Digitale Agenda und Cybersicherheit

Hans-Wilhelm Dünn

Den offensichtlichsten Digitalisierungsschub des vergangenen Jahres stellt wohl die verstärkte Nutzung des Homeoffice dar. Waren zum Beispiel in Deutschland vor der Covid-19-Pandemie nur 4 Prozent aller Beschäftigten ausschließlich oder überwiegend im häuslichen Rahmen beruflich tätig, so steigerte sich dieser Wert durch die Pandemie auf bis zu 27 Prozent.[1] 58 Prozent davon arbeiten auch mit eigenen Endgeräten.[2] Was in den ersten Tagen des Lockdowns überstürzt begonnen wurde, zog so manche Sicherheitslücke nach sich, die sich bedrohlich auswirken kann. Angriffe nehmen zu, denn auch Cyberkriminelle erkennen das Potential des schnellen Wachstums an Einfallstoren.

Wirtschaftliche Risiken bei kleinen und mittleren Unternehmen

Für nicht wenige der kleinen und mittleren Unternehmen (KMU) wirkten sich Hackerangriffe in der Vergangenheit existenzbedrohend aus.[3] Dies stellt besonders in Deutschland ein großes Problem dar, wo KMU das Rückrat der Wirtschaft bilden, indem sie einen nicht zu unterschätzenden Anteil zur Konjunktur beitragen. Diesem Umstand trägt auch die neue Cybersicherheitsstrategie der Europäischen Union (EU) Rechnung, die insbesondere den KMU sowie Einzelunternehmen ein schwach ausgeprägtes Bewusstsein für Cybersicherheit bescheinigt.[4] In der im Dezember 2020 von der Europäischen Kommission vorgelegten und im Juni 2021 vom Europäischen Parlament angenommenen Cybersicherheitsstrategie für die digitale Dekade wird ein Netz von KI-gestützten[5] Sicherheitseinsatzzentren für ein echtes Cybersicherheitsschutzschild entworfen. Dieses soll frühzeitige Signale von Cyberangriffen erkennen und präventive Maßnahmen ermöglichen. KMU sollen im Rahmen digitaler Innovationszentren unterstützt werden. Ähnlich lautende strategische Ansätze finden sich auch im Entwurf der Cybersicherheitsstrategie für Deutschland 2021 des Bundesministeriums des Innern, für Bau und Heimat (BMI), allerdings wird hier unter dem Punkt „Unternehmen in Deutschland schützen" hauptsächlich auf die seit Jahren bestehenden Programme und Angebote hingewiesen (unter anderem Mittelstand-Digital-Zentren, Transferstelle IT-Sicherheit, Allianz für Cybersicherheit), ohne die Notwendigkeit neuer Förderprogramme und Maßnahmen zur niedrigschwelligen Implementierung von Sicherheitsmechanismen zu erkennen.[6] Die zahlreichen Angriffe auf IT-Infrastruktur der vergangenen Monate haben gezeigt, dass die vorhandenen Bemühungen

1 Helge Emmler/Bettina Kohlrausch: Homeoffice: Potenziale und Nutzung, in: Policy Brief WSI 3/2021, S. 5–9, hier S. 5.
2 Bundesamt für Sicherheit in der Informationstechnik: IT-Sicherheit im Home-Office unter besonderer Berücksichtigung der COVID19 Situation, in: Ergebniskurzbericht einer repräsentativen Umfrage des BSI 2021, S. 5.
3 Bundesamt für Sicherheit in der Informationstechnik: IT-Sicherheit im Home-Office, 2021, S. 17.
4 Europäisches Parlament: Entschließung des Europäischen Parlaments vom 10. Juni 2021 zu der Cybersicherheitsstrategie der EU für die digitale Dekade, 10.6.2021, 2021/2568(RSP), S. 4.
5 KI = Künstliche Intelligenz.
6 Bundesministerium des Inneren, für Bau und Heimat: Cybersicherheitsstrategie für Deutschland 2021, Juni 2021, Entwurfsversion, S. 51.

auf nationaler Ebene nicht ausreichend sind, um präventive Schutzmaßnahmen bei der Mehrheit der wirtschaftlichen Player etablieren. Der Verweis auf Bestehendes darf hier nicht dazu führen, weitere notwendige Schritte zu gehen.

