Antrag 215/II/2019
ASJ Landesvorstand + Forum Netzpolitik
Der Landesparteitag möge beschließen:
Der Bundesparteitag möge beschließen:

Empfehlung der Antragskommission
Annahme (Konsens)

IT-Sicherheit stärken und digitale Freiheit schützen (IT-Sicherheitsgesetz 2.0)

Unser Grundgesetz garantiert eine Reihe von Bürger*innen- und Freiheitsrechte, welche dem Eingriff des Staates in die freie und umfassende Entfaltung der eigenen Persönlichkeit Grenzen setzen. Dazu gehören neben dem Fernmeldegeheimnis auch die Unverletzlichkeit der Wohnung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht). Leider wird die zunehmende Digitalisierung aller Lebensbereiche immer öfter zum Vorwand genommen, die Grundrechte mehr und mehr einzuschränken, oft mit dem Argument eines vermeintlichen Sicherheitsgewinns. Die Digitalisierung darf nicht zum Reflex führen, im digitalen Raum Freiheitsrechte stärker einzuschränken, als in der analogen Welt. Vielmehr müssen wir auch in der digitalen Welt unsere Freiheiten schützen.

Eingriffe in das informationelle Selbstbestimmungsrecht und in die Vertraulichkeit digitaler Systeme dürfen auch im digitalen Netz nur nach strengen gesetzlichen Vorgaben erfolgen. Das digitale Netz ist aber kein rechtsfreier Raum, auch im Netz müssen Straftaten aufgeklärt und verfolgt, Gefahren erkannt und beseitigt werden. Strafverfolgungsmaßahmen dürfen aber nur bei einem konkreten Anfangsverdacht, Gefahrenabwehrmaßnahmen nur bei einem konkreten Gefahrenverdacht und beides mit Richtervorbehalt zugelassen werden. Der nemotenetur-Grundsatz, die Grundrechte und der Grundsatz der Verhältnismäßigkeit müssen uneingeschränkt gelten

Mit Blick auf das kommende IT-Sicherheitsgesetz 2.0 fordern wir daher:

1. Recht auf Verschlüsselung und Anonymität
Niemand darf unter einen Generalverdacht gestellt werden, weil er vertrauliche und sichere Kommunikationswege nutzt oder sie anderen zur Nutzung bereitstellt. In Zeiten der weltweit steigenden staatlichen Einflussnahme auf die Funktionsweise und Inhalte zentraler Netzwerkdienste, darf die Nutzung verschlüsselter, dezentraler und/oder anonymer Kommunikationswege nicht kriminalisiert werden, sondern sollte gefördert werden. Für viele Menschen weltweit sind starke Verschlüsselungsmethoden, das TOR-Netzwerk („Darknet“) sowie andere dezentrale Kommunikationswege essenziell, um die Gefahr von Stigmatisierung oder staatlicher Repression zu umgehen.

Gesetzesverschärfungen, die das Zugänglichmachen entsprechender internetbasierter Leistungen oder das Erleichtern von Straftaten unter Strafe stellen, lehnen wir ab. Diese Dienste dienen insbesondere auch Journalist*innen und Whistleblowern, die unter teils hohen persönlichen Risiken für die Allgemeinheit wichtige Informationen aus einem geheimen oder geschützten Zusammenhang an die Öffentlichkeit bringen. Aber auch unabhängig von besonderen beruflichen Geheimhaltungspflichten und -interessen gilt, dass alle Bürger*innen ein Recht auf verschlüsselte Kommunikation haben und dieses weder im Einzelfall noch generell rechtfertigen oder begründen müssen. Messenger-Dienste wie Whatsapp/Telegram sollten ihre Daten zum Schutz der Nutzer*innen ohne Hintertüren verschlüsseln dürfen.

2. Kein Zwang zur Herausgabe von Passwörtern

Das Verbot des Zwangs zur Selbstbelastung und die Aussagefreiheit des Beschuldigten sind im Grundgesetz verankert. Sie sind Ausdruck einer auf der Achtung der Menschenwürde beruhenden rechtsstaatlichen Grundhaltung. Niemand muss sich selbst belasten. Dieser Grundsatz muss auch im digitalen Raum gelten. Einen Zwang zur Herausgabe von Passwörtern oder anderen Zugangsdaten unter Androhung von Beugehaft, lehnen wir als verfassungswidrig ab. Auch die Übernahme von Nutzerkonten durch staatliche Behörden gegen den Willen des Inhabers und die Kontaktaufnahme ggü. Dritten über dieses Konto lehnen wir als unverhältnismäßig ab. Ebenso lehnen wir die Pläne ab, den Strafverfolgungsbehörden anderer EU-Mitgliedstaaten im Rahmen der derzeit auf EU-Ebene verhandelten E-Evidence-Verordnung zu erlauben, Zugangsdaten bei Providern in Deutschland und in anderen Mitgliedstaaten sowie Drittstaaten mittels einer Herausgabeanordnung zu erlangen.

