Bayerischer Landtag

17. Wahlperiode 03.09.2018 **Drucksache 17/21716**

Schriftliche Anfrage

der Abgeordneten **Claudia Stamm (fraktionslos)**
vom 05.03.2018

Datensicherheit im bayerischen Behördennetzwerk

Anfang März 2018 wurde bekannt, dass das sogenannte Regierungsnetzwerk des Bundes Ziel eines geplanten Hackerangriffes wurde. Nach bisherigem Kenntnissstand soll für den Angriff eine Gruppe (snake) mit Kontakten zum russischen Geheimdienst verantwortlich sein. Für den Angriff wurde eine Schadsoftware mit dem Namen „Uruburos“ eingesetzt, die 2014 von der deutschen Firma G-Data entdeckt wurde. Die Schadsoftware wird möglicherweise seit 2008 eingesetzt und verbreitet, nach einigen Meldungen sogar seit 2005. Auch das Land Bayern betreibt ein Behördennetzwerk, an das u. a. der Landtag, die Staatsministerien, Ämter und zahlreiche Kommunen und Landkreise angeschlossen sind. Bereits in der Vergangenheit wurde auf Systemen in bayerischen Behörden Schadsoftware gefunden (vgl. Drs. 17/11799, 17/16078).

Ich frage die Staatsregierung:

1. a) Wo und wann wurde in den letzten zehn Jahren die Schadsoftware Uruburos auf Systemen, die Teil des bayerischen Behördennetzwerks sind, gefunden (bitte Angabe des Datums und der betroffenen Stelle für jede Meldung)?
   b) Welcher Schaden entstand durch die Schadsoftware?
   c) Wurde das bayerische Behördennetzwerk in den letzten Monaten gezielt nach Spuren von Uruburos durchsucht?

2. a) Welche Schlüsse zieht die Staatsregierung aus dem Angriff auf das Regierungsnetzwerk des Bundes?
   b) Wie stellt die Staatsregierung sicher, dass das bayerische Behördennetzwerk nicht Ziel eines ähnlich gearteten Angriffes wird?
   c) Welche privaten Unternehmen sind mit der Abwehr und Analyse von Angriffen auf das bayerische Behördennetzwerk befasst (z. B. als Dienstleister zur Betreuung von Computersystemen in Behörden, als Lieferanten von Software zur Bekämpfung von Schadsoftware)?

3. a) Welcher Schaden entstand den Kommunen bzw. dem Freistaat Bayern in den letzten zehn Jahren durch sogenannte Hackerangriffe (bitte auflisten nach: Abfluss von Daten, Löschung von Daten, Manipulation von Daten, Blockade von Rechnern, Mißbrauch von Rechnern in einem Botnet etc.)?
   b) In wie vielen Fällen hat in 2017 das Landesamt für Sicherheit in der Informationstechnik (LSI) auf Angriffe von außen reagiert?
   c) Welcher Natur waren die Fälle, in denen das LSI tätig wurde?

4. a) Gab es in den letzten fünf Jahren in bayerischen Behörden sogenannte Penetrationstests zur Überprüfung des Sicherheitskonzepts bzw. des Sicherheitsstatus?
   b) In welchem Umfang setzt die Staatsregierung auf Verschlüsselungstechnologien (Verschlüsselung von Datenträgern etc.)?
   c) Welche Richtlinien verfolgt die Staatsregierung bei der Verwendung privater Endgeräte wie Smartphones, Tablets, Notebooks, USB-Sticks etc. im Behördenumfeld („Bring Your Own Device“, BYOD)?

5. a) Setzen Ämter, Behörden etc. für die Realisierung eines Zugangs zum bayerischen Behördennetzwerk auch WLAN-Geräte ein?
   b) Welche Sicherheitsvoraussetzungen werden für die WLAN-Geräte gefordert und werden diese eingehalten (Anmeldung auf MAC-Ebene, Verschlüsselungstechnologie)?
   c) In welchem Umfang und unter welchen Maßgaben ist die Verwendung von Smartphones und Tablets mit Zugang zum bayerischen Behördennetzwerk möglich (BYOD)?

