



HESSISCHER LANDTAG

04. 11. 2024

Kleine Anfrage

**Markus Fuchs (AfD), Karsten Bletzer (AfD), Christian Rohde (AfD),
Sandra Weegels (AfD), Maximilian Mürger (AfD), Bernd Erich Vohl (AfD) und
Pascal Schleich (AfD) vom 05.06.2024**

Digitaler Katastrophenschutz und Cyberangriff auf die Hochschule der Polizei und

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Die Zahl der Cyberangriffe auf Unternehmen und staatliche Institutionen nimmt stetig zu. Dies gerade auch wegen internationaler Krisen, welche dazu führen, dass die überwiegende Zahl der in Deutschland festgestellten Cyberangriffe mit staatlicher Steuerung inzwischen überwiegend Russland, China und dem Iran zugeordnet werden. Diese Cyberangriffe können dem Ausspähen beziehungsweise Stehlen von Daten, der Desinformation, der Sabotage oder der Erpressung per Ransomware dienen. Am 30.04.2024 feierte das Hessen3C (CyberCompetenceCenter – CCC) sein fünfjähriges Bestehen. Nach eigener Darstellung erstreckt sich das Aufgabenspektrum vom Schutz der Landesverwaltung vor Cybersicherheitsbedrohungen über die Unterstützung der Sicherheitsbehörden, der Ausbildung von Experten, der Bekämpfung von Cyberkriminalität und Cyberspionage, bis hin zur Beratung von Kommunen, Unternehmen und Betreibern kritischer Infrastrukturen (KRITIS). Hierbei arbeite es sehr eng mit der Hessischen Polizei und dem Landesamt für Verfassungsschutz Hessen zusammen. Das genannte CCC unterhält „einen Schrank auf Rädern“ mit 20 Laptops für einen provisorischen IT-Neustart von Gemeinden. Gemäß BKA registrierte die Polizei alleine im vergangenen Jahr 136.865 Cyberstraftaten. Laut Bericht der F.A.Z. Rhein-Main Zeitung kam es in der Zeit vom 08. bis 13.02.2024 zu einem Cyberangriff auf die Hochschule der Polizei und Verwaltung, es wurden personenbezogene Daten erbeutet, welche bis in das Jahr 2010 zurückreichen.

Die Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1 Mit welchen Auswirkungen rechnet die Landesregierung bei einem Cyberangriff auf Hessen im schlimmsten Fall? Antwort bitte erläutern.

Die Auswirkungen eines Cyberangriffs können sehr unterschiedlich sein. Primäre Schutzziele der Informationssicherheit könnten (schwerwiegend) beeinträchtigt sein und vernetzte IT-Systeme, -Verfahren und -Infrastrukturen nicht mehr zur Verfügung stehen. Davon kann potenziell jedes angeschlossene System betroffen sein, sodass Daten nicht mehr zur Verfügung stehen, Kommunikationswege abgeschnitten sind und die Arbeitsfähigkeit gestört ist.

Frage 2 Welche konkreten Maßnahmen sind zum Schutze der Bevölkerung im Falle eines erfolgreichen Angriffes auf die folgenden Bereiche der KRITIS getroffen worden: Energieversorgung, Informationstechnik und Telekommunikation, Transportwesen und Verkehr, Gesundheitsversorgung, Wasserversorgung und -entsorgung, Ernährungsversorgung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung? Antwort bitte erläutern.

Die Betreiber der Kritischen Infrastruktur sind für die Erbringung der Infrastrukturleistungen zuständig und verantwortlich. Die Fachbehörden stehen mit den KRITIS-Betreibern in regelmäßigem Austausch, um Maßnahmen zum Schutz der Bevölkerung abzustimmen, Organisationsstrukturen auszubilden und Mittel zum Krisenmanagement zu verzahnen.

