Franz-Josef Lersch-Mense, Minister für Bundesangelegenheiten, Europa und Medien: Herr Präsident! Meine Damen und Herren Abgeordnete! Eine Million € – darauf wurde schon hingewiesen – investiert die Landesregierung, damit Freifunkinitiativen an bis zu 100 landeseigenen Gebäuden offene WLAN-Netze einrichten können. Das tun wir, weil wir natürlich denken, dass solche freien Zugänge ins Internet wichtig sind, dass sie möglichst flächendeckend vorhanden sein sollten. Wir wollen dazu einen eigenen Beitrag leisten – auch als ausdrückliche Ermutigung an andere, diesem Beispiel zu folgen.

Deshalb haben wir uns auch für eine Abschaffung der Störerhaftung eingesetzt. Wir haben auf Bundesebene intensiv an der Entwicklung eines neuen Telemediengesetzes mitgearbeitet. Nicht zuletzt ist es auch der Initiative der NRW-Landesregierung zu verdanken, Herr Schwerd, dass nun das Providerprivileg für alle Anbieter offener Netze gilt. Der Schutz vor Haftungs- und Unterlassungsansprüchen ist jetzt in der Gesetzesbegründung ausdrücklich als Zielsetzung benannt.

Wir haben uns auch dafür stark gemacht, dass offene Netze nicht mit einem Passwort geschützt werden müssen. Am 27. Juli 2016 ist die Novelle des Telemediengesetzes nun in Kraft getreten. Die Fraktion der Piraten kritisiert in ihrem Antrag, dass trotzdem noch Abmahnungen möglich seien. Mir sind allerdings bisher keine konkreten Fälle von entsprechenden Verfahren oder gar Urteilen bekannt, Herr Lamla. Wir werden die weitere Entwicklung abwarten müssen.

Ich gebe aber gerne zu, dass das Urteil des Europäischen Gerichtshofes vom 9. September 2016, auf das Ihr Antrag auch Bezug nimmt, hier neue Fragen aufwirft. Der EuGH musste entscheiden, inwieweit das Prinzip der Störerhaftung europäischen Richtlinien zuwiderläuft, also europäischem Recht widerspricht. Im Zuge dessen hat er zunächst bestätigt, dass Anbieter nicht auf Schadensersatz haften.

Wenn aber aus einem offenen WLAN-Netz Rechtsverletzungen begangen werden, sagt der EuGH, dass der Schutz dieses Anschlusses durch ein Passwort grundsätzlich eine geeignete Maßnahme sein kann, um wiederholte Rechtsverletzungen zu verhindern. Damit scheint der Passwortschutz wieder im Gespräch zu sein. Das löst sicherlich Unsicherheit bei denen aus, die offene Internetzgänge ausbauen – nicht zuletzt auch mit einer Förderung der Landesregierung.

Aber der EuGH schreibt diese Maßnahmen natürlich keineswegs zwingend vor. Er sagt nur, dass sie nach europäischem Recht nicht ausgeschlossen wären.

Nach unserer Bewertung lässt die Novelle des deutschen Telemediengesetzes auch keinen Raum mehr für Unterlassungsansprüche. Daran ändert auch das EuGH-Urteil nichts.

Sicherungsmaßnahmen, wie sie das Urteil beschreibt, sind nach deutschem Recht nicht mehr erforderlich. Wir müssen jetzt abwarten, ob die Gerichte auch diese Rechtsauffassung bestätigen. Aber ich bin da durchaus optimistisch.

Zum jetzigen Zeitpunkt ist jedenfalls aus unserer Sicht eine groß angelegte politische Initiative nicht angebracht. Aber die Landesregierung teilt grundsätzlich die Ziele der antragstellenden Fraktion. Auch wir wollen offene Netzzugänge. Auch wir wollen deshalb keine Störerhaftung und keinen Passwortzwang.

Sie können sicher sein, wir werden sehr genau beobachten, wie deutsche Gerichte das neue Telemediengesetz anwenden, wie sie mit dem Urteil der EuGH umgehen. Sollte es dann nötig werden, werden wir sofort auch politisch aktiv werden im Sinne einer Fortsetzung unserer Politik für offene Netzwerke. – Herzlichen Dank für die Aufmerksamkeit.

(Beifall von der SPD und den GRÜNEN)

Vizepräsident Oliver Keymis: Vielen Dank, Herr Minister Lersch-Mense. Weitere Wortmeldungen gibt es nicht.

Es gibt aber einen Vorschlag: Der Ältestenrat empfiehlt die **Überweisung** des **Antrags Drucksache 16/13030** an den **Ausschuss für Kultur und Medien** – federführend – sowie an den **Ausschuss für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk**. Die abschließende Abstimmung soll im federführenden Ausschuss in öffentlicher Sitzung erfolgen. Wer stimmt der Überweisung zu? – Gibt es Gegenstimmen? – Enthaltungen? – Das ist nicht der Fall. Damit ist einstimmig so überwiesen.

Ich rufe auf:

9 Zweites Gesetz zur Änderung des Gesetzes zur Verbesserung der Sicherheit in Justizvollzugsanstalten des Landes Nordrhein-Westfalen

Gesetzentwurf
der Landesregierung
Drucksache 16/12434

Beschlussempfehlung und Bericht
des Rechtsausschusses
Drucksache 16/13047 – Neudruck

zweite Lesung

Alle fünf im Landtag vertretenen Fraktionen haben sich zwischenzeitlich darauf verständigt, ihre Reden zu Protokoll zu geben. *(Siehe Anlage 2)*

Somit kommen wir direkt zur Abstimmung. Der Rechtausschuss empfiehlt in Drucksache 16/13047 – Neudruck –, den Gesetzentwurf Drucksache 16/12434 unverändert anzunehmen. Wir stimmen also über den Gesetzentwurf ab. Wer stimmt dem zu? – Gibt es Gegenstimmen? – Gibt es Enthaltungen? – Eine Enthaltung bei der CDU. FDP?

