LANDTAG NORDRHEIN-WESTFALEN
17. Wahlperiode

Drucksache **17/17101**

04.05.2022

Antwort

der Landesregierung

auf die Kleine Anfrage 6543 vom 5. April 2022
des Abgeordneten Gordan Dudas SPD
Drucksache 17/17006

Haben Cyberangriffe auf Unternehmen keine Priorität für die Landeregierung?

Vorbemerkung der Kleinen Anfrage

Seit Jahren gibt es zunehmend Berichte über Cyberangriffe, gerade auch auf die Wirtschaft. Neben Wirtschaftsspionage wird dabei auch immer wieder über Erpressungsversuche berichtet, bei denen Unternehmen in Folge eines Cyberangriffs den Zugriff auf eigene Daten verlieren. Diese werden von den Erpressern verschlüsselt und sollen nach der Zahlung eines Lösegeldes in digitaler Währung angeblich wieder freigegeben werden. Solche kriminellen Machenschaften sind eine Bedrohung für die betroffenen Unternehmen. Neben dem Verlust von Daten drohen immer wieder auch Produktionsausfälle.

Vielfach wird davor gewarnt, auf den Erpressungsversuch einzugehen sondern stattdessen geraten, die Polizei einzuschalten. Denn mit der Zahlung ist das Problem meistens nicht behoben. Daher ist es gut, wenn betroffene Unternehmen sich umgehend an die zuständigen Stellen wenden. Zuletzt gab es jedoch einen Bericht über einen Vorfall bei einer Firma aus Südwestfalen, die laut Presseberichten zuerst einmal ergebnislos in den Austausch mit dem Landeskriminalamt getreten sei; die erhoffte Unterstützung sei ausgeblieben. Laut Berichterstattung habe sich fünf Tage nach der Meldung das LKA gemeldet und von einem Cyberangriff berichtet[1]. Für betroffene Unternehmen ist im Falle von derartigen Angriffen jedoch schnelle Hilfe dringend geboten.

Der Minister des Innern hat die Kleine Anfrage 6543 mit Schreiben vom 4. Mai 2022 namens der Landesregierung im Einvernehmen mit dem Minister für Wirtschaft, Innovation, Digitalisierung und Energie sowie dem Minister der Justiz beantwortet.

1. Wie bewertet die Landesregierung den genannten Vorfall?

2. Wie ist das übliche Verfahren seitens der zuständigen Behörden in Fällen von Cyberabgriffen auf Unternehmen?

[1] Vgl. https://www.come-on.de/lennetal/werdohl/cyberangriff-auf-werdohler-firma-kracht-91454845.html.

Datum des Originals: 04.05.2022/Ausgegeben: 10.05.2022

3. Wie eng werden Unternehmen in Fällen von Cyberangriffen durch die Strafverfolgungsbehörden begleitet?

Die Fragen 1, 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das Landeskriminalamt Nordrhein-Westfalen (LKA NRW) ist über den Single Point of Contact für Wirtschaft und Industrie des Landeskriminalamts Nordrhein-Westfalen (SPoC Cybercrime) durchgängig für Unternehmen aller Art in Nordrhein-Westfalen erreichbar, die von Cybercrime-Angriffen betroffen sind. Der SPoC Cybercrime prüft beim Erstkontakt mit dem jeweiligen Unternehmen, welche Art von Angriff vorliegt und ob weitere Gefahrenüberhänge bestehen. In diesem Gespräch erhalten die Verantwortlichen des angegriffenen Unternehmens zudem Hinweise zu möglichen präventiven Maßnahmen. Unmittelbar nach diesem Erstkontakt zur Abklärung der Sachlage wird die zuständige Kreispolizeibehörde (KPB) über den Angriff informiert, damit von dort die erforderlichen Ermittlungen und gefahrenabwehrenden Maßnahmen veranlasst werden können. Bei besonders schweren Fällen werden die Ermittlungen und Maßnahmen in der zuständigen KPB mittels einer besonderen Aufbauorganisation geführt. Handelt es sich um technisch hochversierte Täter oder sind besonders große Datenmengen zu sichern, entsendet das LKA NRW das Mobile Datensicherungs- und Analyselabor (MODAL). Sind kritische Infrastrukturen oder Menschenleben gefährdet, begleiten die Quick Reaction Force oder die Ermittlungskommissionen des LKA NRW den Einsatz oder übernehmen ihn vollständig. Im Jahr 2021 wurden durch den SPoC Cybercrime mehr als 2 000 Kontaktgespräche mit betroffenen Firmen geführt.

