Bayerischer Landtag

18. Wahlperiode 26.07.2022 Drucksache 18/23215

Schriftliche Anfrage

der Abgeordneten **Dr. Helmut Kaltenhauser, Albert Duin**
vom 11.05.2022

IT-Bedrohungslage im Zusammenhang mit der Invasion Russlands in der Ukraine

Die Staatsregierung wird gefragt:

Antwort

des Staatsministeriums des Innern, für Sport und Integration im Einvernehmen mit dem Staatsministerium der Finanzen und für Heimat
vom 16.06.2022

Vorbemerkung
Die von Behörden und Unternehmen der kritischen Infrastruktur zur Herstellung eines hinreichenden Cybersicherheitsniveaus umgesetzten technischen und organisatorischen Maßnahmen orientieren sich an den jeweils bestehenden Gefährdungen. Im Rahmen des fortlaufenden Monitorings werden diese Maßnahmen auf Angemessenheit, Wirksamkeit, Vollständigkeit und Notwendigkeit geprüft und ggf. an die geänderte Bedrohungslage angepasst. Dabei stehen derzeit Bedrohungen aus Russland besonders im Fokus, um bei Vorliegen von Angriffsanzeichen schnell konkrete Abwehrmaßnahmen einzuleiten.

Vor dem Hintergrund einer allgemein dynamischen Bedrohungslage im Cyberraum erwächst im Kontext des Ukraine-Kriegs aus den Aktivitäten politisch motivierter „hacktivistischer“ sowie staatlich gesteuerter Gruppen zwar ein zusätzliches Bedrohungspotenzial. Dieses wird jedoch durch die etablierten Strukturen der Behörden und Einrichtungen mit Cybersicherheitsaufgaben aufmerksam beobachtet und es wird ggf. lageangepasst reagiert.

Allerdings war die Cybersicherheitslage bereits vor dem Ukraine-Krieg angespannt. Bei der Beantwortung der Fragen werden daher nur kriegsbezogene Lageveränderungen und Maßnahmen betrachtet.

1.1 Wie schätzt die Staatsregierung aktuell die Cybersicherheitslage ein?

Der Angriffskrieg Russlands gegen die Ukraine wird nach wie vor durch Cyberangriffe und Versuche der Einflussnahme begleitet. Für Deutschland und Bayern besteht nach wie vor eine erhöhte abstrakte Gefährdungslage. Lageverschärfend wirken sich die Aktivitäten nichtstaatlicher, „hacktivistisch“ motivierter Cyberakteure sowie möglicherweise staatlich gesteuerter Gruppierungen aus.

1.2 Welche Aktivitäten im Internet einschließlich Social Media lassen sich auf den Krieg in der Ukraine zurückführen?

1.3 Welche Auswirkungen haben diese Aktivitäten auf Bayern?

Die Fragen 1.2 und 1.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Seit Beginn des Angriffskriegs Russlands gegen die Ukraine am 24.02.2022 ist es in Deutschland lediglich zu wenigen, unzusammenhängenden IT-Sicherheitsvorfällen gekommen, die nur vereinzelt Auswirkungen hatten.

Weiterhin positionieren sich verschiedenste Hacker-Gruppierungen im Rahmen der Auseinandersetzung und greifen mit verschiedenen Angriffsszenarien in den Konflikt ein.

In der Nacht vom 02.05.2022 auf den 03.05.2022 kam es zu mehreren „Distributed Denial of Service“ (DDoS)-Angriffen auf die Webpräsenz der Bayerischen Polizei. Einem Telegram-Eintrag zufolge ist der Angriff der prorussischen Gruppierung KILLNET zuzuschreiben.

Trotz der hohen Latenzzeit sowie längeren Ladezeiten ist die Website der Bayerischen Polizei immer erreichbar geblieben.

2.1 Sieht die Staatsregierung die Gefahr „digitaler Kollateralschäden“ des Kriegs für Bayern?

Vor dem Hintergrund der dynamischen Bedrohungslage im Cyberraum im Allgemeinen sowie der erhöhten Bedrohungslage im Kontext des Ukraine-Kriegs können Schäden an digitalen Infrastrukturen in Bayern in der Folge von Cyberangriffen nicht vollumfänglich ausgeschlossen werden. Im Übrigen darf auf die Vorbemerkung verwiesen werden.

