Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Ausschussdrucksache
17(24)064-A

TOP 1 am 14.1.2013

11.01.2013

Änderungsantrag von der Fraktion DIE LINKE.

zu Ausschussdrucksache 17(24)064

Erläuterung: DIE LINKE. zieht ihre Handlungsempfehlungen in der Ausschussdrucksache 17(24)064 (Zeilen 4359 bis 4391 sowie Zeilen 5410 bis 5527) zurück.

DIE LINKE. schließt sich stattdessen den

Ergänzenden Handlungsempfehlungen der Fraktionen der SPD und BÜNDNIS 90/DIE GRÜNEN und der Sachverständigen Alvar Freude, Constanze Kurz, Prof. Dr. Wolfgang Schulz, Lothar Schröder und Cornelia Tausch

- **zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“ Empfehlungen hinsichtlich der Einführung des Internetprotokolls in der Version 6 (IPv6) (Zeile 4319 bis 4353)**
- **zum Kapitel „Schutz Kritischer Infrastrukturen im Internet“ (Zeile 4838 bis 5179; ausgenommen die Zeilen 5133 bis 5154)**
- **zum Kapitel „Kriminalität im Internet“ (Zeile 5251 bis 5406)**

an.

DIE LINKE. beantragt die ergänzende Abstimmung der folgenden ergänzenden Handlungsempfehlungen. Hierbei handelt es sich nicht um neue Texte, sondern um eine gekürzte Fassung der zurückgezogenen Handlungsempfehlungen von DIE LINKE.

Ergänzende Handlungsempfehlungen der Fraktion DIE LINKE. zum Kapitel „Zugang zum Internet und Infrastruktur des Internets“

Empfehlungen hinsichtlich der Einführung des Internetprotokolls in der Version 6 (IPv6)

- Um Rechtsunsicherheit zu vermeiden, sollte zweifelsfrei festgeschrieben werden, dass es sich bei IP-Adressen um personenbezogene Daten handelt.“
- Anbieter sollten verpflichtet werden, ihren Kunden die Möglichkeit einzuräumen, ein anonymisierendes Netzwerk (Multi-hop-Proxy-Routing) zu betreiben.“

– Um die im Telekommunikationsgesetz ausdrücklich vorgesehene Möglichkeit der anonymen Nutzung nicht zu unterlaufen, sollten die Hersteller darauf verpflichtet werden, nur solche Endgeräte auf den Markt zu bringen, die dem Kunden die freie Wahl zwischen anonymer oder identifizierbarer Netznutzung lassen. Die jeweilige Option sollte einfach und leicht wählbar sein, etwa durch einen leicht zugänglichen Button. Die Grundeinstellung sollte verpflichtend ein anonymes Surfen vorsehen."

Ergänzende Handlungsempfehlungen der Fraktion DIE LINKE.

zum Kapitel „Kriminalität im Internet"

Thema Staatstrojaner

Die Enquete-Kommission empfiehlt der Bundesregierung

– den Kernbereich privater Lebensgestaltung unter den digitalen Bedingungen stärker gesetzlich zu schützen,
– die Befugnis der Ermittlungsbehörden der Länder zu Online-Durchsuchungen aufzuheben und gänzlich darauf zu verzichten, informationstechnische Systeme mittels Infiltration zu durchsuchen,
– die Befugnis des Bundeskriminalamts zum verdeckten Eingriff in informationstechnische Systeme (§20k des Bundeskriminalamtgesetzes) und zur Verwendung und Übermittlung solcher Daten (§ 20v BKAG) aufzuheben,
– den Quellcode der Trojaner, die im Rahmen der Quellen-TKÜs verwendet wurden, zu veröffentlichen und die Öffentlichkeit in transparenter Weise über die finanzielle Förderung und Erforschung und die Anschaffungskosten von Spionage- und Überwachungssoftware sowie verwandter Technik zu informieren.

Thema Cybersicherheit

Der Begriff Sicherheit hat in den letzten Jahren einen schleichenden Bedeutungswandel erfahren. Traditionell ist die Schutzpflicht des Staates für seine Bürger im Sinne einer social security verstanden worden, also einer Schutzverpflichtung im Sinne existentieller, kultureller und sozialer Existenzsicherung. Dieser bürgerzentrierte Schutzgedanke ist in den letzten Jahren jedoch zunehmend von einem militärischen Sicherheitsbegriff verdrängt worden. Seit es den „Krieg gegen den Terror" gibt, ist die Gefahrenabwehr als Paradigma der Sicherheitspolitik auf immer weitere, zunehmend auch auf zivilgesellschaftliche Bereiche

ausgedehnt worden. Im digitalen Zeitalter betrifft dieses Denken auch die Netze, also die zentrale Kommunikationsinfrastruktur der modernen Gesellschaft.

Vor diesem Hintergrund empfiehlt die Enquete der Bundesregierung die Beachtung folgender Punkte

- Forschungsgelder, die für zivile Zwecke bestimmt sind, dürfen nicht unter der Hand für militärische Zwecke benutzt werden. Eine klare Trennung beider Bereiche ist hier geboten. Der Forschungsetat des Bundes darf nicht zur Förderung von High-Tech-Projekten eingesetzt werden, die letztlich primär militärischen Zwecken dienen.
- Anbieter von Cloud-Diensten sollten verpflichtet werden, ihre Kunden über erkannte Angriffe umfassend zu informieren. Gerade Clouds stellen für Angreifer attraktive Ziele dar, da hier nicht nur die Daten eines einzelnen Unternehmens, sondern eine Vielzahl unterschiedlicher Informationen zu bekommen sind. Umso wichtiger ist es, dass die Betroffenen über IT-Sicherheitsprobleme ihres jeweiligen Dienstleisters umfassend informiert werden.
- Dem grauen Markt sollte das Geld entzogen werden: Die Kunden von Exploits, die unerkannte Schwachstellen ausnutzen, sind heutzutage überwiegend Staaten. Die Aufrüstung für staatsterroristische Akte hat zu einem erheblichen Anstieg der Preise geführt, die für Zero-Day-Exploits gezahlt werden. Dieses Geld sollte eher in die Entwicklung besserer IT-Sicherheit investiert werden.
- Die GSM-Verschlüsselung kann nicht mehr als sicher betrachtet werden, seit sie 2009 geknackt wurde. Mittlerweile steht für den Einbruch in die Privatsphäre der Nutzer von Mobiltelefonen einfache Software zur Verfügung. Die Bundesregierung sollte sich bei der GSM Association für ein sicheres Verschlüsselungsverfahren einsetzen.
- Die vom AK Kritis des Bundesministerium des Inneren gehandhabte Definition der Kritischen Infrastrukturen (KRITIS) sollte nicht in einer Weise ausgeweitet werden, die befürchten lässt, dass es durch eine solche Neudefinition zu einer unverhältnismäßigen Einschränkungen von Grundrechten kommen kann. Vielmehr sollte der Begriff der kritischen Infrastrukturen möglichst eng gefasst sein und sich an dem konkreten Schutzziel einer Sicherung der existenziellen Bedürfnisse der Bevölkerung orientieren.
- Auch im Rahmen einer Neudefinition kritischer Infrastrukturen darf es zu keiner Vermischung des Schutzes ziviler kritischer Infrastrukturen mit Strategien zur militärischen Cybersicherheit kommen.