April 2018 · Jan-Peter Kleinhans

Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit

Stiftung
Neue
Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

Die Zahl internetfähiger und gleichzeitig unsicherer Produkte wächst täglich. Zugleich versagt der Markt bisher darin, verhältnismäßig vertrauenswürdige Produkte herzustellen. Das haben auch politische Entscheidungsträger:innen erkannt, sodass im aktuellen Koalitionsvertrag Konzepte wie Gütesiegel oder Produkthaftung erwähnt werden und auf der Ebene der Vereinten Nationen von “Cyber Stability” und vertrauensbildenden Maßnahmen gesprochen wird. Um die IT-Sicherheit nachhaltig zu verbessern, ist es aber insbesondere für Politiker:innen wichtig, die zugrundeliegenden Prozesse und Akteure zu kennen, die für die Sicherheit in der Informations- und Kommunikationstechnologie (IKT) verantwortlich sind. Denn wie sicher die einzelnen über das Internet verbunden Systeme und deren Kommunikation über das Netzwerk selbst sind, hängt in hohem Maße von den implementierten technischen Standards ab: Internationale Standardisierungsgremien, Normungsorganisationen und Zertifizierungsprozesse bestimmen maßgeblich die IT-Sicherheit der IKT.

Die Standardisierung, also die Definition der Anforderungen, die ein Produkt in Hinblick auf IT-Sicherheit erfüllen muss, wird dabei von unterschiedlichsten Gremien geleistet. Die IKT-Standardisierung verteilt sich international auf eine Vielzahl an Normungs- und Standardisierungsorganisationen (SDO). Sie ist fragmentiert, hochgradig verflochten und komplex. Ganz gleich, ob globaler Branchenverband (IEEE), Industriekonsortium (Bluetooth SIG), offene Interessengruppe (IETF) oder staatlich anerkannte Normungsorganisationen (ISO), sie alle definieren Spielregeln für IKT – der Grundlage unserer digitalen Gesellschaft. Ihnen fällt dabei eine hohe Bedeutung zu, da durch die zunehmende Vernetzung von Geräten immer mehr Sicherheitsaspekte relevant werden und somit auch Standards stetig aktualisiert werden müssen um nicht zu veralten.

Die so entstehenden Standards bilden die Grundlage von Zertifizierungsverfahren in der IKT. IT-Sicherheitszertifizierung dient dazu, die Vertrauenswürdigkeit eines Produktes oder Systems einzuschätzen. Sie ermöglicht es, festzustellen, ob ein Produkt Sicherheitsanforderungen erfüllt. Die formulierten Auflagen referenzieren oftmals Standards, sodass deren Güte auch für die Zertifizierung von Relevanz ist. Dabei zeigt sich, dass die Zertifikate keine Aussage darüber treffen können, wie sicher ein Produkt de facto ist, sondern nur, wie gut es die vorher als relevant definierten Sicherheitsanforderungen erfüllt.Die Nützlichkeit einer IT-Sicherheitszertifizierung hängt weiterhin davon ab, ob sie international anerkannt wird: Fehlt die internati-

onale Anerkennung, müssen Unternehmen ihre Produkte unter Umständen mehrmals zertifizieren lassen, was für sie nicht nur einen langwierigen, sondern auch teuren Prozess darstellt. Auch das meistgenutzte Zertifizierungsschema, Common Criteria, weist hier große Schwächen auf. Beide Faktoren, hohe finanzielle und zeitliche Kosten und mangelnde internationale Anerkennung, haben dazu geführt, dass es kaum zertifizierte Produkte am Markt gibt.

Zertifizierung allein garantiert aber noch keine sicheren Geräte, denn dafür benötigt es darüber hinaus eine effektive und effiziente Marktüberwachung. Dies ist aber gerade hinsichtlich IT-Sicherheit schwierig: Zertifizierung ist immer nur eine Momentaufnahme, daher kann es passieren, dass kurze Zeit nachdem die IT-Sicherheit eines Produktes erfolgreich evaluiert wurde, eine bisher unentdeckte Sicherheitslücke das zuvor zertifizierte Produkt de facto “unsicher” macht. Diese zertifizierten aber unsicheren Produkte müssen am Markt zügig identifiziert werden. Dies fällt schon heute, zum Beispiel bei der CE-Kennzeichnung für physische Produktsicherheit, schwer. Wie Marktüberwachung modernisiert werden muss, um adäquat auf IT-Sicherheit zu achten, ist noch völlig ungeklärt.

IT-Sicherheitspolitik muss daher an die technische und wirtschaftliche Realität angepasst werden. Für Gesetzgeber ist es entscheidend zu erkennen, dass die aufeinander aufbauenden Elemente Standardisierung, Zertifizierung und Marktüberwachung stets zusammen gedacht und überprüft werden müssen, um möglichst sichere Produkte zu erhalten: Ohne robuste und sichere Standards können keine sicheren Produkte entworfen werden. Ohne effektive Zertifizierung und sinnvolle Evaluationskriterien kann die Vertrauenswürdigkeit eines Produktes nicht überprüft werden. Ohne eine effektive und responsive Marktüberwachung können schwarze Schafe und unsichere Produkte nicht schnell genug vom Markt entfernt werden. Soll die IT-Sicherheit von Produkten und des Internets selbst daher langfristig gestärkt werden, müssen sich politische Entscheidungsträger:innen das Zusammenspiel aus Standardisierung, Zertifizierung und Marktüberwachung anschauen. Eine Stärkung eines einzelnen Elementes, wie beispielsweise derzeit im Zuge des EU Cybersecurity Acts, wird langfristig keine signifikante Stärkung der IT-Sicherheit mit sich bringen.

Inhalt

Die vorliegende Studie wurde vom Auswärtigen Amt gefördert und gibt ausschließlich die Auffassung des Autors wider.. Der Autor bedankt sich bei allen Gesprächsteilnehmer:innen für das Vertrauen und die interessanten Erkenntnisse.

1. Einleitung

Wie angreifbar das Internet als „Netzwerk von Netzwerken" auf den verschiedenen Ebenen ist, ist seit vielen Jahren bekannt.[1] Nicht nur die Endpunkte des Netzwerks, wie Laptops, Smartphones, Maschinen und (immer mehr) Dinge sind angreifbar, sondern auch der Kern des Internets selbst: Internetknoten, Netzwerkbetreiber oder Datenzentren. Die Sicherheit dieser Infrastruktur wird daher zu einer immer größeren Herausforderung. Gleichzeitig scheinen Lösungen kompliziert, da die Funktionstüchtigkeit des Internets von einem komplexen Zusammenspiel verschiedenster Akteure abhängt, die alle einen bestimmten Teil zum reibungslosen Betrieb des gesamten Systems beitragen. Kollaterale und kaskadierende Schäden sind Alltag in einem Netzwerk aus Netzwerken. Wie schwerwiegend und weitreichend diese Schäden sein können, zeigen Schadsoftware-Kampagnen, wie WannaCry und NotPetya. Die Kampagnen wurden zwar von unterschiedlichen Akteuren mit verschiedenen Zielen durchgeführt, der Effekt war jedoch immer der gleiche: Weltweit wurden massenhaft Computer und Systeme lahmgelegt, indem deren gesamter Inhalt verschlüsselt wurde. So hat allein die Schadsoftware WannaCry im Mai 2017 weltweit mehr als 200.000 Windows-Rechner in über 100 Ländern infiziert. Besonders betroffen war der britische National Health Service – dutzende Krankenhäuser mussten ihre gesamte IT-Infrastruktur, bis hin zu medizinischen Geräten, ausschalten.[2] Im selben Jahr hat der Verschlüsselungstrojaner NotPetya dutzende internationale Konzerne betroffen und zu finanziellen Schäden in Milliardenhöhe geführt.[3] WannaCry und NotPetya haben jedoch nicht nur für ökonomischen Schaden gesorgt, sondern haben auch die internationalen Beziehungen strapaziert.[4] So hat das Außenministerium des Vereinigten Königreichs in einer Mittei-

1 Hall, Chris, Ross Anderson, Richard Clayton, Evangelos Ouzounis, und Panagiotis Trimintzios. 2012. „Resilience of the Internet Interconnection Ecosystem". In Economics of Information Security and Privacy III, 119–48. Springer New York. https://doi.org/10.1007/978-1-4614-1981-5_6.

2 National Audit Office. 2017. "Investigation: WannaCry cyber attack and the NHS". National Audit Office (NAO). https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

3 Zeljka Zorz. 2017. „NotPetya aftermath: Companies lost hundreds of millions". https://www.helpnetsecurity.com/2017/08/17/notpetya-losses/

4 Jack Goldsmith. 2017. „The Strange WannaCry Attribution". https://www.lawfareblog.com/strange-wannacry-attribution

lung NotPetya dem russischen Militär zugeschrieben[5] und die USA machten Nordkorea für die WannaCry-Attacken verantwortlich.[6]

Einige Regierungen haben erkannt, dass es im gemeinsamen Interesse liegt, die Stabilität des Internets und der damit verbundenen Informations- und Kommunikationstechnologie (IKT) zu unterstützen. So hat sich Europa der Förderung eines verlässlichen, sicheren und offenen „Cyber Ökosystems" verschrieben.[7] Ebenso sprechen die USA seit einigen Jahren von „Cyber Stability".[8] Deutschland schreibt im Bericht an die Vereinten Nationen, man setze sich für einen offenen, sicheren, stabilen und friedvollen staatlichen Umgang mit IKT ein.[9] Zur nachhaltigen Förderung eines sicheren und resilienten Internets benötigt es jedoch deutlich mehr als Lippenbekenntnisse und vertrauensbildende Maßnahmen auf internationaler Ebene. Wie sicher die einzelnen über das Internet verbunden Systeme und deren Kommunikation über das Netzwerk selbst sind, hängt in hohem Maße von den implementierten technischen Standards ab: Internationale Standardisierungsgremien haben Definitionshoheit darüber, was „sicher" tatsächlich bedeutet. Die Entwicklung vertrauenswürdiger und robuster technischer Standards hat daher direkte positive Auswirkungen auf die Sicherheit heutiger und zukünftiger IKT und reduziert somit die politischen, wirtschaftlichen und gesellschaftlichen Risiken fehlender IT Sicherheit.