6. a) Welches Präventionskonzept verfolgt die Staatsregierung zur Verhinderung von Cyberattacken?
   b) Welche Institutionen sind bei der Planung und Umsetzung der Präventionsstrategie in den einzelnen Behörden und Dieststellen mit Zugang zum bayerischen Behördennetzwerk befasst?
   c) Welche Rolle hat das Cyber-Allianz-Zentrum Bayern (CAZ) bei der Prävention von Angriffen gegen Institutionen, die an das bayerische Behördennetzwerk angeschlossen sind?

7. a) Inwieweit wurde die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (2013) in Bayern umgesetzt?
   b) Wie sehen die Zusammenarbeit und die Aufgabenteilung zwischen CAZ, LSI und dem Landesbeauftragten für Datenschutz (BayLDA) aus?
   c) Wie sieht die Kooperation zwischen mit der Cybersicherheit befassten bayerischen Behörden (CAZ, LSI, BayLDA) und Bundesbehörden (Bundesamt für Sicherheit in der Informationstechnik – BSI, Informationstechnikzentrum Bund – ITZBund – etc.) aus?

Antwort

des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat in Abstimmung , insbesondere zu den Fragen 6a ,6b, 6c, 7b, 7c, mit dem für Cybersicherheit zuständigen Staatsministerium des Innern und für Integration
vom 16.04.2018

1. a) Wo und wann wurde in den letzten zehn Jahren die Schadsoftware Uruburos auf Systemen, die Teil des bayerischen Behördennetzwerks sind, gefunden (bitte Angabe des Datums und der betroffenen Stelle für jede Meldung)?

Die Schadsoftware „Uruburos“ ist nicht bekannt. Soweit sich die Frage auf die Schadsoftware „Uroburos“ bezieht, ist festzustellen, dass in den letzten zehn Jahren kein Sicherheitsvorfall bekannt wurde, bei dem diese Schadsoftware auf einem System im Bayerischen Behördennetz gefunden wurde.

b) Welcher Schaden entstand durch die Schadsoftware?

Da kein bestätigter IT-Sicherheitsvorfall zu „Uroburos“ existiert, ist kein Schaden bezifferbar.

c) Wurde das bayerische Behördennetzwerk in den letzten Monaten gezielt nach Spuren von „Uruburos“ durchsucht?

In den letzten Monaten wurden Signaturen, die sich auf die Schadsoftware „Uroburos“ beziehen, in den Überwachungssystemen hinterlegt und bei der automatischen Auswertung der Daten berücksichtigt.

2. a) Welche Schlüsse zieht die Staatsregierung aus dem Angriff auf das Regierungsnetzwerk des Bundes?

Der Angriff ist ein deutliches Zeichen der sich verschärfenden IT-Sicherheitslage. Der IT-Sicherheit ist große Bedeutung einzuräumen, um den fortwährenden und auch gezielten Angriffen in entsprechend personeller Stärke entgegentreten zu können. Basierend auf dieser Erkenntnis richtete Anfang Dezember 2017 der Freistaat Bayern als erstes Bundesland ein eigenes Landesamt für Sicherheit in der Informationstechnik (LSI) ein. Das LSI wird in enger Abstimmung mit den bayerischen Rechenzentren und den weiteren Akteuren in den Bereichen IT- und Cybersicherheit den Schutz von BayernServer und BayernNetz weiter verbessern. Weiterhin wird ein Beratungsangebot für Kommunen und öffentliche Betreiber kritischer Infrastrukturen sowie ein Informationsangebot für Bürger bereitgestellt.

b) Wie stellt die Staatsregierung sicher, dass das bayerische Behördennetzwerk nicht Ziel eines ähnlich gearteten Angriffes wird?

Das Bayerische Behördennetz ist durch eine Vielzahl von Sicherheitsmechanismen geschützt. Diese Sicherheitsmaßnahmen sind teils technischer Natur, teils handelt es sich um organisatorische Vorgaben. Diese technischen und organisatorischen Maßnahmen können die Auswirkungen eines solchen Angriffs im Idealfall vollständig unterbinden. Weiterhin wird auf die Antwort zu Frage 2 a verwiesen.

c) Welche privaten Unternehmen sind mit der Abwehr und Analyse von Angriffen auf das bayerische Behördennetzwerk befasst (z. B. als Dienstleister zur Betreuung von Computersystemen in Behörden, als Lieferanten von Software zur Bekämpfung von Schadsoftware)?

