LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/998**

21.09.2022

Antwort

der Landesregierung

auf die Kleine Anfrage 357 vom 28. August 2022
der Abgeordneten Marc Lürbke und Dr. Werner Pfeil FDP
Drucksache 18/658

Möglicher Cyberangriff auf die Industrie- und Handelskammern (IHK) – was unternimmt die Landesregierung?

Vorbemerkung der Kleinen Anfrage

Seit spätestens 2005 werden zielgerichtete Cyberangriffe gegen Behörden, Körperschaften des öffentlichen Rechts, Politik und Wirtschaftsunternehmen festgestellt. Diese finden auf hohem technischem Niveau statt und gefährden daher massiv die Informationssicherheit in diesen Bereichen. Für Unternehmen und die öffentliche Verwaltung können durch Hackerangriffe beispielsweise Schäden in Millionenhöhe, etwa durch die Entwendung geheimer Daten und den Verlust von Geschäftsgeheimnissen, die Infizierung von Hard- und Software, Betriebsausfälle und Imageverluste entstehen. Auch kann die öffentliche Sicherheit und Ordnung in Gefahr geraten. Problematisch ist stets, dass solche Angriffe oftmals nicht entdeckt werden und für eine technische Störung gehalten werden.

Die Industrie- und Handelskammern (IHK) haben seit Monaten vor Cyberangriffen auf Unternehmen auf ihren Internetseiten gewarnt. Nun sind sie möglicherweise selbst Opfer eines Cyberangriffes geworden.

In der Aachener Zeitung vom 08.08.2022 heißt es:

„Seit dem späten Mittwochabend geht bei der Industrie- und Handelskammer Aachen kaum noch etwas – jedenfalls was nahezu alle Formen des digitalen Arbeitens und Kommunizierens angeht. Die IHK ist offline, die Webseite nicht mehr aufrufbar.

Die Mitarbeiterinnen und Mitarbeiter der Kammer können ihre E-Mail-Accounts nicht mehr abrufen, sie sind auf elektronischem Wege nicht mehr erreichbar. Und auch das Telefonsystem ist massiv gestört. Allenfalls sporadisch seien vereinzelt Kollegen erreichbar, doch keiner wisse, wer und wann telefonieren könne, heißt es aus Mitarbeiterkreisen. Auch diverse interne Systeme seien zurzeit nicht nutzbar. Das Arbeiten im Hause sei aktuell sehr eingeschränkt.

Datum des Originals: 21.09.2022/Ausgegeben: 27.09.2022

Verursacht hat diese Probleme möglicherweise ein groß angelegter Cyberangriff, der nicht nur die IHK Aachen betrifft. Denn aktuellen Medienberichten zufolge sind derzeit landauf, landab etliche Industrie- und Handelskammern offline“.[1]

Der Deutsche Industrie- und Handelskammertag (DIHT), der Dachverband der 79 IHK in Deutschland, spricht auf seiner Webseite selbst von einer „möglichen Cyberattacke“. Die Gesellschaft für Informationsverarbeitung (GfI) mit Sitz in Dortmund ist für die Informationstechnologie der IHK in Deutschland und des Deutschen Industrie- und Handelskammertages zuständig. Aus Sicherheitsgründen hatte der IT-Dienstleister letzte Woche die Systeme heruntergefahren.

Auch über eine Woche nach dem möglichen Hackerangriff auf IT-Systeme der IHK in Deutschland stehen weiter wichtige Systeme nicht zur Verfügung. So ist zum Beispiel die IHK Ostwestfalen weiterhin nur per Telefon zu erreichen.

Der Minister des Innern hat die Kleine Anfrage 357 mit Schreiben vom 21. September 2022 namens der Landesregierung im Einvernehmen mit der Ministerin für Wirtschaft, Industrie, Klimaschutz und Energie und dem Minister der Justizbeantwortet.

1. Welche IHK in NRW waren von den Störungen in der Zeit vom 04.08.2022 – 15.08.2022 betroffen?

Der zentrale IT-Dienstleister aller 79 deutschen Industrie- und Handelskammern, die IHK Gesellschaft für Informationsverarbeitung mbH, hat zur Minimierung weiterer Schäden und Gefahren eine Trennung aller Industrie- und Handelskammern vom Internet vorgenommen, so dass auch alle in Nordrhein-Westfalen angesiedelten Industrie- und Handelskammern betroffen waren.