Kompatibilität nationaler und europäischer Cyberstrategien und Aufbau von Cyberkompetenz

Auch wenn die Überarbeitung der seit 2016 bestehenden deutschen Cybersicherheitsstrategie vor dem Hintergrund technischer und gesellschaftlicher Weiterentwicklungen grundsätzlich zu begrüßen ist, so wirft sie doch ein Schlaglicht auf die teils parallelen, teils redundanten, teils gegensätzlichen Bemühungen, der globalen Herausforderung IT-Sicherheit zu begegnen. So soll die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in die Lage versetzt werden, neu entdeckte Sicherheitslücken offenzuhalten, um diese für deutsche Sicherheitsbehörden nutzbar zu machen. Seit Juni 2021 dürfen Verfassungsschutzbehörden und Bundespolizei zudem mit einem sogenannten Staatstrojaner die Geräte von Verdächtigen überwachen und auslesen.[7] Ein ähnliches Vorhaben wurde 2019 vom österreichischen Verfassungsgerichtshof für verfassungswidrig erklärt.[8] Hier zeigt sich, dass eine einheitliche EU-weite Regelung in relevanten Themenfeldern vor großen Herausforderungen steht. Sicherheitsbedrohungen machen an Staatsgrenzen nicht Halt, umso erstaunlicher ist die Tatsache, dass die Cyberssicherheitsstrategie als „eine der obersten Prioritäten der Europäischen Kommission und ein Eckpfeiler des digitalen und vernetzten Europas“[9] im Rahmen einer Richtlinie verabschiedet wurde, die erst ihre Wirkung entfalten kann, wenn sie innerhalb von 18 Monaten in den Mitgliedsstaaten in einzelnen Gesetzgebungsverfahren und Strategien etabliert worden sein wird.

Die EU versteht sich als Wertegemeinschaft und sollte auch im Digitalen den Anspruch verfolgen einen nach rechtsstaatlichen, demokratischen Prinzipien gestalteten Raum zu schaffen. Um die Wettbewerbsfähigkeit und Autonomie der Cybersicherheitsbranche der EU zu steigern sowie Cyberbedrohungen zu erkennen, wurde im Dezember 2020 das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich Cybersicherheit (European Cybersecurity Competence Centre, ECCC) gegründet das in ein Netz nationaler Koordinierungszentren eingebettet ist. Diese geschaffene Struktur soll Cyberfachwissen bündeln und die Etablierung von Sicherheitslösungen fördern. Das Zentrum mit Sitz in Bukarest ergänzt die Tätigkeit der Agentur der Europäischen Union für Cybersicherheit (European Union Agency for Cybersecurity, ENISA).[10]

Schutz kritischer Infrastruktur und Cyber-TÜV

Die Ransomware-Angriffe des letzten Jahres zeigen, welche Risiken mangelnde Sicherheitsvorkehrungen haben können. Bei diesen Attacken handelt es sich in der Regel um Trojaner-Software, mit der Hacker ins System eindringen und Nutzung und Zugriff auf Daten für das gesamte System verhindern. Oft werden diese Instrumente eingesetzt, um

7 Patrick Beuth: Bundestag genehmigt Staatstrojaner für alle, in: Der Spiegel, 10.6.2021.

8 Simon Koenigsdorff: Österreichisches Verfassungsgericht stoppt Staatstrojaner, in: Heise online, 11.12.2019.

9 Europäische Kommission: Pressemitteilung, Neue Cybersicherheitsstrategie der EU und neue Vorschriften zur Erhöhung der Widerstandsfähigkeit kritischer physischer und digitaler Einrichtungen, 16.12.2020, IP/20/2391.

10 Rat der Europäischen Union: Pressemitteilung, Neues Kompetenzzentrum und Netz für Cybersicherheit: informelle Vereinbarung mit dem Europäischen Parlament, 11.12.2020, IP/20/2384.

