Landtag Brandenburg **Drucksache 6/8681**
6. Wahlperiode

Antwort
der Landesregierung

auf die Kleine Anfrage Nr. 3448
der Abgeordneten Steeven Bretz (CDU-Fraktion) und Björn Lakenmacher (CDU-Fraktion)
Drucksache 6/8458

Sicherheitsvorkehrungen für die Informations- und Kommunikationstechnik der (IKT) Verwaltungen im Land

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

Vorbemerkungen der Fragesteller: Im Jahr 2017 erreichte die Zahl der weltweit registrierten Software-Sicherheitslücken nach Untersuchungen des Potsdamer Hasso Plattner Instituts (HPI) mit 11.000 Meldungen einen neuen Höchststand. Damit stieg die Zahl innerhalb eines Jahres um 3.000 Vorfälle. Im Zuge der Veröffentlichung der Zahlen mahnte der Direktor des HPI Christoph Meinel die Politik an, Computerhersteller rechtlich zu verpflichten, grundlegende Sicherheitsstandards für Hard- und Software einzuhalten. Ereignisse wie der Hack des Bundestagsnetzes oder aktuell der Angriff auf die Netze der Bundesregierung zeigen, dass auch die Verwaltung in Deutschland teilweise unzureichend auf digitale Angriffe vorbereitet ist. Gleichzeitig kündigte die Stadtverwaltung Potsdam im Oktober 2017 an, ein neues Online-Portal für Bürgerinnen und Bürger zu schaffen und somit mehr Verwaltungsvorgänge ins Internet auslagern zu können. So sollen Anträge für Personalausweise, Kitaplätze oder eine KfZ-Zulassung künftig online gestellt werden können. Der Austausch von teilweise sensiblen Daten erfolgt dann also auf digitalem Wege und muss entsprechend abgesichert sein.

Vorbemerkungen der Landesregierung: Einige Fragen haben einen kommunalen Bezug, deren Beantwortung nicht in die Zuständigkeit der Landesregierung fällt. In diesem Zusammenhang wird auf das Urteil vom 15.04.2011, S-Nr.: 3096, VfGBbg: 45/09 des Verfassungsgerichtes Brandenburg verwiesen:
Zitat:
„Eine eigenverantwortliche Aufgabenerledigung setzt eine organisatorische Gestaltungsbefugnis voraus; eine gewisse Organisationsfreiheit ist deshalb notwendige Grundlage der Selbstverwaltung. Daher verpflichtet Art. 97 LV den Gesetzgeber, bei der Ausgestaltung des Kommunalrechts den Gemeinden eine Mitverantwortung für die organisatorische Gewährleistung ihrer Aufgaben einzuräumen. Den Gemeinden haben nicht nur nennenswerte organisatorische Befugnisse zu verbleiben. Es hat ihnen auch bei der Wahrnehmung der je einzelnen Aufgabenbereiche ein hinreichender organisatorischer Spielraum offengehalten zu werden, damit sie selbst noch auf die besonderen Anforderungen am Ort durch eigene Maßnahmen reagieren können (vgl. BVerfGE 91, 228, 241 sowie Bundesverfassungsgericht [BVerfG], Beschluss vom 13. März 2000“.

Eingegangen: 25.04.2018 / Ausgegeben: 30.04.2018

1. Wie schätzt die Landesregierung aktuell die IKT-Sicherheit der Landes- sowie der Kommunalverwaltungen ein?

zu Frage 1: Die Landesregierung schätzt die IKT-Sicherheit der Landesverwaltung - auch im Vergleich mit den anderen Ländern auf Grund der entsprechenden Erhebungen im IT-Planungsrat - als angemessen ein. Die zentralen IT-Komponenten und damit die zentralen Sicherheitsthemen werden im zentralen IT-Dienstleister (ZIT-BB) bearbeitet. Beispielsweise wurde im Rahmen einer Auditierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) der Untersuchungsgegenstand „Netzübergang vom ‚Verbindungsnetz NdB' zum Landesnetz Brandenburg" auf Basis des IT-Grundschutzes erfolgreich im Januar diesen Jahres zertifiziert. Für den kommunalen Bereich liegen der Landesregierung keine Angaben zu Sicherheitsvorfällen vor. Es wird auf die Vorbemerkungen verwiesen.

2. Wann wurde die IT-Standardisierungsrichtlinie zuletzt beschlossen und wird diese gegenwärtig überarbeitet?

zu Frage 2: Die Richtlinie über die Anwendung der IT-Strategie und von IT-Standards in der Landesverwaltung Brandenburg **(**IT-Standardisierungsrichtlinie) wurde am 15.6.2004 beschlossen und gilt unverändert fort. Die Anlage 2 der Richtlinie, welche die IT-Standards des Landes beinhaltet, wurde zuletzt am 15.2.2017 fortgeschrieben. Gegenwärtig wird die nächste Fortschreibung vorbereitet.

