LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/11693**

05.11.2020

Antwort

der Landesregierung

auf die Kleine Anfrage 4528 vom 7. Oktober 2020
der Abgeordneten Alexander Langguth und Marcus Pretzell FRAKTIONSLOS
Drucksache 17/11421

Auf neuem Höchststand: Hacker-Angriffe auf Krankenhäuser und Kritische Infrastrukturen

Vorbemerkung der Kleinen Anfrage

Bedingt durch einen IT-Ausfall bei dem Universitätsklinikum Düsseldorf (UKD) musste in der Nacht vom 11. September auf den 12. September 2020 eine lebensbedrohlich erkrankte Patientin an ein weiter entferntes Krankenhaus in Wuppertal verwiesen werden. Aufgrund dessen habe sich die ärztliche Behandlung der Frau um etwa eine Stunde verzögert. Sie starb am selben Tag.[1] Nach Vorlage der Akten von der Staatsanwaltschaft Wuppertal erfolge die Prüfung der Übernahme des Todesermittlungsverfahrens und „Ausweitung des hiesigen Verfahrens auf den Vorwurf der fahrlässigen Tötung“[2].

Laut des Leitenden Oberstaatsanwalts in Köln bestand eine Sicherheitslücke in einer Software des UKD[3], welche am 27. Januar durch einen Patch des Herstellers Citrix geschlossen worden sei.[4] Offenbar hätten unbekannte Hacker es jedoch geschafft, das verwendete Klinik-Interface „Citrix NetScaler Gateway“ bereits vor dem Zeitpunkt des Updates mit einem Schadprogramm zu infiltrieren.[5]

Bei dem verwendeten Produkt „Citrix NetScaler Gateway“ handele es sich um eine „marktübliche und weltweit verbreitete kommerzielle Software“[6], die dazu diene, externen Benutzern einen Fernzugriff auf interne IT-Infrastrukturen zu ermöglichen. Die unbekannten Hacker hätten es geschafft, durch einen sogenannten „Loader“ (Malware) einen Verschlüsselungstrojaner mit der Bezeichnung „DoppelPaymer“ in das Klinik-System

[1] Vgl. https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3855.pdf (abgerufen am 30.09.2020)

[2] ebd.
[3] Vgl. https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3869.pdf (abgerufen am 30.09.2020)
[4] Vgl. https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3934.pdf (abgerufen am 30.09.2020)
[5] Vgl. https://rp-online.de/nrw/staedte/duesseldorf/hackerangriff-duesseldorf-uniklinik-wurde-wohl-schon-im-januar-gehackt_aid-53637045 (abgerufen am 30.09.2020)
[6] https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3869.pdf (abgerufen am 30.09.2020)

Datum des Originals: 05.11.2020/Ausgegeben: 11.11.2020

einzuspeisen. Ebenjener Trojaner sei bereits in zahlreichen Fällen weltweit gegen Unternehmen und Institutionen von einer Hacker-Gruppe eingesetzt worden. Nach Einschätzung privater Sicherheitsunternehmen sei diese Gruppe in der russischen Föderation beheimatet. Folglich würden sich die Ermittlungen auf die Annahme stützen, der Angriff auf das UKD könne Teil einer „weltweiten kommerziellen Malware-Kampagne“ sein.[7]

Auf „heise online“ heißt es über die Cybercrime-Gruppe hinter „DoppelPaymer“:
Sie setze „sehr ausgefeilte Techniken ein, um sich in den Netzen auszubreiten und dabei unbemerkt zu bleiben, bis sie tatsächlich Daten verschlüsseln“[8]. Ihre Lösegeldforderungen würden sich nach dem „Wert“ des jeweiligen Angriffsziels richten und könnten Millionenhöhe erreichen. Im März soll die „DoppelPaymer“-Gruppe eine sogenannte „Corona-Pause“ für Krankenhäuser versprochen haben – woran sie sich ausweislich des Cyber-Angriffs auf das UKD letztlich nicht gehalten hat.[9]

Der Nachrichtenseite „Business Insider“ zufolge hätten Hacker überdies bereits im Juli mehrere Kliniken in Rheinland-Pfalz und dem Saarland attackiert, um auf diese Weise Geld zu erpressen. Der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) habe den NRW-Gesundheitsminister Anfang Oktober 2019 in einem Brief vor der gestiegenen Bedrohungslage gewarnt und ferner auf den Nachholbedarf beim Schutz der Krankenhaus-IT hingewiesen.[10] In der Vorlage 17/3940 des Ministeriums für Arbeit, Gesundheit und Soziales räumt der Gesundheitsminister ein:

„Bedauerlicherweise musste bei der Überprüfung des Vorgangs erkannt werden, dass dem Präsidenten des BSI nicht geantwortet wurde.“[11] Dies werde nun angeblich „zeitnah nachgeholt“[12].

