Beschluss

Für eine gute IT-Sicherheit und eine wehrhafte Demokratie - auch im Digitalen

Gremium: LPT
Beschlussdatum: 23.03.2019
Tagesordnungspunkt: 1. Anträge

Antragstext

Ob Stuxnet 2010, die Veröffentlichungen vom Edward Snowden 2013, der erfolgreiche Angriff auf den Deutschen Bundestag 2015, WannaCry 2017 oder der Angriff auf das deutsche Regierungsnetz - seit Jahren diskutieren wir nicht nur über zahlreiche Datenskandale, sondern auch über weitreichende Angriffe auf IT-Infrastrukturen.

Im Zuge des jüngsten Doxing-Skandals wurden die Daten von Zehntausenden Politiker*innen, Journalist*innen und Personen des öffentlichen Lebens erbeutet und mit Diffamierungsabsicht veröffentlicht. Nur kurz darauf fanden Forscher Datenbanken mit Online-Zugangsdaten von 2,1 Milliarden Menschen weltweit. Das zeigt: Um die Sicherheit privater Kommunikationen und digitaler Infrastrukturen steht es extrem schlecht.

Zugleich erleben wir weitreichende Versuche der intransparenten Einflussnahme auf demokratische Willensbildungsprozesse und der gezielten Manipulation von Wahlen und öffentlichen Diskursen, nicht nur in Großbritannien im Zuge des Brexit-Referendums, in den USA im Rahmen der US-Präsidentschaftswahlen sondern beispielsweise auch bei der zurückliegenden bayerischen Landtagswahl, wo rechte Netzwerke eine regelrechte Desinformationskampagne führten, auch und gerade gegen uns Grüne. Bewusst lancierte Desinformation wird mit Hilfe ganzer „Trollarmeen“ und „social bots“ verbreitet und so Meinungsführerschaft vorgegaukelt, Diskurse werden vergiftet.

IT-Angriffe und intransparente Einflussnahme auf demokratische Willensbildungsprozesse unterlaufen das Vertrauen in öffentliche Diskurse und sind für Demokratien mittlerweile ein sehr ernstzunehmendes Problem. Diese teils seit langem diskutierten Probleme, teils gänzlich neuen Formen hybrider Bedrohungen müssen wir uns als Rechtsstaaten mit aller Entschlossenheit stellen, um Grundrechte, demokratische Willensbildungsprozesse und Wahlen bestmöglich zu schützen.

Die Bundesregierung tut dies bislang nicht. Im Gegenteil: Sie hat es verpasst, soziale Netzwerke an klare rechtliche Vorgaben, beispielsweise zur Überprüfung von strafbaren Meinungsäußerungen, zu erinnern. Offensichtliche, über Jahre andauernde Rechtsverstöße hat sie nicht sanktioniert und die Datenschutzaufsichtsbehörden bei ihren Bemühungen alleine gelassen. Stattdessen hat sie mit dem Netzwerkdurchsetzungsgesetz (NetzDG) Maßnahmen ergriffen, die in weiten Teilen ungeeignet sind und die Meinungsfreiheit im digitalen Raum gefährden. Auch hat es die Bundesregierung verpasst, sich im Rahmen der Verhandlungen um die E-Privacy-Verordnung für eine eindeutige Regulierung

einzusetzen. Neue Transparenzverpflichtungen und Regelungen, zum Beispiel gegen „Microtargeting“ und intransparente Werbeschaltung im Vorfeld von Wahlen, sind weiterhin überfällig.

Insgesamt verfolgt die Bundesregierung bis heute eine IT-Sicherheitspolitik, die IT-Sicherheit eher gefährdet als stärkt. Wir brauchen eine echte Kehrtwende im Bereich der IT-Sicherheit. Hierzu gehört auch, die eigene IT-Sicherheitspolitik der vergangenen Jahre grundlegend zu überdenken. Statt den staatlichen Handel mit Sicherheitslücken und verfassungsrechtlich hoch umstrittener ”Hackbacks”, statt eines cyberpolitischen Wettrüstens mit Staaten wie Russland, China und Nordkorea, das man - zumindest als Demokratie - nur verlieren kann und einem neuen ”Cyberwar” brauchen wir eine auf Verteidigung und Härtung der eigenen Infrastrukturen ausgerichtete IT-Sicherheitsstrategie, die auch dem verbesserten Schutz privater Kommunikation dient.

Behörden wie ZITIS, die bis heute ohne irgendeine Rechtsgrundlage daran arbeiten, Sicherheitslücken offen zu halten und Kryptographie zu brechen oder immer neue Datenberge völlig unbescholtener Bürgerinnen und Bürger durch verdachtsunabhängige Massenüberwachung à la Vorratsdatenspeicherung & Fluggastdatenspeicherung - all das gefährdet Grundrechte und ist Gift für die IT-Sicherheit in Deutschland, Europa und der Welt.

Wir werden nicht müde daran zu erinnern, dass dem Staat eine direkte Verantwortung für den Schutz privater Kommunikation und digitaler Infrastrukturen zukommt, ob darauf nun unsere private Kommunikation oder sensitive Unternehmensdaten laufen. Dieser sich aus unserer Verfassung ergebenden Schutzverantwortung muss die Bundesregierung endlich gerecht werden - und das längst nicht nur, wenn es um den Schutz der eigenen Netze und kritischer Infrastrukturen geht.