3. Wann wurde die IT-Sicherheitsleitlinie der Landesverwaltung zuletzt beschlossen und wird diese gegenwärtig überarbeitet?

zu Frage 3: Die letzte Fassung der Informationssicherheitsleitlinie für Brandenburg wurde 2014 beschlossen. Im Zuge einer Veränderung der Gremienstruktur durch die im Raume stehende E-Government-Gesetzgebung ist eine Überarbeitung vorgesehen.

4. Inwiefern sind im Rahmen der Weiterentwicklung der IT-Strategie des Landes Brandenburg Verbesserungen/Veränderungen im Bereich der Sicherheitsmaßnahmen geplant?

zu Frage 4: In der IT-Standardisierungsrichtlinie sind in den zwei Anlagen die Strategie und die Methode der Umsetzung der IT-Standardisierung in der Landesverwaltung Brandenburg festgelegt. Dabei gibt die Anlage „IT-Strategie" den Rahmen für IT-Sicherheitsmaßnahmen vor. Die im kurzen Zyklus fortzuschreibende Anlage „IT-Standards" wird dann weiterhin konkrete Aussagen in den Bereichen IT-Sicherheitskonzeption, Firewall, Virenschutz und Verschlüsselung/Elektronische Signatur enthalten. Wegen der jüngeren Sicherheitsvorfälle im Bund (Bundestag 2015 und aktuell um das Netz der Bundesregierung) wird zudem die Angriffsabwehr im Landesverwaltungsnetz durch neue Elemente im Rahmen einer neuen mehrdimensionalen IT-Sicherheitsstrategie „New-Security-Cubus" (neuer Sicherheits-Würfel) verstärkt (z. B. Einsatz von Ablenkungssystemen - sogenannten „HoneyPots"). Darüber hinaus wird die Internetsicherheit der Landesverwaltung durch Einsatz neuer Sicherheitsstandards erhöht. So wurde eine Umstellung der Internetadressauflösung (Domain Name System - DNS) auf eine kryptografisch gesicherte Variante (Domain Name System Security Extensions - DNSSEC) vorgenommen, um Benutzer vor der Umleitung zu betrügerischen Websites zu schützen. Auch können DNS-basierende Verfügbarkeitsattacken - sogenannten „Distribu-

ted Denial of Service“ - Angriffe (DDoS) oder auch Adressdiebstähle minimiert werden. DNSSEC dient zudem als eigener Sicherheitsanker für weitere Internetdienste (z. B. DNS-based Authentication of Named Entities - DANE. Es wird angestrebt, derartige Sicherheitskomponenten in die IT-Standards aufzunehmen.

5. Welche Vorkehrungen treffen die Verwaltungen des Landes und der Kommunen, um Hacker-Angriffe auf ihre IKT-Infrastruktur zu verhindern?

zu Frage 5: Für die Landesverwaltung wird zunächst auf die Antwort zu Frage 4 der Kleinen Anfrage 3321 (Drucksache 6/8152) - verwiesen. Die IKT-Infrastruktur der Landesverwaltung wird überwiegend durch den zentralen Brandenburgischen IT-Dienstleister (ZIT-BB) betrieben. Dieser sorgt mit umfangreichen Sicherungsmaßnahmen gem. BSI-Grundschutz dafür, dass Angriffe abgewehrt werden. Beispiele für Vorkehrungen sind:

- die mehrstufige Filterung auf bekannten Schadcodes (Virenschutz),
- die Abschottung der Landesnetze und Überwachung der Netzübergänge,
- die Etablierung eines Teams von Sicherheitsexperten, die Sicherheitsvorfälle und Schwachstellen behandeln (CERT),
- die konsequente Umsetzung landesweit abgestimmter Sicherheitsrichtlinien,
- die regelmäßige Sensibilisierung und Schulung der Mitarbeiter.

Für den kommunalen Bereich liegen der Landesregierung keine Angaben zu Sicherheitsvorkehrungen vor. Es wird auf die Vorbemerkungen verwiesen.

6. Der Angriff auf das Netz der Bundesregierung war offenbar Teil einer weltweiten Kampagne. Inwieweit war das Computernetzwerk von Brandenburger Landesbehörden von diesem konzertierten Hack ebenfalls betroffen?

zu Frage 6: Nach aktuellem Kenntnisstand konnte eine Betroffenheit nicht festgestellt werden.