Lösegeld zu erpressen oder anderweitigen Schaden anzurichten. Das Ausnutzen bestehender Sicherheitslücken ist also kein staatliches Privileg zur Kriminalitätsbekämpfung, sondern kann auch von kriminellen oder terroristischen AkteurInnen verwendet werden. Ein Offenhalten dieser Sicherheitslücken ist somit kritisch einzuordnen, da sie die Sicherheit von Unternehmen, Institutionen und BürgerInnen gefährden kann. Wer alle Tresorschlüssel für den Zugang zu Systemen sammelt und aufbewahrt, muss nur selbst Opfer eines Angriffs werden, um die Schwachstellen aller anderen preiszugeben. Besonders der Schutz der kritischen Infrastruktur (KRITIS) kann zur Achillesverse für die europäische Gesellschaft werden. Ein Ausfall von Systemen in diesem Bereich könnte Versorgungsengpässe und andere gravierende Folgen nach sich ziehen. Als im Mai 2021 die irische Gesundheitsbehörde Health Service Executive nach einem Angriff ihr IT-System herunterfahren musste, hatte dies unmittelbare Auswirkungen auf Termine für Untersuchungen, die Terminvergabe von Hausärzten und die Veröffentlichung von Testergebnissen.[11]

Doch nicht nur Sicherheitslücken in der KRITIS stellen eine Gefahr dar. Auch die Abhängigkeit von Software aus Drittländern verhindert eine umfassende Sicherheitsarchitektur im Netz. Zuletzt wurde dies deutlich als durch einen Ransomware-Angriff auf das US-IT-Unternehmen Kaseya die Kassen der schwedischen Supermarktkette Coop ausfielen und 800 Filialen im Land geschlossen werden mussten.[12]

Das Dilemma in dem sich die europäische Cyberpolitik bewegt, zeigt sich an der Nutzung von Softwareprodukten in öffentlichen Verwaltungen. So arbeiten 96 Prozent der Bundesverwaltungen mit den Produkten eines einzigen US-amerikanischen Herstellers[13] – und dies trotz Bedenken des Europäischen Datenschutzbeauftragten bezüglich der Kontrolle, Weitergabe und Verarbeitung von Daten auch durch Drittstaaten.[14] Die bestehenden Systeme auf Grundlage der Produkte aus Drittstaaten bilden die Grundlage unseres Cyberraumes und lassen sich nicht ohne weiteres ersetzen. Dies wäre auch nicht wünschenswert, da Europa in einer globalisierten Welt auch auf die Kompatibilität im weltweiten Maßstab angewiesen ist. Entscheidend sollte sein, die Hoheit über die Zusammensetzung und Funktionsweise der eigenen Systeme zu erlangen. Durch Einblick in bestimmte Soft- und Hardwarekomponenten können technische Lösungen gefunden werden, die Praktikabilität und den Anspruch von Cybersouveränität vereinbaren.

Doch wie könnte eine Lösung aussehen? Wenn Europa sowohl als wirtschaftliche Macht, als auch als Wertegemeinschaft die eigenen Zielsetzungen verfolgen und eigenen Ansprüchen im digitalen Raum gerecht werden möchte, muss dies mit einem Kompetenzgewinn auf dem Softwaremarkt einhergehen. Software aus Drittstaaten wird derzeit oft ohne Einsicht in den Aufbau und die Beschaffenheit übernommen. Ähnlich wie bei der Anschaffung von Autos sollten Softwarenutzer ein durchsetzbares Interesse haben, vor dem Kauf einen Blick unter die Motorhaube zu werfen. Der Aufbau von sogenannten Security Labs kann dabei helfen, Software zu prüfen und insbesondere für kritische Bereiche eine Verwendungsempfehlung oder Warnung auszusprechen, die dann zu entsprechenden Konsequenzen führen würde. Mit diesem unabhängigen Software-TÜV

11 Volker Briegleb: Ransomware legt IT des irischen Gesundheitswesens lahm, in: Heise online, 14.5.2021.
12 Katharina Heflik/Jona Spreter: Cyberattacke trifft 800 Filialen einer schwedischen Supermarktkette, in: Zeit Online, 3.7.2021.
13 Jana Ballweber: Deutsche Verwaltung nutzt Microsoft-Produkte nicht rechtskonform, in: netzpolitik.org, 14.9.2020.
14 Euroäischer Datenschutzbeauftragter: Outcome of own-initiative investigation into EU institutions‘ use of Microsoft products and services, 2.7.2020.

