Ministerium der Justiz
des Landes Nordrhein-Westfalen
Der Minister

Ministerium der Justiz Nordrhein-Westfalen, 40190 Düsseldorf

Präsident des Landtags
Nordrhein-Westfalen
Herrn André Kuper MdL
40221 Düsseldorf

für die Mitglieder
des Rechtsausschusses

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

VORLAGE
17/3869

A14

21. September 2020

Aktenzeichen
4059 E - III. 23/20
bei Antwort bitte angeben

Bearbeiter: Herr Landskrone
Telefon: 0211 8792-296

63. Sitzung des Rechtsausschusses des Landtags Nordrhein-Westfalen am 23.09.2020
TOP „Stand des Ermittlungsverfahrens zum Cyberangriff auf die Uniklinik Düsseldorf"

Anlage
1 Bericht

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Rechtsausschusses übersende ich als Anlage einen weiteren öffentlichen Bericht zu dem o. g. Tagesordnungspunkt.

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

63. Sitzung des Rechtsausschusses
des Landtags Nordrhein-Westfalen
am 23.09.2020

Schriftlicher Bericht zu dem TOP:

„Stand des Ermittlungsverfahrens zum
Cyberangriff auf die Uniklinik Düsseldorf“

Mit dem vorliegenden Bericht der Landesregierung erfolgt eine ergänzende Unterrichtung zu dem vorbezeichneten Tagesordnungspunkt.

Der Leitende Oberstaatsanwalt in Köln hat in einem am Nachmittag des 17.09.2020 bei dem Ministerium der Justiz eingegangenen Bericht u. a. Folgendes mitgeteilt:

> *„Die fortgeführten Ermittlungen haben weitere Erkenntnisse zu der Begehungsweise der Tat ergeben. So konnte festgestellt werden, dass für den Angriff auf das Universitätsklinikum Düsseldorf eine Sicherheitslücke [...] zur Infiltration des Serversystems ausgenutzt wurde. Bei der vorgenannten Anwendung handelt es sich um eine marktübliche und weltweit verbreitete kommerzielle Software, die hauptsächlich dazu verwendet wird, externen Benutzern einen Fernzugang zu einer internen IT-Infrastruktur zu gewährleisten. Auf diese Weise konnten die Täter durch einen sogenannten ‚Loader', eine Malware zum Nachladen der eigentlichen Schadsoftware, einen Verschlüsselungstrojaner mit der Bezeichnung ‚DoppelPaymer' in das System des Klinikums einbringen. Dieser Verschlüsselungstrojaner wurde bereits in zahlreichen weiteren Fällen weltweit zum Nachteil von Unternehmen und Institutionen durch eine Hackergruppierung eingesetzt, die - nach Einschätzung privater Sicherheitsunternehmen - in der russischen Föderation beheimatet sein soll*. Die weiteren Ermittlungen beziehen sich daher auch auf die Hypothese, dass der Angriff auf das Universitätsklinikum Teil einer weltweiten kommerziellen Malware-Kampagne sein könnte."*

Der Generalstaatsanwalt in Köln hat am 18.09.2020 berichtet, er habe gegen die staatsanwaltschaftliche Sachbehandlung keine Bedenken.

---

* *Vgl. https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.*