Bayerischer Landtag

17. Wahlperiode

09.01.2015 17/4165

Schriftliche Anfrage

der Abgeordneten **Katharina Schulze, Verena Osgyan BÜNDNIS 90/DIE GRÜNEN**
vom 10.09.2014

Datensicherheit bei bayerischen Behörden

Im April dieses Jahres wurde ein 51-jähriger Ingolstädter des Versuchs beschuldigt, die Internetpräsenz der bayerischen Polizei mit einer DOS-Attacke (Denial of Service) lahmlegen zu wollen. (vgl. „Cyberangriff auf Polizeiserver“, Donaukurier.de vom 30.04.2014)

In diesem Zusammenhang frage ich die Staatsregierung:

1. Besteht die Möglichkeit, für einen Mailserver der Bayerischen Polizei oder andere Teile des Behördennetzwerks mit einer über einen einzelnen Rechner durchgeführten DOS-Attacke eine Nichterreichbarkeit herbeizuführen?
   a) Falls ja, werden bereits weitere Schritte geplant, um diesem Risiko entgegenzuwirken?
   b) Falls nein, wie rechtfertigt die Staatsregierung in diesem Fall den Einsatz des LKA und die Beschlagnahme zahlreicher Gegenstände des Beschuldigten?

2. Bei welcher Behörde ist das sog. Computer Emergency Response Team angesiedelt und wie ist es in behördenübergreifende Prozesse eingebunden?
   a) Über wie viele Planstellen verfügt das Computer Emergency Response Team?
   b) Beauftragt das Computer Emergency Response Team auch private Dienstleister?

3. Welche EDV- und Kommunikationsdienstleistungen die früher an private Auftragnehmer vergeben wurden, werden mittlerweile wieder intern bei staatlichen Stellen durchgeführt (bitte Auflistung nach Tätigkeitszuschnitt und übergeordneten Behörden)?

4. Wie gestaltet sich die Zusammenarbeit des Computer Emergency Response Team mit dem Cyber Allianz Zentrum Bayern?
   a) Welche weiteren öffentlichen Stellen sind im Rahmen ihres Aufgabenzuschnitts mit der Datensicherheit in Bayern betraut?
   b) Wie gestaltet sich die Zusammenarbeit mit den Ermittlungsbehörden, z. B. dem LKA sowie dem Landesamt für Verfassungsschutz?

5. Aus welchen Herkunftsländern verzeichnet die Staatsregierung die meisten Cyberangriffe (bitte Aufschlüsselung nach Angriffsart und Nation)?
   a) In welchem Prozentsatz werden dabei Angriffe aus Deutschland verzeichnet?

6. Bestehen beim Einsatz von IuK-Technik im Bereich von kritischen Infrastrukturen, z. B. Kraftwerken, Telekommunikationseinrichtungen und Stadtwerken, besondere Anforderungen an den Betreiber?
   a) Falls ja, welche staatliche Stelle, beaufsichtigt die Einhaltung dieser Anforderungen im privaten Sektor?
   b) Wie viele Angriffe auf kritische Infrastrukturen verzeichnete der Freistaat Bayern jeweils in den Jahren 2011, 2012, 2013 und 2014 (bitte Aufschlüsselung nach Sektor)?

Antwort

des Staatsministeriums der Finanzen, für Landesentwicklung und Heimat
vom 06.11.2014

1. Besteht die Möglichkeit, für einen Mailserver der Bayerischen Polizei oder andere Teile des Behördennetzwerks mit einer über einen einzelnen Rechner durchgeführten DOS-Attacke eine Nichterreichbarkeit herbeizuführen?
a) Falls ja, werden bereits weitere Schritte geplant, um diesem Risiko entgegenzuwirken?
b) Falls nein, wie rechtfertigt die Staatsregierung in diesem Fall den Einsatz des LKA und die Beschlagnahme zahlreicher Gegenstände des Beschuldigten?

Die aus dem Internet erreichbaren zentralen IT-Systeme des Bayerischen Behördennetzes und der Bayerischen Polizei inkl. der Mailserver sind bestmöglich geschützt. Zur Überprüfung der aktuellen Sicherheitsvorkehrungen finden unter anderem regelmäßige extern beauftragte Penetrationstest statt. Darüber hinaus dienen sogenannte Audits gemäß BSI-Grundschutz der regelmäßigen Überprüfung zur Umsetzung und Einhaltung von bestehenden Sicherheitsregularien.

Unabhängig vom etwaigen Erfolg einer Attacke werden verfolgungsrelevante Angriffe auch beim Versuch zur Anzeige gebracht.

2. Bei welcher Behörde ist das sog. Computer Emergency Response Team angesiedelt und wie ist es in behördenübergreifende Prozesse eingebunden?
a) Über wie viele Planstellen verfügt das Computer Emergency Response Team?
b) Beauftragt das Computer Emergency Response Team auch private Dienstleister?

Das Computer Emergency Response Team (CERT) befindet sich im Landesamt für Finanzen. Es ist aktuell mit 7 Planstellen ausgestattet. Im nächsten Doppelhaushalt 2015/16 sollen weitere 5 Planstellen ausgebracht werden. Aufgaben und Einbindung in die bayerische Staatsverwaltung sind der „Richtlinie zur IT-Sicherheitsorganisation der bayerischen Staatsverwaltung (BayITSiR-O)“ zu entnehmen (http://connect.juris.bybn.de/jportal/?quelle=connect&linked=t&docId=VVBY-VVBY000040414&uid=bystin). Private Dienstleister werden bedarfsweise beauftragt, müssen allerdings eine BSI-Zertifizierung nachweisen.