3. Forschung zur IT-Sicherheit und -Schwachstellen nicht kriminalisieren, sondern fördern

Die Arbeit der IT-Sicherheits- und Schwachstellenforschung ist ein essenzieller Beitrag für eine starke IT-Sicherheit und sollte durch Anreizsysteme, wie Bug-Bounty-Programme, gefördert werden. Aktuelle Forderungen nach Einführung eines Tatbestands des “digitalen Hausfriedensbruchs”, der bereits die unbefugte Ingebrauchnahme informationstechnischer Systeme unter Freiheitsstrafe stellen möchte lehnen wir ab, da auch eine Vielzahl alltäglicher Vorgänge betroffen wäre. Es gilt, Rechtsunsicherheiten zu reduzieren, statt neue zu erschaffen. Auch Reverse Engineering, also die Analyse geschlossener Hard- oder Software, indem „rückwärts“ der enthaltene Quellcode extrahiert wird, sollte gefördert werden.

4. Weiterentwicklung des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu einer unabhängigen, defensiven und neutralen Stelle für IT-Sicherheit

4a) Weiterentwicklung des BSI - endlich Unabhängigkeit
Aufgrund der vorgegebenen Interessenkonflikte zwischen Belangen der inneren Sicherheit und denen der Sicherheit und Integrität informationsverarbeitender Systeme, muss das BSI in Anbetracht seiner wachsenden Relevanz aus der fachlichen Weisungsgebundenheit des Bundesministers des Innern, für Heimat und Bau herausgelöst werden. Das könnte z. B. durch Anknüpfung an die Stelle des Bundesdatenschutzbeauftragten oder durch eine vergleichbare organisatorische Ausgestaltung erreicht werden.

4b) Das BSI sollte eine neutrale und defensive Stelle für IT-Sicherheit bleiben und darf nicht selbst zum Angreifer werden
Die Rolle des BSI als neutrale und defensive Stelle für IT-Sicherheit zu Gunsten von Bürger*innen und Unternehmen darf nicht vermischt werden mit staatlichen Verfolgungsinteressen. Dazu muss, z.B. im IT-Sicherheitsgesetz 2.0, eine Bindung der gewonnenen Erkenntnisse und Daten an defensive Zwecke vorgeschrieben werden. Eine Mischlösung, nach denen das BSI Informationen, die es im Vertrauen auf seine Neutralität erhalten hat, für sich oder andere Behörden zurückhält um damit staatliche Eingriffe zu ermöglichen, lehnen wir ab.

Begründung
Der Antrag ist aus Anlass des BMI-Entwurfs für das sog. IT-Sicherheitsgesetz 2.0 (s. Link unten) entstanden, gilt aber grundsätzlich und über diesen Anlass hinaus für ein ausgewogenes Verhältnis zwischen Sicherheit und Freiheit im digitalen Raum.

Zu 1. Recht auf Verschlüsselung und Anonymität
Es gibt viele gute Gründe, warum Nutzer*innen ihre Daten oder Kommunikation verschlüsseln und/oder anonymisieren wollen/müssen. Der Staat sollte die Bürger*innen dabei unterstützen und sie nicht kriminalisieren. Wer die Entschlüsselung von Nachrichten durch Messenger-Anbietern verlangt, würde sie dazu zwingen, absichtlich Schwachstellen in der Technik einbauen zu müssen. Der Hinweis auf Straftaten, die unter Zurhilfenahme von Verschlüsselungstechniken wie dem sog. “Dark Net” erfolgen, kann dem Staat nicht als Argument dienen, diese Selbstschutz-Maßnahmen unter einen Generalverdacht oder gar unter Strafe zu stellen. Die aktuellen diesbzgl. Bestrebungen wie im Entwurf des BMI für das IT-Sicherheitsgesetz 2.0 in einem § 126a StGB-E, bereits auch das Zugänglichmachen entsprechender internetbasierter Leistungen unter Strafe stellen, sind daher der fal-