7. Inwieweit hat die Landesregierung Einfluss auf die digitalen Sicherheitsstandards der kommunalen Verwaltungen? Welche Maßnahmen werden Seitens der Landesregierung getroffen, um die Sicherheit der IKT auf der kommunalen Ebene zu erhöhen?

zu Frage 7: Die „Informationssicherheitsleitlinie in der öffentlichen Verwaltung“ des IT-Planungsrates (Informationssicherheitsleitlinie des IT-Planungsrates) als auch die daraus abgeleitete landesweite brandenburgische Informationssicherheitsleitlinie stellen ausdrücklich Umsetzungsempfehlungen für die kommunalen Verwaltungen dar. Die brandenburgischen Kommunalverwaltungen werden landesseitig durch eine Netzwerkanbindung an das Landesverwaltungsnetz (LVN-Kommunal) unterstützt. Im Rahmen des LVN-Kommunal partizipieren die Kommunen von den zentralen Sicherheitsmaßnahmen der Landesverwaltung.

8. Wie stellt sich aus Sicht der Landesregierung die IKT-Sicherheitsarchitektur in der Stadtverwaltung Potsdam dar?

zu Frage 8: Unter Verweis auf die Antworten zu den Fragen 1, 5 und 7 ist eine entsprechende Einschätzung auf die IKT-Sicherheitsarchitektur der Stadt Potsdam nicht möglich. Es wird im Übrigen auf die Vorbemerkungen verwiesen.

9. Inwieweit kooperieren die Landesregierung und die Landeshauptstadt hinsichtlich der IKT-Sicherheitsvorkehrungen der in Potsdam ansässigen Landesverwaltungen und der kommunalen Behörden (Software, Informationsaustausch, Meldewesen, Mitarbeiterfortbildung etc.)?

zu Frage 9: Zwischen der Landesregierung und der Landeshauptstadt gibt es keine direkte institutionalisierte Kooperation im Themengebiet IKT-Sicherheit. Der ZIT-BB tritt jedoch als Auftragsbetreiber kommunaler Anwendungen (z. B. internetbasierende KFZ-Zulassung - iKFZ) auf. Ferner kooperiert Brandenburg in der Arbeitsgruppe Informationssicherheit (AG-InfoSic) des IT-Planungsrates mit allen Ländervertretern, den Vertretern des Bundes und dem Vertreter des Deutschen Landkreistages bzw. des Städtetages. Im Rahmen des „LVN-Kommunal“ (Fachnetz, das die Kommunen an das Landesverwaltungsnetz anbindet und durch den ZIT-BB betrieben wird) stellt das CERT-Brandenburg Sicherheitsinformationen für alle angeschlossenen Teilnehmer - also auch den angeschlossenen Kommunalverwaltungen - zur Verfügung. Zudem unterstützt der ZIT-BB entsprechend seinem Servicekatalog auch die kommunalen Verwaltungen zur Erhöhung der IT-Sicherheit und stellt entsprechende Schulungs- und Sensibilisierungsangebote bereit.

10. Gab es jeweils in den Jahren 2013 bis 2018 Auffälligkeiten in Zusammenhang mit der IKT-Sicherheit beziehungsweise Angriffe auf die IKT-Infrastruktur der Verwaltung des Landes oder der Kommunen insbesondere der Stadt Potsdam? (Bitte nach Jahren, Intensität und Quelle aufschlüsseln)

zu Frage 10: Die Anzahl der Sicherheitsvorfälle 2013-2017 nach Jahren für die Landesverwaltung wurde bereits in der Antwort der Landesregierung zur Kleinen Anfrage Nr. 3321 (Drucksache 6/8152) aufgeschlüsselt. Die Daten wurden nachfolgend um das Jahr 2018 (Stichtag 31.3.) ergänzt. Bezüglich der Intensität kann nach Betroffenheit in einem Endplatzsystem bzw. nach Betroffenheit mehrerer Endplatzsysteme oder in die Betroffenheit zentraler IT-Dienste unterschieden werden. Als Quelle der Erkennung der Sicherheitsvorfälle kommen
a) eigene CERT-Systeme,
b) Meldungen von Betroffenen oder
c) Meldungen externer CERTs und anderer Sicherheitsbehörden
in Betracht.