Ziel dieses Papiers ist es daher, politischen Entscheidungsträger:innen die Verbindung zwischen technischen Standards und Zertifizierung zur nachhaltigen Stärkung von IT-Sicherheit aufzuzeigen. Hierfür werden zunächst zentrale ökonomische Herausforderungen für Hersteller aufgezeigt, bei der Produktentwicklung auf IT-Sicherheit zu achten. Anschließend wird die Arbeit und Rolle von Standardisierungs- und Normungsorganisationen besprochen. Darauffolgend wird dargelegt, wie IT-Sicherheitszertifizierung

5 Foreign & Commonwealth Office. 2018. „Foreign Office Minister condemns Russia for NotPetya attacks". https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

6 White House. 2017. „Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea". https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

7 The European Commisson. (2017). "Resilience , Deterrence and Defence : Building strong cybersecurity in Europe". https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe

8 Kristen Eichensehr. 2015. „"International Cyber Stability" and the UN Group of Governmental Experts". https://www.justsecurity.org/24614/international-cyber-stability-un-group-governmental-experts/

9 United Nations, Office for Disarmament Affairs. 2017. "German report on Developments in the field of information and telecommunications in the context of international security". 2017–A/72/315. https://www.un.org/disarmament/topics/informationsecurity/

auf technischen Standards aufbaut und welche Rolle Zertifizierung derzeit zur Stärkung von IT-Sicherheit spielt. Am Ende werden einige nationale und internationale Handlungsempfehlungen ausgesprochen, um durch Standardisierung und Zertifizierung die Sicherheit und Resilienz des Internets langfristig zu stärken.

2. IT-Sicherheit – Status Quo

IT-Sicherheit ist eine große Herausforderung – gerade für Hersteller traditionellerer Produkte, die im Zuge der Digitalisierung erst in den letzten Jahren begonnen haben, ihre Geräte zu vernetzen. Durch die zunehmende Vernetzung von Gegenständen zum sogenannten Internet der Dinge (IoT) bedeutet mangelnde IT-Sicherheit (*security*) potenziell direkte Auswirkungen auf Leib und Leben (*safety*).[10] Schon heute ist es möglich, ein vernetztes Auto über das Internet zu hacken und Kontrolle über die Motorsteuerung zu übernehmen.[11] Solche Risiken werden zukünftig durch die voranschreitende Vernetzung unserer Wirtschaft zunehmen. Neben solchen direkten physischen Gefahren durch mangelnde IT-Sicherheit stellen Massen unsicherer IoT-Geräte auch eine Gefahr für das Internet als Ganzes dar. So erschufen kriminelle Hacker:innen in den letzten Jahren Botnetze aus mehreren Hunderttausend kompromittierten IoT-Geräten:[12] Die Schadsoftware eines Botnetzes verbreitet sich selbstständig über das Internet, indem bekannte Schwachstellen bestimmter IoT-Geräte ausgenutzt werden.[13] Das so entstehende Botnetz ist unter der vollständigen Kontrolle der Kriminellen und kann für Angriffe auf beliebige IT-Infrastrukturen genutzt werden.

Hersteller können viel Erfahrung hinsichtlich physischer Produktsicherheit (*safety*) besitzen, beispielsweise da sie seit Jahrzehnten Autos, Haushaltsgeräte oder Maschinen herstellen. Mit der Digitalisierung ihrer Produktpalette müssen sie sich jedoch auf einmal Gedanken um IT-Sicherheit (*security*) machen. IT-Sicherheit ist allerdings kein einmalig zu erreichender Zustand, sondern ein Prozess, den es ständig zu optimieren gilt. So wird bei IoT-Pro-

10 Wolf, Marilyn und Dimitrios Serpanos. 2018. „Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems“. Proceedings of the IEEE 106 (1): 9–20. https://doi.org/10.1109/jproc.2017.2781198.

11 Miller, Charlie und Chris Valasek. 2015. “Remote exploitation of an unaltered passenger vehicle.” Black Hat USA 2015. http://illmatics.com/Remote Car Hacking.pdf

12 Antonakakis, Manos, et al. 2017. „Understanding the mirai botnet.“ USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

13 Kolias, Constantinos, Georgios Kambourakis, Angelos Stavrou und Jeffrey Voas. 2017. „DDoS in the IoT: Mirai and Other Botnets“. Computer 50 (7): 80–84. https://doi.org/10.1109/mc.2017.201.

dukten nicht nur eigene Software, sondern auch fremde Software verwendet. Wenn beispielsweise Sicherheitsforscher:innen neue Angriffsmöglichkeiten für oder Schwachstellen in weit verbreiteten Softwarebibliotheken entdecken, hat das Auswirkungen auf alle IT-Anwendungen, die diese kompromittierbaren Softwarebibliotheken einsetzen. Aufgrund dieser Problematik reichen sichere Software-Entwicklungsprozesse nicht aus, sondern müssen mit einem Patch-Management und entsprechend Ressourcen für den Softwaresupport alter Produkte verknüpft werden. Dies geschieht regelmäßig nicht.[14] Stattdessen wird auf Funktionalität und Time-to-Market fokussiert. Es gibt zwei zentrale Dynamiken, weswegen viele Hersteller auch zukünftig bei der Entwicklung kaum auf Best Practices und Security-by-Design achten werden:

- Informationsasymmetrie: Für Nutzer:innen ist es kaum möglich, die Softwarequalität eines Produktes von außen zu beurteilen. Ob und inwieweit sich der Hersteller an Best Practices bei der Softwareentwicklung gehalten hat, kann man ohne Blick in den Quellcode nicht herausfinden. Unabhängig davon weiß der:die Nutzer:in ebenso wenig, wie schnell der Hersteller auf einmal bekannt gewordene Sicherheitslücken reagieren wird oder wie lange Softwareupdates zur Verfügung gestellt werden. Dieser Mangel an verbindlichen Aussagen hinsichtlich der Vertrauenswürdigkeit eines Produktes ist gerade bei Smart Home-Geräten ein Problem. Eine solche Informationsasymmetrie zwischen Hersteller und Nutzer:in hinsichtlich der IT-Sicherheit eines Produktes hat direkte negative Effekte auf den Markt: Beim Kauf fokussieren Nutzer:innen vorrangig auf Funktionalität – IT-Sicherheit wird vom Markt nicht honoriert.[15] Dies wiederum führt dazu, dass Hersteller weniger in IT-Sicherheit investieren.[16]

- Externe Kosten: Negative Externalitäten oder „externe Kosten“ sind Kosten, die unbeteiligte Dritte tragen müssen: Luftverschmutzung, Überfischung oder passives Rauchen. Schäden, die durch Softwareschwachstellen, gerade bei mit dem Internet ver-

14 Kleinhans, Jan-Peter. 2017. „Internet of Insecure Things“. Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

15 Leverett, Éireann, Richard Clayton und Ross Anderson. 2017. “Standardisation and Certification of the ’Internet of Things”. Proceedings of WEIS 2017. https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

16 Moore, Tyler. 2010. „The Economics of Cybersecurity: Principles and Policy Options“. International Journal of Critical Infrastructure Protection 3 (3–4). Elsevier BV: 103–17. https://doi.org/10.1016/j.ijcip.2010.10.002.

bundenen Geräten, entstehen, können ebenso als externe Kosten klassifiziert werden[17]: 2016 griff ein krimineller Hacker mithilfe eines Botnetzes aus rund 600.000 IoT-Geräten Internetinfrastruktur an der US-amerikanischen Ostküste an, woraufhin Twitter, Soundcloud und andere Dienste für mehrere Stunden in diesen Gebieten ausfielen.[18] Der geschätzte Schaden beläuft sich auf über $110 Millionen.[19] Weder die Hersteller der kompromittierten IoT-Geräte, noch die IoT-Betreiber mussten für die Kosten aufkommen. Die Schäden mussten stattdessen der attackierte Internetinfrastrukturprovider, die betroffenen Diensteanbieter und letztlich auch deren Nutzer:innen tragen. Ähnlich zur Luftverschmutzung oder Überfischung trägt regelmäßig die Gesellschaft als Ganzes die Kosten eines solchen Angriffs.[20] Negative Externalitäten führen dazu, dass weder Hersteller verstärkt versuchen ihre Produkte sicherer zu machen, noch dass IT-Sicherheit zum Kaufkriterium wird.

Politischen Entscheidungsträger:innen wird immer stärker bewusst, dass eine Intervention notwendig ist, um IT-Sicherheit zu stärken. So findet man im aktuellen Koalitionsvertrag zwischen CDU/CSU und SPD sowohl Überlegungen zu einem „IT-Sicherheits-Gütesiegel“, einem „gesetzlichen Mindeststandard“ als auch eine Ausweitung der Produkthaftung, um Hersteller stärker in die Verantwortung zu nehmen.[21] Vermutlich benötigt es eine Kombination mehrerer Maßnahmen und internationale Kooperation, damit langfristig der Markt vertrauenswürdige Produkte produziert und honoriert.[22] Viele der derzeit besprochenen Initiativen setzen implizit auf robuste IT-Sicherheitsstandards, effiziente Zertifizierung und effektive Marktüberwachung. Ohne das Zusammenspiel dieser drei Elemente werden die erwähnten Initiativen mit großer Wahrscheinlichkeit scheitern. So müssen beispielsweise in einer Mindestanforderung etablierte technische Standards referenziert werden, um Herstellern einen Weg aufzuzeigen, wie sie das geforderte Regulierungs-

17 Jentzsch, Nicola. 2016. „State-of-the-Art of the Economics of Cyber-Security and Privacy“. http://hdl.handle.net/10419/126223

18 Antonakakis, Manos, et al. 2017. „Understanding the mirai botnet.“ USENIX Security Symposium. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

19 McKinsey. 2017. “Security in the Internet of Things”. https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

20 Bauer, Johannes M., und Michel J.G. van Eeten. 2009. „Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options“. Telecommunications Policy 33 (10–11). Elsevier BV: 706–19. https://doi.org/10.1016/j.telpol.2009.09.001.

