LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/8457**

14.01.2020

Kleine Anfrage 3306

des Abgeordneten Sven W. Tritschler AfD

Kritische Sicherheitslücke in der Fernzugriffs-Software der Firma Citrix – Sind auch Einrichtungen des Landes in Nordrhein-Westfalen betroffen?

Seit Montag, den 13. Januar 2020 wird bundesweit verstärkt von einer eklatanten Sicherheitslücke bei einer Serversoftware der Firma Citrix berichtet. Von dieser Sicherheitslücke sollen laut Medienberichten[1] u.a. der Sächsische Landtag, die CSU-Landtagsfraktion, Behörden in Hessen, das Bundeseisenbahnvermögen (BEV) sowie zahlreiche Krankenhäuser, Kommunen Kraftwerksbetreiber und Stadtwerke betroffen sein. EU-weit betroffen sind z.B. das europäische Patentbüro, die europäische Arzneimittelagentur (EMA) und die europäische Polizeiakademie.

Die Sicherheitslücke war seit dem 17. Dezember 2019 bekannt und veröffentlicht. Seit wenigen Tagen wird diese jedoch durch verschiedene Exploits[2] im großen Maßstab ausgenutzt, so sind u.a. auch schon sogenannte Cryptominer[3] in betroffenen Systemen entdeckt worden.

Die Firma Citrix will erst Ende Januar ein Update zur Schließung dieser Sicherheitslücke veröffentlichen[4] und bietet vorerst nur eine Anleitung zur Änderung der Serverkonfiguration an[5]. Bis dahin, so der Rat der Experten, hilft nur abschalten und das System neu aufsetzen, da die Wahrscheinlichkeit hoch wäre, dass das System kompromittiert ist.

Ich frage daher die Landesregierung:

1. Welche Einrichtungen des Landes nutzen die von der Sicherheitslücke betroffenen Produkte der Firma Citrix?

[1] https://www.golem.de/news/shitrix-das-citrix-desaster-2001-146047.html
[2] https://github.com/projectzeroindia/CVE-2019-19781
[3] https://www.datenschutzbeauftragter-info.de/crypto-miner-wachsende-gefahr-im-hintergrund/
[4] https://www.citrix.com/blogs/2020/01/11/citrix-provides-update-on-citrix-adc-citrix-gateway-vulnerability/
[5] https://support.citrix.com/article/CTX267679

Datum des Originals: 14.01.2020/Ausgegeben: 16.01.2020

2. Wann wurde der Landesregierung erstmals die Sicherheitslücke in der Citrix Serversoftware bekannt?

3. Welche Maßnahmen wurden zur Weiterverbreitung dieser IT-sicherheitsrelevanten Informationen getroffen?

4. Wie wurde sichergestellt, dass diese sicherheitsrelevanten Informationen bei den potentiell betroffenen kommunalen Einrichtungen und kommunalen Versorgern angekommen sind und ebenso auch die Verantwortlichen entsprechende Schritte eingeleitet haben?

5. Hat die Landesregierung einen genauen Überblick über die in den Landeseinrichtungen und Landesbehörden sowie in den Kommunalen Verwaltungen verwendete Serversoftware?

Sven W. Tritschler