Im Falle von staatlich gelenkten oder staatlich beeinflussten Cyberangriffen auf Unternehmen steht den Unternehmen neben der Polizei auch der Verfassungsschutz mit den Arbeitsbereichen Wirtschaftsschutz und Cyberabwehr zur Verfügung. Der Wirtschaftsschutz berät im Schwerpunkt interessierte Unternehmen präventiv bei der Erstellung von Sicherheits- und Notfallkonzepten mit dem Ziel, Ausspäh- und Sabotageversuche im Sinne der Wirtschaftsspionage zu erschweren. Die Cyberabwehr bietet, neben Informationen zur Prävention von Cyberangriffen, technische Unterstützung insbesondere während und nach Ausspäh- oder Sabotageversuchen an.

Zudem gibt es bei der Koordinierungsstelle für Cybersicherheit etablierte Prozesse zum Umgang mit Warn- und Informationsmeldungen zu Cyberangriffen, die durch verschiedene Kanäle, wie zum Beispiel dem Computer Emergency Response Team Nordrhein-Westfalens oder dem Bundesamt für Sicherheit in der Informationstechnik, eingehen. Die Koordinierungsstelle steht dazu im kontinuierlichen Austausch mit den Strafverfolgungsbehörden. Nach Eingang werden die Meldungen innerhalb der Landesverwaltung koordiniert und gezielt an die zuständigen Ermittlungsbehörden und / oder Aufsichten weitergeben.

Die Justiz berichtet, dass in Fällen von Cyberangriffen auf Unternehmen die Vorgehensweise den jeweiligen – teils auch unvorhersehbaren – Gegebenheiten im Einzelfall obliegt. Mit Blick auf die Heterogenität angegriffener Infrastrukturen und die besondere Bedeutung des Verhältnismäßigkeitsgrundsatzes bei Ermittlungen in Unternehmensnetzen sowie die jeweils technischen Gegebenheiten der konkreten Kompromittierung sind sachgerechte Ermittlungen auf ein in hohem Maß individualisiertes Vorgehen angewiesen. Eine allgemeine Betreuung oder Beratung von Unternehmen ist mit den gesetzlichen Aufgaben einer Staatsanwaltschaft nicht vereinbar. Die verfahrensbezogene Kommunikation mit den Unternehmen erfolgt daher jeweils einzelfallbezogen. Im Zuge der Neustrukturierung der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) auf Grundlage der AV d. JM vom 15.03.2016 in der Fassung vom 17.12.2021 (4100 – III.274) besteht in der neu eingerichteten Abteilung eine Zuständigkeit für grundsätzliche, verfahrensunabhängige Fragestellungen aus dem Bereich

des Cybercrime im engeren und weiteren Sinne, im Rahmen derer regelmäßig auch generelle Fragestellungen im Kontext mit Cyberattacken auf Unternehmen zu thematisieren sind. Als Kontaktstelle zu Wissenschaft und Wirtschaft gemäß Abschnitt 4. 2 der vorbezeichneten Einrichtungs–AV stehen insoweit auch die Dezernentinnen und Dezernenten der ZAC NRW den (betroffenen) Unternehmen als Ansprechpartner zur Verfügung.

Zu dem in der Kleinen Anfrage erwähnten Einzelfall kann Folgendes ausgeführt werden:

Am 18.02.2022 meldete sich das geschädigte Unternehmen beim Bereitschaftsbeamten des SPoC Cybercrime des LKA NRW und informierte über einen Cyberangriff auf das Unternehmen.