21 Koalitionsvertrag zwischen CDU, CSU und SPD. 2018. https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1

22 OECD .2018. „Consumer product safety in the Internet of Things“. OECD Digital Economy Papers No. 267. OECD Publishing. http://dx.doi.org/10.1787/7c45fa66-en

ziel erreichen können. Ebenso muss überprüft werden, inwieweit Hersteller tatsächlich die Sicherheitsanforderungen erfüllen. Dies kann unter anderem durch eine Selbstauskunft des Herstellers geschehen und dann durch unabhängige Prüflabore stichprobenhaft überprüft werden. Robuste technische Standards und effektive Zertifizierung stellen in jedem Fall die Basis dar, auf der regulatorische Interventionen aufbauen. Im folgenden Abschnitt wird daher zunächst analysiert, wie internationale, technische Standards und Normen entwickelt werden und welche Rolle sie für IT-Sicherheit spielen.

3. Technische Normen und Standards

Technische Standards definieren Anforderungen an ein Produkt oder einen Prozess. Seitens der Unternehmen ist das vorrangige Ziel der Standardisierung Marktdurchdringung, Wettbewerbsfähigkeit, Kompatibilität und Interoperabilität.[23] Häufig wird daher durch den Standard lediglich festgelegt, *was* erfüllt werden muss und nicht *wie* es erfüllt werden muss. Denn *wie* ein Unternehmen eine bestimmte Anforderung des Standards erfüllt, um Kompatibilität mit Produkten anderer Hersteller zu erreichen, ist Teil der Innovationskraft und des Wettbewerbs. Mit voranschreitender Digitalisierung unserer Gesellschaft hat nicht nur die Zahl an Standardisierungsorganisationen[24] (SDO) zugenommen, sondern auch die Anzahl technischer Standards. Als mitgliederbasierte und teils mitgliederfinanzierte Organisationen sind SDOs vor allem industriegetrieben. SDOs stehen daher auch untereinander im Wettbewerb neue Technologien zu standardisieren. Da Standards zunächst freiwillig durch Unternehmen implementiert werden, stehen SDOs unter dem Druck möglichst gute und relevante Standards zeitnah zu produzieren, die auf Nachfrage am Markt stoßen. Mitglieder schlagen einen potenziellen neuen Standard vor und in Arbeitsgruppen der SDO wird entschieden, ob und inwieweit der vorgeschlagene Standard allgemeine Relevanz besitzt und vorangetrieben werden sollte. So wurden beispielsweise um die Jahrtausendwende durch unterschiedliche Standardisierungsorganisationen konkurrierende WLAN-Standards[25] entwickelt:

- Das Europäische Institut für Telekommunikationsnormen (ETSI) entwickelte den HIPERLAN/2 Standard. (*High Performance Radio Local Area Network*)

23 Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung. http://eur-lex.europa.eu/eli/reg/2012/1025/oj

24 Standard Development Organisations (SDO)

25 Doufexi, A., S. Armour, M. Butler, A. Nix, D. Bull, J. McGeehan und P. Karlsson. 2002. „A comparison of the HIPERLAN/2 and IEEE 802.11a wireless LAN standards“. IEEE Communications Magazine 40, Nr. 5 (Mai). http://dx.doi.org/10.1109/35.1000232.

- Das Institute of Electrical and Electronics Engineers (IEEE) definierte den WLAN-Standard 802.11.
- In Japan wurde der HiSWAN WLAN-Standard entwickelt. (*High Speed Wireless Access Network*)

Heute wissen wir, dass sich der IEEE 802.11 am Markt als WLAN-Standard durchgesetzt hat. Dies verdeutlicht zum einen, dass technische Standards im Wettbewerb zueinander stehen können und Unternehmen, die einen (jungen) Standard implementieren, auch immer ein gewisses Risiko eingehen, ob dieser Standard auch noch in ein paar Jahren relevant sein und weiterentwickelt werden wird. Zum anderen zeigt das Beispiel des WLAN-Standards den Innovationsdruck, der auf SDOs lastet, zeitnah relevante Standards für neue Technologien zu entwickeln. So gründen Unternehmen immer wieder sogenannte Special Interest Groups (SIG) abseits etablierter SDOs, um einen Standard außerhalb der Abstimmungsprozesse innerhalb der SDOs schneller und fokussierter entwickeln zu können. Beispiele für erfolgreiche SIGs sind Bluetooth SIG oder ZigBee SIG, die beide an Standards für funkgestützte Kommunikation arbeiten.

Standards können weiterhin veralten, wenn die vormals definierten Anforderungen nicht mehr den Stand der Technik widerspiegeln. Dies ist gerade hinsichtlich IT-Sicherheit von entscheidender Bedeutung. SDOs sind daher gefragt, Standards immer wieder zu überarbeiten, falls Schwachstellen aufgedeckt wurden. Ein gutes Beispiel ist hier der erwähnte *802.11* WLAN-Standard. Seit der Veröffentlichung des *802.11b* WLAN-Standards im September 1999, hat sich die *802.11* Standardfamilie stetig weiterentwickelt.[26] Ebenso wurde über die Jahre hinweg durch Sicherheitsforscher:innen immer wieder aufgezeigt, dass die verwendeten Mechanismen zur Authentifizierung oder Verschlüsselung des Datenverkehrs verhältnismäßig leicht gebrochen werden können.[27] Ein weiteres Beispiel ist der *ZigBee Light Link* Standard, der von vielen smarten LED-Leuchten unterstützt wird. Sicherheitsforscher:innen haben hier ebenfalls mehrfach darauf hingewiesen, dass selbst aktuelle Versionen des Standards unzureichend Wert auf starke Authentifizierung und Verschlüsselung legen.[28] Ähnlich zu Softwareherstellern müssen daher auch SDOs ihre Standards aktualisieren, um neu entdeckte Sicherheitslü-

26 IEEE. 2018. “Official IEEE 802.11 Working Group Project Timelines”. http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

27 Vanhoef, Mathy und Frank Piessens. 2013. “Practical verification of WPA-TKIP vulnerabilities”. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS ’13. http://dx.doi.org/10.1145/2484313.2484368.

28 Morgner, Philipp, and Zinaida Benenson. “Exploring Security Economics in IoT Standardization Efforts.” https://www1.cs.fau.de/filepool/publications/ndss-diss_iot_standardization_economics.pdf

cken zu adressieren. Im nächsten Schritt müssen die Unternehmen ihre Produkte aktualisieren, in denen die Standards verwendetet werden oder neue Revisionen auf den Markt bringen. Sicherheitsschwachstellen in Standards sind daher aus zwei Gründen potenziell schwerwiegender, als Schwachstellen in Produkten einzelner Hersteller:

- Die Sicherheitslücke betrifft potenziell alle Produkte, die den betroffenen Standard implementieren.
- Die Sicherheitslücke ist für eine relativ lange Zeit ausnutzbar, da zunächst der Standard aktualisiert werden muss, damit dann die Unternehmen den aktualisierten Standard implementieren können.[29] Je nachdem, wie schwerwiegend die Sicherheitslücke ist, reicht es, die Software der betroffenen Produkte zu aktualisieren (falls möglich) oder es müssen neue Produkt-Revisionen auf den Markt gebracht werden.[30]

Im Folgenden werden europäischen und internationalen SDOs kurz skizziert. An dieser Stelle muss zwischen Standardisierungsorganisationen und Normungsorganisationen unterschieden werden. Letztere sind durch Regierungen offiziell anerkannt und wie im Falle der Europäischen Union durch das New Legislative Framework fester Bestandteil der Regulierung. Weiterhin haben sich Normungsorganisationen den durch die WTO aufgestellten Grundprinzipien der Normung verschrieben: *Kohärenz, Transparenz, Offenheit, Konsens, Freiwilligkeit der Anwendung, Unabhängigkeit von Einzelinteressen und Effizienz*.[31] Standardisierungsorganisationen können demgegenüber durch verschiedenste Stakeholder ins Leben gerufen werden, haben sich meist nicht explizit den Grundprinzipien der WTO verschrieben und haben unterschiedlichste Governancestrukturen und Entscheidungsfindungsprozesse. Aufgrund der erwähnten Masse an SDOs werden lediglich einige der etablierten SDOs besprochen. Ziel ist nicht ein umfassender Überblick sondern vielmehr die institutionellen Verflechtungen und Unterschiede zwischen Industriestandards und Normen herauszuarbeiten.

29 Vanhoef, Mathy und Frank Piessens. 2017. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17. http://dx.doi.org/10.1145/3133956.3134027.

30 Rapid7. 2017. „The Wi-Fi KRACK Vulnerability: What You Need To Know". https://blog.rapid7.com/2017/10/16/the-wi-fi-krack-vulnerability-what-you-need-to-know/

31 World Trade Organization. 2000. "Second Triennial Review of the Operation and Implementation of the Agreement on Technical Barriers To Trade". G/TBT/9. https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=231,4879&CurrentCatalogueIdIndex=1

3.1 Normungsorganisationen

Für IKT gibt es verschiedene relevante nationale, europäische und internationale Normungsorganisationen, die im Folgenden kurz skizziert werden. Zur Steigerung der Effizienz sind Normungsorganisationen untereinander über Arbeitsgruppen stark vernetzt, um möglichst wenig Normungsarbeit parallel zu leisten.

