Cybersicherheit: Vom Dialog zur Ko-Kreation

Zusammenfassung

Schon heute werden Angriffe auf Computer und Smartphones zunehmend komplexer und professioneller. Zukünftig nehmen potentielle Angriffspunkte mit der Vernetzung (IoT) und Automatisierung der Produktion, des Verkehrs und der Dienstleistungsbranche sowie der automatisierten Nutzung von Sensoren zu. Cybersicherheit bedeutet die Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit in digitalen Infrastrukturen und damit den Schutz von IKT-Systemen (Hardware, Software und zugehörige Infrastruktur), Daten und den bereitgestellten Diensten. Staaten und Unternehmen beobachten zunehmend systematisch die Entwicklung der Cyberkriminalität und entwickeln entsprechende Maßnahmen.[1] Angesichts der hohen Dynamik digitaler Dienstleistungen, wie Automatisierung von Produktion (Industrie 4.0, Internet der Dinge) und Verkehr (siehe Mobilitätsplattformen), wird Cybersicherheit zunehmend zu einem umfassenden Prozess, der einen hohen Wissensstand nicht nur bei Unternehmen und Betreibern von kritischen Infrastrukturen voraussetzt, sondern auch eine Kultur der Cybersicherheit in allen gesellschaftlichen Bereichen erfordert.

Überblick zum Thema

Mit der Entwicklung von cyber-physischen Systemen, bei denen informations- und softwaretechnische mit mechanischen Komponenten verbunden sind und der Datentransfer sowie die Steuerung über das Internet in Echtzeit erfolgen, nehmen die Risiken für Störungen durch Cyberbedrohungen stark zu. Cyber-physische Systeme vereinen avancierte Elektronik, fortschrittliche Sensorik und bestehende Infrastrukturen. Sie führen zu einer hohen Abhängigkeit von digitalen Komponenten untereinander[2] und zu einer Bedrohung dieser Systeme durch Cyberangriffe, die durch das steigende Maß an autonomer Steuerung und global zugänglicher Systeme (z. B. Navigationssysteme) auch ein höheres Bedrohungspotential nach sich ziehen. Das Internet der Dinge trägt durch die zunehmende Integration ungenügend geschützter Geräte im Internet zu neuen Angriffspunkten bei und eröffnet neuartige Angriffsszenarien.

In Österreich sind die „Cyber Sicherheit Plattform (CSP)“ und die Österreichische Strategie für Cyber-Sicherheit darauf ausgerichtet, die gesamt-

[1] Vgl. den Bericht Cyber-Sicherheit 2018, 2019 und 2020: bundeskanzleramt.gv.at/themen/cybersicherheit/bericht-cybersicherheit.html.

[2] Unter anderem durch jeweils unterschiedliche Sicherheitsmerkmale und Kommunikationsstandards, vgl. Burg, et al. (2018). Ein weiteres Problem ist, dass Sicherheit und Gefahrenabwehr in der Ingenieurs- und Informatikbranche traditionell unterschiedliche Probleme sind, die einer Vereinheitlichung bedürfen Wolf/ Serpanos (2018).

staatlichen Zusammenarbeit in diesem Bereich zu gewährleisten.[3] Für aktuelle Gefährdungen der Onlinesicherheit, die BürgerInnen und KonsumentInnen betreffen, gibt es bereits Ansätze, eine breitere Cyber-Sicherheitskultur zu fördern; dazu gehört z. B. das IKT-Sicherheitsportal als interministerielle Initiative in Kooperation mit der österreichischen Wirtschaft, welches aktuelle Themen der Cybersicherheit für breite Kreise bündelt und auf aktuelle Bedrohungen und mögliche Maßnahmen hinweist.[4]

Zugleich entwickeln die EU-Mitgliedstaaten gemeinsame Initiativen weiter. So wurde die Einrichtung eines „Kompetenzzentrums für Cybersicherheit in Industrie, Technologie und Forschung (ECCC)“ und eines „Netzes nationaler Koordinierungszentren (NCCs)“ verhandelt und 2021 umgesetzt.[5] Zur Reform der Cybersicherheit in Europa gehören verschiedene Dimensionen:

