Landtag Brandenburg **Drucksache 6/00000**
6. Wahlperiode

Antwort
der Landesregierung

auf die Kleine Anfrage Nr. 3321
des Abgeordneten Thomas Jung (AfD-Fraktion)
Drucksache 6/8152

Internetsicherheit im Land Brandenburg

Namens der Landesregierung beantwortet der Minister des Innern und für Kommunales die Kleine Anfrage wie folgt:

Vorbemerkungen des Fragestellers
Die Zahl der Angriffe aus dem Internet steigt rapide an. Ob Algorithmen eines Angreifers Daten manipulieren oder Spam-Angriffe auf Großrechner den Polizeifunk lahmlegen: Die Gefahren aus dem Netz erfordern von der Brandenburger Landesregierung eine klare Gegenreaktion in Form eines IT-Sicherheitskonzeptes und einer stringenten Umsetzung hiervon. Das Bundesland Bayern reagierte zwischenzeitlich mit der Errichtung eines neuen Landesamtes für Sicherheit in der Informationstechnik (LSI) und ergänzt so seine Anti-Hacker-Einheit. Auf Bundesebene existiert schon seit längerem das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das neue LSI in Bayern sichert die zentralen Server des Freistaats und die Datenleitungen, über die alle Behörden miteinander kommunizieren. Ein Profiling-Team soll künftig neue Bedrohungen analysieren und Gegenmaßnahmen entwickeln, ein Beraterteam alle bayerischen Behörden bei der Etablierung und Weiterentwicklung von IT-Sicherheitskonzepten begleiten. Bis zum Jahr 2020 sollen alle kommunalen Bereiche miteinander vernetzt sein und die Zahl der IT-Fachleute auf rund 200 anwachsen. 60 Millionen Euro sollen investiert werden.

1: Wie viele internetbasierte Attacken auf öffentliche und auf private Einrichtungen gab es in den letzten fünf Jahren in Brandenburg (bitte nach Jahr aufschlüsseln)?

2:
Welcher finanzielle Schaden entstand im öffentlichen und im privaten Bereich dadurch?

zu den Fragen 1 und 2:
Die Fragen 1 und 2 werden auf Grund des Sachzusammenhanges gemeinsam beantwortet.

Für den Bereich innerhalb der Landesverwaltung werden nur die Sicherheitsvorfälle registriert, die nicht durch automatische Filter-Prozesse (per Virenscanner, SPAM-Filter etc.) abgewehrt werden konnten. Gezählt wurden in

Eingegangen: tt.mm.jjjj / Ausgegeben: tt.mm.jjjj

2013 26 Sicherheitsvorfälle,
2014 96 Sicherheitsvorfälle,
2015 40 Sicherheitsvorfälle,
2016 75 Sicherheitsvorfälle und
2017 85 Sicherheitsvorfälle.

Mögliche finanzielle Schäden durch Angriffe aus dem Internet auf die EDV-Systeme der Landesverwaltung werden nicht gesondert erfasst. Die dadurch verursachten Störungen werden in der Landesverwaltung mit den vorhandenen Mitteln abgedeckt.

Eine Vernetzung des kommunalen Bereichs ist im Aufbau und wird derzeit unter der Begrifflichkeit „Landesverwaltungsnetz (LVN) Kommunal“ subsummiert und durch den ZIT-BB betrieben. Für den kommunalen Bereich liegen der Landesregierung bisher keine Angaben zu Sicherheitsvorfällen vor. Zu dem wird eine entsprechende Passage zur Meldung von Sicherheitsvorfällen durch Kommunen an das Landes-CERT (Computer-Notfallteam in der Landesverwaltung) in den Entwurf des neuen brandenburgischen E-Government-Gesetzes aufgenommen.