Internationale Normungsorganisationen

- **Internationale Organisation für Normung (ISO)**
  Bestehend aus 161 nationalen Normungsorganisationen (beispielsweise DIN für Deutschland). Enge Kooperation mit IEC und ITU.[32]

- **Internationale Elektrotechnische Kommission (IEC)**
  Bestehend aus 84 *National Committees (NC)*. NCs sind je Land teils unterschiedlich organisiert, sollen jedoch die Perspektive aller Stakeholder miteinbringen.[33] In Deutschland ist dies die *Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE* (DKE).

- **Joint Technical Committee 1 (ISO/IEC JTC 1)**
  Das JTC1 ist ein Zusammenschluss aus ISO und IEC zur IKT-Standardisierung.[34] JTC1 ist in mehrere Arbeitsgruppen (Sub Committee) organisiert. Für IT-Sicherheit ist SC27 zuständig.[35]

- **Internationale Fernmeldeunion (ITU)**
  ITU Telecommunication Standardization Sector (ITU-T) ist für internationale Standardisierung innerhalb der ITU zuständig. Mitglieder sind Regierungen und Unternehmen. Die Arbeit ist in *Study Groups (SG)* organisiert, *SG17* Security ist zuständig für IT-Sicherheit.[36]

Europäische Normungsorganisationen

In Europa gibt es drei offiziell anerkannte Normungsorganisationen, die zentraler Bestandteil des europäischen *New Legislative Frameworks*[37] sind:

32 ISO Website. "Structure and Governance". https://www.iso.org/structure.html

33 IEC Website. "Who we are". http://www.iec.ch/about/profile/members.htm

34 ISO Website. "ISO/IEC JTC 1 – Information Technology". https://www.iso.org/isoiec-jtc-1.html

35 ISO Website. "ISO/IEC JTC 1/SC 27". https://www.iso.org/committee/45306.html

36 ITU Website. "ITU-T Study Groups (Study Period 2017-2020)". https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx

37 Europäische Kommission. "New Legislative Framework". https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_de

Europäische Gesetzgebung definiert übergeordnete Regulierungsziele und verweist auf technische Normen zur konkreten Ausgestaltung.[38] Nach Aufforderung durch die Europäische Kommission können die drei europäischen Normungsorganisationen dann die benötigten Normen entwickeln.[39] Am Ende dieses Prozesses steht die Veröffentlichung eines harmonisierten Standards (EN) im Amtsblatt der Europäischen Union. Dies bedeutet gleichzeitig für Mitgliedstaaten, dass nationale Standards zum selben Thema in der Regel zurückgezogen werden müssen. Die Anwendung der Standards bleibt jedoch freiwillig (zum Beispiel für Hersteller). Die Befolgung des Standards stellt allerdings in den meisten Fällen die effizienteste und günstigste Variante zur Erreichung der Regulierungskonformität dar.[40] Die drei europäischen Normungsorganisationen stehen weiterhin im engen Austausch mit den internationalen Normungsorganisationen:

- **Europäisches Komitee für Normung (CEN)**
  CEN setzt sich aus den nationalen Normungsorganisationen der Mitgliedsstaaten (und einigen weiteren Ländern) zusammen – für Deutschland ist dies zum Beispiel das Deutsche Institut für Normung (DIN).[41] Es besteht enge Kooperation und Abstimmung mit den internationalen Normungsinstituten: etwa 50% der derzeit in Entwicklung befindlichen CEN-Standards sind identisch zu ISO-Standards.[42]

- **Europäisches Komitee für Elektrotechnische Normung (CENELEC)**
  Ähnlich zu CEN setzen sich auch die Mitglieder von CENELEC aus den nationalen Normungsorganisationen zusammen. Auch hier besteht eine sehr enge Kooperation auf internationaler Ebene (IEC): etwa 70% der derzeit in Entwicklung befindlichen CENELEC-Standards sind identisch zu IEC-Standards.

38 Europäische Kommission. 2016. “Commission Notice — The “Blue Guide” on the implementation of EU products rules 2016”. Official Journal of the European Union. 59 C272. http://ec.europa.eu/DocsRoom/documents/18027

39 Europäische Kommission. “Standardisation Requests – Mandates”. http://ec.europa.eu/growth/single-market/european-standards/requests_en

40 CEN-CENELEC. (2015). European Guide on Standards and Regulation - Better regulation through the use of voluntary standards - Guidance for policy makers (CEN-CENELEC GUIDE 30). ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/30_CENCLCGuide30.pdf

41 CEN Website. “CEN Members”. https://standards.cen.eu/dyn/www/f?p=CENWEB:5:0

42 CEN-CENELEC. (2015). European Guide on Standards and Regulation - Better regulation through the use of voluntary standards - Guidance for policy makers (CEN-CENELEC GUIDE 30). ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Guides/30_CENCLCGuide30.pdf

- **Europäisches Institut für Telekommunikationsnormen (ETSI)**
  ETSI ist historisch bedingt für die europäische Normung im Telekommunikationsbereich zuständig. Im Gegensatz zu CEN/CENELEC können bei ETSI Unternehmen ebenso (stimmberechtigte) Mitglieder sein. Behörden, Normungsorganisationen und Unternehmen müssen Stimmanteile kaufen, die sie dann bei Abstimmungen über Standards geltend machen (gewichtetes Abstimmungsverfahren).

Grundsätzlich ist festzuhalten, dass der Austausch und die Verflechtungen zwischen nationalen, europäischen und internationalen Normungsorganisationen sehr intensiv sind. So basiert beispielsweise das 3rd Generation Partnership Project (3GPP), das international den Mobilfunk standardisiert, auf einem Zusammenschluss von sieben Normungsorganisationen, unter anderem aus China, Europa, Indien, Japan, Südkorea und den USA.[43] Weiterhin ist es gängig, dass Normungs- und Standardisierungsorganisationen über „Liaisons" untereinander Kontakt halten und sich austauschen. So wird die Arbeit des ISO/IEC JTC1 unter anderem von der europäischen Artikel-29-Datenschutzgruppe, der OECD und der ITU über Liaisons verfolgt.

3.2 Standardisierungsorganisationen

Im Gegensatz zu staatlich anerkannten Normungsorganisationen können Standardisierungsorganisationen durch unterschiedlichste Stakeholder oder Interessensgruppen gegründet werden. Sie unterscheiden sich teils stark hinsichtlich Governance, Transparenz und Entscheidungsfindungsprozessen. Im Folgenden werden lediglich drei der etablierten SDOs vorgestellt, die eine zentrale Rolle für IKT und IT-Sicherheit spielen.

- **Internet Engineering Task Force (IETF)**
  Die IETF ist eine lose Organisation, in der sich seit 1986 Internetexpert:innen zusammenfinden, um Internetstandards zu entwerfen und weiterzuentwickeln.[44] Im Gegensatz zu den zuvor erwähnten Normungsorganisationen beruht die IETF nicht auf formaler Mitgliedschaft, sondern verfolgt ein vollständig offenes Konzept: jede Person kann an Workshops und den mehrmals im Jahr stattfindenden IETF Meetings teilnehmen. Die Arbeit der IETF findet vorrangig über die Mailinglisten der Arbeitsgruppen statt. Der US-amerikanische Informatiker Dave Clarke sagte

43 3GPP. 2017. „Partners". http://www.3gpp.org/about-3gpp/partners

44 IETF Website. "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force". https://www6.ietf.org/tao.html

bezüglich Governance der IETF: *„We reject kings, presidents and voting. We believe in rough consensus and running code.“*[45] Die IETF hat tragende Protokolle des heutigen Internets standardisiert und ist für seine offene Weiterentwicklung verantwortlich. Die Bedeutung der IETF für Hersteller und Netzbetreiber zeigt sich an deren Beteiligung: Manche Unternehmen senden 30-90 Mitarbeiter:innen zu den mehrtägigen IETF Meetings.[46] Alle Dokumente der IETF, einschließlich der Protokolle der Treffen und Diskussionen, sind frei verfügbar, um so eine hohe Nachvollziehbarkeit des Standardisierungsprozesses sicherzustellen.[47] In ihren Arbeiten berücksichtigt die IETF auch die gesellschaftlichen Auswirkungen durch die globale Vernetzung.[48]

- **Institute of Electrical and Electronics Engineers (IEEE)**
  Mit über 423.000 Mitgliedern aus über 160 Ländern ist IEEE der größte technische Berufsverband der Welt.[49] Die Arbeit ist thematisch in verschiedene „Societies“ gegliedert (unter anderem Computer Society, Photonics Society, Power & Energy Society). Die Standardisierung findet in der IEEE Standards Association statt. Dort werden maßgeblich die LAN und WLAN-Standards (802.3, 802.11, 802.15) vorangetrieben.[50]

- **World Wide Web Consortium (W3C)**
  Das W3C ist die zentrale Standardisierungsorganisation zur Definition von Web-Standards, wie HyperText Markup Language (HTML) oder Extensible Markup Language (XML). W3C wurde 1994 gegründet und hat mittlerweile fast 500 Mitgliedsorganisationen.[51] Die Standardisierungsorganisation finanziert sich über Mitgliedsbeiträge, Spenden und Forschungsförderung.[52] Ähnlich zur IETF sind sowohl alle durch die W3C

45 Dave Clark. 1992. “A Cloudy Crystal Ball – Visions of the Future”. https://groups.csail.mit.edu/ana/People/DDC/future_ietf_92.pdf