Im Rahmen des vorliegenden Angriffs hat der Bereitschaftsbeamte des SPoC Cybercrime aufgrund der Struktur des angegriffenen Unternehmens (kein KRITIS), des dargestellten Schadensausmaßes, der bis zu diesem Zeitpunkt fehlenden Ransomnote (digitales Erpresserschreiben), der erfolgten Beauftragung eines Fachunternehmens, vorhandener unbeschädigter Backups sowie der zu diesem Zeitpunkt nicht vorhandenen Hinweise auf eine Tätergruppierung die Entscheidung getroffen, die Bearbeitung der örtlich zuständigen KPB Märkischer Kreis zuzuordnen. Dabei unterließ der Beamte allerdings eine sofortige Information der zuständigen KPB und verabredete mit der Kontaktperson des geschädigten Unternehmens, dass dieses selbstständig eine Anzeige bei der KPB Märkischer Kreis erstatte. Diese Anzeigenerstattung und damit die Aufnahme der ersten Ermittlungen durch die KPB Märkischer Kreis erfolgte hierdurch verzögert erst am 22.02.2022. Da sich im Rahmen der eingeleiteten Ermittlungen aufgrund der Tatbegehung herausstellte, dass die Täter über ein hohes Maß an IT-Fachwissen verfügten, wurden die Ermittlungen am 01.03.2022 an die zuständige Kriminalhauptstelle Hagen abgegeben.

Die Bearbeitung des Vorfalls durch das LKA NRW ist in Teilen als nicht sachgerecht anzusehen. Nach der Kontaktaufnahme des Unternehmens mit dem Bereitschaftsbeamten des SPoC Cybercrime hätte eine unverzügliche Informationssteuerung an die KPB Märkischer Kreis und die zuständige Kriminalhauptstelle Hagen erfolgen müssen, so wie es die geregelten Prozessabläufe des LKA NRW vorsehen. Das Vorgehen wurde durch das LKA NRW bereits intern aufgearbeitet und alle Bereitschaftsbeamten des SPoC Cybercrime wurden diesbezüglich erneut auf die geregelten Prozessabläufe hingewiesen, die durch eine detaillierte Prozessübersicht allen Angehörigen des SPoC Cybercrime verfügbar sind.

4. Ist die Personalausstattung bei den zuständigen Stellen zur Bearbeitung von Fällen der Cyberkriminalität auf Landesebene vor dem Hintergrund zunehmender Attacken auf Unternehmen noch ausreichend?

5. Welche Schritte wird die Landesregierung unternehmen, um die zuständigen Stellen beim Land ausreichend auszustatten?

Die Fragen 4 und 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Zur Bekämpfung der sowohl unter quantitativen als auch qualitativen Aspekten dynamisch wachsenden Cyberkriminalität wurden in den vergangenen Jahren bedarfsorientiert zusätzliche Experten bei der Polizei Nordrhein-Westfalen in den Sachraten Cybercrime und digitale Forensik eingestellt und vorhandenes Personal weiter qualifiziert. Allein im Haushaltsjahr 2022 stellt die Landesregierung den Polizeibehörden 110 hochwertige Stellen zur Bekämpfung der Cyberkriminalität zur Verfügung. Neben personellen Zuwächsen wird in einem stetigen

Prozess die materielle Ausstattung, zum Beispiel mit notwendigen Softwaretools, der Polizeibehörden in Nordrhein-Westfalen ausgebaut.

Die Personalausstattung der ZAC NRW ist für die Bearbeitung von Fällen der Cyberkriminalität gegen Unternehmen ausreichend. Hierzu haben namentlich die von der Landesregierung in dieser Legislaturperiode vorgenommenen erheblichen personellen Verstärkungen beigetragen.

Die Landesregierung wird auch in Zukunft die Entwicklung der Cyberkriminalität kontinuierlich beobachten und die erforderlichen personellen, strukturellen und materiellen Anpassungen vornehmen.