Server- und Clientmanagement werden grundsätzlich von der Staatsverwaltung selbst wahrgenommen, auch hinsichtlich der Informationssicherheit. Ebenso werden Abwehr und Analyse von Angriffen durch das LSI selbst geleistet, ggf. unterstützt von anderen Behörden. Private Unternehmen treten als Lieferanten von speziellen IT-Systemen auf, insbesondere in den Bereichen Überwachung und Prognose (SIEM-System), Perimeterschutz und Virenscanner. Die eingesetzten Produkte sind State-of-the-Art, die Auswahl der Hersteller erfolgt anhand entsprechender Vorgaben und Vergabekriterien. Zu den privaten Lieferanten zählen u. a. die Unternehmen Infodas und Secunet. Weitere konkrete Namen können aus Sicherheitsgründen nicht genannt werden, da ansonsten Rückschlüsse auf die eingesetzten Produkte möglich sind.

3. a) Welcher Schaden entstand den Kommunen bzw. dem Freistaat Bayern in den letzten zehn Jahren durch sogenannte Hackerangriffe (bitte auflisten nach: Abfluss von Daten, Löschung von Daten, Manipulation von Daten, Blockade von Rechnern, Mißbrauch von Rechnern in einem Botnet etc.)?

Eine Übersicht über den bei Kommunen bzw. dem Freistaat Bayern in den letzten zehn Jahren durch Hackerangriffe entstandenen Schaden liegt nicht vor.

b) In wie vielen Fällen hat in 2017 das Landesamt für Sicherheit in der Informationstechnik (LSI) auf Angriffe von außen regaiert?

Im Jahr 2017 wurden vom Bayern-CERT bzw. vom LSI 2.683 Fälle bearbeitet, bei denen ein Anfangsverdacht auf einen IT-Sicherheitsvorfall bestand.

c) Welcher Natur waren die Fälle, in denen das LSI tätig wurde?

Bei den Fällen, die vom Bayern-CERT bzw. vom LSI bearbeitet wurden, handelt es sich um Phishing-E-Mails, Trojaner, DDoS-Angriffe und Angriffe auf Webseiten.

4. a) Gab es in den letzten fünf Jahren in bayerischen Behörden sogenannte Penetrationstests zur Überprüfung des Sicherheitskonzepts bzw. des Sicherheitsstatus?

In den letzten fünf Jahren (2013–2017) wurden vom Bayern-CERT bzw. LSI 369 Penetrationstests durchgeführt.

b) In welchem Umfang setzt die Staatsregierng auf Verschlüsselungstechnologien (Verschlüsselung von Datenträgern etc.)?

Verschlüsselung nimmt eine zentrale Rolle zur Erreichung der Informationssicherheitsziele der Staatsverwaltung ein.

Bereits seit vielen Jahren werden die Daten im Bayern-Netz verschlüsselt. Aktuell werden neue Verschlüsselungskomponenten ausgerollt, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen sind. Das Schlüsselmaterial wird vom Freistaat Bayern selbst generiert – ein zusätzliches Plus an Sicherheit.

Der Zugang zum Behördennetz von außerhalb ist nur über Verschlüsselung durch Virtual Private Network (VPN) und eine 2-Wege-Authentifizierung möglich. Generelle Regelungen zur Verschlüsselung mobiler Endgeräte und Datenträger sind im IKT-Standard BayITS-19 geregelt.

c) Welche Richtlinien verfolgt die Staatsregierung bei der Verwendung privater Endgeräte wie Smartphones, Tablets, Notebooks, USB-Sticks etc. im Behördenumfeld („Bring Your Own Device", BYOD)?

Die Verwendung privater Endgeräte im Sinne von „Bring Your Own Device" (BYOD) ist gemäß der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern nicht gestattet. Danach dürfen für die Erledigung dienstlicher Aufgaben nur dienstlich bereitgestellte Geräte und Datenträger sowie freigegebene Programme (Ausstattung) benutzt werden.

5. a) Setzen Ämter, Behörden etc. für die Realisierung eines Zugangs zum bayerischen Behördennetzwerk auch WLAN-Geräte ein?