- die Einrichtung einer wirksamen EU-Agentur für Cybersicherheit[6];
- die Einführung eines EU-weiten Zertifizierungssystems für Cybersicherheit;
- die rasche Umsetzung der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie).[7]

Für eine EU-Cyberdiplomatie, die zur Konfliktverhütung, zur Eindämmung von Cyberbedrohungen und zur Förderung der Zusammenarbeit dient, ist eine „Cyber Diplomacy Toolbox“ als Teil des EU-Ansatzes geplant.[8]

Die Fragestellungen für die zukünftige Cybersicherheitsforschung zeigen, dass Cybersicherheit zukünftig auf die Nutzerintegration ausgerichtet ist (Jang-Jaccard/Nepal 2014). Damit würde das Thema verstärkt in Politikbereichen aufgegriffen werden müssen, die bisher wenig mit Cybersicherheit verbunden sind. Somit stellen sich Fragen, die auf eine Integration der NutzerInnen verweisen: Hinsichtlich des Datenschutzes geht es darum, Möglichkeiten zu finden, wie InternetnutzerInnen die Vertraulichkeit ihrer personenbezogenen Daten wirksamer schützen und kontrollieren können (Mögliche Ansätze dazu finden sich im Beitrag Zukunft des Internets: zentral vs. dezentral?). In Bezug auf ein sicheres Internet der nächsten Generation stellt sich die Frage, wie es möglich ist, das aktuelle Internet-System von Grund auf neu zu gestalten, ohne dadurch das bestehende System einzuschränken (z. B. Konzepte wie Security-by-Design, oder der Zusammenschluss heterogener Netzwerkumgebungen, Architekturdesign).

---

[3] bundeskanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html.

[4] onlinesicherheit.gv.at. Vgl. international das Europäische Institut für Telekommunikationsnormen (ETSI), das anerkannte bewährte Verfahren zur Sicherheit IoT zusammenfasst, um alle an der IoT-Entwicklung beteiligten Parteien mit Hinweisen zur Sicherung ihrer Produkte zu unterstützen. etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf.

[5] eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32021R0887.

[6] cybersecurity-centre.europa.eu/index_en.

[7] consilium.europa.eu/de/policies/cyber-security/.

[8] Vgl. Zu aktuellen Entwicklungen: wms.flexious.be/editor/plugins/imagemanager/content/2140/PDF/2019/pub_9081_responding_cyberattacks.pdf.

Eine weitere zentrale Frage ist die eines globalen Identitätsmanagements (siehe Digitale Identität) und den damit verbundenen Rückverfolgungstechniken und schließlich die umfassende Frage einer tatsächlich benutzerInnenfreundlichen Sicherheit: Wie lässt sich ein Sicherheitssystem entwickeln, das von BenutzerInnen mit unterschiedlichen Kenntnissen und Ansprüchen tatsächlich verwaltet und kontrolliert werden kann? Alle diese Frage verweisen auf die Herausforderung, dass die etablierten Akteure nicht mehr für Staat, Wirtschaft und Gesellschaft Cybersicherheit entwickeln und implementieren, sondern dass dies zukünftig viel stärker im Zusammenspiel mit den entsprechenden Stakeholdern in vielfältigen Ko-Design-Prozessen geschieht.

Relevanz des Themas für das Parlament und für Österreich

Digitalisierung bedeutet Komplexität und die Allgegenwärtigkeit der Onlinevernetzung; sie bietet einer immer noch zunehmenden Zahl an Akteuren in Österreich mehr Möglichkeiten im privaten, im wirtschaftlichen, im beruflichen und im öffentlichen Bereich. Digitalisierung bedeutet aber auch eine Zunahme an Cybergefahren, auf die die Akteure vorbereitet sein müssen. Insofern ist Cybersicherheit eine zentrale Voraussetzung für das Gelingen der Digitalisierung und das Vertrauen in Digitalisierungsprozesse.

