**LANDTAG NORDRHEIN-WESTFALEN**
16. Wahlperiode

Drucksache **16/13033**

27.09.2016

# Antrag

**der Fraktion der PIRATEN**

**Digitale Gefahrenabwehr - Sicherheitslücken entdecken und schließen**

## I. Sachverhalt

Viele Unternehmen und auch öffentliche Einrichtungen wie Krankenhäuser[1] oder jüngst nordrhein-westfälische Ministerien waren schon Opfer von Angriffen auf ihre Netzinfrastruktur. Kriminelle führen mit komplexen und höchstmodernen Mitteln Online-Erpressungen durch und demonstrieren, dass sie sogar Industriesteuerungen für Hochöfen[2] kontrollieren können.

Überhaupt ermöglicht werden Angriffe dadurch, das Softwaresysteme niemals fehlerfrei sind. IT-Systeme stürzen ab oder tun manchmal nicht das, was von ihnen erwartet wird. Viele dieser Fehler lassen sich dann dazu nutzen, ein System zu kompromittieren, um Schadsoftware einzuschleusen und zu installieren.

Da IT-Systeme heutzutage überall zu finden sind, in Autos, in Ampelsteuerungen, in Insulinpumpen, Hörgeräten, Herzschrittmachern, Industriesteuerungen, Mobiltelefonen und in Kritischen Infrastrukturen, kommt dem Schutz der Systeme eine besondere Bedeutung zu.

Digitale Einbrüche benötigen Fehler, benötigen Schwachstellen und digitale Hintertüren. Die Suche nach diesen Fehlern ist deshalb ein lukrativer Markt geworden. Gefundene Fehler, die einen unerwünschten Zugang zu einem IT-Systems öffnen, sog. Sicherheitslücken, können für viel Geld auf dem Schwarzmarkt an Kriminelle verkauft werden oder häufig gegen eine Belohnung an den Hersteller gemeldet werden. Nur wenn die Hersteller von den Sicherheitslücken erfahren, können sie die Lücken schließen und mit Updates ihre Kunden schützen.

Ohne eine Information und ohne ein Update des Herstellers sind die Systeme von Unternehmen, der Bevölkerung und der öffentlichen Hand nicht sicher und einer Gefahr ausgesetzt.

[1] https://www.welt.de/regionales/nrw/article153011989/Hacker-erpressen-Kommunen-und-Kliniken-mit-Viren.html

[2] http://www.spiegel.de/netzwelt/web/bsi-bericht-hacker-legten-deutschen-hochofen-lahm-a-1009191.html

Datum des Originals: 27.09.2016/Ausgegeben: 27.09.2016

Eine vorhandene Sicherheitslücke ist eine offene Hintertür, die innerhalb kürzester Zeit von Kriminellen ausgenutzt werden kann. Daher ist die Erstellung von Updates durch die Hersteller und eine Aktualisierung der Softwaresysteme durch die Nutzer extrem zeitkritisch.

Gleichzeitig erfahren und entdecken unterschiedliche Teile der Landesverwaltung, das Landes-CERT und Forscher an den nordrhein-westfälischen Universitäten von unterschiedlichen Sicherheitslücken diverser IT-Produkte. Dennoch ist die "Verbreitung bzw. Weiterleitung von Warnmeldungen zu Schwachstellen in Applikationen, Netzwerk-Diensten und Betriebssystemen" bislang ausschließlich Aufgabe des Landes-CERT.

Die Veröffentlichung einer Sicherheitslücke, oft auch erst nach einer Benachrichtigung an den Hersteller, ist häufig der einzige Weg, viele Nutzer zu warnen und ihnen so die Gelegenheit zu geben, gefährdete Systeme abzusichern. Aus diesem Grund ist es in der Wirtschaft inzwischen weit verbreitet, dass Unternehmen sich Richtlinien zur verantwortungsbewussten Veröffentlichung von Sicherheitslücken geben und diese öffentlich bekannt machen.

Um Onlinekriminalität vorzubeugen, ist ein Schutz der Systeme und ihrer Kommunikationswege unabdingbar. Interessenkonflikte, wie es diese bei dem CERT des Bundes gab, sollen mit diesem Antrag verhindert werden.

