»Cybersicherheit« – ein Beitrag für einen sicheren digitalen Raum

Positionspapier, 07. Januar 2019

Positionspapier der Arbeitskreise Kultur, Wissen, Lebensweisen (AK IV) und Bürger*innenrechte und Demokratie (AK V) der Fraktion DIE LINKE. im Bundestag zur digitalen Sicherheit.

Positionspapier als PDF herunterladen

Im Jahr 1983 kam der Film „War Game“ in die Kinos und wurde für die nächsten Jahrzehnte bildgebend für die Vorstellung von Hackern und Cyber-War: ein Schüler dringt in das Netz des Pentagon ein und aktiviert das Atomwaffenarsenal der USA, die Welt steht am Rande der Vernichtung. Nun ist das Pentagon seitdem sicherlich besser gegen Zugriffe geschützt – doch die seit den 90er Jahre rasant zunehmende Anwendung von Computern für alle erdenklichen Anwendungen hat das Risiko, Opfer eines Angriffs auf das eigene System zu werden, omnipräsent gemacht. Nicht zuletzt das Internet der Dinge (Internet of Things, IoT) rückt das Bewusstsein

für die Bedrohungen der digitalen Sicherheit ebenso in den Fokus öffentlicher Debatten, wie die zunehmende Berichterstattung über Attacken auf die Netze von Regierungen, Parlamenten, Parteien, öffentlichen Verwaltungen, Stiftungen, aber auch sog. Kritischer Infrastruktur (Kritis). Anders als bspw. der Fraktionsvorsitzende der Unionsfraktion Kauder glauben machen möchte, ist die Digitalisierung und damit verbunden auch die Frage nach deren Sicherheit, nicht erst das „Megathema der kommenden Jahre“[1], sondern mindestens seit zwei Dekaden Realität.

Durch das IoT geraten Gegenstände des täglichen Gebrauchs in den Fokus potentieller Angreifer. Für Besitzer*innen des viel zitierten smarten Kühlschrankes[2] mag es auf den ersten Blick nicht so problematisch sein, wenn sich das Gerät zu einem Botnetz[3] verbindet. Bei einer gehackten smarten Haustür- und Fenstersteuerung oder Heizung und einem damit unmittelbar verbundenen individuellen Schaden mag das schon ganz anders aussehen. Neben Endverbraucher*innen sind aber auch öffentliche Verwaltungen oder Kritische Infrastrukturen (Kritis) Ziel von Attacken. Im letzten Fall mit möglicherweise unabsehbaren Folgen. Dominierten früher Inselnetze, so scheint heute alles miteinander verbunden zu sein.

In vielen Lebensbereichen sorgt die Digitalisierung für erhebliche Erleichterungen. Öffentliche Verwaltungen können im Idealfall schneller und bürger*innenfreundlicher arbeiten. Gleichzeitig führt dies zu einer immer größer werdenden Menge an gespeicherten Daten. Kam es nach quälend langsamen Schritten in diesem Bereich zu Fortschritten, vergaß und vergisst man in dem nun folgenden Rausch der digitalen Glückseligkeit allzu oft die Frage nach der digitalen Sicherheit.

Im Vergleich zur analogen Welt stellt die Frage der

Attribution ein ungleich größeres Problem bei Angriffen im digitalen Raum dar. Aggressor*innen können vom einzelnen Nationalstaat über kriminelle Banden bis hin zu Einzeltäter*innen alles sein und von überall aus agieren. Je professioneller die Angreifer*innen vorgehen, umso schwerer wird es herauszufinden, wer die eigentlichen Angreifer*innen sind. Die digitale Forensik bewegt sich zwangsweise in einem Graubereich und kann lediglich Indizien sammeln.