Mit dem bleibenden Spannungsverhältnis der Gewährleistung von Cybersicherheit, dem Schutz der Privatsphäre und steigendem Datenaustausch im Kontext von Digitalisierung sind zwei Risiken verbunden: Die steigende Gefahr für Staat, Wirtschaft und BürgerInnen, Opfer von Cyberkriminalität und Cyberspionage zu werden, und das Risiko, durch Sicherheitstechnologien in Bürgerrechten eingeschränkt zu werden. Auf grundsätzlicher Ebene stellen sich Fragen nach Freiheit, Anonymität und Handlungsautonomie im Kontext eines hohen Cybersicherheitsniveaus. Diese Fragen zu bearbeiten, wäre die Voraussetzung, um langfristig zu einer breiten gesellschaftlichen Ko-Kreation von Cybersicherheitsprodukten und -dienstleistungen zu kommen.

Vorschlag weiteres Vorgehen

Das Parlament als zentraler Ort der politischen Meinungsbildung und Kontrolle kann wesentlich zur politikfeldübergreifenden Koordination österreichischer staatlicher, privater und zivilgesellschaftlicher Aktivitäten sowie zur übergreifenden Bewusstseinsbildung zur Cybersicherheit[9] in der Öf-

[9] In einem Hearing mit ExpertInnen im Ausschuss für Konsumentenschutz zum Thema Internet of Things am 9.5.2019 wurde das Thema Cybersicherheit als wesentlich für die Entwicklung und Akzeptanz sowie für die zukünftige Konsumentenschutzpolitik im Bereich IoT erkannt, siehe parlament.gv.at/PAKT/PR/JAHR_2019/PK0508/index.shtml. Neben den dort geführten Diskussionen über die Grenzen einer technisch von den Herstellern erzwungen Datenübertragung und der Frage der Regulierung wäre zukünftig auch die Frage zu stellen, welche ganz neue Art von Cybersecurity-Dienstleistungen den KonsumentInnen Services und Tools zur Verfügung stellen, die ihnen eine einfachere und höhere Souveränität über ihre eigenen Daten/die Daten ihrer Geräte sichert.

fentlichkeit beitragen. Wenn Cybersicherheit zukünftig auf einer breiten Kompetenz in der Gesellschaft basiert, wäre zu identifizieren, was die Anforderungen in verschiedenen Bereichen der Gesellschaft an eine zukünftige Cybersicherheitskultur sind. Aufgrund der steigenden Relevanz des Themas und des Spannungsverhältnisses von Sicherheit, Schutz der Privatsphäre und freiem Datenaustausch wäre eine umfassende, auf Österreich fokussierende Foresight- und TA-Studie mit partizipativen Elementen sinnvoll, die über die Analyse heutiger Cybersicherheit hinaus zukünftige Optionen umfassend antizipiert. Einen ersten Schritt in diese Richtung macht die Studie ‚Cybersecurity: Systematisierung, Forschungsstand und Innovationspotenziale' die vom Parlament im Rahmen des F&TA Monitorings 2021 beauftragt und gemeinsam mit ExpertInnen aus Wirtschaft, Wissenschaft, öffentlicher Verwaltung und Interessensvertretungen umgesetzt wurde. Eine transdisziplinäre Studie kann das Wissen von ExpertInnen aus den Bereichen der Sicherheitsdienstleistungen, Landesverteidigung und autonomer Systeme mit Wissensbeständen aus dem Bereich Sicherung der Privatsphäre und KI-Forschung und den divergierenden Interessen unterschiedlicher Stakeholder verbinden, um unterschiedliche Zukunftsoptionen festzustellen. Ziel wäre es, partizipativ Leitlinien für eine Cybersicherheitskultur zu entwerfen und mögliche Innovationspfade zu definieren, die den langfristigen Anforderungen unterschiedlicher Akteure entsprechen und damit auch eine proaktive Cybersicherheitskultur unterstützen.

Zitierte Literatur

Jang-Jaccard, J. und Nepal, S., 2014, A survey of emerging threats in cybersecurity, Journal of Computer and System Sciences 80(5), 973-993.