(Angela Freimuth [FDP]: Hat zugestimmt!)

– Hat zugestimmt. Der fraktionslose Kollege Schwerd hat sich enthalten. Also haben wir bei Enthaltung der CDU-Fraktion und bei Enthaltung von Herrn Schwerd, fraktionslos, eine breite und damit einstimmige **Zustimmung zum Gesetzentwurf Drucksache 16/12434**. Damit ist dieser **in zweiter Lesung** einstimmig **verabschiedet**.

Ich rufe auf:

10 Digitale Gefahrenabwehr – Sicherheitslücken entdecken und schließen

Antrag
der Fraktion der PIRATEN
Drucksache 16/13033

Ich eröffne die Aussprache. Für die Piratenfraktion hat Herr Kollege Herrmann das Wort.

Frank Herrmann (PIRATEN): Vielen Dank. – Sehr geehrter Herr Präsident! Sehr geehrte Kolleginnen und Kollegen! Liebe Zuschauer hier im Saal und zu Hause! Die Europäische Union hat den Oktober 2016 zum Cyber Security Month erklärt. Ich denke, unser Antrag passt ganz gut dazu.

Sie erinnern sich vielleicht an die Meldung vom Dienstag vergangener Woche, als bekannt wurde, dass es eine Hintertür, also einen unbekannten Zugang, in einem Netzwerk-Videoüberwachungssystem gibt. In einem System, das hauptsächlich in Hochsicherheitsumgebungen weltweit eingesetzt wird! Dieser der Öffentlichkeit unbekannte Zugang wurde von einem Geheimdienst genutzt, von der NSA. Dieser Geheimdienst hatte also weltweit im wahrsten Sinne des Wortes Einblicke in vermeintlich gesicherte Räume, und das seit mindestens dem Jahr 2005. Dass dem BND dieser Zugang, diese Sicherheitslücke, auch seit 2005 wohl bekannt war, kommt noch erschwerend hinzu.

Es wäre natürlich naiv, anzunehmen, dass dies die einzige Lücke in Netzwerk-Sicherheitssystemen ist. Genauso naiv wäre es, anzunehmen, dass dies die einzige Lücke ist, die der NSA oder dem BND bekannt ist. Noch naiver wäre es, anzunehmen, dass derartige Lücken den Kriminellen dieser Welt und insbesondere der organisierten Kriminalität nicht bekannt sind.

Damit komme ich zum Kern unseres Antrags. Angriffe aus dem Netz, sogenannte „Hackerangriffe“, aber auch staatlicher Cyberwar existiert nur, weil es Lücken, also Fehler in Software gibt.

Wir möchten mit unserem Antrag öffentliche Stellen in Nordrhein-Westfalen verpflichten, entdeckte Softwarefehler umgehend den verantwortlichen Herstellern zur Fehlerbehebung zu melden und nach einer festgelegten Zeit zu veröffentlichen. Die Veröffentlichung ist dabei der wichtige Punkt; denn nur wenn ich weiß, wo eine Lücke ist, kann ich sie auch schließen bzw. eine neue Softwareversion einspielen und damit das Netz und die Nutzung von Computern sicherer machen. Jede bekannte und geschlossene Lücke trägt zur Sicherheit weltweit bei. Das Entdecken, Schließen und Veröffentlichen von Softwarefehlern ist für uns Piraten digitale Gefahrenabwehr.

Leider wird aber seit längerer Zeit das Gegenteil praktiziert, leider auch und gerade von Behörden und ganzen Regierungen. Ich war gestern auf einem sehr interessanten Vortrag hier in der Akademie der Wissenschaften in Düsseldorf. Dort hat Professor Paar von der Ruhr-Uni Bochum über Sicherheit und Unsicherheit im Internet der Dinge referiert. Er hat dabei ein sehr interessantes Schaubild über den Anstieg der sogenannten Hackerangriffe im Internet gezeigt. Es war eine stetig ansteigende Kurve von 2005 bis heute. Die These dazu: Kriminalität entwickelt sich da, wo es einen Markt gibt, wo es Möglichkeiten gibt.

Dazu gehört auch, dass ab ca. 2004/2005 die Aktivitäten der Geheimdienste im Internet merkbar und wirksam wurden. Nach 09/11 hat es eine Zeit gedauert, bis die Milliarden, die in den USA in die NSA und andere Geheimdienste gesteckt wurden, sich bemerkbar gemacht haben und auch über das Internet Lücken in Software ausgenutzt worden sind. Überwachung funktioniert übrigens auch nur über Lücken in Software.

Jetzt muss man nur eins und eins zusammenzählen, um zu erkennen, dass Sicherheitslücken geheimzuhalten und zum eigenen Vorteil zu verwenden – als kriminelle Gruppe, als Scriptkiddie oder auch als Geheimdienst –, eben nicht funktioniert und zu Unsicherheit führt. Das ist wie mit Waffen. Die werden auch nicht nur von Guten verwendet, sondern die Bösen haben halt auch immer welche. Wir sollten den Markt, der auch gerade in Deutschland entsteht, zum Beispiel durch das Hochrüsten der Bundeswehr zu einer Cyberarmee, nicht fördern, sondern austrocknen.

Deswegen dürfen Softwarefehler nicht geheim bleiben, sondern müssen, wenn sie entdeckt worden sind, geschlossen und bekanntgemacht werden. Das ist digitale Gefahrenabwehr. Hier sollte Nordrhein-Westfalen Vorbild werden.

(Beifall von den PIRATEN)