Zur Realisierung eines Zugangs zum bayerischen Behördennetzwerk können auch WLAN-Geräte eingesetzt werden. Es gelten die Regelungen der IT-Sicherheitsrichtlinie für die Staatsverwaltung zum Einsatz drahtloser Netze (BayITSiR-03).

b) Welche Sicherheitsvoraussetzungen werden für die WLAN-Geräte gefordert und werden diese eingehalten (Anmeldung auf MAC-Ebene, Verschlüsseltungstechnologie)?

Auf die Antworten zu den Fragen 4 b und 5 a wird verwiesen.

c) In welchem Umfang und unter welchen Maßgaben ist die Verwendung von Smartphones und Tablets mit Zugang zum bayerischen Behördennetzwerk möglich (BYOD)?

Auf die Antwort zu Frage 4 c wird verwiesen.

6. a) Welches Präventionskonzept verfolgt die Staatsregierung zur Verhinderung von Cyberattacken?

Es ist eine gemeinsame Herausforderung für Staat, Wirtschaft und Gesellschaft, ein hohes Maß an Cybersicherheit zu erreichen. Der Freistaat Bayern hat daher im April 2013 die Bayerische Cybersicherheitsstrategie auf den Weg gebracht. Diese verfolgt folgende Kernziele:

- Schutz der Bürgerinnen und Bürger (Aufklärung und Sensibilisierung der Nutzer über die Gefahren im Netz),
- Schutz staatlicher Handlungsfähigkeit sowie Stärkung der Sicherheitsbehörden,
- Schutz der Wirtschaft vor Spionage und Sabotage,
- Vernetzung aller für Cybersicherheit wichtigen Akteure (Staat, Wirtschaft, Forschung, Wissenschaft),
- Koordination im Staatsministerium des Innern und für Integration (StMI).

Zum Zwecke der Koordinierung wurde hierzu unter Beteiligung aller betroffenen Staatsministerien und Behörden ein Ressortkreis „Strategie für Cybersicherheit" (RSC) unter Federführung des StMI geschaffen.

Als Teil dieser Initiative wurde am 01.07.2013 das Cyber-Allianz-Zentrum (CAZ) im Landesamt für Verfassungsschutz (BayLfV) ins Leben gerufen. Das CAZ unterstützt in Bayern ansässige Unternehmen, Hochschulen und Betreiber kritischer Infrastruktur bei der Prävention, Aufklärung und Bewältigung von elektronischen Angriffen mit Spionage- oder Sabotagehintergrund. Darüber hinaus stellt das BayLfV auch im Rahmen der Initiative Wirtschaftsschutz von StMI und Staatsministerium für Wirtschaft, Energie und Technologie (StMWi) ein großes Informationsangebot für bayerische Unternehmen zur Verfügung.

b) Welche Institutionen sind bei der Planung und Umsetzung der Präventionsstrategie in den einzelnen Behörden und Dieststellen mit Zugang zum bayerischen Behördennetzwerk befasst?

Zur Rolle des LSI wird auf die Antwort zu Frage 2 a verwiesen. Die Umsetzung des jeweiligen Präventionsrahmens obliegt den Ressorts. Der Ressortkreis „Strategie für Cybersicherheit", siehe die Antwort zu Frage 6 a, nimmt im Informationsaustausch eine wichtige Rolle ein.

c) Welche Rolle hat das Cyber-Allianz-Zentrum Bayern (CAZ) bei der Prävention von Angriffen gegen Institutionen, die an das bayerische Behördennetzwerk angeschlossen sind?

Allein aus der Anbindung an das Bayerische Behördennetz heraus erwachsen beim CAZ keine Aufgaben oder Funktionen. Der Verfassungsschutz hat als Inlandsnachrichtendienst jedoch grundsätzlich den gesetzlichen Auftrag, Spionagetätigkeiten ausländischer Nachrichtendienste in Deutschland aufzuklären. Insofern teilt er Erkenntnisse, die dem Schutz staatlicher Netze dienen, den zuständigen Stellen mit.

7. a) Inwieweit wurde die Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung (2013) in Bayern umgesetzt?

