LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/876**

09.09.2022

Antwort

der Landesregierung

auf die Kleine Anfrage 315 vom 10. August 2022
des Abgeordneten Sven W. Tritschler AfD
Drucksache 18/485

Bereits seit Mittwochabend, dem 3. August findet eine massive Cyberattacke auf die Industrie- und Handelskammern (IHK) in Deutschland statt. – Weder Mitarbeiter noch Kunden können digital Kontakt aufnehmen.

Vorbemerkung der Kleinen Anfrage

Wie Medien am 04. August vermeldeten[1], wurde höchstwahrscheinlich die IT der Industrie- und Handelskammern (IHK) in Deutschland massiv von einer Cyberattacke bedroht. Der in Dortmund beheimatete zentrale IT-Dienstleister, die IHK Gesellschaft für Informationsverarbeitung (GfI), fuhr laut eigenen Angaben „zur Sicherheit“ die Computersysteme bei allen 79 IHK-Kammern herunter. Der Angriff scheint jedoch so schwerwiegend zu sein, dass bis einschließlich 08. August die meisten Webseiten der IHK-Kammern nicht erreichbar waren.

Nicht nur Angestellte, sondern auch IHK-Mitglieder und -Kunden sowie Auszubildende und Ausbildungsbetriebe sind deutschlandweit von dem Shutdown betroffen.

Eine einheitliches Vorgehen der GfI ist nicht erkennbar, denn online verfügbar sind beispielsweise in NRW die Website der Ausfuhranmeldung der IHK Bonn/Rhein-Sieg und deren Folgewebseiten[2], jedoch nicht die Außenwirtschaftswebseite der IHK Düsseldorf[3].

Der o.g. Vorfall gibt Anlass zu der Frage, ob die bereits vorhandene Infrastruktur zur Bekämpfung von Cyberangriffen in NRW und der Bundesrepublik Deutschland auch auf die 2022 vermehrt gestiegenen Hackerangriffe auf Unternehmen, Verwaltungen und Infrastruktur ausreichend sind oder ggf. erforderliche Anpassungen vorzunehmen sind.

Der Minister des Innern hat die Kleine Anfrage 315 mit Schreiben vom 9. September 2022 namens der Landesregierung im Einvernehmen mit der Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie, der Ministerin für Heimat, Kommunales, Bau und Digitalisierung sowie dem Minister der Justiz beantwortet.

[1] https://www1.wdr.de/nachrichten/ruhrgebiet/ihk-hackerangriff-dortmund-102.html
[2] https://www.ihk-bonn.de/international
[3] https://www.ihk.de/duesseldorf/aussenwirtschaft/

Datum des Originals: 09.09.2022/Ausgegeben: 15.09.2022

1. Wann wurde der Landesregierung erstmals der aktuelle Angriff auf die IHK bekannt?

Die Landesregierung hat am 04.08.2022 Kenntnis erlangt.

2. Welche Maßnahmen wurden seitens der Landesregierung und des CIO des Landes getroffen?

Zu der im Wirtschafts-Service-Portal.NRW (WSP.NRW) medienbruchfrei angeschlossenen Verwaltungsleistung „Versicherungsberater*in - Erlaubnis (gem. § 34d GewO)“ wurde ein Hinweis hinterlegt, dass die Onlineanträge aufgrund einer Cyberattacke derzeit nicht zugestellt werden. Weitergehende Maßnahmen waren nicht erforderlich, da das WSP.NRW systemisch nicht unmittelbar hiervon betroffen ist.

Dem Beauftragten der Landesregierung für Informationstechnik CIO ist keine Zuständigkeit für den benannten Sachverhalt zugeordnet, da die Industrie- und Handelskammer (IHK) kein Teilnehmer des Landesverwaltungsnetzes ist.

Die Kreispolizeibehörde Dortmund hat die Ermittlungen aufgenommen.

3. Wie und auf welchen Ebenen erfolgt die Zusammenarbeit des Landes mit dem in Dortmund beheimateten IT-Dienstleister sowie den Behörden des Bundes und den zuständigen Stellen der anderen Bundesländer?