46 IETF Website. “IETF Meeting Registration System – IETF 101”. https://www.ietf.org/registration/ietf101/attendance.py?sortkey=3&login=4323

47 IETF Website. “The Tao of IETF: A Novice‘s Guide to the Internet Engineering Task Force”. https://www6.ietf.org/tao.html

48 Ibid.

49 IEEE Website. “IEEE at a Glance”. https://www.ieee.org/about/today/at_a_glance.html?WT.mc_id=ab_lp_qui

50 IEEE Website. “IEEE Standards”. https://www.ieee.org/education_careers/education/standards/standards_index.html

51 W3C Website. „Current Members“. https://www.w3.org/Consortium/Member/List

52 W3C Website. „Facts about W3C“. https://www.w3.org/Consortium/facts

entwickelten Standards frei verfügbar, als auch die Teilnahme an der Standardisierungsarbeit für jeden möglich.[53]

3.3 Herausforderungen für und mit Standardisierung

Nicht zuletzt durch die voranschreitende Digitalisierung stehen internationale Normung und Standardisierung vor zentralen Herausforderungen:

- Standardisierung wird zunehmend komplexer und differenzierter, das heißt es wird schwieriger, die tatsächlichen Auswirkungen eines technischen Standards im Voraus abzuschätzen. Dies ist besonders in Europa vor dem Hintergrund des *New Legislative Frameworks* problematisch: Regulierungsziele werden durch Richtlinien und Verordnungen definiert, die durch Normung dann ausgestaltet und erfüllt werden müssen. Um sicherzustellen, dass verabschiedete Normen tatsächlich das definierte Regulierungsziel erreichen, hat die Europäische Kommission *Harmonised Standards Consultants* eingesetzt.[54] Diese sollen als unabhängige Expert:innen Normungsarbeit der drei europäischen Normungsorganisationen begleiten und sicherstellen, dass die entwickelten Normen tatsächlich konform zur Regulierung sind.

- Wie Unternehmen und Regierungen stehen auch SDOs durch die Digitalisierung als Querschnittsthema vor der Herausforderung, dass Digitalisierung alle Sektoren und Anwendungsbereiche betrifft. Dadurch ist oft eine klare Abtrennung von Standardisierungstätigkeiten nicht mehr möglich und unvorhergesehene Wechselwirkungen entstehen.[55] Als Reaktion auf die Digitalisierung als Querschnittsthema wurde daher JTC1 gemeinsam durch ISO und IEC ins Leben gerufen. Weiterhin haben Entscheidungen von Industriekonsortien (Bluetooth SIG, ZigBee SIG, und andere) unter Umständen Auswirkungen auf Normungsorganisationen. Wie viel an gegenseitiger Abstimmung und Kooperation notwendig ist, lässt sich zum einen gut an der stetig steigenden Zahl an Liaisons in den verschiedenen Gremien ablesen.[56] Zum anderen veröffentlicht die Europäische Kommission mit dem *Rolling Plan for ICT Standardization* einen Bericht, mit dem die

53 Laura DeNardis. 2015. „The Global War for Internet Governance." Yale University Press.

54 Europäische Kommission. "Call for expression of interest for Harmonised Standards Consultants". http://ec.europa.eu/growth/content/call-expression-interest-harmonised-standards-consultants_de

55 Europäische Kommission. 2016. "ICT Standardisation Priorities for the Digital Single Market". COM(2016) 176. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=15265

56 ISO Website. "ISO/IEC JTC 1/SC 27". https://www.iso.org/committee/45306.html

europäischen und internationalen Standardisierungsinitiativen zumindest in einigen zentralen Technologiebereichen nachverfolgt werden sollen.[57]

- Die entwickelten Standards von internationalen SDOs, wie IETF, IEEE oder W3C finden global Anwendung. Dadurch haben die in den SDOs getroffenen Entscheidungen direkt Auswirkungen auf Nationalstaaten und ihre Bevölkerung. Gleichzeitig ist es für Regierungen unter Umständen schwierig, die eigenen Interessen in besagten SDOs durchzusetzen.[58] Vor diesem Hintergrund hat die Europäische Kommission ein Förderprogramm aufgesetzt, das die Partizipation europäischer Expert:innen in internationalen SDOs unterstützen soll.[59]

- Da IKT einen immer stärkeren Einfluss auf unseren beruflichen und privaten Alltag hat, haben technische Standards ebenso potenzielle Auswirkungen auf Menschenrechte – beispielsweise Schutz der Privatsphäre, freie Meinungsäußerung. Daher sollten bei der Standardisierung diese Auswirkungen mitbedacht werden. So hat die *Internet Research Task Force* (IRTF), als Teil der IETF, eine eigene Forschungsgruppe ins Leben gerufen, die sich mit den Auswirkungen von Internetprotokollen auf Menschenrechte befasst.[60] Ebenso integrieren die Normungsorganisationen (nationale, europäische, internationale) unter anderem Verbraucherschutzorganisationen in die Standardisierungsarbeit.[61]

Damit ist die internationale IKT-Standardisierung ein Geflecht aus unzähligen SDOs in dem Industriekonsortien, lose Interessensgruppen und nationale Normungsorganisationen die Spielregeln der digitalen Welt definieren. Letztlich sind robuste und gute Standards zur Stärkung von IT-Sicherheit jedoch nur der erste Schritt, da nicht sichergestellt ist, dass sie zeitnah und vollständig befolgt werden.[62] Im folgenden Abschnitt soll daher die Beziehung zwischen Standardisierung und IT-Sicherheitszertifizierung näher beleuchtet werden.

57 Europäische Kommission. 2018. “Rolling Plan for ICT Standardisation 2018”. http://ec.europa.eu/growth/industry/policy/ict-standardisation_en#rolling_plan_ict_standardisation

58 Adam Langley. 2018. „TLS 1.3 and Proxies“. https://www.imperialviolet.org/2018/03/10/tls13.html

59 StandICT Website. “Supporting European Experts Contribution To International ICT Standardisation Activities”. https://standict.eu/

60 Internet Research Task Force. “Human Rights Protocol Considerations (hrpc)”. https://datatracker.ietf.org/rg/hrpc/about/

61 CEN-CENELEC. “Standardization and societal stakeholders”. https://www.cencenelec.eu/societal/Pages/default.aspx

62 Internet Society. 2014. “Anti-Spoofing, BCP 38, and the Tragedy of the Commons”. https://www.internetsociety.org/blog/2014/07/anti-spoofing-bcp-38-and-the-tragedy-of-the-commons/

4. Zertifizierung

Es mangelt weder an Protokollen zur sicheren Kommunikation und Datenübertragung[63] noch an Guidelines und Best Practices zur sicheren Softwareentwicklung.[64] Das bedeutet jedoch nicht, dass Unternehmen automatisch sichere Softwareentwicklung und Security-by-Design praktizieren.[65] Zertifizierung wird daher genutzt, um zu überprüfen und nachzuweisen, wie vertrauenswürdig ein Produkt, Prozess oder System einer Organisation ist. Zertifizierung baut grundsätzlich auf Standards auf, da Produkte oder Systeme gegen einen oder mehrere Standards evaluiert werden. Beispielsweise stellt die Europäische Union durch die CE-Kennzeichnung[66] bestimmte Anforderungen an die physische Sicherheit *(safety)* von Produkten auf dem europäischen Markt. Durch die CE-Kennzeichnung auf einem Produkt versichert der Hersteller, dass sein Produkt konform zu den relevanten Normen ist – im einfachsten Fall erfolgt diese Konformitätsbescheinigung durch den Hersteller selbst.[67] Je nach Produktgruppe kann es jedoch auch sein, dass eine Konformitätsbescheinigung durch ein externes, unabhängiges Prüflabor gefordert wird. Die CE-Kennzeichnung umfasst zwar (bisher) keine Tests bezüglich IT-Sicherheit, an ihr lassen sich jedoch die Zusammenhänge zwischen Standards, Zertifizierung und Akkreditierung verdeutlichen:

- **Standards:** Standards definieren Anforderungen und dienen als Referenz für die Zertifizierung.

- **Zertifizierung (IT-Sicherheit):** Überprüfung der Vertrauenswürdigkeit eines Produktes. Die zertifizierende Organisation (Prüflabor) überprüft, inwieweit das Produkt den zuvor definierten Sicherheitsanforderungen entspricht.

- **Akkreditierung:** Legt fest, welche Organisationen Zertifizierungen durchführen dürfen. Die Akkreditierung erfolgt regelmäßig durch

63 ENISA. (2017). “Improving recognition of ICT security standards: Recommendations for the Member States for the conformance to NIS Directive”. https://www.enisa.europa.eu/publications/improving-recognition-of-ict-security-standards/at_download/fullReport

64 Bruce Schneier. 2017. „Security and Privacy Guidelines fort he Internet of Things“. https://www.schneier.com/blog/archives/2017/02/security_and_pr.html

65 Heitzenrater, C., & Simpson, A. 2016. „A case for the economics of secure software development“. Proceedings of the 2016 New Security Paradigms Workshop. ACM Press. https://doi.org/10.1145/3011883.3011884

66 Europäische Kommission. “CE Marking”. https://ec.europa.eu/growth/single-market/ce-marking_de

67 Europäische Kommission. 2016. “Commission Notice — The “Blue Guide” on the implementation of EU products rules 2016”. Official Journal of the European Union. 59 C272. http://ec.europa.eu/DocsRoom/documents/18027

nationale Stellen. Im Rahmen des *New Legislative Frameworks* (CE-Kennzeichnung) ist dies in Deutschland die *Deutsche Akkreditierungsstelle* (DAkkS). Für IT-Sicherheit (Common Criteria, siehe nachfolgend) erfolgt die Akkreditierung jedoch durch das *Bundesamt für Sicherheit in der Informationstechnik* (BSI).[68]

Wie zuvor erwähnt umfasst die CE-Kennzeichnung bisher keine Überprüfung der IT-Sicherheit eines Produktes. Im weiteren Verlauf werden daher sowohl Rahmenwerke zur Zertifizierung der IT-Sicherheit als auch multinationale Abkommen der gegenseitigen Anerkennung solcher Zertifizierungen betrachtet.