2.2 Sind der Staatsregierung weitere Aktivitäten vergleichbar dem Hack auf den Satelliten-Anbieter Viasat im Zusammenhang mit dem Krieg in der Ukraine bekannt?

Der Staatsregierung liegen hierzu keine Erkenntnisse vor.

2.3 Welche Aktivitäten des Hacker-Kollektivs „Anonymous“ aus Bayern heraus sind der Staatsregierung bekannt?

Der Staatsregierung liegen hierzu keine Erkenntnisse vor.

3.1 Welche Aktivitäten des Hacker-Kollektivs „Anonymous“ mit Auswirkungen auf Bayern sind der Staatsregierung bekannt?

Der Staatsregierung liegen hierzu keine Erkenntnisse vor.

3.2 Welche Maßnahmen ergreift die Staatsregierung dagegen (insbesondere Erhöhung von Schutzmaßnahmen)?

3.3 Welche Maßnahmen werden insbesondere im Cyber-Allianz-Zentrum des Landesamts für Verfassungsschutz, beim Landesamt für Sicherheit in der Informationstechnik sowie beim Landeskriminalamt und den Polizeipräsidien ergriffen?

Die Fragen 3.2 und 3.3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Auf die Vorbemerkung wird verwiesen.

4.1 Sieht sich die Staatsregierung ausreichend gegen Attacken wie die des Hacker-Kollektivs „Anonymous“ gegen russische Seiten, wie die der russischen Weltraumagentur, des belarussischen Militärs sowie zahlreiche weitere Regierungsseiten beider Länder gewappnet?

Ja. Auf die Vorbemerkung wird verwiesen.

4.2 Sieht die Staatsregierung besonderen Handlungsbedarf beim Schutz der kritischen Infrastruktur und der öffentlichen Verwaltung?

Es wird auf die Vorbemerkung verwiesen.

4.3 Inwiefern steht die Staatsregierung bezüglich der IT-Bedrohungslage im Austausch mit der Bundeswehr (insbesondere Kommando Cyber- und Informationsraum und Landeskommando Bayern)?

Die bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben stehen – über einen ständigen Vertreter im Nationalen Cyber-Abwehrzentrum (Cyber-AZ) – im regelmäßigen Austausch mit den Sicherheitsbehörden des Bundes. Zu diesen Behörden zählt auch das Bundeswehr-Kommando Cyber- und Informationsraum.

5.1 Inwiefern steht die Staatsregierung bezüglich der IT-Bedrohungslage im Austausch mit Behörden des Bundes?

5.2 Inwiefern steht die Staatsregierung bezüglich der IT-Bedrohungslage im Austausch mit anderen Ländern?

Die Fragen 5.1 und 5.2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Über die Einbindung der Cyberabwehr Bayern als Partnerbehörde des Cyber-AZ ist ein permanenter Lageabgleich der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben mit den Behörden des Bundes gewährleistet. Darüber hinaus findet ein regelmäßiger Austausch innerhalb des Verwaltungsverbunds und den Säulen Polizei und Verfassungsschutz statt.

Zur Abwehr von Bedrohungen der öffentlichen IT arbeitet das Landesamt für Sicherheit in der Informationstechnik (LSI) mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und den entsprechenden Stellen der Länder im Verwaltungs-CERT-Verbund (VCV) eng zusammen.

Im Übrigen ist eine möglichst weitreichende Vernetzung der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben zu den in anderen Ländern vorhandenen Zentralstellen für Cyber- und Informationssicherheit (z.B. H3C, CSBW) Teil der bayerischen Cybersicherheitsstrategie.

5.3 Welche Gefahren aus Cyberangriffen sieht die Staatsregierung aktuell für die Wirtschaft?

Die in der Antwort zu Frage 1.1 beschriebene Bedrohungslage wirkt auch auf die bayerische Wirtschaft. Vor allem Unternehmen, die Geschäftsbeziehungen mit Russ-

land haben, müssen von einer erhöhten Gefährdung ausgehen, Ziel „hacktivistischer“ Gruppierungen zu werden. Im Übrigen wird auf die Vorbemerkung verwiesen.