2. Welche Folgen hatte der mögliche Cyberangriff mit Blick auf den Zugang der Daten für Dritte oder den Verlust von Daten?

Der Leitende Oberstaatsanwalt in Köln, bei dem die ermittlungsführende Zentral- und Ansprechstelle Cybercrime (ZAC NRW) angesiedelt ist, hat dem Ministerium der Justiz am 02.09.2022 berichtet, dass das mögliche Abhandenkommen von Daten Gegenstand der laufenden Ermittlungen sei. Gegenwärtig lägen Erkenntnisse darüber, ob und ggf. in welchem Umfang Daten Dritten zugänglich geworden sind, noch nicht vor.

Hinsichtlich des nicht von diesem etwaigen Cyberangriff direkt betroffenen Wirtschafts-Service-Portal.NRW werden eingegangene Onlineanträge unter Beachtung geltender Datenschutzanforderungen gespeichert und können zu einem späteren Zeitpunkt an die zuständige Stelle der Industrie- und Handelskammer weitergeleitet werden. Die temporär fehlende Empfangsfähigkeit seitens der Industrie- und Handelskammern führt somit nicht zu einem Verlust von Daten der Antragsstellerinnen und Antragssteller.

[1] Aachener Zeitung: „Staatsanwaltschaft ermittelt wegen Cyberangriff auf IHK Aachen“, abrufbar unter https://www.aachener-zeitung.de/nrw-region/staatsanwaltschaft-ermittelt-wegen-cyberangriff-auf-ihk-aachen_aid-74599287 (abgerufen am 08.08.2022).

3. Welche Sofortmaßnahmen werden in solchen Fällen seitens der Landesregierung, insbesondere seitens des Innenministeriums des Landes Nordrhein-Westfalen, unternommen?

Der Single Point of Contact Cybercrime des Landeskriminalamts Nordrhein-Westfalen ist rund um die Uhr an allen Tagen der Woche für Betroffene von Cyberangriffen aus der Wirtschaft und der Industrie erreichbar. Wenn der Single Point of Contact kontaktiert wird, wird durch das Landeskriminalamt Nordrhein-Westfalen zunächst verifiziert, welche Art von Angriff vorliegt, in welchem Status sich der Angriff befindet und ob weitere Gefahrenüberhänge bestehen. Die verantwortlichen Personen des angegriffenen Unternehmens werden zudem auf alle einzuleitenden Sofortmaßnahmen und auf ergänzende präventive Maßnahmen hingewiesen. Zudem überführt das Landeskriminalamt Nordrhein-Westfalen den Vorfall in ein geordnetes Ermittlungsverfahren. Dazu wird der geschilderte Sachverhalt strafrechtlich eingeordnet und im Anschluss an die zuständige Kreispolizeibehörde übergeben. In der Regel werden von dort aus die Ermittlungen geführt und die weiteren Maßnahmen veranlasst. Im Rahmen besonders schwerwiegender Fälle setzt das Landeskriminalamt Nordrhein-Westfalen seine „Digitale Einsatzgruppe“ sowie sein „Mobiles Datensicherungs- und Analyselabor“ ein und übernimmt die Ermittlungsführung.

Im Falle von staatlich gelenkten oder gestützten Angriffen bietet auch die Cyberabwehr des Verfassungsschutzes begleitende Unterstützung etwaiger Sofortmaßnahmen an. Hierzu gehört zum Beispiel die Bereitstellung technischer Parameter zur Erkennung des Angriffs und zur Sensibilisierung weiterer möglicher Opfer.

Im Wirtschafts-Service-Portal.NRW wurde ein Hinweisbanner geschaltet.

4. Wie wird das Innenministerium den präventiven Schutz vor großangelegten Cyberangriffen im Vorfeld und die polizeiliche Aufklärung von landesweit erfolgten Cyberangriffen im Nachhinein zukünftig weiter ausbauen?

Das Ministerium des Innern setzt zahlreiche Maßnahmen zur Erhöhung der Cybersicherheit der Bürgerinnen und Bürger sowie von Unternehmen um.

Die Intensivierung der Zusammenarbeit und Kommunikation zwischen den Ressorts ist eine der Kernaufgaben der Koordinierungsstelle Cybersicherheit, die im Ministerium des Innern angesiedelt ist.