Common Criteria

Common Criteria for Information Technology Security Evaluation (CC)[69] ist das am weitesten verbreitete und anerkannteste Framework zur Evaluierung beziehungsweise Zertifizierung der IT-Sicherheit von Produkten.[70] Das Common Criteria Development Board ist zuständig für deren Weiterentwicklung.[71] Da die CC ebenso anerkannter ISO/IEC Standard sind, werden sie auch durch das zuvor erwähnte ISO/IEC JTC1 weiterentwickelt.[72] Nachfolgend wird kurz der grundsätzliche, stark vereinfachte Ablauf bei CC Evaluierungen skizziert:

- Nutzer:innen (meist eine Expert:innengruppe) entwickeln ein **Schutzprofil (Protection Profile)** für eine bestimmte Anwendungsklasse. So entwarf beispielsweise das BSI ein Schutzprofil für Smart Meter Gateways, in dem definiert ist, welchen Sicherheitsanforderungen ein Smart Meter genügen muss, um in Deutschland eingesetzt werden zu können.[73]

- Ein Unternehmen beauftragt ein **unabhängiges Prüflabor** mit der Evaluierung ihres Produktes und spezifiziert durch **Sicherheitsvorgaben**

68 BSI Website. "Anerkennung von Stellen und Zertifizierung von IT-Sicherheitsdienstleistern". https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html

69 Ebenso gehört dazu die *Common Methodology for Information Technology Security Evaluation (CEM)*

70 Ein anderer, noch recht junger, Zertifizierungsstandard ist beispielsweise *IEC62443*, der eher auf Industrial Control Systems (ICS) fokussiert.

71 ENISA. 2018. "Overview of the practices of ICT Certification Laboratories". https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe/at_download/fullReport

72 ISO Website. "ISO/IEC JTC 1/SC 27 – Standards Catalogue". https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0

73 BSI Website. "Übersicht über die Schutzprofile und Technischen Richtlinien nach § 22 Abs. 2 Satz 1 MsbG" https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_node.html

(Security Target), welche Sicherheitsanforderungen eines oder mehrerer Schutzprofile erfüllt werden. Formales Ziel der Zertifizierung ist, die Erfüllung der definierten Sicherheitsvorgaben, die wiederum generische Schutzprofile referenzieren können, aber nicht müssen.

- Je nach Land muss das Prüflabor das Ergebnis der Evaluierung zunächst der **nationalen Zertifizierungsstelle** (in Deutschland dem BSI) vorlegen. Erst nach deren Zustimmung ist das Produkt erfolgreich nach CC zertifiziert.[74]

- Das Ergebnis einer Zertifizierung ist dabei nie, dass ein Produkt „sicher" ist, sondern lediglich, dass es **konform zu den Sicherheitsvorgaben** ist: Werden beispielsweise bestimmte Gefahren in den Sicherheitsvorgaben (bewusst) nicht beachtet, werden diese im Zuge der Zertifizierung auch nicht evaluiert. Umso wichtiger ist daher, dass die Sicherheitsvorgaben die tatsächlichen Gefahren (Angriffsszenarien) möglichst gut abbilden. In der Vergangenheit wurde weiterhin die geforderte Prüftiefe durch das *Evaluation Assurance Level* (EAL) ausgedrückt. Je höher das EAL, desto umfassender hat das Prüflabor getestet, inwieweit das Produkt tatsächlich die Anforderungen des Schutzprofils erfüllt.

4.1 Gegenseitige Anerkennung von Zertifizierung

Eine Zertifizierung nach Common Criteria kostet den Hersteller verhältnismäßig viel Zeit und Geld. Daher hat er ein Interesse daran, dass ein ausgestelltes Zertifikat möglichst international anerkannt wird, um den zeitlichen und finanziellen Aufwand mehrfacher Zertifizierung zu vermeiden. Zu diesem Zweck wurden Abkommen der gegenseitigen Anerkennung geschlossen (*Recognition Arrangements* oder *Agreements*). Gegenseitige Anerkennung bedeutet bei IT-Sicherheitszertifizierung vor allem, dem Gegenüber zu vertrauen. Zum einen wird darin vertraut, dass die nationalen Stellen die Prüflabore entsprechend beaufsichtigen. Weiterhin muss man darauf vertrauen, dass die ausländischen Prüflabore ähnlich gute Arbeit leisten wie die eigenen. Relevante Abkommen sind hier zum einen das internationale *CCRA* und das europäische *SOG-IS*. Beide sollen im Folgenden kurz vorgestellt werden:

Common Criteria Recognition Arrangement (CCRA)
CCRA ist das am weitesten verbreitete Abkommen zur gegenseitigen Anerkennung von Zertifizierung. Das Abkommen unterscheidet zwischen Ländern,

74 Europäische Kommission. 2017. "COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Cybersecurity Act"". SWD(2017) 500 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0500

die Zertifikate ausstellen und anerkennen (*Authorizing*) und Ländern, die Zertifikate lediglich anerkennen, aber selbst keine ausstellen (*Consuming*) – das heißt im Land selbst keine Zertifizierung durchführen.[75] Die Mitglieder des CCRA entwickeln gemeinsam Schutzprofile für bestimmte Produktgruppen beziehungsweise Anwendungsbereiche und definieren allgemeingültige Sicherheitsanforderungen. Die gegenseitige Anerkennung geht jedoch auch innerhalb der CCRA nur bis zu einer bestimmten Tiefe. In der Vergangenheit galt die Anerkennung nur auf recht niedrigen Stufen (EAL2), die kaum Rückschlüsse auf die tatsächliche Vertrauenswürdigkeit des Produktes zulassen.[76] Auch mit den 2012 neu eingeführten, gemeinsam entwickelten Schutzprofilen (*collaborative Protection Profiles*) ist die gegenseitige Anerkennung innerhalb der CCRA trotzdem deutlich beschränkt.[77]

- *Authorizing*: Australien, Kanada, Frankreich, Deutschland, Indien, Italien, Japan, Malaysia, Niederlande, Neuseeland, Norwegen, Südkorea, Spanien, Schweden, Türkei, Großbritannien, USA
- *Consuming*: Österreich, Tschechische Republik, Dänemark, Äthiopien, Finnland, Griechenland, Ungarn, Israel, Pakistan, Katar, Singapur

Senior Officials Group – Information Systems Security (SOG-IS)

SOG-IS ist ein Zusammenschluss einiger europäischer IT-Sicherheitsbehörden, mit dem Ziel der gegenseitigen Anerkennung gemeinsam entwickelter Schutzprofile und der Schaffung eines europäischen Marktes an Common Criteria zertifizierten Produkten.[78] Im Vergleich zu CCRA ist SOG-IS deutlich kleiner, sowohl hinsichtlich der teilnehmenden Länder als auch der gemeinsam entwickelten und anerkannten Schutzprofile.[79] Der technische Fokus liegt bei SOG-IS vor allem auf Smartcards (beispielsweise Personalausweise und Reisepässe), Tachographen und Hochsicherheitsmodulen.[80] Aufgrund der geringen Zahl an Mitgliedern und des starken Fokus auf wenige Anwen-

75 Common Criteria Recognition Arrangement. “Members of the CCRA”. https://www.commoncriteriaportal.org/ccra/members/

76 Common Criteria Recognition Arrangement. 2012. “Common Criteria Management Committee Vision Statement 2.0”. https://www.commoncriteriaportal.org/files/ccfiles/2012-09-001_Vision_statement_of_the_CC_and_the_CCRAv2.pdf

77 Europäische Kommission. 2017. “COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document “Cybersecurity Act””. SWD(2017) 500 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0500

78 Senior Officials Group Information Systems Security (SOG-IS). 2010. “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates 3.0”. https://www.sogis.org/documents/mra/20100107-sogis-v3.pdf

79 SOGIS Website. “Introduction”. https://www.sogis.org/index_en.html

80 SOGIS Website. “Protection Profiles”. https://www.sogis.org/uk/pp_en.html

dungsgebiete ist die gegenseitige Anerkennung jedoch deutlich höher als bei CCRA.[81]

- *Authorizing*: Deutschland, Frankreich, Großbritannien, Italien, Niederlande, Norwegen, Spanien, Schweden
- *Consuming*: Estland, Finnland, Kroatien, Luxemburg, Österreich, Polen

4.2 Herausforderungen von Zertifizierung und Anerkennung

IT-Sicherheit hat viel mit Vertrauen zu tun: Wie vertrauenswürdig ist der Hersteller des Produktes und seine Entwicklungsprozesse? Wie vertrauenswürdig sind das Prüflabor und wie kompetent die Mitarbeiter:innen, die die Zertifizierung durchführen? Wie vertrauenswürdig ist die nationale Stelle, die das Prüflabor beaufsichtigt? Wie vertrauenswürdig ist das Gremium, das die zugrundeliegenden Sicherheitsanforderungen definiert hat? Dies sind nur einige der Fragen, die entscheidend für die letztlich aufzubauende „Vertrauenskette" sind. Derzeit praktizierte Zertifizierung und die etablierten Regime der gegenseitigen Anerkennung stehen einigen grundsätzlichen Herausforderungen gegenüber:

- **Kosten und zeitlicher Aufwand**
  Eine Zertifizierung nach Common Criteria ist meist mit hohen Kosten für das Unternehmen verbunden. Die Zertifizierung eines Smart Meters würde nach Schätzungen von Expert:innen etwa 150.000€ in Frankreich und Großbritannien kosten. In Deutschland vermutlich 1.000.000€.[82] Schon in der Vergangenheit wurde immer wieder bemängelt, dass die Zertifizierung nach CC auch deutlich zu lange dauert – gerade hinsichtlich der immer kürzeren Innovationszyklen von IKT.[83] Je nach Prüftiefe kann eine Zertifizierung 9-24 Monate dauern – und länger.