sche Weg. Auch im Bereich des sogenannten „Darknet“ konnten Ermittlungsbehörden in der Vergangenheit große Fahndungserfolge erzielen, sodass eine generelle Kriminalisierung des Einsatzes solcher Dienste nicht erforderlich ist. Plattformbetreiber, auf dessen Plattform die Waffe des Münchner Attentäters gekauft wurde, ist u.a. wegen Beihilfe zu unerlaubtem Handeltreiben mit einer Schusswaffe und zum vorsätzlichen unerlaubten Handeltreiben mit einer Schusswaffe in Tateinheit mit fahrlässiger Tötung in neun Fällen in weiterer Tateinheit mit fahrlässiger Körperverletzung in fünf Fällen, verurteilt worden.

Mit großer Sorge ist zudem international zu beobachten, wie mehr und mehr Staaten Angst aus Angst vor den Freiheiten des Internets ihre Netze regionalisieren. China ist dort mit seiner “großen Firewall” bereits fast am Ziel einer totalen Überwachung der Inhalte angekommen. Russland wird nun mit seinem “Gesetz über das souveräne Internet” versuchen, einen ähnlichen Weg einzuschlagen. Weitere Länder eifern ebenfalls nach und können dafür z.B. hoch effiziente Überwachungstechnik aus China erwerben.

Zu 2. Im Entwurf des BMI zum IT-Sicherheitsgesetz 2.0 wird in § 163g StPO-E vorgeschlagen, verdächtigte Menschen gesetzlich zu verpflichten, Zugangsdaten zur Nutzung virtueller Identitäten herauszugeben. Diese Verpflichtung soll gegen den Willen des Verpflichteten auch mit Zwangsmitteln durchsetzbar sein, d.h. per Ordnungsgeld oder Haft von bis zu 6 Monaten. In der Praxis könnte es somit dazu kommen, dass ein Verdächtiger ins Gefängnis muss, weil er seine Passwörter nicht herausgibt.

Juristen halten diesen Ansatz für höchst problematisch und für einen Verstoß gegen den Grundsatz der Freiheit, sich nicht selbst belasten zu müssen. Strafverteidiger Udo Vetter hält das in einem SZ-Interview (9.4.2019) für einen “krassen Systembruch und eine der weitest gehenden Aufweichungsversuche der Bürgerrechte überhaupt.” Auch Zeugen könnten bislang die Herausgabe verweigern, wenn sie befürchteten, sich dadurch verdächtig zu machen.

Zu 3. Der im BMI-Entwurf zum IT-Sicherheitsgesetz 2.0 als § 200e StGB-E vorgesehene Straftatbestand, der u.a. die unbefugte Ingebrauchnahme informationstechnischer Systeme unter Freiheitsstrafe stellen möchte, ist abzulehnen. Der Tatbestand ist so ungenau definiert, dass viele Analysetätigkeiten ohne Schädigungsabsicht künftig in einem rechtlichen Graubereich erfolgen müssten. Sog. Hacker-Tools sind notwendig, um die Sicherheit von Systemen zu testen und zu erhöhen. Dafür ist auch das sog. Reverse Engineering wichtig, das ein wichtiges Instrument der Sicherheitsforschung, aber auch bei der Weiter-

entwicklung neuer Software ist.

Zu 4. 4b des BMI-Entwurfs zum IT-Sicherheitsgesetz 2.0 beschreibt die Aufgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). Eine Bindung der gewonnenen Erkenntnisse und Daten an defensive Zwecke ist dort nicht enthalten. Gleichzeitig erhält der Staat immer mehr nicht-defensive Befugnisse, wie die Nutzung von Staatstrojanern oder die Diskussionen zu sog. Hackbacks zeigen. Schwachstellenforscher*innen können sich somit nicht mehr sicher sein, ob BSI umgehend veranlasst, dass gemeldete Schwachstellen an die Hersteller gemeldet werden, oder ob Schwachstellen wie von den amerikanischen Geheimdiensten bekannt, teilweise auch bewusst nicht beseitigt werden, um diese für nicht-defensive Maßnahmen für einen gewissen Zeitraum auszunutzen. Dieses Vertrauen sollte aber bestehen.

Link zum Gesetzesentwurf: https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll