LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/5912**

20.05.2014

Antwort

der Landesregierung

auf die Kleine Anfrage 2215 vom 15. April 2014
der Abgeordneten Lukas Lamla, Marc Olejak, Daniel Schwerd
und Kai Schmalenbach PIRATEN
Drucksache 16/5599

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

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 2215 mit Schreiben vom 19. Mai 2015 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin und allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

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

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?

In der anliegenden Übersicht sind die betroffenen Server und Dienste der Landesverwaltung aufgeführt, die zum Stichtag 07.04.2014 (Bekanntwerden der Sicherheitslücke) in den Rechenzentren bzw. den Behörden und Einrichtungen unmittelbar aus dem Internet heraus erreichbar und aufgrund der Sicherheitslücke in dem weltweit verbreiteten Open-Source-

Datum des Originals: 19.05.2014/Ausgegeben: 23.05.2014

Produkt OpenSSL möglichen Angriffen ausgesetzt waren. Soweit bei Stellen außerhalb der Landesverwaltung Web-Anwendungen betrieben wurden, sind die jeweiligen Betreiber von den auftraggebenden Ressorts um die Beantwortung der Fragen gebeten worden; drei Antworten stehen derzeit noch aus. Gegebenenfalls betroffene Systeme externer Betreiber wirken sich nur auf die jeweilige Web-Anwendung aus; sie haben keinen Einfluss auf die Sicherheit innerhalb des Landesverwaltungsnetzes.

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

In der Regel konnte die Analyse und Behebung des Fehlers innerhalb von drei Tagen erfolgen; in einigen Fällen musste zunächst ein Update des Herstellers abgewartet werden. Bis Ende April war bei allen betroffenen Systemen der Landesverwaltung die Sicherheitslücke geschlossen.

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

Wie die Antworten zu den Fragen 1 und 2 belegen, hat die Landesregierung unverzüglich die notwendigen Maßnahmen zur Beseitigung der Sicherheitslücke in ihren Systemen getroffen. Da nicht ausgeschlossen werden kann, dass in der zurückliegenden Zeit, in der der Programmierfehler in den Herstellersystemen vorlag, Angriffe stattgefunden haben, wurden vorsorglich weitere Maßnahmen bei den betroffenen Systemen, wie beispielsweise Änderung von Zertifikaten und Benutzerkennungen (siehe auch Antwort auf Frage 4), eingeleitet und inzwischen größtenteils abgeschlossen. Unmittelbare Folgen für die Struktur der IT-Landschaft des Landes durch diesen Sicherheitsvorfall sind nicht erkennbar. Vielmehr hat nicht zuletzt die IT-Struktur der Landesverwaltung mit ihren zentralen Übergängen zum Internet eine schnelle Reaktion auf diese unvorhersehbaren Gefährdungen ermöglicht.

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

Die registrierten Nutzer von möglicherweise betroffenen Anwendungen der Landesverwaltung werden von den zuständigen Behörden und Einrichtungen des Landes vorsorglich aufgefordert, ihre Passwörter zu erneuern. Soweit Fehlerbehebungen noch nicht zur Verfügung stehen, werden die Dienste vorübergehend deaktiviert.

Anlage zur Antwort auf die Kleine Anfrage 2215

Die von dem "Heartbleed"-Fehler betroffenen Systeme der Landesverwaltung

Institution	Plattform	Version	Dienst
IT.NRW	imail 12.3 (Windows 2008 Server)	imail 12.3	TLS/Mail
IT.NRW	Mail Relay 2, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	TLS
IT.NRW	www.zentrales-schuldnerverzeichnis.de,	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.gis.nrw.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.geo-wss.nrw.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.gistest1.nrw.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.bildungsmonitoring.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.landesdatenbank.nrw.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.regionalstatistik.de, RHEL 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.handelsregister.de, RHEL	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	www.bscw.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.blb.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.lanuv.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.lzg.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.mgepa.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.msw.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.studienseminare.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
IT.NRW	bscw.wrrl.nrw.de, RHEL Vers. 6	Red Hat Enterprise Linux Server release 6.5 (Santiago)	https
diverse Kreispolizeibehörden	Ubuntu/LINUX Derivate		VPN/Firewall
LZPD	Miss Marple (Lizenzmanagement)	Fa. Amando Version 3.2.4	Da bei der Standalone Inventarisierung Apache als Web-Server zum Einsatz kommt, wird Open SSL verwendet.
LZPD	Schutz vor Schadprogrammen	McAfee ePolicy Orchestrator	
LZPD	Mobile Device Management	Apptec 360	Apache auf Ubuntu
Bezirksregierung Münster	LINUX		öffentlicher Internetdienst
LIA NRW	x86 / Ubuntu	12.04LTS	https
GIB NRW	x64 / Debian	6.0.6	https
HBZ NRW	4 Server Linux Intel Opensuse	12.3	https
HBZ NRW	ca. 20 VPN Clients	verschiedene	VPN