- **Einmalige Prüfung und Updates**
  Eine Zertifizierung ist immer lediglich eine Momentaufnahme. Selbst wenn das Prüflabor den Hersteller bei der Entwicklung begleitet, kann ein Zertifikat keine Aussage über die Zukunft machen. Da immer mehr Funktionalität heutiger Produkte über Software definiert wird, stellt sich

81 SOGIS Website. "Status of SOG-IS participants / schemes". https://www.sogis.org/uk/status_participant_en.html

82 Europäische Kommission. 2017. "COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document "Cybersecurity Act"". SWD(2017) 500 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0500

83 Kaluvuri, Samuel Paul, Michele Bezzi und Yves Roudier. 2014. „A Quantitative Analysis of Common Criteria Certification Practice". Trust, Privacy, and Security in Digital Business, 132–143. Springer International Publishing. http://dx.doi.org/10.1007/978-3-319-09770-1_12.

ebenso die Frage, nach wie vielen und welcher Art von Softwareupdates ein Zertifikat seine Aussagekraft verliert. Aufgrund der angesprochenen finanziellen und zeitlichen Kosten einer Zertifizierung, scheuen Hersteller daher eine Re-Zertifizierung.[84] Im schlimmsten Fall führt dies auf Herstellerseite dazu, dass Systeme nicht weiterentwickelt werden, um die Zertifizierung nicht zu verlieren. Seitens der Anwender:innen werden im schlimmsten Fall nur aufgrund des Zertifikates veraltete Systeme gekauft.

- **Kein Markt für zertifizierte Produkte**
  Es gibt in Europa rund 30 Prüflabore, die CC-Evaluierungen durchführen dürfen[85] und seit 1999 wurden etwas über 2000 Produkte (weltweit) nach Common Criteria zertifiziert.[86] Beide Zahlen verdeutlichen, dass der Markt für zertifizierte Produkte sehr klein ist. Zwar fordern Regierungen in bestimmten Bereichen der öffentlichen Beschaffung (Personalausweis, Smart Meter Gateway und andere Projekte) zertifizierte Produkte, dies geschieht jedoch nur punktuell.[87] In Verbindung mit den zuvor genannten Problemen ergibt sich das derzeitige Bild, dass es kaum zertifizierte Produkte am Markt gibt.[88]

In der Theorie erfüllt Zertifizierung eine wichtige Aufgabe, indem nachvollzogen werden kann, inwieweit ein Produkt den geforderten Sicherheitsanforderungen entspricht. In der Praxis muss jedoch konstatiert werden, dass Common Criteria dies zumindest derzeit nicht leisten.[89] Dies liegt zum einen am Zertifizierungsprozess selbst, der mit hohem zeitlichem und finanziellem Aufwand verbunden ist. Zum anderen am grundsätzlichen Mechanismus der Zertifizierung, die als Momentaufnahme immer weniger der Realität ständi-

84 Anderson, Ross und Shailendra Fuloria. 2009. “Certification and evaluation: A security economics perspective”. IEEE Conference on Emerging Technologies & Factory Automation. http://dx.doi.org/10.1109/ETFA.2009.5347129.

85 ENISA. 2018. “Overview of the practices of ICT Certification Laboratories”. https://www.enisa.europa.eu/publications/overview-of-the-practices-of-ict-certification-laboratories-in-europe/at_download/fullReport

86 Europäische Kommission. 2017. “COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document “Cybersecurity Act””. SWD(2017) 500 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0500

87 ENISA. 2016. Workshop on Security Certification of ICT products in Europe. https://www.enisa.europa.eu/events/ict-security-certification-for-industry/ict-security-certification-for-industry-meeting-minutes

88 ECORYS. 2011. “Security Regulation , Conformity Assessment & Certification”. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/security/pdf/secerca_final_report_volume__1_main_report_en.pdf

89 Leverett, Éireann, Richard Clayton und Ross Anderson. 2017. “Standardisation and Certification of the ’Internet of Things”. Proceedings of WEIS 2017. https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

ger Softwareupdates entspricht. So bedingen sich letztlich auch die derzeit unzureichende IT-Sicherheitszertifizierung und die fragmentierte gegenseitige Anerkennung in Abkommen, wie CCRA oder SOG-IS. In einer Welt, die immer stärker von digitaler Kommunikation abhängig ist, sollte IT-Sicherheitszertifizierung eine zentrale Rolle bei der Identifikation vertrauenswürdiger Produkte spielen. Stattdessen ist sie nur für einige wenige öffentliche Projekte und in ganz bestimmten Anwendungsbereichen von Relevanz.

4.3 EU Cybersecurity Act

Im September 2017 hat die Europäische Kommission den Regulierungsentwurf des *Cybersecurity Acts*[90] vorgelegt. Eines der Ziele ist die Schaffung eines europaweit einheitlichen Zertifizierungsrahmens zur Stärkung der IT-Sicherheit. Im Rahmen des Cybersecurity Acts würde die *European Union Agency for Network and Information Security* (ENISA) beauftragt, gemeinsam mit nationalen Sicherheitsbehörden, Unternehmen und Wissenschaft Zertifizierungsschemata für verschiedene Produktklassen beziehungsweise Sektoren zu entwickeln. Da es sich zum Zeitpunkt des Schreibens um einen Regulierungsentwurf handelt und die Trilogverhandlungen noch bevorstehen, soll nachfolgend lediglich auf zentrale Konzepte eingegangen werden:

- **Verhältnismäßigkeit**
  Ein neues europäisches Zertifizierungssystem muss es leisten, gerade vor dem Hintergrund eines voranschreitenden Internets der Dinge, Sicherheitsanforderungen und Prüftiefe ins Verhältnis zu setzen.[91] Common Criteria ist zu aufwendig, um sinnvoll Smart Home-Produkte zu zertifizieren[92] – genau diese machen jedoch schon heute die Masse an vernetzten Geräten aus. Es benötigt daher Zertifizierungsschemata, durch die eine „Basissicherheit“ für Smart Home-Produkte und andere günstige IoT-Geräte sichergestellt werden kann.[93] Welche Sicherheitsanforderungen und Prüftiefe gefordert werden, sollte daher von mehreren Faktoren abhängen, unter anderem: Wahrscheinlichkeit eines physi-

90 Europäische Kommission. 2017. “Cybersecurity Package”. COM(2017) 477. https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

91 Verbruggen, Paul, Pieter Wolters, Carla Sieburgh und Corjo Jansen. 2016. „Towards Harmonised Duties of Care and Diligence in Cybersecurity“. http://dx.doi.org/10.2139/ssrn.2814101

92 Baldini, Gianmarco, Antonio Skarmeta, Elizabeta Fourneret, Ricardo Neisse, Bruno Legeard und Franck Le Gall. 2016. “Security certification and labelling in Internet of Things”. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). http://dx.doi.org/10.1109/WF-IoT.2016.7845514

93 Department for Digital, Culture, Media & Sport. 2018. “Secure by Design : Improving the cyber security of consumer Internet of Things Report”. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

schen Schadens (vernetzter Herd gegenüber Webcam), voraussichtliche Produktlebenszeit (Kühlschrank gegenüber Smartphone), Preis (smarte Beleuchtung gegenüber Smart-Lock).

- **Vergleichbarkeit**
  Bisher waren nach Common Criteria zertifizierte Produkte kaum untereinander vergleichbar.[94] Dies hat sich zwar durch die Einführung gemeinsamer Schutzprofile verbessert,[95] für ein zukünftiges Zertifizierungsregime muss die Sicherheit zertifizierter Produkte untereinander jedoch vergleichbar sein.[96] Je vergleichbarer die Vertrauenswürdigkeit von Produkten innerhalb eines Zertifizierungsschemas ist, desto eher wird Zertifizierung von Unternehmen als Wettbewerbsvorteil wahrgenommen werden.

- **Marktdurchdringung**
  Was den bisherigen Zertifizierungssystemen, wie Common Criteria, fehlt, ist Relevanz am Markt. Gerade in der Anfangsphase eines neuen Zertifizierungsrahmens auf EU-Ebene sollten die Mitgliedsstaaten ihre Kaufkraft durch die öffentliche Beschaffung flankierend einsetzen, um langfristig zertifizierte Produkte am Markt zu etablieren.

- **Skalierbarkeit**
  Damit Zertifizierung für viele Anwendungsbereiche an Bedeutung gewinnt, werden nationale Sicherheitsbehörden sich auf wenige Bereiche zurückziehen müssen, in denen der Staat besondere Schutzpflichten zu erfüllen hat – Ausweißdokumente, Smart Meter, und andere. In allen anderen Bereichen, gerade mit Blick auf Smart Home und das Internet der Dinge, sollte die Umsetzung von Mindestanforderungen statt Hochsicherheit im Mittelpunkt stehen. Langfristig sollte daher die Erweiterung der CE-Kennzeichnung um IT-Sicherheitsaspekte angestrebt werden. Dies hat mehrere Vorteile:

94 Kaluvuri, Samuel Paul, Michele Bezzi und Yves Roudier. 2014. „A Quantitative Analysis of Common Criteria Certification Practice“. Trust, Privacy, and Security in Digital Business, 132–143. Springer International Publishing. http://dx.doi.org/10.1007/978-3-319-09770-1_12.

