Ministerium der Justiz
des Landes Nordrhein-Westfalen
Der Minister

Ministerium der Justiz Nordrhein-Westfalen, 40190 Düsseldorf

Vorsitzenden des Rechtsausschusses
Herrn Dr. Werner Pfeil MdL
Platz des Landtages 1
40221 Düsseldorf

nachrichtlich:

Rechtsausschuss des Landtags
- Referat I 1 -
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

VORLAGE
17/1300

A14

05.11.2018

Aktenzeichen
1500 - IT. 90 /IT-Sicherheit-Sicherheitsvorfälle
bei Antwort bitte angeben

Bearbeiter: Herr Ausetz
Telefon: 0211 8792-559

24. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 07.11.2018
Öffentlicher Bericht der Landesregierung zum TOP „Sicherheitslücken bei NRW-Staatsanwaltschaften“

Anlage
1 Bericht

Sehr geehrter Herr Vorsitzender,

als Anlage übersende ich den öffentlichen Bericht der Landesregierung zu dem von Herrn Stefan Engstfeld MdL, Mitglied der Landtagsfraktion Bündnis 90/Die Grünen, mit Schreiben vom 16.10.2018 angemeldeten Tagesordnungspunkt

„Sicherheitslücken bei NRW-Staatsanwaltschaften“

zur Weiterleitung an die Mitglieder des Rechtsausschusses.

Mit freundlichen Grüßen

Peter Biesenbach

Dienstgebäude und
Lieferanschrift:
Martin-Luther-Platz 40
40212 Düsseldorf
Telefon: 0211 8792-0
Telefax: 0211 8792-456
poststelle@jm.nrw.de
www.justiz.nrw

Ministerium der Justiz des Landes Nordrhein-Westfalen

24. Sitzung des Rechtsausschusses
des Landtags Nordrhein-Westfalen
am 7. November 2018

Schriftlicher Bericht zu TOP

„Sicherheitslücken bei NRW-Staatsanwaltschaften“

I.

Sachverhalt

Die Landesverwaltung wurde durch den WDR mit Erkenntnissen konfrontiert, die auf eine mögliche Gefährdung der Informationssicherheit der Landesverwaltung hindeuteten. Es wurde angegeben, ein externer Sicherheitsfachmann habe Informationen erlangt, die in kürzester Zeit zum Kompromittieren von sensiblen IT-Systemen genutzt werden können.

Der Bericht bezog sich zwar nur auf die Staatsanwaltschaft Dortmund und die E-Mail-Konten der dort Beschäftigten. Tatsächlich jedoch sind alle E-Mail-Konten mit der Endung „nrw.de" in derselben Weise betroffen. Betroffen waren über die Systeme der Staatsanwaltschaft hinaus also alle entsprechenden Systeme im Landesverwaltungsnetz.

Der in der Presse bemängelte Sachverhalt stellte sich so dar, dass das automatische Antwortverhalten von E-Mailsystemen bei der Adressierung nicht existierender Adressen eine E-Mail an den Absender zurücklieferte, die interne Serverinformationen enthielt (sog. Auto-Responder-Nachricht). Nach der Behauptung der Presseberichterstattung soll mit Hilfe dieser Informationen ein Angriff auf die Server der Staatsanwaltschaft (einschließlich aller E-Mailkonten, s.o.) ohne weiteren Aufwand möglich sein.

Zudem ergebe sich aus den Informationen, dass die Software nicht auf dem aktuellsten Stand sei. Dadurch könnten Hacker die noch nicht durch regelmäßige Updates und Patche geschlossenen Sicherheitslücken identifizieren, was wiederum einen Angriff erleichtere.

II.

Bewertung

Das Computer Emergency Response Team CERT NRW hat die Vorwürfe gründlich analysiert und ist zu folgenden Ergebnissen gekommen:

Zunächst sei festzuhalten, dass sich der Inhalt der Auto-Responder-Nachricht im Einklang mit den empfohlenen einschlägigen Internetstandards für derartige Nachrichten befand.

