Michael Sparenberg, Norbert Pohlmann

Cybersecurity made in EU

Ein Baustein europäischer Sicherheit

Europa will in allen Bereichen enger zusammenwachsen. Cybersicherheit ist dabei ein bedeutender Faktor. Die allumfassende Digitalisierung birgt enorme Chancen und schafft zugleich neue Risiken. Grenzüberschreitende Lösungen sind gefragt.

Neue Dynamik

Im Dezember 2017 beschlossen 24 EU-Mitgliedsstaaten in Brüssel die ständige militärische Zusammenarbeit und legten damit den Grundstein für die bereits seit 2003 geplante Europäische Sicherheits- und Verteidigungsunion (ESVU). Obwohl damit lediglich der Rahmen für weitere Schritte geschaffen wurde, gilt der symbolträchtige Schritt als Bekenntnis zur Stärkung der europäischen Souveränität in Sicherheitsfragen. In Anbetracht gemeinsamer Herausforderungen wächst offenkundig auch Bereitschaft, dem europäischen Staatenbündnis mehr Verantwortung zu übertragen. Selbst das Krisenthema Finanzierung kommt in Bewegung, seitdem sich Regierungsvertreter aus Frankreich und Deutschland für die Schaffung eines europäischen Finanzministeriums ausgesprochen haben.

Fortschritte im Einigungsprozess gibt es auch bei der zivilen Sicherheit, beispielsweise beim Datenschutz. Die Europäische Datenschutz-Grundverordnung EU-DSGVO, die ab Mai 2018 vollständige Rechtswirkung auch in Deutschland entfaltet, vereinheitlicht die Regeln für den Umgang mit personenbezogenen Daten. Mit der nun vollzogenen Angleichung wird der Nachteil einer fragmentierten Rechtslage innerhalb der EU beseitigt. Kritiker warnen indes vor bürokratischen Auswüchsen, die vor allem kleine Organisationen treffen. Mit Blick auf den Binnenmarkt für digitale Güter und Leistungen (Digital Single Market) bringt die Harmonisierung jedoch vor allem Transparenz und Rechtssicherheit. Der damit verbundene Investitionsschutz stärkt die Grundlage für Innovation und Wachstum. Daher erscheint es plausibel, dass der juristische Abgleich auch ökonomisch positive Impulse setzt.

Michael Sparenberg

ist wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

E-Mail: sparenberg@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann

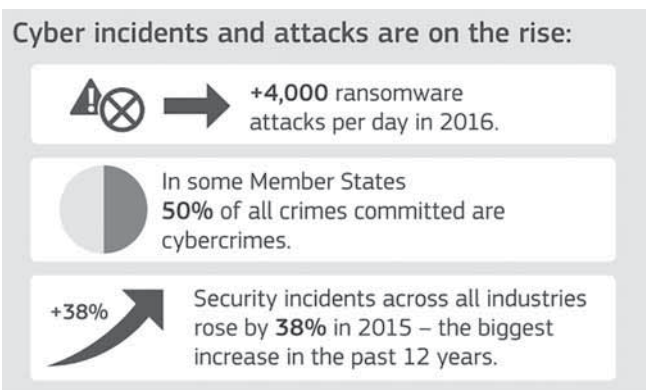
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.
E-Mail: pohlmann@internet-sicherheit.de

Höchste Priorität

Grenzüberschreitende Lösungen sind nicht nur vorteilhaft, mitunter sind sie unabdingbar für die Wirksamkeit. Dass insbesondere beim Thema Cybersicherheit akuter Handlungsbedarf besteht, verdeutlicht der aktuelle Lagebericht State of the Union, den Jean-Claude Juncker im November 2017 präsentierte. [1] Demnach erwarten 86 Prozent der befragten Europäer eine deutliche Zunahme von Cyberangriffen und zugleich eine höhere Wahrscheinlichkeit, selbst Opfer digitaler Kriminalität zu werden.

Spektakuläre Fälle von Datendiebstahl und Onlinebetrug häufen sich, vor allem die als Ransomware bekannte Form digitaler Erpressung. Über 4000 registrierte Angriffe pro Tag entsprechen einer beachtlichen Zunahme um 300 Prozent gegenüber 2015. Im selben Jahr verzeichnet die Statistik ein Plus von 38 Prozent bei der Gesamtzahl sicherheitsrelevanter Vorfälle und damit den höchsten Anstieg in 12 Jahren. In einigen Staaten entfällt bereits die Hälfte aller Delikte auf den Bereich Cybercrime.