Folgende Bereiche gehören zum KRITIS-Schutz:

- Vorbeugung / Prävention – Vermeidung / Verhinderung von Störungen beziehungsweise Ausfällen der KRITIS durch risikoangepasste und schutzzielorientierte Sicherungsmaßnahmen,
- Vorbereitung – auf (unvermeidbare) Störungen beziehungsweise Ausfälle durch Notfallkonzepte und Krisenvorhaltungen sowie Redundanzsicherungen,

- Bewältigung (Reaktion) – von Schadenslagen und KRITIS-Störungen/-Ausfällen durch Maßnahmen zur Abmilderung von Auswirkungen, störresiliente Alternativversorgung und Wiederherstellung sowie
- Nachsorge (oder Nachbereitung) – im Anschluss an die akute Bewältigungsphase im Sinne von Lernen aus Ereignissen und daraus resultierenden Verbesserungen (und Übergang zur neuerlichen Vorsorge).

Bei den Maßnahmen zur Vorbereitung auf KRITIS-Ausfälle bezüglich der in der Fragestellung genannten KRITIS-Bereiche handelt es sich um schutzbedürftige Informationen. Aus Sicherheitsgründen können deshalb keine Angaben gemacht werden.

Frage 3 Inwieweit wurden die „Rahmenempfehlungen zur Einsatzplanung des Brand- und Katastrophenschutzes bei flächendeckendem, langandauerndem Stromausfall“ des Innenministeriums umgesetzt? Antwort bitte erläutern.

Die Verantwortung für eine uneingeschränkte und sichere Versorgung mit (elektrischer) Energie tragen die Stromnetzbetreiber als Betreiber dieser kritischen Infrastrukturen. Die Energieaufsicht nimmt vor diesem Hintergrund die ihr übertragenen Aufgaben wahr.

Zur Vorbereitung auf ein Blackout-Szenario hat das Land „Rahmenempfehlungen zur Einsatzplanung des Brand- und Katastrophenschutzes bei flächendeckendem, langandauerndem Stromausfall“ herausgegeben.

Die zuständigen Fachministerien/-behörden definieren zudem den Rahmen für die Notfallplanungen. Daneben wurde speziell für die einzelnen Stellen der Landesverwaltung eine Checkliste „Vorbereitung auf einen langanhaltenden, großflächigen Stromausfall („Blackout“)“ erarbeitet und den Dienststellen für deren eigene Vorkehrungen zur Verfügung gestellt.

Es obliegt den unteren Katastrophenschutzbehörden, sich für ihren örtlichen Zuständigkeitsbereich umfassend auf mögliche Krisenlagen vorzubereiten. Die Erarbeitung der Alarm- und Einsatzpläne erfolgt in eigener Zuständigkeit. Das Land erarbeitete im Sommer des Jahres 2022 die „Handlungsempfehlung zur Einsatzplanung des Brand- und Katastrophenschutzes bei einer Gas-mangellage“ und stellte dies den unteren Katastrophenschutzbehörden des Landes zur Verfügung. Hierin wurde explizit auf die Möglichkeit von flächendeckenden, langandauernden Stromausfällen eingegangen und die Vorgaben der „Rahmenempfehlungen zur Einsatzplanung des Brand- und Katastrophenschutzes bei flächendeckendem, langandauerndem Stromausfall“ Bezug genommen.

Frage 4 Wie bereiten sich die zur Gefahrenabwehr zuständigen Behörden auf einen Angriff vor, insbesondere auf Bedrohungen durch Ransomware? Antwort bitte erläutern.

Grundlage ist der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Im Bereich der Polizei wurde beispielsweise eine „AG IT-Notfallmanagement“ eingerichtet, welche sich auch dem Schutz vor Ransomware als eines der möglichen Bedrohungsszenarien widmet.

Frage 5 Plant die Landesregierung das Funktionieren der vorgesehenen Maßnahmen (im Sinne einer länger dauernden Stromversorgungsunterbrechung) im Rahmen einer Katastrophenschutzübung zu testen? Antwort bitte begründen.