Der Leitende Oberstaatsanwalt in Köln, bei dem die ermittlungsführende Zentral- und Ansprechstelle Cybercrime (ZAC NRW) angesiedelt ist, hat dem Ministerium der Justiz bzw. dem Generalstaatsanwalt in Köln berichtet, dass eine Zusammenarbeit der ZAC NRW mit der IHK Gesellschaft für Informationsverarbeitung mbH (IHK GfI) ausschließlich im Rahmen der Ermittlungen erfolge und in dem Ermittlungsverfahren eine Zusammenarbeit mit Bundesbehörden und den zuständigen Stellen der anderen Bundesländer auf der polizeilichen Ebene praktiziert werde.

Im Rahmen des WSP.NRW als zentrales digitales Zugangstor für die Wirtschaft in Nordrhein-Westfalen (NRW) wurden Online-Dienste, die im Vollzug der Industrie- und Handelskammern (IHK) liegen, gemeinsam mit Vertreterinnen und Vertretern der IHK NRW entwickelt. Diese werden über das WSP.NRW als Online-Dienst bereitgestellt. Antragsdaten für Kammerleistungen werden medienbruchfrei an die Kammern geliefert. Konkret bedeutet dies, dass diese an die IHK Gesellschaft für Informationsverarbeitung (GfI) als technischen Dienstleister für die IHKn in NRW weitergeleitet werden. Aktuell werden Antragsdaten auf einem Server im WSP.NRW zwischengespeichert, bis sie durch die zuständige IHK entgegengenommen werden können.

4. Welche Erkenntnisse über die Art und die Urheber des Cyberangriffs hat die Landesregierung bereits?

Der Leitende Oberstaatsanwalt in Köln hat dem Ministerium der Justiz mitgeteilt, dass sich die unbekannten Täter auf bislang ungeklärte Art und Weise Zugang zu den IT-Systemen der Geschädigten verschafft hätten. Die Ermittlungen zum genauen Tathergang, seiner Reichweite und den Tatmotiven dauern an.

5. Sieht die Landesregierung einen Zusammenhang zwischen den vermehrten Angriffen auf hiesige Unternehmen und Verwaltungen seit den letzten Monaten bzw. dem Krieg in der Ukraine bzw. der beobachteten verstärkten Tätigkeit russischer Hackerkollektive?

Im Kontext des Angriffskriegs Russlands gegen die Ukraine haben verschiedene pro-ukrainische und pro-russische „Hacktivisten“ zu Cyberangriffen aufgerufen. In vielen Fällen werden die Cyberangriffe mittels Überlastungsangriffen auf Web-Seiten, sogenannte DDoS-Attacken, durchgeführt. Die Angriffe führen oft dazu, dass die Web-Seiten der Opfer vorübergehend nicht mehr erreichbar sind. Darüberhinausgehende Schäden treten in der Regel aber nicht auf. Insbesondere Ende April und im Mai 2022 konnten in Deutschland vermehrt DDoS-Attacken auf verschiedene Unternehmen und Behörden beobachtet werden. Den Angriffen vorausgegangen waren Aufrufe der pro-russischen Cyber-Aktivisten „KILLNET“, die ihre Angriffsziele offen auf einem Telegram-Kanal kommunizierten. Aufgrund der verteilten Angriffsstruktur und verschiedener Verschleierungstechniken sind die Urheber der DDoS-Angriffe nur schwer zu ermitteln. Ein Zusammenhang mit dem Ukraine-Konflikt erscheint im Fall von „KILLNET“ aber offensichtlich.

Der nordrhein-westfälische Verfassungsschutz stellt darüber hinaus eine erhöhte Bedrohungslage bezogen auf staatlich gesteuerte Cyberangriffe infolge des Angriffskriegs Russlands gegen die Ukraine fest. Insbesondere bei einer Eskalation des Konfliktes oder als Reaktion auf Sanktionen besteht die Gefahr, dass Russland vermehrt Cyberangriffe in westlichen Staaten durchführt. Die Operationsziele der staatlichen Akteure können sowohl im Bereich der Sabotage, der Spionage aber auch im Bereich der Desinformation und Einflussnahme liegen.