Abb. 1 | Zunahme an Cyberangriffen



In Anbetracht des evidenten Bedarfs ist die Anbieterseite derweil nicht untätig. Mit dem Feature Cyber Threat Intelligence bewirbt sich eine neue Produktgeneration am Markt. Auch europäische Firmen haben ihr Portfolio technologisch aufgerüstet. Gemessen am Nachfragevolumen der EU fällt deren Marktanteil allerdings noch immer vergleichsweise gering aus. In diesem Zusammenhang wird häufig vom Strukturproblem der Fragmentierung als Nachteil Europas im globalen Wettbewerb gesprochen.

In Deutschland ist vor allem der Mittelstand das Rückgrat technologischer Innovation, gestützt durch eine leistungsfähige Infrastruktur öffentlicher und privater Forschungs- und Bildungseinrichtungen. In vielen Wirtschaftsbereichen hat sich diese Konstellation bestens bewährt.

Was der heimischen IT bisweilen fehlt, ist die Marktmacht kapitalstarker Unternehmen. Anbieter entsprechender Größenordnung gibt es zwar auch in Europa, Anzahl und Verbreitung sind jedoch bei weitem nicht vergleichbar mit der Ansammlung bekannter Branchengrößen in den USA und Fernost. Die gegenwärtige Dominanz außereuropäischer Anbieter im IT-Markt führt erkennbar zu kritischen Abhängigkeiten und unerwünschten Einschränkungen der technologischen Souveränität. In Verbindung mit unterschiedlichen Grundsatzpositionen bei Datenschutz und Überwachung ergibt sich hier ein deutlicher Handlungsbedarf mit dem Ziel eines eigenständigen Binnenmarktes für Cybersicherheit. Finanzielle Anschubhilfen der öffentlichen Hand können private Investitionen verstärken und die gewünschte Entwicklung beschleunigen. Entsprechend breit gefächert sind Beschaffungs- und Förderprogramme für Forschung und Entwicklung, die hierfür gezielte Anreize setzen. Das aktuelle Forschungsrahmenprogramm der EU stellt im Zeitraum 2014 bis 2020 insgesamt rund 80 Mrd. Euro für Forschung und Entwicklung bereit. [2] In Technologiebereichen mit besonderer strategischer Bedeutung (Beispiel Elektromobilität, Energieeffizienz, neue Produktionsformen) ist außerdem die Public-Private Partnership (PPP) als spezielle Implementierungshilfe vorgesehen. Dies zielt auf einen Kanalisierungseffekt bei der Entwicklung innovativer Technologien und soll die Wettbewerbsfähigkeit in Schlüsselindustrien durch gezielte Schwerpunktförderung forcieren. Mit zunehmender Digitalisierung rückt IT-Sicherheit auch hier stärker in den Fokus. Seit 2013 betonen alle führenden Strategieprogramme der EU-Kommission explizit die Notwendigkeit einer europäisch koordinierten Sicherheitsförderung, etwa die EU Cybersecurity Strategy, die NIS Direktive und der Umsetzungsplan Digital Single Market. Letzterer schreibt auch die Einrichtung einer Cybersecurity PPP fest.

Am 5. Juli 2016 wurde diese schließlich unter der Leitung von EU-Kommissar Oettinger und Kommissionsvizepräsident Ansip formell etabliert. [3]

European Cybersecurity Organisation

Zur Institutionalisierung und operativen Umsetzung dieser Partnerschaft ging noch im selben Monat eine neu geschaffene Kooperationsplattform für Cybersicherheit an den Start: die European Cyber Security Organisation, kurz ECSO.

Als Vertragspartner der EU-Kommission koordiniert sie die Interessenvertretung und Mitwirkung aller Stakeholder aus Wirtschaft, Wissenschaft und Verwaltung in Fragen europäischer Cybersicherheit. [4] Trotz ihrer schlanken Struktur mit nur sieben hauptamtlichen Mitarbeitern betreut die nach belgischem Recht als ASBL (Association sans but lucratif) gegründete Non-Profit Organisation mit Sitz in Brüssel eine Vielzahl an Aktivitäten und zählt aktuell bereits über 230 Mitgliedsorganisationen – Unternehmen ebenso wie Hochschulen, Forschungseinrichtungen und Regionalverwaltungen. Die Anzahl deutscher ECSO-Mitglieder stieg anfangs überraschend langsam, während Interessenten aus Italien, Frankreich und Spanien bereits frühzeitig die neue Dialogplattform nutzten und bis heute zahlenmäßig stärker repräsentiert sind. Substanzielle Unterstützung kam allerdings sehr früh auch aus Deutschland. Gerd Müller, Sales Director der Secunet AG und Mitglied des ECSO Strategie- und Koordinierungskomitees, hat die Entstehungsgeschichte der Organisation wesentlich mitgestaltet. Ebenfalls seit Gründung mit an Bord sind das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der TeleTrusT – Bundesverband IT-Sicherheit e.V., der in Brüssel mit drei Delegierten die Interessen seiner Verbandsmitglieder vertritt. Auch das Bundesland Nordrhein-Westfalen engagiert sich mit einem Vernetzungsbeauftragten in den Beratungsgremien der ECSO, um regionale Akteure aus NRW beim Ausbau europäischer Partnerschaften zu unterstützten. In ihrer Eigenschaft als Cluster zählt hierzu auch die Region selbst. Seit Jahresbeginn ist NRW Partner eines europaweiten Pilotprojekts für interregionale Kooperation zur Stärkung der EU-Cybersicherheit. Die gemeinsame Arbeit in ECSO bietet ideale Anknüpfungspunkte für überregionale Vernetzung und Kooperation.