Der Blick auf den Status quo der Ausgestaltung digitaler Sicherheit, bspw. in Form der 2016 novellierten Cybersicherheitsstrategie der Bundesregierung[4], aber auch die unzähligen Beiträge der Vertreter*innen deutscher Sicherheitsbehörden, zeigt, dass eine klare Zielrichtung fehlt. Vielmehr gibt es ein buntes Durcheinander der Kompetenzen. Ergänzt durch teilweise widerstrebende Interessen: Nicht erst seit der Einführung des Bundestrojaners ist klar, dass es für Geheimdienste, aber auch Strafverfolgungsbehörden wichtig ist, Sicherheitslücken zu kennen, um diese später nutzen zu können. Gleichzeitig werden dieselben Akteure, die auf die Kenntnis von Sicherheitslücken angewiesen sind, als Akteure der gesamtstaatlichen Cyber-Sicherheitsarchitektur eingebunden. Da ist er also wieder, der viel zitierte Bock als Gärtner. Die Verabredungen im Koalitionsvertrag sowie die Kompetenzaufteilungen der Bundesregierung lassen auf wenig Besserung hoffen. Der Koalitionsvertrag enthält lediglich inhaltlich unklare Verabredungen beispielsweise für eine sichere digitale Authentifizierung im Netz, ohne dass eine klare Idee zu ihrer Ausgestaltung erkennbar wäre. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) soll gleichzeitig zur „Cybersicherheitsbehörde“ werden und „in seiner Rolle als unabhängige und

neutrale Beratungsstelle für IT-Sicherheitsfragen“ gestärkt werden[5]. Hinsichtlich einer überfälligen stärkeren Regulierung des IT-Marktes soll es offenbar bei unverbindlichen Standards bleiben – die zudem von den Anbietern selbst entwickelt werden. Wie sich zukünftig Bundesinnenministerium, Bundeswirtschaftsministerium und das Bundeskanzleramt in ihrer Politik der digitalen Sicherheit miteinander abstimmen werden, ist vollkommen offen.

Mit dem vorgelegten Positionspapier zeigen die Autor*innen auf, welche (offensichtlichen) Missstände die aktuelle Ausgestaltung der digitalen Sicherheit in Deutschland mit sich bringt und welche Interessenkonflikte hierbei vorherrschen. Darüber hinaus werden Ansätze aufgezeigt, welche es ermöglichen, mehr digitale Sicherheit zu gewährleisten. Mit dem Begriff der „digitalen Sicherheit“ soll all das umfasst sein, was unter den Schutzbereich des vom Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung neu aus dem allgemeinen Persönlichkeitsrecht abgeleiteten „digitalen Grundrecht“, dem Recht auf Schutz der Vertraulichkeit, Integrität und Verfügbarkeit informationstechnischer Systeme und Daten fällt.[6] Im erweiterten Sinne verstehen wir darunter auch jene informationstechnischen Systeme, auf die die Bürgerinnen und Bürger zur Lebensführung in der digitalen Welt angewiesen sind. Wir verzichten dabei bewusst weitestgehend auf den schillernden Begriff „Cyber“ bzw. „Cyber-Sicherheit“, weil er aus unserer Sicht mehr verunklart, worum es eigentlich geht und was genau als Bedrohung dieser Sicherheit ausgemacht wird. Aus dem so gebrauchten Begriff der „digitalen Sicherheit“ erhellt beispielsweise unmittelbar, dass davon die Nutzung von Verschlüsselung in der privaten Kommunikation umfasst ist; von den Protagonisten der „Cyber-

Sicherheit“ wird Verschlüsselung mal als Bedrohung, mal als wichtiges Instrument begriffen.

Der Begriff der „digitalen Sicherheit“ umfasst aus Sicht der Autor*innen natürlich auch private Lebensbereiche und damit die persönliche Sicherheit der Nutzer*innen. Die Bandbreite ist kaum überschaubar und umfasst beispielsweise Identitätsdiebstahl, Mobbing und Kreditkartenbetrug aber auch die Privatisierung des Rechts durch Zuständigkeitsverlagerungen auf Unternehmen. Gerade die Angriffe im digitalen Raum gegen Andersdenkende, -liebende oder -gläubige und insbesondere Mädchen und Frauen haben ein Ausmaß erreicht, dass eine explizite Positionierung in diesem Positionspapier den Autor*innen notwendig erscheint.

Das vollständige Positionspapier als PDF herunterladen

---

[1]welt.de

[2] In der Praxis dürften aktuell smarte Fernseher, Smartwatches, Router o.ä. deutlich lebensnäher sein, der beschriebene Effekt bleibt jedoch der gleiche.

[3] Viele Netzwerkgeräte, die durch ein Schadprogramm zusammengeschlossen sind und ferngesteuert zu bestimmten Aktionen missbraucht werden, meist ohne dass die Nutzer*innen etwas davon bemerken.

[4]Bundesministerium des Inneren

[5] Vgl. Koalitionsvertrag von CDU, CSU und SPD für die 19. Wahlperiode, S. 44

[6] BVerfGE 129, 274-350