Über die durch die Zentral- und Ansprechstelle Cybercrime (ZAC NRW) geführten Ermittlungen wurde im Bericht des Justizministeriums wie folgt berichtet:

„Die ZAC NRW führt ein Ermittlungsverfahren gegen Unbekannt wegen des Verdachts der Erpressung und anderer Delikte zum Nachteil des Universitätsklinikums Düsseldorf.“[13]

Die Verschlüsselung von 30 Servern des Klinikums durch die Hacker habe dazu geführt, dass Notfallpatienten nicht aufgenommen und versorgt werden konnten. Zusätzlich sei ein Erpresserschreiben aufgefunden worden, adressiert an die Heinrich-Heine-Universität, an welche das UKD angegliedert ist. In diesem Schreiben hätten die unbekannten Täter zur Kontaktaufnahme aufgefordert, jedoch keine Geldsumme als Gegenleistung für die Entschlüsselung der Daten verlangt. Nach der Kontaktaufnahme durch das Polizeipräsidium Düsseldorf, welches die Täter darüber informierte, dass durch den Hacker-Angriff eine erhebliche Patientengefährdung gegeben sei, händigten diese einen Schlüssel zur

[7] https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3869.pdf (abgerufen am 30.09.2020)
[8] https://www.heise.de/news/Uniklinik-Duesseldorf-Ransomware-DoppelPaymer-soll-hinter-dem-Angriff-stecken-4908608.html (abgerufen am 30.09.2020)
[9] ebd.
[10] Vgl. https://www.businessinsider.de/politik/deutschland/hackerangriff-uniklinik-duesseldorf-nrw-minister-laumann-wurde-schon-vor-einem-jahr-vor-sicherheitsproblemen-in-landes-krankenhaeusern-gewarnt-doch-er-reagierte-darauf-nicht/ (abgerufen am 30.09.2020)
[11] https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3940.pdf (abgerufen am 30.09.2020)
[12] ebd.
[13] https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMV17-3855.pdf (abgerufen am 30.09.2020)

Datenwiederherstellung aus. Laut des Leitenden Oberstaatsanwalts in Köln nähre dies „die Hypothese, dass das Universitätsklinikum Düsseldorf zufällig betroffen wurde und der Angriff eigentlich der Heinrich-Heine-Universität galt“[14]. Eine vollständige Wiederherstellung der Daten werde nach Auskunft des UKD mehrere Wochen beanspruchen.

Die Notfallambulanz habe den regulären Betrieb seit dem 23. September 2020 wieder aufnehmen können und die digitale Wiederanbindung für den internen Betrieb sei „umfangreich angelaufen“[15].

Laut einer Statistik der US-amerikanischen Temple University liege die Zahl der Hacker-Angriffe mit Erpresser-Software dieses Jahr auf dem Höchststand seit 2013. Hierbei würden jedoch nur die öffentlich bekannten Hacker-Angriffe erfasst. Es sei von einer hohen Dunkelziffer auszugehen, bei der Unternehmen auf die Forderungen der Erpresser eingehen.[16]

Der Minister des Innern hat die Kleine Anfrage 4528 mit Schreiben vom 5. November 2020 namens der Landesregierung im Einvernehmen mit dem Minister für Wirtschaft, Innovation, Digitalisierung und Energie, dem Minister für Arbeit, Gesundheit und Soziales, dem Minister der Justiz und der Ministerin für Kultur und Wissenschaft beantwortet.

1. Welche Ziele werden nach aktuellem Wissensstand der Landesregierung bzw. laut Selbstauskunft der Täter durch die Angriffe auf Objekte der Kritischen Infrastruktur in Nordrhein-Westfalen verfolgt?

Der Landesregierung liegen diesbezüglich keine Erkenntnisse aus statistischen Erhebungen vor. Täter der Cybercrime verschleiern zumeist ihre Identität. Dies erschwert erheblich die Aufklärung solcher Taten. Insoweit liegen zu den Motiven der Täter keine allgemeingültigen Erkenntnisse vor. Die bislang ermittelten Motive sind im Übrigen vielfältig. Diese reichen von schlichtem Spaß an der Überwindung von IT-Zugangssperren über Erpressung bis hin zur Spionage und Sabotage.

2. Durch welche Erkenntnisse wird die These gestützt, bei der sogenannten „DoppelPaymer“-Gruppe handele es sich um ein in der russischen Föderation beheimatetes bzw. von dort aus agierendes Kollektiv?