Im Einzelnen:

- 2013: 26 Sicherheitsvorfälle, davon 3 Fälle mit Betroffenheit mehrerer Endplatzsystems oder zentraler IT-Dienste (Quelle a und b)),
- 2014: 96 Sicherheitsvorfälle, davon 6 Fälle mit Betroffenheit mehrerer Endplatzsystems oder zentraler IT-Dienste (Quelle a, b und c),
- 2015: 40 Sicherheitsvorfälle, davon 4 Fälle mit Betroffenheit mehrerer Endplatzsystems oder zentraler IT-Dienste (Quelle a, b und c)),
- 2016: 75 Sicherheitsvorfälle, davon 7 Fälle mit Betroffenheit mehrerer Endplatzsysteme oder zentraler IT-Dienste (Quelle a und b),
- 2017: 85 Sicherheitsvorfälle, davon 1 Fall mit Betroffenheit mehrerer Endplatzsysteme oder zentraler IT-Dienste (Quelle a),
- 2018: 34 Sicherheitsvorfälle, davon 1 Fall mit Betroffenheit mehrerer Endplatzsysteme oder zentraler IT-Dienste (Quelle c).

Zu Auffälligkeiten in Zusammenhang mit der IKT-Sicherheit beziehungsweise zu Angriffen auf die IKT-Infrastruktur der Kommunen insbesondere der Stadt Potsdam liegen keine Erkenntnisse vor. Das Kommunalverfassungsrecht sieht eine Verpflichtung zur Anzeige entsprechender Auffälligkeiten oder von Angriffen nicht vor.

11. Inwieweit entsprechen die Sicherheitsvorkehrungen für die IKT der Landesregierung und der Kommunen dem bundesweiten Standard?

zu Frage 11: „Bundesweiter Standard“ ist entsprechend der IT-Sicherheitsleitlinie des IT-Planungsrates als auch der landesweiten brandenburgischen IT-Sicherheitsleitlinie der „IT-Grundschutz nach BSI“. Die Landesbehörden sind zur Umsetzung der IT-Sicherheitslinie verpflichtet. Für die Kommunen geben o. g. Leitlinien eine entsprechende Empfehlung zur Anwendung des IT-Grundschutzes nach BSI vor. Für den kommunalen Bereich liegen der Landesregierung keine Angaben zu den Umsetzungen o. g. Empfehlungen vor. Es wird im Übrigen auf die Vorbemerkungen verwiesen.

12. Plant die Landesregierung ein gemeinsames IKT-Sicherheitscluster Brandenburg-Berlin, um den Sicherheitsinteressen beider Bundesländer besser gerecht zu werden?

zu Frage 12: Nein, derzeit gibt es keine Planungen der Landesregierung für ein gemeinsames IKT-Sicherheitscluster Brandenburg-Berlin.

13. Scheint aus Sicht der Landesregierung ein gemeinsames Landesamt für IKT-Sicherheit Brandenburg-Berlin sinnvoll?

zu Frage 13: Der Meinungsprozess der Landesregierung, in wie weit ein gemeinsames Landesamt für IKT-Sicherheit Brandenburg-Berlin sinnvoll zu sein scheint, ist nicht abgeschlossen. Wie schon in der Kleinen Anfrage Nr. 3321 (Drucksache 6/8152) - dort zur Frage 5 dargestellt, gibt es in Brandenburg keine Pläne zum Aufbau eines Landesamtes für IT-Sicherheit - auch nicht für ein gemeinsames Landesamt für IKT-Sicherheit Berlin - Brandenburg. Vielmehr 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) zusammen, um auch über Verwaltungsgrenzen hinweg den Informationsaustausch zu Sicherheitsvorfällen sicherzustellen. Darüber hinaus kooperiert das CERT-Brandenburg mit dem CERT-Berlin und dem CERTMecklenburg-Vorpommerns.

14. Welche (Forschungs-)Mittel stellt die Europäische Union bis zum Jahr 2020 für den Bereich der IKT-Sicherheit zur Verfügung?

zu Frage 14: Die Europäische Union stellt grundsätzlich Forschungsmittel für den Bereich der IT-Sicherheit in verschiedenen Programmen zur Verfügung. Das wichtigste und größte Programm zur Forschungsförderung ist das europäische Rahmenprogramm für Forschung und Innovation „Horizont 2020“ (2014-2020). „Horizont 2020“ beinhaltet in der 2. Säule „Industrial Leadership“ die Programmlinie „Information and Communication Technologies“. Für die gesamte Laufzeit von „Horizont 2020“ umfasst diese Programmlinie insgesamt ein Budget von rd. 5,05 Mrd. €. Da IT-Sicherheit als ein Querschnittsthema in dieser Programmlinie konzipiert und in allen Ausschreibungen adressiert werden kann, ist eine Bezifferung des konkreten Fördervolumens für diesen Themenbereich nicht möglich.