können die NutzerInnen Produkte besser einordnen und sicher verwenden. Insbesondere für den Schutz der KRITIS scheint eine unabhängige Institution unabdingbar, die den Einsatz unsicherer Komponenten untersagen kann. In Deutschland übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) diese Überprüfung, ist dabei jedoch dem BMI unterstellt.[15]

Perspektivisch erscheint es sinnvoll, den Aufbau einer unabhängigen Stelle auf europäischer Ebene zu forcieren, die die Überprüfung von Soft- und Hardware unter Bezug auf verbindliche europäische Maßstäbe vornimmt. Als ersten Schritt zu einem europäischen Security Lab kann man das Label „Cybersecurity Made in Europe" verstehen, das von der European Cyber Security Organisation (ECSO) initiiert wurde und von 16 autorisierten Verbänden vergeben wird. Unternehmen deren Hauptsitz und Kernmarkt Europa ist und deren Mehrheit der Mitarbeitenden hier tätig ist, können das Label führen. Sie müssen den Sicherheitsanforderungen für die Beschaffung sicherer Informations- und Kommunikationstechnologien der ENISA zustimmen. Dazu gehören unter anderem Security by Design (das permanente Mitdenken sicherheitstechnischer Aspekte in der Entwicklung), Strong Authentification (die Ergänzung von Passwörtern durch weitere Elemente wie Captchas oder Sicherheitsfragen) sowie die Sicherheit von Lieferketten.[16] Das Label fungiert als Marketingmaßnahme für Unternehmen und kann die Kaufentscheidung von AnwenderInnen beeinflussen. Darüber hinaus benötigt die EU jedoch eine Institution, die nicht nur auf Bewusstseinsbildung der VerbraucherInnen setzt, sondern mit Kompetenz und Durchsetzungskraft transparente Kriterien für den Einsatz von IT-Technologie definiert und überprüft.

Security by Design im Internet der Dinge

Insbesondere das Kriterium Security by Design ist entscheidend für die Entwicklung praktikabler IT-Lösungen und gewinnt immer mehr Raum. So wie in einem Auto der Sicherheitsgurt bei der Konstruktion mitgeplant wird, so erfordern auch Programme und Technologien einen kontinuierlichen Fokus auf Sicherheitsaspekte. Besonders im Internet der Dinge mit seiner zunehmenden Vernetzung verschiedener Schnittstellen müssen diese Aspekte von Anfang an mitgedacht werden, um die Angriffsfläche zu reduzieren und am Ende nicht aufwendig Sicherheitslücken schließen zu müssen. Im Rahmen der deutschen EU-Ratspräsidentschaft wurden im Dezember 2020 dazu Ratsschlussfolgerungen getroffen, die dafür sorgen sollen, dass wirksame Sicherheitsmaßnahmen im Internet der Dinge integriert werden. Die aufgezeigten Leitlinien sollen zukünftig in allen netzwerkfähigen Geräten ein Mindestmaß an Sicherheit gewährleisten und basieren auf dem europäischen Rahmenwerk für Cybersicherheitszertifizierung. Security by Design umfasst in diesem Fall nicht nur die Sicherung der Endgeräte, sondern der gesamten Lieferkette inklusive aller Soft- und Hardware sowie Dienstleistungen.[17] Inwieweit der Ratsbeschluss weiterverfolgt wird, hängt vom Handeln der Kommission ab, die eine Initiative in den europäischen Gesetzgebungsprozess einbringen müsste.[18]

15 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, in: Bundesgesetzblatt Teil 1, Nr. 25, 27.5.2021, S. 1122.

16 Agentur der Europäischen Union für Cybersicherheit: Indispensable baseline security requirements for the procurement of secure ICT products and services, 21.1.2017.