Zu diesem Zweck wurde der „Interministerielle Ausschuss Cybersicherheit“ eingerichtet, in dem sich alle Ministerien unter der Geschäftsführung der Koordinierungsstelle regelmäßig zu aktuellen Fragen der Cybersicherheit austauschen.

Außerdem wurden weitere Gremien, wie der „Operative und der Strategische Austausch Cybersicherheit“ initiiert. Diese ermöglichen eine tiefergehende Vernetzung innerhalb und außerhalb der Landesverwaltung und schaffen Synergieeffekte in der Zusammenarbeit der unterschiedlichen Ministerien. Ein Schwerpunkt ist zudem die Prävention. Im Ministerium des Innern und anderen Ministerien stehen Ansprechpersonen zur Verfügung, die Fragen von Unternehmen beantworten und Informationsveranstaltungen bei den Unternehmen organisieren.

Durch den Ausbau und die Weiterentwicklung der Website Cybersicherheit.NRW wird das Informationsangebot für Bürgerinnen und Bürger, aber auch für Unternehmen ausgeweitet und noch einfacher zugänglich gemacht.

Die Cybersicherheitsstrategie für das Land Nordrhein-Westfalen wird fortgeschrieben.

Die Kreispolizeibehörden sowie das Landeskriminalamt Nordrhein-Westfalen werden für die Aufnahme komplexer, digitaler Tatorte weitere personelle Verstärkung erhalten. Damit einhergehend werden die notwendigen Fortbildungen und die Ausstattung mit entsprechender Ermittlungssoftware weiter optimiert.

Zudem wird, basierend auf dem Studiengang „Cyber Security Management“ des Cyber Campus Nordrhein-Westfalen, bis zum Wintersemester 2023/2024 ein „Cyberkriminalistik“-Studiengang gemeinsam mit dem Cyber Campus Nordrhein-Westfalen entwickelt. Schon ab dem Wintersemester 2022/2023 werden Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte akademisch für Ermittlungen im digitalen Raum zusätzlich qualifiziert und können ihr neuerworbenes Wissen unmittelbar in aktuelle Ermittlungsverfahren miteinbringen.

Im Falle von staatlich gelenkten oder gestützten Angriffen auf Unternehmen steht diesen neben der polizeilichen Organisation auch die Abteilung Verfassungsschutz des Ministeriums des Inneren mit den Arbeitsbereichen Wirtschaftsschutz und Cyberabwehr zur Verfügung. Der Wirtschaftsschutz berät Unternehmen bei der Erstellung von Sicherheits- und Notfallkonzepten, um weitere Angriffe zu erschweren. Die Cyberabwehr bietet Früherkennung und begleitende, technische Unterstützung bei der Abwehr staatlich gesteuerte Cyberangriffe an. Die Angebote der Abteilung Verfassungsschutz werden stetig aktualisiert und erweitert.

5. Wie viele (mögliche) großangelegte Cyberangriffe diesen Ausmaßes sind in den letzten zehn Jahren auf die Körperschaften des öffentlichen Rechts und auf die Behörden in Nordrhein-Westfalen erfolgt?

Datenquelle für die Beantwortung von Fragen zur Kriminalitätsentwicklung ist die Polizeiliche Kriminalstatistik. Sie wird nach bundeseinheitlich festgelegten Richtlinien erstellt. Die in der Polizeilichen Kriminalstatistik erfassten Taten aus dem Bereich Cybercrime lassen sich nicht bezüglich der Opfer auswerten. Das heißt, dass in der Statistik nicht zwischen angegriffenen Privatpersonen, Unternehmen oder sonstigen Institutionen differenziert werden kann. Damit ist eine Beantwortung auf Grundlage der Polizeilichen Kriminalstatistik nicht möglich.

Cyberangriffe auf Körperschaften des öffentlichen Rechts und auf Behörden in Nordrhein-Westfalen werden im Ministerium der Justiz und seinem staatsanwaltschaftlichen Geschäftsbereich statistisch nicht gesondert erfasst, so dass hierzu keine statistikbasierten Aussagen getroffen werden können.

Eine entsprechende Einzelauswertung der Verfahren ist mit vertretbarem Verwaltungsaufwand nicht zu leisten.