439-022-00064-9.

[47] Vgl. ISO/IEC 29147:2018 (Anforderungen an Verantwortliche), ISO/IEC 30111:2019 (Umgang mit Meldungen) und ISO/IEC TR 5895:2022 (Multiple Verantwortliche).

[48] Vgl. *Householder*, The CERT Guide to Coordinated Vulnerability Disclosure, Fassung vom 12.12.2019, abrufbar unter https://vuls.cert.org/confluence/display/CVD; *Goerke/Obermaier/Schink/Schuster/Wagner*, in: Balaban u. a., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, 2021, S. 27 ff., abrufbar unter https://sec4research.de.

setzgeber hat auf die Festlegung von Mindestzeiträumen über die gesetzliche Gewährleistung hinaus verzichtet, was auch für die Versorgung mit Sicherheitsupdates gilt. Zudem werden Altprodukte (Legacy) nicht explizit reguliert.[49] Die resultierende Ungewissheit (für die Nutzer) sowie die Frage der tatsächlichen Wirksamkeit der Prozesse zur Beseitigung von Schwachstellen belassen durchaus Zweifel daran, ob die Regelungen zu einer Erhöhung des allgemeinen IT-Sicherheitsniveaus führen. Sie erscheinen jedoch als ein erster (ggf. nachzubessernder) Schritt in die richtige Richtung.

Entschließt sich die Entdeckerin einer Schwachstelle die gewonnenen Informationen an den oder die Verantwortlichen zu melden, ergeben sich im weiteren Verlauf mannigfaltiger Potenziale für Probleme und Konflikte.[50] Eingangs gilt es die richtigen Verantwortlichen zu identifizieren, dort einen technisch verständigen Ansprechpartner zu finden und einen sicheren Kommunikationskanal zu etablieren. Nachfolgend kommt es darauf an, dass die Informationen zur Sicherheitslücke hinsichtlich ihrer Kritikalität[51] richtig beurteilt werden. Nur dann kann mit geeigneten Maßnahmen zeitlich adäquat reagiert werden. Schwachstellen, die allein oder in Verkettung mit anderen etwa einfach, unbemerkt und/oder mit besonders großem Schadenpotenzial in der Praxis ausgenutzt werden können, verlangen nach einer möglichst schnellen priorisierten Entwicklung von wirksamen Patches oder anderweitiger Schutzmaßnahmen (Mitigation) sowie Information und Warnung der Betroffenen.

Insbesondere Meldungen über Schwachstellen mit hoher Kritikalität haben einen erheblichen Marktwert. Dieser liegt in der Bedeutung für Angreifer und Nutzer, aber auch für (Produkt- oder Dienste-)Verantwortliche etwa mit Blick auf die zukünftige Geschäftsentwicklung, Reputation und Haftungsrisiken. Melderinnen verdienen daher einen respektvollen Umgang auf Augenhöhe samt Achtung ihrer Bedürfnisse nach Transparenz und Feedback. Dies gilt besonders bei unentgeltlichen Meldungen, durch die der Einsatz zur Erhöhung des IT-Sicherheitsniveaus und zum Schutz der Nutzer mit entsprechendem guten Willen gezeigt wird. IT-Sicherheitsforscherinnen als Melderinnen sollte (jedenfalls nach Beseitigung der Schwachstelle) Gelegenheit zu Veröffentlichungen etwa in Form von Aufsätzen oder Vorträgen gewährt werden, ohne sie mit juristischen Konsequenzen zu bedrohen.[52] Damit zeigen die betroffenen Unternehmen, dass eine Fehlerkultur auch tatsächlich gelebt wird.

---

[49] Zu den Schwierigkeiten von Modernisierungsansätzen bei Legacy-Systemen aus Sicht der Programmiererinnen *Bellotti*, Kill it with fire, 2021, S. 37 ff.

[50] *Wagner/Vettermann* u. a., Verantwortungsbewusster Umgang mit IT-Sicherheitslücken, 2023, S. 11 ff., https://doi.org/10.25353/ubtr-xxxx-8597-6cb4.

[51] Vgl. *Kreutzer/Schreiber*, in: Balaban u. a., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, 2021, S. 34 ff., abrufbar unter https://sec4research.de.

[52] Vertiefend *Dickmann*, in: Balaban u. a., Whitepaper zur Rechtslage der IT-Sicherheitsforschung, 2021, S. 20 ff., abrufbar unter https://sec4research.de.