Die Beantwortung der Fragen 1 und 2 in Bezug zu finanziellen Schäden im privaten Bereich kann nur auf der Grundlage der bundeseinheitlich geführten Polizeilichen Kriminalstatistik (PKS) erfolgen. Die Erfassung erfolgt auf Grundlage eines bundeseinheitlichen Straftatenschlüssels, fallseitig ergänzt um weitere Informationen zur Tat wie z. B. Tatbegehungsweisen, Tatörtlichkeiten, erstrebtes erlangtes Gut etc. Die Veröffentlichung von Daten des laufenden Jahres soll nach einer Übereinkunft der Innenministerkonferenz gänzlich unterbleiben, weil diese Daten bis zur Veröffentlichung im Folgejahr noch Veränderungen unterworfen sein können. Insofern sind auch die Angaben für das Jahr 2017 unter Vorbehalt und als nicht abschließend zu betrachten.

Die in den Fragestellungen aufgeworfenen Begrifflichkeiten der „öffentlichen“ und „privaten“ Einrichtungen sind nicht in der PKS hinterlegt. Auch der Begriff der „Internetattacke“ ist nicht eindeutig definiert. Aus diesen Gründen können die Fragen 1 und 2 im Sinne der Fragestellung so nicht beantwortet werden.

Die allgemeine Entwicklung der Cybercrime/Internetkriminalität stellt sich im 5-Jahres-Vergleich wie folgt dar:

Cybercrime im engeren Sinne[1]	**Entwicklung in den Jahren**				
	2013	**2014**	**2015**	**2016**	**2017**
erfasste Fälle (insgesamt)	1.274	952	837	756	**528**
Aufklärungsquote (AQ) in %	33,4	37,5	49,2	47,5	**50,9**
Tatverdächtige (insgesamt)	390	307	368	345	**258**

[1] Cybercrime (im engeren Sinne) umfasst die Delikte „Computerbetrug“, „Missbräuchliche Nutzung von Telekommunikationsdiensten, „Fälschung beweiserheblicher Daten“, „Datenveränderung, Computersabotage“ sowie „Ausspähen von Daten“. Diese Delikte sind Bestandteil des Summenschlüssels für Computerkriminalität.

Internetkriminalität (Tatmittel Internet[2])	Entwicklung in den Jahren				
	2013	2014	2015	2016	2017
erfasste Fälle (insgesamt)	9.790	9,434	7.817	7.291	**7.214**
Aufklärungsquote (AQ) in %	82,8	85,4	84,1	80,0	**83,4**
Tatverdächtige (insgesamt)	4.252	4.400	4.509	4.225	**4.273**

Schadensfälle[3]	Entwicklung in den Jahren				
	2013	2014	2015	2016	2017
Schadensfälle (gesamt)	207	225	310	313	**192**
Schaden in EUR	289.176	239.456	229.927	217.019	**172.866**
Schaden pro Fall	1.397	1.064	742	693	**900**

3:
Wie viele IT-Fachleute hat die Brandenburger Polizei in den letzten fünf Jahren zur Bekämpfung der Internetkriminalität eingestellt und wie viele arbeiten in diesem Sektor?

zu Frage 3:
In den letzten fünf Jahren wurden neun IT-Fachleute zur Bekämpfung der Internetkriminalität eingestellt. Derzeit sind 53 Bedienstete ausschließlich mit der Verfolgung von Internetkriminalität beschäftigt. Darüber hinaus gibt es weitere Bedienstete auf Ebene der Kriminalpolizei der Polizeidirektionen und der Kriminalkommissariate in den Polizeiinspektionen, die neben anderen Aufgaben auch im Bereich der Internetkriminalität-Bekämpfung tätig sind.

4:
Wie werden derzeit im Land Brandenburg die Kernaufgaben des Schutzes und der Gefahrenabwehr der staatlichen IT-Infrastruktur sichergestellt?

zu Frage 4:
Die Grundzüge der Gefahrenabwehr von Angriffen aus dem Internet wurden bereits in der Antwort zur Kleinen Anfrage Nr. 1996 der Abgeordneten Christina Schade (Fraktion der AfD) in Frage 1 skizziert (Landtagsdrucksache 6/4808).