Dialogbereitschaft, Flexibilität und konstruktive Problemlösung sind Kernelemente der praktischen Mitwirkung. Pflichten und Aufgaben übernehmen die Mitglieder mehrheitlich selbst, Abstimmung und Beschlussfassung erfolgen nach transparenten Regeln und Statuten. ECSO ist vollständig eigenfinanziert und trägt sich über Mitgliedsbeiträge, die je nach Organisationstyp und Größe gestaffelt sind. Der niedrigste Tarif beträgt 1.000 EUR pro Jahr und gilt für Start-ups und Kleinstunternehmen, sogenannte „micro-sized companies".

2.000 Euro jährlich entrichten Universitäten, kleinere Forschungseinrichtungen und typische KMU. Weitere Staffelbeiträge für Unternehmen der Privatwirtschaft liegen bei 4.000 und 6.000 EUR. Den mit 12.000 Euro höchsten Jahresbeitrag zahlen Großunternehmen (Jahresumsatz > 1 Mrd. Euro). Für öffentliche Verwaltungen ist eine beitragsfreie Mitgliedschaft möglich. Ein Formular für den Beitrittsantrag finden Interessierte auf der ECSO Homepage, ebenso weiterführende Informationen zu Mandat, Zielen und Arbeitsweise der European Cyber Security Organisation. Ein Publikationsarchiv und News Blog runden den Webauftritt ab.

Thematische Vielfalt prägt nicht nur die Außendarstellung der ECSO, auch intern gilt es, ein breites Spektrum an Arbeitsthemen zu bewältigen. Um die praktische Mitwirkung konstruktiv und effektiv zu gestalten, wurden sechs Arbeitsgruppen (Working Groups) mit speziellen Schwerpunktthemen eingerichtet. Sie koordinieren die Zusammenarbeit der Mitglieder, konsolidieren die Arbeitsergebnisse und leiten diese zur Beschlussfassung an die zuständigen Gremien weiter. Umgekehrt gelangen Informationen und Anfragen über die jeweilige Arbeitsgruppe an die zuständigen Experten. So wird die ECSO ihrer funktionalen Aufgabe als Dialogplattform gerecht und fungiert als zentraler Anlaufpunkt für alle Stakeholder im Bereich Cybersecurity.

Abb. 2 | ECSO Working Groups

Die Arbeitsinhalte gliedern sich wie folgt:
1. Standardisation, certification, and labelling
2. Market deployment, international collaboration
3. Sectoral demand (vertical market applications)
4. Support to SMEs, countries and regions
5. Education, awareness, training, cyber ranges
6. Strategic Research and Innovation Agenda (SRIA)

Je nach Bedarf und Interessenlage ist ein Engagement in mehreren Arbeitsgruppen möglich. Auch zwischen den einzelnen Working Groups werden Prozesse und Arbeitsinhalte abgestimmt. So unterstützen beispielsweise WG 2 und WG 6 mit Beiträgen zur Marktentwicklung und Forschungsagenda die Konzepte zur Regionalentwicklung aus WG 4.

In Zusammenarbeit mit anderen Akteuren wie der Sicherheitsagentur ENISA erarbeitet ECSO strategische Handlungsempfehlungen und gestaltet die künftige EU-Cyberstrategie aktiv mit. Die zielkonforme Priorisierung von Forschungsthemen ist ein wichtiger Teil dieser Arbeit.