In der Regierungserklärung von Ministerpräsidentin Kraft im Januar 2015 wollte sie höchste Sicherheit für elektronische Kommunikation erreichen:

> *"Anbieter von Telemediendiensten, insbesondere von sozialen Netzwerken, sollen verpflichtet werden, die Sicherheitseinstellungen auf der höchsten Sicherheitsstufe gemäß dem Stand der Technik voreinzustellen."*

Auch das Vorhaben der Landesregierung, 1000 Sicherheitsforscher nach Nordrhein-Westfalen zu locken, setzt voraus, dass moderne Sicherheitsprodukte aus Deutschland glaubwürdig bleiben. Hier hat Nordrhein-Westfalen die Chance sich international an die Spitze zu setzen und sich als Standort für Sichere IT zu etablieren, wenn es öffentlichkeitswirksam dafür wirbt, dass die rechtlichen Rahmenbedingungen es Unternehmen in NRW weiterhin erlauben, sichere und datenschutzfreundliche Produkte herzustellen. Während chinesische und amerikanische IT-Produkte mit Blick auf eingebaute staatliche Hintertüren und Spionagezugänge kritisch betrachtet werden, kann NRW hier einen Standortvorteil erzeugen, den es nutzen und ausbauen kann. Sichere Informationstechnik hat einen großen Markt und Datensicherheit gewinnt immer mehr an Bedeutung. Es gibt in Deutschland bislang kein Kryptographie-Verbot und keine Verpflichtung zum Einbau von Hintertüren. Das Land sollte sich daher auch auf allen Ebenen für den Erhalt dieser Rahmenbedingungen einsetzen, um den IT-Security-Standort Nordrhein-Westfalen weiter fördern und ausbauen zu können.

Vorschläge wie von Bundesinnenminister De Maiziere, Unternehmen zum Einbau von Schutzlücken in ihre Software zu verpflichten, verunsichern nordrhein-westfälische Unternehmen, Softwareentwickler und Investoren. Solchen Vorschläge sollte das Land NRW deutlich widersprechen und sich so als Standort für die Digitalwirtschaft weiter zu profilieren.

Auch vor dem Hintergrund, dass das Bundesverfassungsgericht im Jahr 2008 das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme formuliert hat, weil Nordrhein-Westfalen, mit Schadsoftware fremde IT-Systeme im Rahmen einer heimlichen "Onlinedurchsuchung" kompromittieren wollte, ist es die Aufgabe der öffentlichen Stellen in Nordrhein-Westfalen, den Schutz unserer digitalen Infrastruktur und unserer gemeinsamen elektronischen Kommunikation sicherzustellen und zu verteidigen. Digitale Gefahrenabwehr bedeutet, dass das Land offen, transparent und zeitnah vor bekannten Gefahren waren muss.

Vorhaben aus Berlin oder Brüssel, Kommunikationsdienste unsicher zu gestalten und dort Hintertüren einzubauen, sind gefährlich. Neueste Vorschläge gehen sogar soweit, Hintertüren in kryptographischen Verfahren zu platzieren, um die Verschlüsselung insgesamt unbrauchbar zu machen.

Offene ‚Hintertüren' in Software können nicht nur von Strafverfolgungsbehörden etwa zur Durchführung einer Online-Durchsuchung genutzt werden, sondern auch von Kriminellen und fremden Staaten. Die in Rede stehenden Vorschläge dienen daher nicht der Sicherheit, sondern würden viele Unbeteiligte einer Gefahr aussetzen, die ohne diese Hintertüren nicht da wären. Wenn Kommunikationswege wie WhatsApp, Threema und andere künstlich unsicher gestaltet werden, dann schafft man eine Gefahr und leistet Beihilfe zum digitalen Einbruch.

## II. Der Landtag stellt fest

1. IT-Sicherheit ist ein gemeinsames Ziel der Öffentlichen Hand, der Bevölkerung und der Wirtschaft. Durch Austausch von Informationen über Sicherheitslücken wird die IT-Sicherheit gestärkt.

2. Wenn dem Land Informationen und Kenntnisse über Sicherheitslücken vorliegen, muss es darüber informieren, damit sich die Bevölkerung schützen kann.

3. Sichere Verschlüsselung ist in der heutigen Zeit der elektronischen Informationsübermittlung notwendige Grundlage für die Sicherstellung der grundgesetzlichen Rechte auf Brief- Post und Fernmeldegeheimnis sowie Achtung des Privatlebens und der Kommunikation.

4. Sichere Verschlüsselung ist mit Forderung nach Schlüsselhinterlegung, Generalschlüsseln oder Hintertüren (Backdoors) nicht vereinbar.

5. Das CERT des Landes hat die Aufgabe, Sicherheitslücken zu kommunizieren. Interessen von Sicherheitsbehörden an der Geheimhaltung von Sicherheitslücken dürfen nicht berücksichtigt werden.

## III. Der Landtag fordert die Landesregierung auf:

1. sich auf allen Ebenen und in allen Gremien für sichere elektronische Kommunikation einzusetzen, ohne Lücken oder Hintertüren.

2. noch in dieser Legislaturperiode für die öffentliche Hand in Nordrhein-Westfalen ein verbindliches Verfahren zu Veröffentlichung von Sicherheitslücken basierend auf den "Responsible disclosure"-Prinzipien einzuführen

Michele Marsching
Marc Olejak
Frank Herrmann

und Fraktion