Statt wie bislang nur auf erfolgreiche Angriffe zu reagieren und diejenigen zu bestrafen, die Opfer geworden sind, brauchen wir eine proaktive Politik zum Schutz von privater Kommunikation, digitaler Infrastrukturen und unserer Demokratie. Dem Grundrecht auf Vertraulichkeit informationstechnischer Systeme müssen wir auch angesichts gänzlich neuer Bedrohungslagen endlich zum politischen Durchbruch verhelfen. Denn Vertrauen in die Privatheit von Kommunikation ist zentral für einen effektiven Grundrechtsschutz und die Demokratie im digitalen Zeitalter.

Als Grüne in Schleswig-Holstein fordern wir die Landesregierung auf, sich auf Landes- Bundes- und europäischer Ebene für eine an realen Gefährdungslagen orientierte, besonnene und proaktive Politik zur Erhöhung der IT-Sicherheit und zum Schutz demokratischer Diskurse und Wahlen einzusetzen.

Wir brauchen unter anderem:

· überfällige gesetzgeberische Handlungen im Bereich des Datenschutzes. Dazu zählt insbesondere die aktive politische Begleitung der E-Privacy-Verordnung. Auch für die Anpassung des nationalen Datenschutzrechts bedarf es weiterer gesetzlicher Anstrengungen.

· eine angemessene Regulierung der sozialen Netzwerke und einen effektiven Grundrechtsschutz von mehr als 30 Millionen deutschen Nutzerinnen und Nutzern

· die schnellstmögliche Vorlage des von der Bundesregierung seit langem angekündigten IT-Sicherheitsgesetzes 2.0, das proaktiv ansetzen und diejenigen

belohnen muss, die in gute IT-Sicherheitstechnologien investieren

· klare Zuständigkeiten innerhalb der Bundesregierung, die Herauslösung der IT-Sicherheit aus dem Zuständigkeitsbereich des Bundesinnenministeriums und neue Strukturen zur Erkennung hybrider Bedrohungslagen sowie eine stärkere Kooperation zwischen Bund und Ländern über den IT-Planungsrat

· klare Rechtsgrundlagen, z.B. für die Zusammenarbeit im Cyber-Abwehrzentrum sowie für die Quellen-Telekommunikationsüberwachung und Online-Durchsuchung sowie einen Verzicht auf diese Instrumente, so lange es diese nicht gibt und ein Verzicht auf die Zusammenarbeit mit dubiosen IT-Sicherheitsfirmen, die die Software bislang liefern

· ein - zumindest in Teilen - vom Bundesinnenministerium unabhängig gestelltes Bundesamt für Sicherheit in der Informationstechnik (BSI), das seiner Beratungsfunktion ohne Interessenkonflikte gerecht werden kann

· eine personelle Stärkung der bestehenden Datenschutzaufsichtsstrukturen, die den stark gestiegenen Herausforderungen durch die digitale Welt gerecht werden muss

· durchgehende Ende-zu-Ende-Verschlüsselungen bei allen staatlichen IT-Großprojekten statt unsicherer E-Government-Angebote, die niemand nutzt

· eine unabhängige und systematische Überprüfung des Quellcodes von Software, um IT-Sicherheitslücken frühzeitig zu erkennen und zu schließen

· ein neues, erweitertes Haftungsregime und verpflichtende Mindeststandards sowie Sicherheitsupdates für Hard- und Software sowie internetbasierten Dienste und klare gesetzliche Vorgaben für (neue) Zertifizierungs- und Auditierungsverfahren in Ergänzung zu den bestehenden datenschutzrechtlichen Zertifizierungsmöglichkeiten der EU-DSGVO

· den Verzicht auf IT-Sicherheit gefährdende Maßnahmen wie „Hack backs“, den staatlichen Ankauf, das Offenhalten und die Nutzung von bislang nicht öffentlich bekannten Sicherheitslücken (sogenannte „Zero-Day-Exploits“) und auf Überlegungen einer gesetzlichen Verpflichtung für Unternehmen, Hintertüren in Hard- und Software zu verbauen

· eine Abkehr von anlasslosen Massenüberwachungen, die sicherheitspolitisch kontraproduktiv wirken und Grundrechte gefährden

· mehr freie und offene Software als zentraler Baustein für eine sichere und zukunftsfähige IT-Landschaft und eine Überarbeitung von Ausschreibungsbedingungen

· zur Überprüfbarkeit die Offenlegung des Quellcodes bei Wahlsoftware und den Verzicht auf elektronische Wahlsysteme und Wahlcomputer

· neue gesetzliche Regelungen für das Schalten von Werbung in sozialen Netzwerken, gerade hinsichtlich sogenannter ”dark ads” im Zuge von Wahlen

· eine Kennzeichnungspflicht für social bots und andere automatisierte Programme, die in direkten Austausch mit NutzerInnen treten, um intransparente, bewusst herbeigeführte Diskursverschiebungen ohne eigene Meinungsmacht zu unterbinden

· neue internationale Übereinkommen zum Schutz digitaler Infrastrukturen und privater Kommunikation und die Ächtung militärischer Operationen auf zivilen Infrastrukturen

· einen verbesserten Schutz von HinweisgeberInnen (”Whistlebowern”), die immer wieder auch auf Missstände im Bereich der IT-Sicherheit hinweisen