17 Agentur der Europäischen Union für Cybersicherheit: Guidelines for Securing the Internet of Things, 9.11.2020, S. 38.

18 Rat der Europäischen Union: Council Conclusions on the cybersecurity of connected devices, 2.12.2020.

Fachkräftegewinnung und Sensibilisierung der NutzerInnen

Mit zunehmender Durchdringung des analogen Alltags mit digitalen Hilfsmitteln, Endgeräten und vernetzten Lösungen wird deutlich, dass die gesellschaftliche Entwicklung nicht immer mit dem technischen Fortschritt mithalten kann. Während Haushaltsgeräte „smart" miteinander kommunizieren können, ist ein Großteil der deutschen Bevölkerung nicht ausreichend für Schutzmaßnahmen sensibilisiert. Mehr als die Hälfte verwendet keine sicheren Passwörter, nur 20 Prozent legen Sicherheitskopien für ihre Daten an.[19] Diese Diskrepanz zwischen technischen Möglichkeiten und digitaler Kompetenz hat auch die Europäische Kommission im März 2021 im Rahmen der Digitalziele der EU für 2030 ausgedrückt. Demnach sollen bis zum Ende des Jahrzehnts 80 Prozent der Erwachsenen über grundlegende digitale Kompetenzen verfügen.[20] Darauf aufbauend sollen Europäisches Parlament und Rat ein Maßnahmenprogramm beschließen, um dieses und weitere Ziele zu erreichen.

Das BMI identifiziert vor allem im Bereich der schulischen und betrieblichen Bildung erhebliche Defizite. Ob die in der Cybersicherheitsstrategie dargestellte Forschungsförderung und eine aufgelegte Sensibilisierungskampagne ausreichen, um in der Breite der Bevölkerung digitale Kompetenzen zu vermitteln, wird sich zeigen.[21] Insbesondere die als defizitär analysierte schulische und betriebliche Bildung benötigt weitere Unterstützung. Vor allem junge Menschen müssten mit den Chancen und Risiken des Internets vertraut gemacht werden, einerseits um die sich bietenden Möglichkeiten der Digitalisierung risikoarm nutzen zu können. Zum anderen rekrutieren sich aus diesem Pool junger Menschen die IKT-Fachkräfte von morgen. 20 Mio. davon sollen EU-weit bis 2030 tätig sein. In der Realität fehlen heute allein dem deutschen Arbeitsmarkt 86 000 Fachkräfte, 2015 hatte es noch halb so viele offene Stellen gegeben.[22] Dort wo junge Menschen am leichtesten mit IT-Kenntnissen in Berührung kommen könnten, in der Schule, stellt sich aufgrund der Zuständigkeit der Länder die Situation sehr differenziert und teilweise desolat dar. In zwei Bundesländern (Bremen und Hessen) gibt es überhaupt keinen Informatikunterricht in der Sekundarstufe I, neun weitere Bundesländer bieten dies lediglich im Wahlbereich an. Der angebotene Unterricht unterscheidet sich zudem stark im Umfang.[23] Daran konnte bisher auch der 2019 ins Leben gerufene Digitalpakt nichts ändern von dem bis Ende 2020 lediglich 112 Mio. Euro von zur Verfügung stehenden 5 Mrd. Euro abgerufen wurden.[24] Im Zuge der Pandemie wurde zwar ein gut genutztes Sofortausstattungsprogramm für die Ausrüstung mit digitalen Endgeräten auf den Weg gebracht, jedoch müssten Medien in sinnvoller und pädagogischer Weise in den Unterricht eingebunden werden. So wie ein Buch ohne die entsprechenden Lesekompetenzen keinen pädagogischen Wert hat, so muss auch für digitale Medien ein didaktischer Rahmen gestaltet werden. Dies ist im Digital-

19 BSI/Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK): Digitalbarometer: Bürgerbefragung zur Cybersicherheit. Kurzbericht zu den Umfrageergebnissen der ProPK und des BSI, August 2020, S. 5.

20 Europäische Kommission: Mitteilung, Digitaler Kompass 2030: Der europäische Weg in die digitale Dekade, 9.3.2021, IP/21/983.