95 Rannenberg, Kai. 2000. “IT Security Certification and Criteria: Progress, Problems and Perspectives”. Information Security for Global Information Infrastructures, IFIP. http://dx.doi.org/10.1007/978-0-387-35515-3_1

96 Europäische Kommission. 2017. “COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document “Cybersecurity Act””. SWD(2017) 500 final. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017SC0500

- **Verbindung von *Safety* und *Security***:
  Die CE-Kennzeichnung deckt bisher nur physische Produktsicherheit ab. Wie zuvor erwähnt, bedingen sich jedoch *Safety* und *Security* und sollten daher auch gemeinsam überprüft werden.
- **Vordefinierte Produktgruppen:**
  Für die CE-Kennzeichnung gib es bereits vordefinierte Produktgruppen, für die zügig IT-Sicherheitsanforderungen definiert werden könnten.[97]
- **Verpflichtende Mindestanforderung:**
  Durch die Erweiterung der CE-Kennzeichnung um IT-Sicherheitsanforderungen würde gewährleistet werden, dass internetfähige Geräte im europäischen Binnenmarkt nicht „unzumutbar gefährlich" sind, indem eine Mindestanforderung an die IT-Sicherheit gestellt wird.[98]

5. Schlussfolgerungen

Der Markt versagt derzeit verhältnismäßig vertrauenswürdige IT-Produkte zu produzieren.[99] Der Erfolg von Malware-Kampagnen, wie WannaCry oder Mirai zeigt, dass wir es mit einem globalen Problem zu tun haben. Für Regierungen bedeutet dies, dass eine Lösung des Problems nicht auf nationalen Alleingängen basieren kann – Kooperation und Kompromisse sind dringend nötig, um IT-Sicherheit langfristig, weltweit zu stärken. Geplante Initiativen des Koalitionsvertrags, wie gesetzliche Mindeststandards, sollten daher zumindest europäisch abgestimmt sein. Gerade der Cybersecurity Act besitzt das Potenzial, dass IT-Sicherheitszertifizierung zukünftig eine zentrale Rolle spielen kann, um die Vertrauenswürdigkeit eines Produktes verbindlich zu belegen. Gleichzeitig darf Zertifizierung als Mechanismus nicht überschätzt werden: Zertifizierung ist kein Allheilmittel, sondern kann immer nur ein Baustein einer nachhaltigen IT-Sicherheitspolitik sein. Weiterhin ist Zertifizierung grundsätzlich ein Kompromiss zwischen Aktualität und Prüftiefe (und damit Aussagekraft). So ist effektive und effiziente Zertifizierung in der Vergangenheit selten an der Technologie, sondern an Rahmenbedingungen, fehlender Anerkennung und falsch gesetz-

97 Europäische Kommission. „Harmonised Standards". http://ec.europa.eu/growth/single-market/european-standards/harmonised-standards_de

98 Zwetsloot, Gerard I.J.M., Sander Zwanikken und Andrew Hale. 2011. "Policy expectations and the use of market mechanisms for regulatory OSH certification and testing regimes". Safety Science 49, Nr. 7 (August): 1007–1013. http://dx.doi.org/10.1016/j.ssci.2010.12.006.

99 Jan-Peter Kleinhans. 2017. „Internet of Insecure Things".Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

ten ökonomischen Anreizen gescheitert.[100] Regulierer sollten daher immer das gesamte Ökosystem aus Standardisierung, Zertifizierung, Akkreditierung und Marktüberwachung betrachten:

- **Standardisierung, Zertifizierung und Haftung**
  Durch Zertifizierung und Konformität zu relevanten Standards kann ein Hersteller im Schadensfall regelmäßig Haftung ausschließen. Dadurch gibt es einen direkten Zusammenhang zwischen Standardisierung, Zertifizierung und Haftung.[101] Im Sinne des Verbraucherschutzes ist es daher umso wichtiger, dass bei der Standardentwicklung auf IT-Sicherheit geachtet wird und Zertifizierungsanforderungen möglichst hoch sind. Zu diesem Zweck sollten unter anderem Verbraucherschutzorganisationen und Wissenschaft deutlich stärker und institutionalisierter in die Standardisierung und (im Rahmen des Cybersecurity Acts) in die Entwicklung der Zertifizierungsschemata eingebunden werden.

- **Gegenseitige Anerkennung basiert auf Vertrauen**
  IT-Sicherheitszertifizierung zur Überprüfung der Vertrauenswürdigkeit muss eine stärkere Rolle in Europa spielen – durch den *Cybersecurity Act* könnte zukünftig ein tatsächlich einheitlicher Zertifizierungsrahmen geschaffen werden. Hierfür ist gegenseitige Anerkennung von entscheidender Bedeutung. Es müssen daher transparente Prozesse und Formate der gegenseitigen Kontrolle entwickelt werden, um die notwendige Vertrauensbasis für diese gegenseitige Anerkennung zu schaffen. Alle europäischen Mitgliedsstaaten werden sich nicht direkt in gleichem Maße vertrauen: Staaten werden auch weiterhin im Bereich der nationalen Sicherheit und bei kritischen Infrastrukturen die Zertifizierung lieber im eigenen Land durchführen wollen. Um gegenseitiges Vertrauen in die zu etablierende Zertifizierungsinfrastruktur aufzubauen, sollte daher zunächst auf Smart Home-Produkte und andere „nicht kritische“ Anwendungen fokussiert werden.

- **Marktüberwachung**
  Schon heute ist die Marktüberwachung der CE-Kennzeichnung unzureichend.[102] Stichproben durch Prüflabore zeigen immer wieder, dass es un-

100 Murdoch, Steven, Mike Bond und Ross J. Anderson. 2012. “How Certification Systems Fail: Lessons from the Ware Report”. IEEE Security & Privacy Magazine. http://dx.doi.org/10.1109/MSP.2012.89.

101 Leverett, Éireann, Richard Clayton und Ross Anderson. 2017. “Standardisation and Certification of the ’Internet of Things”. Proceedings of WEIS 2017. https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

102 Algemene Rekenkamer. 2016. “Products sold on the European market : unravelling the system of CE marking”. https://english.rekenkamer.nl/publications/reports/2017/01/19/products-sold-on-the-european-market-unraveling-the-system-of-ce-marking

sichere Produkte am Markt gibt und dass sich Hersteller nicht an die vorgeschriebenen Sicherheitsanforderungen halten. Wenn es zukünftig auch Anforderungen an die IT-Sicherheit gibt, muss das System der europäischen Marktüberwachung substanziell und zügig modernisiert werden.

- **Öffentliche Beschaffung**
  Die öffentliche Beschaffung muss stärker ihre Rolle am Markt wahrnehmen, indem durchgängig zertifizierte Produkte gefordert werden.

- **Rolle von Verbraucher:innen**
  Schon heute melden unabhängige IT-Sicherheitsforscher:innen und Hacker:innen häufig Schwachstellen an Hersteller und Betreiber. Wie wichtig diese Arbeit ist, sieht man unter anderem an der stetig wachsenden Popularität von Bug Bounty-Programmen.[103] Zukünftig sollten daher bei der Zertifizierung beziehungsweise Konformitätsbewertung und der Marktüberwachung Verbraucher:innen und Sicherheitsforscher:innen besser miteinbezogen werden. Zum einen müssen Erkenntnisse über unsichere Produkte besser und schneller an Verbraucher:innen kommuniziert werden, als dies bisher durch das europäische *Rapid Alert System* geschieht.[104] Zum anderen sollte es für Sicherheitsforscher:innen möglich sein, gefundene Schwachstellen in Produkten nicht nur an die Hersteller, sondern auch an die Marktüberwachung zu melden. Dies ist vor allem wichtig, wenn der eigentliche Gerätehersteller nicht ausfindig gemacht oder kontaktiert werden kann.

103 HackerOne Website. “Bug Bounty Programs”. https://hackerone.com/bug-bounty-programs

104 Europäische Kommission. „Rapid Alert Sytsem for dangerous non-food products“. https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/repository/content/pages/rapex/index_en.htm

Danksagung

Der Autor bedankt sich bei den Gesprächspartner:innen für ihre Offenheit, das Vertrauen und die interessanten Einblicke: Knut Blind, Diny van Est, Sibylle Gabler, Jeannette Hofman-Züter, Olia Kanevskaia, Raoul Kirmes, Linda Meijer-Wassenaar, Giulia Pastorella, Staffan Persson, Martina Rohde, Peter Rost, Ulrich Sandl, Martin Uhlherr und Matthias Waehlisch.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über den Autor

Jan-Peter Kleinhans
Jan-Peter Kleinhans ist Leiter des Projekts IT-Sicherheit im Internet der Dinge und fragt sich, wie eine nachhaltige und effektive IT-Sicherheitspolitik aussehen müsste. Zuvor arbeitete er an verschiedenen Themen der staatlichen Überwachung (parlamentarische Kontrolle der Geheimdienste, Transparenz bei polizeilichen Überwachungsmaßnahmen). Außerdem beschäftigt er sich mit der Frage, ob unsere Gesellschaft ihre digitale Infrastruktur effizient reguliert – vom Breitbandausbau über Netzneutralität bis hin zu Frequenzpolitik. Jan-Peter ist Fellow der Transatlantic Digital Debates 2016. Außerdem ist er Projektbeirat des Projekts „Trusted Computing – Aufbau von Zertifizierungsinfrastrukturen zur Sicherung von Marktzutritt und Wettbewerb“ des Bundesministeriums für Wirtschaft und Energie (BMWi). Vor seiner Zeit bei der SNV arbeitete er 2013 bei netzpolitik.org. Jan-Peter studierte Kommunikationswissenschaften in Uppsala, Schweden und Wirtschaftsinformatik in Darmstadt.

So erreichen Sie den Autor

jkleinhans@stiftung-nv.de
+49 (0)30 81 45 03 78 99
@JPKleinhans

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de