Sodann sei festzustellen, dass eine reale Gefährdung nicht vorlag:

- Der automatisch zurückgemeldete Stand der Patchlevel repräsentiere nicht die Aktualität des Sicherheitszustandes, da entsprechende Hotfixes und vergleichbare Patches keine Anpassung dieser Kennzahl bewirken.
- Das vermeintliche Alter eines Patchlevels gebe den Stand der Funktionen der Software an. IT.NRW prüfe alle angebotenen Herstellerlieferungen auf Notwendigkeit und wendet diese nur an, wenn diese sinnvoll sind und benötigt werden.

- Weitergehende Schutzmaßnahmen, die zusätzlich eine Kompromittierung verhindern, hätten vom externen Sicherheitsfachmann nicht erkannt und demzufolge nicht bewertet werden können.
- Gründliche Analysen hätten keine Anhaltspunkte für eine tatsächliche Gefährdung auf Basis der übermittelten Systeminformationen bei den von der Landesverwaltung betriebenen Systemen erbracht.

Der WDR und der von ihm beauftragte IT-Fachmann haben daher auch nach Angaben des CERT NRW keinen Beleg dafür liefern können, dass ein Zugriff auf die Mails der Staatanwaltschaft tatsächlich möglich war.

Gleichwohl hat das CERT NRW das automatische Antwortverhalten neu bewertet. Allen Betreibern entsprechender Systeme im Landesverwaltungsnetz wurde eine Empfehlung zur weitergehenden Verringerung der möglichen Angriffsfläche erteilt, die dahin geht, die Servereinstellungen in der Weise zu ändern, dass nunmehr nur noch solche Informationen herausgegeben werden, die zweifelsfrei unproblematisch sind. Jedenfalls für die bei IT.NRW gehosteten Mailserver der Justiz wurde dies bereits umgesetzt.

III.
Konkrete Fragestellungen

Die aufgeworfenen konkreten Einzelfragen werden wie folgt beantwortet:

- *Was unternimmt die Landesregierung, um die gravierenden Sicherheitslücken zu beheben?*

  Wie dargestellt, handelte es sich bei dem Inhalt des Autoresponders bei fehlerhaft adressierten E-Mails an Inhaberinnen oder Inhaber von E-Mail-Konten bei IT.NRW (Justiz, Landesregierung, Landtag) nach Analysen des CERT NRW nicht um Angaben, die unmittelbar zu einer Gefährdung der E-Mail-Konten führen konnten. Es wären weitere vertiefte Kenntnisse der Infrastruktur der Mail-Server erforderlich, um unter Ausnutzung der offengelegten Daten die Konten hacken zu können. Das automatische Rückmeldeverhalten der von IT.NRW betriebenen Systeme wurde gleichwohl angepasst. Alle verantwortlichen Betreiber ähnlicher Systeme im Landesverwaltungsnetz wurden aufgefordert, dieses ebenfalls vorzunehmen.

- *Wie schnell können die Sicherheitslücken behoben werden?*

  Die vorgenannten Maßnahmen wurden unverzüglich nach Mitteilung der vermeintlichen Schwachstelle durch den WDR getroffen.

- *Welche finanziellen Mittel sind notwendig, um die entsprechenden Sicherheitslücken zu beheben?*

  Die Veränderung der Einstellungen der E-Mail-Server zur Änderung des Inhaltes der Auto-Responder durch Mitarbeiter von IT.NRW im laufenden Betreuungsbetrieb ist erledigt, so dass lediglich die laufenden Personalkosten für diesen Einsatz anfielen. Es bedurfte weder externer Hilfe, noch der Anschaffung neuer Hard- oder Software, weshalb die Kosten für die Maßnahme nicht beziffert werden können.

- *Kann sichergegangen werden, dass die Server bislang nicht gehackt worden sind?*

  Nach aktuellem Kenntnisstand des CERT NRW gibt es keine Anhaltspunkte dafür, dass IT-Systeme der Landesverwaltung kompromittiert sind.

- *Welche Folgen können durch bislang eventuell erfolgte Hacks entstehen?*

  siehe Antwort Frage 4)