LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/8109**

10.03.2015

Antrag

der Fraktion der PIRATEN

Angriffe von Geheimdiensten auf Integrität und Vertraulichkeit kritischer Infrastruktur und Menschheits-Kommunikationssysteme müssen enden!

I. Sachverhalt

Westliche Nachrichtendienste wie die US-amerikanische National Security Agency (NSA) und die britischen Government Communications Headquarters (GCHQ), aber auch der Bundesnachrichtendienst (BND) spielen eine verhängnisvolle Rolle im Umgang mit Integrität und Vertraulichkeit von Kommunikations- und Authentifizierungssystemen. Digitale Systeme und Netzwerke werden systematisch korrumpiert und gestört, wobei die beteiligten Dienste offenbar selbst nicht einmal davor zurückschrecken, auf illegalem Wege den Schutz dieser Systeme auszuhebeln.

Der britische Geheimdienst GCHQ ist auch in die Systeme des niederländischen Chipkartenherstellers Gemalto eingebrochen und hat dort offenbar Millionen von Schlüsseln entwendet, die für die Authentifizierungs- und Verschlüsselungsfunktionen der u. a. damit erstellten Bankkarten, Krankenkarten und Telefonkarten benötigt werden. Die Integrität der darauf basierten Mechanismen ist grundsätzlich in Frage gestellt worden. Die gesetzlich geschützte Vertraulichkeit der Mobilfunkkommunikation, von Krankenakten wie Bankkonten ist damit mutmaßlich gebrochen worden.

Im vergangenen Monat wurde bekannt, dass es Außenstehenden verhältnismäßig leicht fällt, IP-Telefonate abzuhören. Laut Telekommunikationsanbietern ist die fehlende Standardisierung einer Verschlüsselung dafür ein Grund. Sicherheitsexperten und Datenschützer weisen darauf hin, dass Geheimdienstmitarbeiter an diesen Standardisierungen mitarbeiten und aktiv darauf hinwirken, dass Verschlüsselungen nicht zum Standard werden, damit die Überwachung und Ausforschung solcher Kommunikation einfach fällt. Teilnehmer des Bundesnachrichtendienstes und anderer Geheimdienste nehmen regelmäßig an Standardisierungsdefinitionen von elektronischer Kommunikation und Authentifizierung teil.

Auf dem letztjährigen Chaos Communications Congress haben Sicherheitsexperten Mängel im Signalling System #7 (SS7), einer Sammlung von Signalisierungsprotokollen in Mobilfunknetzen aufgedeckt. Auch hier wird Einfluss von Nachrichtendiensten auf die fehlerhafte Standardisierung angenommen. Diese Lücken erlauben es, Mobilfunk weltweit ohne Zugriff

Datum des Originals: 10.03.2015/Ausgegeben: 10.03.2015

auf die Telefone umzuleiten und abzuhören sowie den Träger eines Mobiltelefons weltweit zu orten.

Für Besorgnis hatte die Information gesorgt, dass die NSA dem IT-Verschlüsselungssystemhersteller RSA Security Inc., eine Tochtergesellschaft der EMC Corporation mit Sitz in Massachusetts und Zweigstellen unter anderem in Irland und Großbritannien, insgesamt 10 Millionen Dollar dafür gezahlt hat, dass sie in die Sicherheitsbibliothek eine Krypto-Backdoor der NSA implementierte hat.

Zuvor hatte die NSA beim National Institute of Standards and Technology (NIST) bewirkt, dass zum vermeintlichen Schutz von Verschlüsselungen ausgerechnet ein fragwürdiger Zufallszahlengenerator der NSA zum Standard für Kryptoanwendungen definiert wurde. Es ist davon auszugehen, dass die Geheimdienste damit Zugriff auf sämtliche mit diesen Standards realisierten Sicherheits- und Verschlüsselungssystemen haben. RSA stellt unter anderem auch Sicherheitstokens für den Zugriff auf IT-Systeme her, wie sie beispielsweise im nordrhein-westfälischen Landtag verwendet werden.

Die NSA unterhält eine Abteilung mit der Bezeichnung Office of Tailored Access Operations (TAO). Diese sammelt und erstellt Sicherheitslücken in IT-Systemen, Soft- und Hardware. Nicht jedoch, um diese dann zu schließen und die diese Systeme nutzenden Organisationen und Menschen zu schützen, sondern um maßgeschneiderte Angriffs- und Spionagewerkzeuge dafür zu bauen. Ein fünfzig seitiger Katalog von darauf basierenden Angriffswerkzeugen ist Ende 2013 bekannt geworden. Sicherheitslücken in Festplatten, Mobiltelefonen, Internet-Infrastruktur, USB-Ports und vielen weiteren Systemen sind darin dokumentiert. Manche weltweit zu beobachtende Malware-Angriffe wie Stuxnet und Regin basieren augenscheinlich auf den dort beschriebenen Sicherheitslücken und Angriffswerkzeugen.

Sicherheitslücken können nicht nur von befreundeten Geheimdiensten, sondern auch von feindlich gesinnten Diensten, Verbrechern und Erpressern genutzt werden. Dieses Vorgehen der Nachrichtendienste sorgt also nicht für Sicherheit, sondern im Gegenteil für eine größere Unsicherheit von Organisationen, Behörden, Unternehmen, Menschen und Gesellschaft. Geheimdienste befördern auf diesem Wege eine Gefährdung der Privatsphäre sowie Vertraulichkeit und Integrität elektronisch basierter Kommunikation. Auch der Industriespionage ist damit Tür und Tor geöffnet

Einzig die Verschlüsselung von Kommunikation, insbesondere wenn sie durchgängig von Nutzer zu Nutzer reicht, schützt die Privatsphäre nachhaltig, da nur der Empfänger die Nachrichten lesen kann. Zudem ist es durch Signierung sofort erkennbar, ob Kommunikation auf dem Transportweg manipuliert worden ist.