ECSO erhält jedoch kein separates Budget, sondern berät inhaltlich bei der Mittelverwendung des bestehenden Rahmenprogramms. Bis 2020 sind Maßnahmen mit einem Fördervolumen von bis zu 450 Millionen Euro vorgesehen, die privatwirtschaftliche Investitionen in dreifacher Höhe freisetzen sollen. Mit diesem Hebeleffekt fließen insgesamt rund 1,8 Milliarden Euro in neue Sicherheitstechnologien.

Zukunft gestalten

In der Strategic Research and Innovation Agenda (SRIA) und der Industrial Policy sind Grundsatzpositionen und Handlungsempfehlungen der ECSO zur Unterstützung strategischer Entscheidungen der EU konsolidiert. Während die SRIA primär Themen und Prioritäten der kurz- und mittelfristigen Forschungsförderung beinhaltet, adressiert die Industrial Policy vor allem langfristige Gestaltungserfordernisse. Ziel aller Maßnahmen ist die Schaffung eines nachhaltigen wirtschaftlichen Ökosystems im europäischen Markt für digitale Sicherheitslösungen.

In dieser Funktion wirkt die ECSO auch an der Gestaltung des Neunten EU-Forschungsrahmenprogrammes (FP9) mit, das im Mai 2018 veröffentlicht und ab 2021 ausgerollt wird. Kernziel ist auch hier Stärkung der Wettbewerbsfähigkeit in technologischen Schlüsselbereichen. Letzteres setzt voraus, dass Europa den künftigen Bedarf an qualifizierten Fachkräften decken kann, was sich in schnell wachsenden Technologbereichen zunehmend als Herausforderung darstellt. Hierzu bedarf es gemeinsamer Anstrengungen in Aus- und Weiterbildung, aber auch zur Erhöhung der Transparenz bestehender Marktlösungen. Standardisierung und Zertifizierung sind zwei der Hauptinstrumente, mit denen die EU technologische Wettbewerbsfähigkeit stärken will.

Dass langfristiger Markterfolg Integrationslösungen erfordert, wird nicht zuletzt bei dem für Deutschland wichtigen Thema Industrie 4.0 deutlich. Gelingt es europäischen Anbietern, ihre Produkte entlang der gesamten Wertschöpfungskette zu etablieren, so kann die globale Wettbewerbsposition nachhaltig ausgebaut werden. Lücken im Ökosystem schwächen hingegen die Markterschließung und manifestieren die Dominanz außereuropäischer Anbieter.

Mit einer stärkeren Koordination bei Qualifizierung und Zertifizierung will die EU-Kommission europaweit technologische Innovationen beschleunigen. Einheitliche Standards sollen Investitionen in Forschung und Entwicklung schützen und Beschaffungsprozesse vereinfachen. Damit – so die Intention – gelangen neue Produkte früher in den Markt.

Innovation bedeutet nicht, das Rad neu zu erfinden. Vorhandene Erfahrung und erfolgreiche Lösungen auf nationaler Ebene können als Orientierungsrahmen dienen. So existieren etwa in Deutschland bewährte und international angesehene Standards zur Zertifizierung, die im Zuge einer europaweiten Harmonisierung nicht aufgeweicht werden sollten. Darauf weist der TeleTrusT Bundesverband IT-Sicherheit e.V. in einer Stellungnahme [5] zu einem entsprechenden Regulierungsvorschlag der EU-Kommission [6] ausdrücklich hin. Die Bedeutung transparenter Qualitätsstandards und security by design betont das „Manifest zur IT-Sicherheit", herausgegeben vom VOICE Bundesverband der IT-Anwender e.V. und TeleTrusT. [7] In sechs Thesen werden hier zentrale Herausforderungen und spezifische Handlungserfordernisse abgeleitet. Das Strategiepapier unterstreicht den Wert nationaler Qualitätsmaßstäbe, etwa beim deutschen Datenschutz, die Europa insgesamt zu einem höheren Maß an Technologiesouveränität verhelfen können.

Die genannten Beispiele belegen das Interesse an gemeinsamen Marktregeln. Es bedarf eines konstruktiven Dialoges, um ausgewogene Standards zu definieren. Diese sollen europaweit praktikabel sein, ohne den regionalen Status quo zu verschlechtern. Vom Erfolg dieser Bemühungen wird es nicht zuletzt abhängen, ob die EU ihr eigenes Portfolio an Cybersicherheitslösungen im globalen Wettbewerb stärken kann.