Bei einem langanhaltenden, flächendeckenden Stromausfall übernehmen die Kommunen das operative Krisenmanagement. Regelmäßige Katastrophenschutzübungen werden auf der Ebene der unteren Katastrophenschutzbehörden durchgeführt. Das Land fungiert strategisch-koordinierend und unterstützt bei der Bewältigung übergeordneter Aufgaben. Zur Bewältigung von Krisen, Großschadenslagen und Katastrophen von landesweiter Bedeutung unterhält die Landesregierung einen Krisenstab und ein Krisenzentrum. Das Land beübt regelmäßig seine Krisenmanagementstrukturen im Rahmen der „Länderübergreifenden Krisenmanagementübung (Exercise)“ (LÜKEX), die seit dem Jahr 2004 regelmäßig zwischen dem Bund und den Ländern unter Federführung des Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) stattfinden. Hessen hat an der letzten LÜKEX teilgenommen, die im Herbst 2023 zum Thema „Cyberangriff auf das Regierungshandeln“ stattgefunden hat.

Frage 6 Gibt es analoge Notfallmechanismen, auf die bei Ausfall digitaler Systeme zurückgegriffen werden kann? Antwort bitte erläutern.

Je nach Einstufung und Bewertung werden entsprechende Redundanzen vorgehalten. Beispielsweise werden Satellitentelefone und Daten in Notfallordnern vorgehalten.

Frage 7 Inwieweit geht die Landesregierung davon aus, im Katastrophenfall Hilfe vom Bund oder aus anderen Bundesländern zu erhalten? Antwort bitte begründen.

Die gegenseitige Hilfeleistung in Notlagen ist bewährte Praxis. Die Zusammenarbeit zwischen Bund und Ländern im Bevölkerungsschutz erfolgt partnerschaftlich.

Frage 8 Wie begründet sich die Zahl von lediglich 20 Ersatzlaptops, im Rahmen des „Schränk auf Rädern“, durch Hessen 3C, angesichts der Tatsache, dass in den Hessischen Verwaltungen mehr als 71.000 HessenPC im Einsatz sind und es im Falle eines erfolgreichen Cyberangriffes auf die Verwaltungen der Landkreise und Kommunen es durchaus denkbar ist, dass mehrere Kommunen in Hessen gleichzeitig angegriffen werden? Antwort bitte begründen.

Das sogenannte Rapid-Aid-Kit, besteht aus 24 Laptops und dient zur Wiederherstellung eines Notfallbetriebs und einer Notfallkommunikation für die von einem Cyberangriff betroffenen Kommunen; es dient nicht dazu, die Funktionen des „HessenPC“ zu substituieren.

Frage 9 Warum sind Rechner der Polizeihochschule mit personenbezogenen Daten überhaupt über das Internet erreichbar und nicht vielmehr physisch gekapselt? Antwort bitte begründen.

Die Hochschule für öffentliches Management und Sicherheit (HöMS) bietet ihren Beschäftigten an, ihre Dienstverrichtung zumindest teilweise im Homeoffice wahrzunehmen. Die Zugriffe auf das Rechenzentrum der HöMS von extern werden über Firewalls, Virens Scanner und durch Rollen- und Rechtekonzepte geschützt. Das Hochschulnetz ist von dem in der Polizei im Einsatzdienst verwendeten Netz getrennt.

Frage 10 Gibt es Pläne der Landesregierung, KI zur Bekämpfung von Cyberkriminalität einzusetzen? Antwort bitte begründen.

Der Einsatz von Künstlicher Intelligenz (KI) erfolgt unter Beachtung der rechtlichen Regelungen. Es ist beabsichtigt, insbesondere bei der automatisierten Datenanalyse im Rahmen von hessen-DATA künftig den Einsatz von KI zu ermöglichen. Zur Bekämpfung schwerer Kriminalität bedarf es der zeitgerechten und automatisierten Auswertung großer Datenmengen, wofür KI eine unerlässliche Unterstützung ist. Da die Nutzung von KI die Möglichkeiten potentieller Angreifer deutlich steigern wird, ist deren Nutzung auch zur Abwehr grundsätzlich geboten. Die Nutzung von KI ist Gegenstand von Forschungsprojekten des Innovationsmanagements Cybersicherheit im Hessischen Ministerium des Inneren, für Sicherheit und Heimatschutz (HMdI). Die daraus gewonnenen Erkenntnisse sowie die Beobachtung technischer Entwicklungen werden im Rahmen der Planung und Konzeption zukünftiger Strategien berücksichtigt.

Wiesbaden, 21. Oktober 2024

Prof. Dr. Roman Poseck