21 Bundesministerium des Inneren, für Bau und Heimat: Cybersicherheitsstrategie für Deutschland 2021, S. 21 f.

22 Bitkom: Pressemitteilung, 86 000 offene Stellen für IT-Fachkräfte, 16.12.2020.

23 Richard Schwarz et al.: Informatikunterricht in Deutschland – Eine Übersicht, in: Informatik Spektrum 44/2021, S.95–103, hier S. 98 f.

24 Bundesministerium für Bildung und Forschung/Kultusministerkonferenz: Pressemitteilung, Karliczek/KMK: „Bund und Länder arbeiten bei der Digitalisierung gut zusammen und kommen voran.", 19.2.2021.

pakt auch verankert, der geringe Mittelabfluss legt jedoch nahe, dass die angestrebten Aus-, Fort- und Weiterbildungen von Lehrenden und der Aufbau von Infrastruktur und entsprechender Managementsysteme nur langsam vorangehen. Nur mit einer qualitativ hochwertigen IT-Bildung kann jedoch langfristig der Bedarf an Fachkräften für Wirtschaft, Politik und Wissenschaft gedeckt werden. Die Kultushoheit liegt klar auf der Ebene der Länder, trotzdem kann auch die EU auf diesem Feld Potenziale freilegen und Förderung forcieren. So könnte durch die Etablierung von Universitätsschwerpunkten Kompetenz und wissenschaftliche Expertise für Bildungsanbieter zur Verfügung gestellt werden. Durch die Bildung neuer Cluster können die Universitäten außerdem als Zentren für die Zusammenarbeit von Schulen, Weiterbildungseinrichtungen und Wirtschaft fungieren.

Bekämpfung von Cyberkriminalität

Auch vor dem Hintergrund des Umgangs mit Internetkriminalität scheint es geboten, weiterhin auf Qualifizierung zu setzen. 25 Prozent der InternetnutzerInnen in Deutschland sind bereits mindestens einmal Opfer von Cyberkriminalität geworden, zwei Drittel hätten dabei Schaden davongetragen.[25] Die gravierenden Auswirkungen solcher Vorfälle korrespondieren mit einer Hilflosigkeit der Betroffenen. Nur jeweils etwa ein Drittel habe sich selbst helfen können oder Anzeige bei der Polizei erstattet. Der Wunsch nach polizeilicher Beratung ist groß. Warum also nutzen BürgerInnen nicht in jedem Fall die Hilfe der Polizei bei Straftaten im Cyberraum? Oftmals werden in Ermittlungsverfahren die Endgeräte und Datenträger der Betroffenen als Beweismittel einbehalten, sodass sensible Daten nicht mehr zur Verfügung stehen. Delikte wie beispielsweise Ransomware-Angriffe erfordern zudem ein schnelles Handeln, was nicht immer mit den langen Ermittlungsverfahren der Polizei kompatibel ist. Hier müssen Strafverfolgungsbehörden schneller Ergebnisse liefern. Ein bewährtes Instrument dafür ist die vermehrte Einrichtung von Schwerpunktstaatsanwaltschaften zum Thema Cybercrime, um Know-How und Manpower zu konzentrieren und so Verfahren zu beschleunigen.

Fazit

Die aufgezeigten Problemfelder machen deutlich, dass ein proaktives Handeln der politischen Ebene, welches über die Erstellung von Konzepten und Strategien hinausgeht, erforderlich ist. Damit die EU in einer globalisierten Welt den Cyberraum mit eigenen Maßstäben und Werten gestalten kann, ist ein harmonisiertes Vorgehen auf europäischer Ebene unentbehrlich. Dazu braucht es vor allem Sensibilität und Problembewusstsein für Cybersicherheit in breiten Teilen der Bevölkerung und des politischen Diskurses.

Weiterführende Literatur

Michael Gehler et al. (Hrsg.): Die Europäische Union als Verantwortungsgemeinschaft: Anspruch und Wirklichkeit, Wien 2020.

Sophie Tschorr: Der Kampf gegen Computerkriminalität in Europa: Normen, Institutionen und Kooperationen, Baden-Baden 2020.

25 Bundesamt für Sicherheit in der Informationsrechnik: Digitalbarometer: Bürgerbefragung zur Cybersicherheit. Kurzbericht zu den Umfrageergebnissen der ProPK und des BSI, August 2020, S. 3.