Nur durch intensive Kooperation der Mitgliedstaaten lassen sich Engpässe frühzeitig identifizieren und vorhandene Ressourcen effizienter nutzen. Die EU-Kommission hat hierfür ein Maßnahmenprogramm verabschiedet, mit dessen Implementierung Ende 2017 begonnen wurde. Im Fokus stehen die Vernetzung regionaler Organisationsstrukturen und eine stärkere Institutionalisierung der gemeinsamen Markterschließung. Neben dem Ausbau vorhandener Ressourcen stehen auch gänzlich neue Instrumente zur Verfügung. Dies beinhaltet z.B. ein EU-weites Zertifizierungsschema für Cybersecurity zur Erhöhung der Sicherheit digitaler Produkte und Dienstleistungen. Der European Agen-

Abb. 3 | Zertifizierungsschemata SOG-IS, CPA (UK), CSPN (FR) und BSPA (NL)

cy for Network and Information Security (ENISA) wird künftig eine European Union Cybersecurity Agency zur Seite gestellt, welche die Mitgliedsstaaten bei der Abwehr von Cyberangriffen unterstützt. Das neu geschaffene European Cybersecurity Research and Competence Centre betreut in Kooperation mit nationalen Kompetenzzentren Forschungs- und Entwicklungsmaßnahmen regionaler IT-Anbieter. Mit der Erweiterung des europäischen Portfolios an marktgerechten Produkten und Dienstleistungen wird sowohl die heimische Wettbewerbsposition als auch die technologische Souveränität der EU gestärkt. Für Qualifizierungsmaßnahmen zur Deckung des Fachkräftebedarfs sind aufgabenspezifische Plattformen für Ausbildung und Training vorgesehen, die ein breites Spektrum an Sicherheitshemen abdecken. Eine stärkere Integration erfährt in diesem Kontext auch der Bereich Cyber Defence, der gemeinsam mit der NATO aufgebaut wird.

Fazit

Europa steht vor großen Aufgaben beim Thema Cybersicherheit. Im Gefolge innovativer Technologien entstehen neuartige Bedrohungen, deren Komplexität und Dynamik völlig neue Abwehrmechanismen erfordern. Eine systematische und ganzheitliche Stärkung der Resilienz ist notwendig, um den Schutz materieller und immaterieller Werte langfristig zu gewährleisten. Nicht nur Technologie und Wirtschaft sind hiervon betroffen, auch rechtliche und gesellschaftliche Aspekte müssen adäquat berücksichtigt werden. Dafür braucht es Konsens und abgestimmtes Handeln über Landes- und Kompetenzgrenzen hinweg. Auch das will immer wieder geübt werden. In der Vergangenheit hat die Europäische Union sich bisweilen in Ermangelung eigener Konsensfähigkeit auf die Eigeninitiative einzelner Staaten verlassen, um partielle Fortschritte zu erzielen. In Bezug auf Cybersicherheit hat dieses pragmatische Krisenkonzept jedoch ausgedient, ein „Europa der zwei Geschwindigkeiten" macht hier keinen Sinn. Vielmehr muss die Bereitschaft zur Umsetzung notwendiger Reformen vom Staatenbündnis gemeinsam getragen werden, wenn die Maßnahmen Wirkung zeigen sollen. Gleichwohl kann Deutschland als größte Volkswirtschaft der EU einen signifikanten Beitrag zur gemeinsamen Initiative leisten und neu geschaffene Organisationsstrukturen wie die ECSO wirksam unterstützen. Europa hat den ersten Schritt getan, um aus der Vision „Cybersecurity made in EU" einen stabilen Baustein europäischer Sicherheit zu formen.

Abbildungen

[1] EC: CYBERSECURITY, (Cybersecurity Factsheet, 11/2017
[2] ECSO: European Cybersecurity cPPP and ECSO, 10/2017
[3] EC: EU AGENCY AND CERTIFICATION FRAMEWORK, ENISA Factsheet, 10/2017

Literatur

[1] EC: State of the Union 2017, https://ec.europa.eu/commission/state-union-2017_en
[2] EC: https://ec.europa.eu/programmes/horizon2020/
[3] EC: http://europa.eu/rapid/press-release_IP-16-2321_en.htm
[4] ECSO: http://ecs-org.eu/documents/ecso-asbl-statutes.pdf
[5] TeleTrusT-Bundesverband IT-Sicherheit e.V.: TeleTrusT-Stellungnahme vom 04.10.2017, https://www.teletrust.de/publikationen/stellungnahmen/
[6] EC: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF
[7] VOICE-Bundesverband der IT-Anwender e.V., TeleTrusT-Bundesverband IT-Sicherheit e.V. (Hrsg.): Das Manifest zur IT-Sicherheit, https://www.teletrust.de/fileadmin/docs/ IT-Sicherheitsstrategien/IT-Sicherheitsgesetz/TeleTrusT_VOICE_Manifest_IT-Sicherheit.pdf