Schon weit vor Inkrafttreten der Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung des IT-Planungsrats wurden für die Staatsverwaltung eine eigene Informationssicherheitsleitlinie (BayITSiLL) und eine IT-Richtlinie zur IT-Sicherheitsorganisation (BayITSiR-O) eingeführt. Zentrale Elemente hieraus waren und sind die Meldekette bei Sicherheitsvorfällen sowie die Einführung eines ressortübergreifenden, strategisch-steuernden Landes-IT-Sicherheitsbeauftragten (CISO), von Ressort-IT-Sicherheitsbeauftragten, von Beauftragten in den jeweiligen Behörden und die Bereitstellung einer „schnellen Eingreiftruppe": das Bayern-CERT.

In Umsetzung der Leitlinie des IT-Planungsrats arbeiten die Ressorts mit hohem Engagement an der Einführung eines Informations-Sicherheits-Management-Systems (ISMS) auf Basis des IT-Grundschutzes.

b) Wie sehen die Zusammenarbeit und die Aufgabenteilung zwischen CAZ, LSI und dem Landesbeauftragten für Datenschutz (BayLDA) aus?

Die Behörden der bayerischen Cybersicherheitsstrategie stehen untereinander in einem engen Austausch.

So wie das LSI jeden Angriff, der einen Sabotage- oder Spionagehintergrund möglich erscheinen lässt, an das BayLfV melden muss, ist auch das CAZ gehalten, dort erkannte Angriffsstrukturen dem LSI zum Zwecke des Schutzes der staatlichen IT mitzuteilen. Die jeweiligen Aufgabenbereiche von LSI und CAZ sind dabei klar voneinander abgegrenzt: So ist das LSI für den Schutz der staatlichen IT-Infrastruktur zuständig, das CAZ dagegen bildet die Schnittstelle zur Wirtschaft. Im Rahmen regelmäßiger „Jour-Fixe-

Termine“ kooperieren LSI und CAZ darüber hinaus eng und laufend in Fragen der Cybersicherheit.

Das CAZ veranstaltet zusammen mit dem Landesamt für Datenschutzaufsicht sowie den IHK bayernweite Roadshows, um die Öffentlichkeit im Sinne der Prävention zum Thema „Gefahren moderner Informations- und Kommunikationstechnologie“ zu sensibilisieren.

c) Wie sieht die Kooperation zwischen mit der Cybersicherheit befassten bayerischen Behörden (CAZ, LSI, BayLDA) und Bundesbehörden (Bundesamt für Sicherheit in der Informationstechnik – BSI, Informationstechnikzentrum Bund – ITZBund – etc.) aus?

Auf Bundesebene sind das Bundesamt für Verfassungsschutz (BfV) und das BSI wichtige Partner der bayerischen Behörden. BfV, Bundeskriminalamt (BKA), Bundesnachrichtendienst (BND) und BSI sind zudem Partner der Initiative Wirtschaftsschutz. Das CAZ des BayLfV ist Ansprechpartner für Bayern in der Initiative Wirtschaftsschutz. Das CAZ gehört zudem seit seiner Gründung als Institution im besonderen staatlichen Interesse (INSI) dem Netzwerk der Nationalen Allianz für Cyber-Sicherheit des BSI an und ist damit fester Bestandteil der behördlichen deutschen Cyberabwehrstruktur. Im Bereich des Schutzes der öffentlichen Informationstechnik findet unter dem Dach des IT-Planungsrats eine enge Abstimmung zwischen dem LSI, den entsprechenden Stellen der anderen Länder und dem BSI statt. Die Arbeitsgruppe Informationssicherheit des IT-Planungsrats (IT-PLR) dient zu diesem Zweck als Abstimmungsgremium der Landes-CISO untereinander und mit dem Bund. Arbeitsgremium ist der Verwaltungs-CERT-Verbund (VCV), unter dessen Dach ein Meldewesen zur gegenseitigen Information bei IT-Sicherheitsvorfällen verabredet ist. Das BayLDA ist in Bayern mit den o. g. Behörden vernetzt. Über einen Vertreter der Datenschutzkonferenz (= Konferenz aller Datenschutzaufsichtsbehörden des Bundes und der Länder) ist das BayLDA im IT-Planungsrat vertreten.