[2] Tatmittel Internet umfasst alle Delikte, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird. Hier kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits Tatbestände erfüllen als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird.
[3] Bei Cybercrime im engeren Sinne werden Schäden nur bei den Delikten Computerbetrug und Missbräuchliche Nutzung von Telekommunikationsdiensten registriert.

Dazu wird entsprechend den Regelungen der Informationssicherheitsleitlinie des Landes Brandenburg die IT-Infrastruktur der Landesverwaltung gemäß den Vorgaben zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) betrieben; soweit höherer Schutzbedarf besteht, wird dieser durch gesonderte Maßnahmen sichergestellt. Das durch den Brandenburgischen IT-Dienstleister (ZIT-BB) betriebene CERT-Brandenburg sorgt zudem für den Schutz der Infrastruktur und bei Bedarf für schnelle Reaktion auf Angriffe aus dem Internet.

Für den Bereich Verfassungsschutz beschränken sich die durch Gesetz der Verfassungsschutzbehörde Brandenburg zugewiesenen Aufgaben im Bereich des Schutzes und der Gefahrenabwehr der staatlichen IT-Infrastruktur auf die Abwehr elektronischer Angriffe, welche erkennbar oder vermutet einem nachrichtendienstlich gesteuerten Hintergrund im Auftrag bzw. Interessen eines fremden Staates zugeordnet werden können. Eine entsprechende Sensibilisierung der zuständigen Bereiche der staatlichen IT-Infrastruktur gehört im Vorfeld dazu.

5:
Gibt es - wie in Bayern - im Land Brandenburg konkrete Pläne für den Aufbau eines Landesamtes für Sicherheit in der Informationstechnik, ein Profiling-Team für Gefahrenanalysen oder ein Beraterteam für die Brandenburger Behörden beim Aufbau einer Sicherheitsstruktur?

Zu Frage 5:
Nein. Für das Land Brandenburg gibt es keine konkreten Pläne für den Aufbau eines Landesamtes für Sicherheit in der Informationstechnik. Die operative Leitstelle für die behördliche IT-Sicherheit im Land Brandenburg ist, wie schon in der Antwort auf Frage 4 dargestellt, das Landes-CERT beim ZIT-BB, dessen strategische Steuerung dem MIK obliegt.

Es wurde allerdings begonnen, die Zusammenarbeit zwischen dem MIK und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu institutionalisieren. Insbesondere wird derzeit eine Zusammenarbeit zwischen dem BSI und dem MIK in den Themengebieten Informationsaustausch, Beratung und technische Unterstützung abgestimmt.

Darüber hinaus bearbeiten weitere IT-Experten im ZIT-BB entsprechende Fachaufgaben im Zusammenhang mit der Vorsorge gegen Schadsoftware, Virenschutz, Backup und Notfallvorsorge. Zudem unterstützt der ZIT-BB entsprechend seinem Servicekatalog die brandenburgischen Behörden bei der Erstellung von IT-Sicherheitskonzepten und stellt entsprechende Schulungsangebote bereit.

Auf strategischer Ebene wird derzeit im MIK ein Kooperationsmodell aus behördlicher IT-Sicherheit mit der Cybersicherheit (der IT-Sicherheit außerhalb der brandenburgischen Verwaltung) beraten. Damit soll ein übergreifendes Lagebild im Land Brandenburg ermöglicht werden, welches die Aspekte der internen IT-Sicherheit in der Verwaltung des Landes Brandenburg mit den Aspekten der Cybersicherheit außerhalb der brandenburgischen Verwaltung (Kritische Infrastrukturen der Wirtschaft, Internetkriminalität, Wirtschaftsschutz) miteinander verbindet.

Zusätzlich arbeitet das Land Brandenburg schon jetzt im Rahmen des Verwaltungs-CERT-

Verbundes mit den anderen Bundesländern und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eng zusammen, um auch über Verwaltungsgrenzen hinweg den Informationsaustausch zu Sicherheitsvorfällen sicherzustellen.