Ein Recht auf Anonymität elektronischer Kommunikation gibt es bereits: In § 4 Abs. 6 Teledienstedatenschutzgesetz heißt es: "Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren". In § 18 Abs. 6 Mediendienstestaatsvertrag ist die gleiche Vorschrift für Anbieter von Mediendiensten niedergelegt. Das Recht auf Verschlüsselung leitet sich aus der Rechtsprechung des Bundesverfassungsgerichtes ab, welches in einem Leitsatz festlegte: „Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Verschlüsselung sichert die Integrität von elektronischer Kommunikation gegen ungewünschte Veränderungen.

Tatsächlich wird allerdings das Recht auf Anonymität sowie das Recht auf Verschlüsselung immer häufiger in Frage gestellt. Derzeit wird über ein Verschlüsselungsverbot oder aber die Pflicht zu einer Hintertür für Geheimdienste diskutiert. Sicherheitspolitiker sehen in verschlüsselter oder anonymer Kommunikation oft eine Gefahr, da sie sich nicht ohne Weiteres überwachen lässt. Es wird die Angst vor Terroranschlägen oder schweren Straftaten zur Argumentation genutzt. Dabei ist offensichtlich, dass wirkliche Verbrecher sich nicht von Verschlüsselungsverboten davon abhalten lassen werden, ihre Kommunikation zu verschlüsseln, und im Zweifel auf Algorithmen ohne staatliche Hintertüren ausweichen werden. Durch Verbote und Hintertüren kann das Schutzniveau in diesem Bereich nicht erhöht werden.

Hintertüren in Verschlüsselungssystemen schwächen die Integrität der Systeme grundsätzlich, da sie systembedingt eine Schwachstelle in der Kryptographie an sich darstellen, die das Auftreten von Angriffen und Sicherheitslücken befördert. Ein Verschlüsselungsverbot selbst wäre der Todesstoß für Privatsphäre und Vertraulichkeit legaler elektronischer Kommunikation generell und würde die Authentifizierungsfunktion elektronischer Systeme grundsätzlich in Frage stellen.

II. Der Landtag stellt fest:

- Die Menschen haben ein grundlegendes Recht auf Vertraulichkeit und Integrität ihrer informationstechnischen Systeme. Kommunikation muss auch anonym möglich sein, wo die Identifikation des Nutzers nicht zwingend erforderlich ist.

- Eine lückenlose Verschlüsselung elektronischer Kommunikation von Sender zu Empfänger ist der beste Schutz für Integrität und Vertraulichkeit dieser Kommunikation. Wo immer es technisch möglich ist, muss Bürgern, Unternehmen und Behörden die Möglichkeit von echter Ende-zu-Ende-Verschlüsselung geboten werden.

- Echte Ende-zu-Ende-Verschlüsselung muss zur Standardeinstellung jeder elektronischen Kommunikation werden.

- Bemühungen von Geheimdiensten, Verschlüsselung und sichere Authentifizierung aufzuheben und systematisch zu zerstören, sind scharf zu verurteilen. Hohe Sicherheitsstandards dürfen nicht daran scheitern, dass Geheimdienste ihren Einfluss geltend machen und sie verhindern oder schwächen, um einfacher überwachen bzw. leichter Unternehmensgeheimnisse ausspionieren zu können.

- Hintertüren in Verschlüsselungs- und Authentifizierungssystemen stellen eine strukturelle Schwäche dar und senken das Sicherheitsniveau der Systeme.

- Es bedarf einer digitalen Abrüstung des Geheimdienstarsenales an Angriffswerkzeugen auf Kommunikation und Verschlüsselung. Die Sammlung von Sicherheitslücken durch Geheimdienste schwächt die Sicherheit unserer elektronischen Systeme insgesamt. Geheimdienste müssen verpflichtet werden, Kenntnisse über Sicherheitslücken an Hersteller und Nutzer der Systeme zeitnah weiterzugeben.

III. Der Landtag fordert die Landesregierung auf

- an allen Stellen politisch darauf hinzuwirken, dass höchstmögliche Sicherheit und Verschlüsselung zum Standard in elektronischer Kommunikation und Authentifizierung wird,

- Versuchen, solche Standards zu verhindern, zu schwächen oder zu schädigen entschieden entgegenzutreten,

- daran mitzuwirken, dass das Recht auf bestmögliche Verschlüsselung und Integrität von Kommunikations- und Authentifizierungssystemen zum Grundrecht wird,

- eine Bundesratsinitiative auf den Weg zu bringen, welches die Kommunikation mit echter Ende-Zu-Ende-Verschlüsselung als Standardeinstellung für alle Kommunikations- und Informationssysteme vorschreibt,

- Forderungen nach staatlichen Hintertüren und Verschlüsselungsverboten eine klare Absage zu erteilen,

- daran mitzuwirken, dass Geheimdiensten die systematische Zerstörung von elektronischen Sicherheitssystemen und Standards sowie der heimliche Besitz von Sicherheitslücken untersagt wird, eine Initiative zu starten bzw. zu fördern, die die lückenlose Ende-zu-Ende-Verschlüsselung als Standard von IP-Telefonie zum Ziel hat,

- weitere Initiativen zu fördern, die lückenlose Ende-zu-Ende-Verschlüsselungen elektronischer Kommunikation zum Ziel haben,

- auf eine Abrüstung der digitalen Arsenale von Angriffswerkzeugen bei Geheimdiensten weltweit hinzuwirken.

Dr. Joachim Paul
Marc Olejak
Daniel Schwerd

und Fraktion