In dem Verfahren der Staatsanwaltschaft Köln – ZAC NRW – dauern die Ermittlungen an. Eine Zuordnung dieser Tat oder einzelner Tatbeiträge zu einzelnen Organisationen oder Staaten ist derzeit nach Maßstäben der Strafprozessordnung nicht belastbar zu treffen.

[14] ebd.
[15] ebd.
[16] Vgl. https://rp-online.de/nrw/staedte/duesseldorf/hackerangriff-duesseldorf-uniklinik-wurde-wohl-schon-im-januar-gehackt_aid-53637045 (abgerufen am 02.10.2020)

3. Laut Medienberichten sei im Namen der „DoppelPaymer“ Gruppe im März verkündet worden, dass Krankenhäuser vorerst von Hacker-Angriffen verschont bleiben würden („Corona-Pause“). Welche Erkenntnisse liegen der Landesregierung hinsichtlich der Gründe vor, weshalb Akteure, die der „DoppelPaymer“-Gruppe zugerechnet werden, dennoch die IT-Systeme von Krankenhäusern angriffen?

Viele Straftäter setzen Schadsoftware ungezielt ein, um eine möglichst große Anzahl von Computersystemen zu infizieren. Diese oft wahllose Verbreitung betrifft insoweit auch den Gesundheitssektor. Schadsoftware dient sehr oft der Verschlüsselung von Daten der angegriffenen Computersysteme und ist in der Folge damit verbunden, dass „Lösegeld“ gezahlt werden soll, um das System wieder zu entschlüsseln.

Bezogen auf die konkrete Nachfrage hat das Landeskriminalamt bei Recherchen in öffentlich zugänglichen Internetquellen Hinweise darauf gefunden, dass die genannte Gruppe versuche, Angriffe auf IT-Systeme von Organisationen und Einrichtungen des Gesundheitssektors zu vermeiden. Zudem wolle sie die Entschlüsselung entsprechender Systeme ohne die Zahlung eines Lösungsgeldes gewährleisten.

4. In wie vielen Fällen kam es in Nordrhein-Westfalen in den letzten fünf Jahren zu Cyber-Angriffen auf Objekte der Kritischen Infrastruktur (KRITIS), welche eine Beeinträchtigung oder Verhinderung des Betriebs dieser Objekte, die Verzögerung medizinischer Behandlung, intensivmedizinische Betreuung, gravierende Folgeschäden oder den Tod von Patienten zur Folge hatten? Bitte mit angeben: Art des KRITIS-Objekts, die jeweils eingesetzte Schad-Software sowie – sofern bekannt – die jeweiligen Forderungen bzw. Motive der (mutmaßlichen) Täter.

Nach Auskunft der fünf Bezirksregierungen gab es in den letzten fünf Jahren, abgesehen von dem Hacker-Angriff im September 2020 auf das Universitätsklinikum Düsseldorf, keine Fälle von Cyber-Angriffen auf Krankenhäuser die nach ihrem Versorgungsvolumen der KRITIS zuzurechnen sind, die eine Beeinträchtigung oder Verhinderung des Betriebs, die Verzögerung medizinischer Behandlung, intensivmedizinische Betreuung, gravierende Folgeschäden oder den Tod von Patienten zur Folge hatten.

Der Landesregierung sind darüber hinaus Cyber-Angriffe auf Unternehmen und Behörden des Gesundheitssektors, wie Krankenhäuser und Arztpraxen bekannt. Beispiel dafür ist der Hackerangriff auf das Lukaskrankenhaus in Neuss im Jahr 2016. Eine spezifische Statistik wird durch die Landesregierung nicht geführt. Für eine vollständige Erhebung hätte es der manuellen Auswertung sämtlicher Ermittlungsverfahren der Cybercrime bedurft. Dies ist in der zur Beantwortung einer Kleinen Anfrage zur Verfügung stehenden Zeit nicht möglich.

5. Welche weiteren Fälle von medizinischen Komplikationen, die mit den IT-Beeinträchtigungen des UKD bis zum 23. September 2020 in Verbindung stehen, sind der Landesregierung bekannt geworden bzw. gibt es Bemühungen, dahingehend Ermittlungen in die Wege zu leiten?

Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz unter dem 16.10.2020 Folgendes berichtet:

„Gegenstand des von der ZAC NRW geführten Ermittlungsverfahrens ist der Vorwurf der fahrlässigen Tötung zum Nachteil einer weiblichen Patientin. Weitere Fälle von medizinischen Komplikationen, die zur Erweiterung des Ermittlungsverfahrens Anlass gegeben hätten, sind nicht bekannt geworden.“