6.1 Welche Unterstützung plant die Staatsregierung für kleine und mittlere Unternehmen bei der Cybersicherheit?

Im Rahmen des Wirtschaftsschutzes wird die Gefährdungslage für die Unternehmen in Bayern durch das Landesamt für Verfassungsschutz (BayLfV) aufmerksam beobachtet. Im Zusammenhang mit dem Ukraine-Konflikt wurde dieses Monitoring intensiviert. Zudem erfolgt fortlaufend eine zielgruppenspezifische Weitergabe technischer Indikatoren zur Gefahrenabwehr und Sensibilisierung von Unternehmen durch das Cyber-Allianz-Zentrum Bayern im BayLfV.

6.2 Welche Aktivitäten fanden bisher zu hybriden Bedrohungen in der Bund-Länder-AG statt?

Die Bund-Länder offene AG „Hybride Bedrohungen“ (BLoAG) versteht sich als Austauschgremium zwischen der Bundes-, Landes- und Kommunalebene und vertritt einen ganzheitlichen Ansatz. Ziel ist u.a. die Koordinierung und Vernetzung der Teilnehmer sowie der strategische Aufbau von Expertise. Die erste Arbeitssitzung der BLoAG Hybrid fand am 12.05.2022 statt.

6.3 Was genau versteht die Staatsregierung unter der „Möglichkeit einer aktiven Cyberabwehr“, wie sie in Nr. 22 des Beschlusses der Besprechung von Bundeskanzler Olaf Scholz mit den Regierungschefinnen und Regierungschefs der Länder am 17.03.2022 genannt wird?

Unter aktiver Cyberabwehr versteht man einen Gegenschlag auf einen erfolgten bzw. noch andauernden Hacking-Angriff. Dabei wird in einem ersten Schritt das täterseitig kontrollierte Computersystem identifiziert und auf Schwachstellen analysiert. Anschließend wird versucht, über die erkannte Lücke in das System einzudringen und mittels gezieltem Gegenschlag das System unschädlich zu machen oder in der Handlungsfähigkeit einzuschränken. Weitere Anschlussmaßnahmen hängen von der jeweiligen Fallgestaltung ab.

7.1 Versteht die Staatsregierung darunter auch die Möglichkeit zu Hackbacks als Möglichkeit der Cyberabwehr?

Ja.

7.2 Welche Maßnahmen ergreift die Staatsregierung, um eine aktive Cyberabwehr in Bayern aufzubauen?

Keine.

7.3 Sind der Staatsregierung Hacker oder Hackergruppen bekannt, die aus Bayern heraus in den Cyberkrieg in der Ukraine eingreifen?

Der Staatsregierung liegen hierzu keine Erkenntnisse vor.

8.1 Welche Erkenntnisse hat die Staatsregierung zur Lage in Bayern bezüglich sogenannter „Wiper“, wie sie durch Russland gegen die Ukraine eingesetzt werden?

8.2 Welche Erkenntnisse hat die Staatsregierung, ob auch in Bayern „Wiper“ – ggf. getarnt als „normale“ Ransomware und auch bereits im vergangenen Jahr – eingeschleust wurden?

Die Fragen 8.1 und 8.2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Staatsregierung liegen hierzu keine Erkenntnisse vor. In den Monitoringsystemen des Bayerischen Behördennetzes (BYBN) sind entsprechende Angriffsindikatoren hinterlegt.

8.3 Wie schätzt die Staatsregierung die Gefahr ein, dass – für den Fall, dass Russland eine Eskalation unter Beteiligung westlicher Staaten mit einkalkuliert haben sollte – Schadsoftware russischer Herkunft schon vor Monaten gängige Schutzmechanismen auch in Bayern umgangen hat, um an Zielorten in Deutschland auf den Einsatz zu warten?

Nach Einschätzung der bayerischen Behörden und Einrichtungen mit Cybersicherheitsaufgaben ist ein solches Angriffsszenario denkbar. Im Übrigen wird auf die Vorbemerkung verwiesen.

Hinweise des Landtagsamts

Zitate werden weder inhaltlich noch formal überprüft. Die korrekte Zitierweise liegt in der Verantwortung der Fragestellerin bzw. des Fragestellers sowie der Staatsregierung.

Zur Vereinfachung der Lesbarkeit können Internetadressen verkürzt dargestellt sein. Die vollständige Internetadresse ist als Hyperlink hinterlegt und in der digitalen Version des Dokuments direkt aufrufbar. Zusätzlich ist diese als Fußnote vollständig dargestellt.

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de/parlament/dokumente abrufbar.

Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de/aktuelles/sitzungen zur Verfügung.