LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/5599**

15.04.2014

Kleine Anfrage 2215

der Abgeordneten Lukas Lamla, Marc Olejak, Daniel Schwerd und
Kai Schmalenbach PIRATEN

Heartbleed – Schwerste Sicherheitslücke in der Struktur der Landes-IT NRW?

Am 07.04.2014 wurde ein schwerer Fehler in der OpenSSL Verschlüsselungssoftware entdeckt. OpenSSL wird auch auf Systemen des Landes Nordrhein-Westfalen eingesetzt. Ein Programmierfehler erlaubt es jedem Kommunikationspartner, den Speicher der Gegenstelle auszulesen. Konkret bedeutet das: Ein Angreifer kann Schlüssel, Passwörter und andere geheime Daten entwenden. Das Bundesamt für Sicherheit in der Informationstechnik hat am 10.04.2014 im Warn- und Informationsdienst unter CB-K14/0406 den Fehler CVE-2014-0160 (Heartbleed) mit hohem Risiko bewertet.
https://www.cert-bund.de/advisoryshort/CB-K14-0406%20UPDATE%203

Aufgrund des dargestellten Sachverhalts fragen wir die Landesregierung:

1. Welche Systeme sowohl in Hardware als auch Software (aufgeschlüsselt nach Institution, Plattform, Version und Dienst, beispielsweise TLS/Mail, HTTPS, VPN etc.) des Landes Nordrhein-Westfalen und seiner Einrichtungen sind beziehungsweise waren von dem 'Heartbleed'-Fehler betroffen?

2. Wann kann mit einer Schließung dieser Sicherheitslücke bei den betroffenen Systemen gerechnet werden bzw. wann wurden sie geschlossen?

3. Welche Folgen hat diese Sicherheitslücke für die IT-Landschaft des Landes, wie beispielsweise die E-Mail-Infrastruktur?

4. Welche Folgen hat diese Sicherheitslücke für die Nutzer der Landes-IT, beispielsweise bzgl. der Erstellung neuer Passwörter nach sicheren Standards?

Lukas Lamla
Marc Olejak
Daniel Schwerd
Kai Schmalenbach

Datum des Originals: 15.04.2014/Ausgegeben: 15.04.2014