Ministerium für Inneres und Kommunales
des Landes Nordrhein-Westfalen

Ministerium für Inneres und Kommunales NRW, 40190 Düsseldorf

Präsidentin des Landtags
Nordrhein-Westfalen
Platz des Landtags 1
40221 Düsseldorf

für die Mitglieder
des Innenausschusses

60-fach

21. November 2016

Aktenzeichen
(bei Antwort bitte angeben)
CIO - 03.02 - 3/16

Dr. Laicher
Telefon 0211 871-2635
Telefax 0211 871-
frank.laicher@mik.nrw.de

Sitzung des Innenausschusses am 27.10.2016
Antrag der Fraktion der PIRATEN Drs.16/13033 vom 27.09.2016
„Digitale Gefahrenabwehr - Sicherheitslücken entdecken und schließen“

Sehr geehrte Frau Landtagspräsidentin,

zur Information der Mitglieder des Innenausschusses des Landtags übersende ich 60 Exemplare des ergänzenden schriftlichen Berichtes zum TOP 12 „Digitale Gefahrenabwehr - Sicherheitslücken entdecken und schließen“ der Sitzung des Innenausschusses am 27.10.2016.

Mit freundlichen Grüßen

Ralf Jäger MdL

Dienstgebäude:
Friedrichstr. 62-80
40217 Düsseldorf

Lieferanschrift:
Fürstenwall 129
40217 Düsseldorf

Telefon 0211 871-01
Telefax 0211 871-3355
poststelle@mik.nrw.de
www.mik.nrw.de

Öffentliche Verkehrsmittel:
Rheinbahnlinien 732, 736, 835,
836, U71, U72, U73, U83
Haltestelle: Kirchplatz

Ergänzender Bericht der Landesregierung zur Sitzung des Innenausschusses vom 27.Oktober 2016

TOP12, Antrag der PIRATEN-Fraktion „Digitale Gefahrenabwehr - Sicherheitslücken entdecken und schließen“

Mit Berichtsersuchen der PIRATEN-Fraktion vom 27.Oktober 2016 zu dem Antrag "Digitale Gefahrenabwehr - Sicherheitslücken entdecken und schließen", Drucksache 16/13033 wurde mit E-Mail vom 23.11.2016 folgende Präzisierung übersandt:

„Da in der Plenardebatte gesagt wurde, der verantwortungsvolle Umgang mit Sicherheitslücken sei in NRW bereits ausreichend geregelt, bitten wir die Landesregierung um einen Bericht über die einzelnen, konkreten, aktuell bestehenden relevanten Dienstvorgaben und -vorschriften zu Umgang, Meldung und Veröffentlichung von Sicherheitslücken den Herstellern und der Öffentlichkeit gegenüber, insbesondere für die Bereiche der IT, der Polizei und der Universitäten des Landes.“

Hierzu nimmt der Minister für Inneres und Kommunales wie folgt Stellung:

Das Computer Emergency Response Team CERT NRW sammelt, bewertet und steuert auf Basis des CERT-Konzeptes seit 2005 alle Informationen zur Informationssicherheit und zu erkannten Sicherheitsvorfällen. Es besteht eine Meldepflicht aller Behörden und Einrichtungen des Landes gegenüber dem CERT NRW. Dazu gehört auch der Bereich der Polizei. Die Universitäten sind nicht verpflichtet, da es sich nicht um Behörden oder Einrichtungen des Landes, sondern um rechtlich selbständige Stellen handelt und diese auch nicht mit dem Landesverwaltungsnetz, sondern mit dem Wissenschaftsnetz verbunden sind. Das Wissenschaftsnetz sieht ein eigenes CERT (sog. DFN-CERT) vor.

In der Landesverwaltung werden alle erkannten Sicherheitslücken, bei Vorliegen von Patches oder sonstiger Empfehlungen von Herstellern, unverzüglich geschlossen. Liegen diese nicht vor, verfährt das CERT NRW nach einer Responsible Disclosure Policy. Diese wurde im Jahr 2013 schriftlich fixiert und im Landesverwaltungsnetz veröffentlicht.

Darin sind die Grundsätze, die Einstufung mittels Common Vulnerability Scoring System CVSS und Szenarien zur Kontaktaufnahme mit Herstellern festgelegt.

Abhängig vom Risikopotential, der Kooperationsbereitschaft des Herstellers und den Erkenntnissen zur bereits laufenden Ausnutzung der Schwachstelle werden darin Fristen festgelegt in denen dem Hersteller die Möglichkeit zur Beseitigung der Schwachstelle eingeräumt wird. Werden die definierten Rahmenbedingungen verletzt, erfolgt in Abwägung des allgemeinen Nutzens notfalls eine Veröffentlichung als Warnmeldung, auch wenn kein Lösungsangebot vorliegt. Sogn. „Exploitkits“ werden nicht veröffentlicht.