Neben der schon aufgeworfenen Frage nach der Dauer des Schwachstellenmanagements für bestimmte Produkte ist zukünftig u. a. zu klären, welche Folgen funktional defekte Prozesse oder Sicherheitsupdates haben, ob eine Aufsicht (in Stichproben) diesbezüglich stattfindet sowie ob die Updates in angemessenen Zeiträumen entwickelt und ausgerollt werden. Dabei soll nicht verschwiegen werden, dass die Implementierung eines Schwachstellenmanagements im Einzelfall hoch komplex und ressourcenaufwendig sein kann. Lange bzw. unübersichtliche Lieferketten, fehlender Zugriff auf den Quellcode, unklare bzw. abgestrittene Verantwortlichkeiten, die Geeignetheit von Alternativmaßnahmen als Patch-Ersatz und der Umgang mit nicht behebbaren Schwachstellen sind nur einige Problemkreise.[53] Nicht unbeachtet bleiben darf auch das Missbrauchspotenzial etwa durch böswillige Falschmeldungen oder Überfluten mit Unkritischem bei Meldungen von Konkurrenten oder böswilligen Melderinnen (Trollen).

Gerade für mittelständische Unternehmen, die Soft- und Hardware für Internetfunktionalitäten zukaufen, schaffen die dargestellten Anforderungen und Probleme erhebliche Herausforderungen.[54] Ob diese innerhalb der oft straffen Umsetzungsfristen gemeistert werden können, erscheint zweifelhaft. Erhöhte Anforderungen und Haftungsrisiken könnten zu längeren Entwicklungszeiträumen und Produktzyklen führen. Dies muss für die Nutzer kein Nachteil sein, weil sie ausgereiftere, jedenfalls aber sicherheitstechnisch gepflegtere und damit nachhaltigere Produkte erhalten. Zudem hat die europarechtlich induzierte Regulierung auch sekundäre Effekte etwa hinsichtlich verwaltungsrechtlicher Maßnahmen, Bußgeldern und Einfuhrverboten. Auch die zivilrechtliche Haftung mit wettbewerbsrechtlichen Abmahnungen, Produkthaftung und Regressen (gegen Dienstleister, Zulieferer, Importeure und Hersteller im EWR-Ausland) gilt es im Blick zu behalten. Vertragliche Vorsorge über Klauseln zur Haftungsbegrenzung und Pflichten etwa zur Zertifizierung werden an Gewicht gewinnen. Die entscheidenden Machtfaktoren werden das Recht am und der Zugriff auf Quellcode sein. Insbesondere letzteres kann mittels Hinterlegung (Code Escrow) abgesichert werden.[55]

---

[53] Vgl. die Auflistung bei *Dickmann*, Int. Cybersecurity Law Review 4 (2023), 21, https://doi.org/10.1365/s43439-022-00064-9.

[54] Vgl. für den Cyber Resilience Act *Dittrich/Heinelt*, RDi 2023, 309. Für die Bereichsausnahme für Open-Source-Software und Zielkonflikte beim Einsatz in kommerzieller Software *Poncza/Keppeler/Lennartz*, ZfPC 2023, 117.

[55] Etwa zum Erhalt der Zugriffsmöglichkeit auf Quellcode für die Weiterentwicklung/Fehlerberichtigung/Pflege, Lizenzinformationen/-schlüssel, kryptografisches Material, Daten (etwa zur Konfiguration von Maschinen oder dem Trainingsstand von AI) oder Dokumentation bei Wahrung der Insolvenzfestigkeit. Vgl. *Peters* und *Fleischhauer/Stiemerling*, in: Remmertz/Kast, Digital Escrow, 2022, insbesondere S. 23 ff. (zu den Interessen der Beteiligten) und 139 ff. (zum Hinterlegungsgegenstand).

Für die Cyberversicherung als Mittel des Risikotransfers kann das Schwachstellenmanagement zu einem wichtigen Baustein in der Risikobewertung werden. Fragen nach dem Umgang mit Schwachstellen und entsprechende Obliegenheiten sind dabei in den Katalog der Versicherer aufzunehmen. Ob allerdings praxisbewehrte sicherere Produkte und eine Erhöhung des allgemeinen IT-Sicherheitsniveaus Resultate der Regulierung sein werden, muss sich erst noch zeigen.[56] Ein mit dem Risiko sich verändernder (erhöhender) Level an Mindest-IT-Sicherheit in Märkten und Gesellschaft ist für eine Stabilisierung des Versicherungsprodukts Cyber wichtig.[57] Dazu kann eine Fehlerkultur beitragen, die Melderinnen von Informationen über Schwachstellen nicht als Angreifer, sondern als Schenkende sieht, denen mit Dankbarkeit begegnet wird.

[56] Kritisch zum Cyber Resilience Act *Siglmüller*, ZfPC 2023, 221.

[57] Vgl. *Wrede/Freers/von der Schulenburg*, ZVersWiss 2019, 405.