3. Welche EDV- und Kommunikationsdienstleistungen, die früher an private Auftragnehmer vergeben wurden, werden mittlerweile wieder intern bei staatlichen Stellen durchgeführt (bitte Auflistung nach Tätigkeitszuschnitt und übergeordneten Behörden)?

Der Freistaat Bayern hat in der Vergangenheit selten vom klassischen Outsourcing Gebrauch gemacht. Vergaben an Externe kommen in erster Linie für Unterstützungsaufgaben in unkritischen Bereichen in Betracht.

4. Wie gestaltet sich die Zusammenarbeit des Computer Emergency Response Team mit dem Cyber-Allianz-Zentrum Bayern?

Das Cyber-Allianz-Zentrum Bayern beim BayLfV steht im ständigen Kontakt mit Vertretern des Bayern-CERT (z. B. vierteljährlicher Informationsaustausch). Hiervon unabhängig werden Warnmeldungen des Cyber-Allianz-Zentrums dem Bayern-CERT zeitnah zur Verfügung gestellt und umgekehrt.

a) Welche weiteren öffentlichen Stellen sind im Rahmen ihres Auftragszuschnitts mit der Datensicherheit in Bayern betraut?

Grundsätzlich sind alle Behörden in Bayern für ihren Bereich mit Datensicherheit betraut. Dementsprechend wurden für Teilnehmer des bayerischen Behördennetzes die Rollen der BITS (Beauftragter für IT-Sicherheit in Behörden) und Ressort-BITS (zentraler Beauftragter für IT-Sicherheit) geschaffen und installiert (s. a. BayITSiR-O, Frage 2). Für die nichtöffentlichen Stellen ist das Bayerische Staatsministerium für Wirtschaft und Medien, Energie und Technologie im Rahmen seines Aufgabenzuschnitts u. a. mit dem Thema Datensicherheit betraut.

b) Wie gestaltet sich die Zusammenarbeit mit den Ermittlungsbehörden, z. B. dem LKA sowie dem Landesamt für Verfassungsschutz?

Die Zusammenarbeit zwischen dem CERT und dem LKA erfolgt analog dem grundsätzlichen Vorgehen in Fällen von IT-Angriffen auf die Bayerische Polizei:

Das CERT Bayern meldet detektierte Angriffe auf polizeiliche IT-Systeme an das CERT der Bayerischen Polizei im BLKA. Das CERT der Bayerischen Polizei erhält vom CERT Bayern sowohl allgemeine (z. B. Heartbleed, Shellshock) als auch anlassbezogene Informationen (z. B. Angriffe auf den Internetauftritt der Bayerischen Polizei, auffällige Zugriffe über den URL-Filter). Die anschließende Informationssteuerung als auch die Initiierung der Bearbeitung eines Sicherheitsvorfalls erfolgt gemäß den Geschäftsprozessen des Informationssicherheitsmanagements der Bayerischen Polizei. Vom CERT der Bayerischen Polizei im BLKA wird die zuständige Verfahrenskoordination informiert.

5. Aus welchen Herkunftsländern verzeichnet die Staatsregierung die meisten Cyberangriffe (bitte Aufschlüsselung nach Angriffsart und Nation)?
a) In welchem Prozentsatz werden dabei Angriffe aus Deutschland verzeichnet?

Das BayLfV hat bereits in den letzten Verfassungsschutzberichten – zuletzt im Verfassungsschutzbericht 2013, Seite 188 ff. – auf die Länder, die aktiv (Wirtschafts-)Spionage betreiben, hingewiesen: Es handelt sich in erster Linie um die russische Föderation und die Volksrepublik China. Eine konkrete Zuordnung ist jedoch wegen der Anonymität des globalen Internets in den allerwenigsten Fällen möglich.

6. Bestehen beim Einsatz von IuK-Technik im Bereich von kritischen Infrastrukturen, z. B. Kraftwerken, Telekommunikationseinrichtungen und Stadtwerken, besondere Anforderungen an den Betreiber?
a) Falls ja, welche staatliche Stelle beaufsichtigt die Einhaltung dieser Anforderungen im privaten Sektor?
b) Wie viele Angriffe auf kritische Infrastrukturen verzeichnete der Freistaat Bayern jeweils in den Jahren 2011, 2012, 2013 und 2014 (bitte Aufschlüsselung nach Sektor)?

Sofern kritische Infrastrukturen in Fragen der Cybersicherheit betroffen sind, sind grundsätzlich primär die jeweiligen Träger bzw. die jeweils zuständigen Fachressorts angesprochen, da diese auch die Verantwortung für die IT-Sicherheit in ihrem jeweiligen Bereich tragen.

Eine Meldepflicht für elektronische Angriffe auf kritische Infrastrukturen ist derzeit gesetzlich nicht geregelt. Das gewünschte Datenmaterial liegt daher nicht vor. Der Entwurf des IT-Sicherheitsgesetzes (IT-SiG) des Bundes, der sich aktuell auf Bundesebene in der Ressortabstimmung befindet, sieht künftig Regelungen für eine Meldepflicht von Angriffen auf kritische Infrastrukturen vor.