Abgeordnetenhaus BERLIN

Drucksache 18 / 26 657
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Bernd Schlömer (FDP)

vom 12. Februar 2021 (Eingang beim Abgeordnetenhaus am 15. Februar 2021)

zum Thema:

Stand und Perspektiven der IT-Sicherheit im Land Berlin

und **Antwort** vom 04. März 2021 (Eingang beim Abgeordnetenhaus am 05. Mrz. 2021)

Die Drucksachen des Abgeordnetenhauses sind bei der Kulturbuch-Verlag GmbH zu beziehen.
Hausanschrift: Sprosserweg 3, 12351 Berlin-Buckow · Postanschrift: Postfach 47 04 49, 12313 Berlin, Telefon: 6 61 84 84; Telefax: 6 61 78 28.

Senatsverwaltung für Inneres und Sport

Herrn Abgeordneten Bernd Schlömer (FDP)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18/26657
vom 12. Februar 2021
über Stand und Perspektiven der IT-Sicherheit im Land Berlin

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vor dem Hintergrund des aktuellen IT-Sicherheitsberichts frage ich den Senat:

1. Welche fachliche Stelle ist der oder die oberste IT-Sicherheitsbeauftragte (CISO) im Land Berlin?
a) Ist der oder die CISO die herausgebende Stelle des IT-Sicherheitsberichts? Wenn Nein, warum nicht?
b) In welchem Rechtsverhältnis steht diese Stelle zu dem CIO oder der IT-Staatsekretärin im Land Berlin?
c) Wie bewertet der Senat die Stellung zueinander?

Zu 1.:
Die oberste fachliche Stelle ist der Bevollmächtigte für Informationssicherheit des Landes Berlin gem. § 21 Abs. 2 Satz 4 EGovG Bln.

Zu 1a.:
Die herausgebende Stelle des Berichtes für Informationssicherheit ist die IKT-Staatssekretärin als schlusszeichnende Instanz vor der Freigabe des Berichtes. Der Bericht wird in der Verantwortung der/des Bevollmächtigten für Informationssicherheit des Landes Berlin (Landes-InfSiBe) erstellt.

Zu 1b.:
Die / der Landes-InfSiBe verfügt über ein direktes Vortragsrecht bei der IKT-Staatssekretärin. Die/Der Landes-InfSiBe übernimmt die Verantwortung für die ihr/ihm übertragenen Aufgaben gem. § 21 Abs. 2 Satz 4 EGovG Bln.

Zu 1c.:
Das direkte Vortragsrecht der/des Landes-InfSiBe entspricht dem Vorgehen nach IT-Grundschutz Standard 200-1 des BSI, wonach dem / der verantwortlichen Informationssicherheitsbeauftragen ein direktes Vortragsrecht gegenüber der Leitung der Institution zu gewähren ist.

2. Wie grenzt der Senat das Handlungsfeld IT-Sicherheit von dem Streben nach Informationssicherheit ab?

a) Welche konkreten und eigenständigen Initiativen und Maßnahmen hat der Senat im Bereich der Informationssicherheit (die nicht durch IT-Sicherheit erfasst sind) im zurückliegenden Berichtszeitraum des o.a. Berichts unternommen?

Zu 2.:
Die Abgrenzung erfolgt ganz im Sinne des BSI-Standards 200-1. Danach hat Informationssicherheit das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dabei können Informationen auf Papier, in IT-Systemen oder auch in den Köpfen der Benutzenden gespeichert sein. IT-Sicherheit als Teilmenge der Informationssicherheit konzentriert sich auf den Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.
Somit ist das Handlungsfeld der IT-Sicherheit ein Teil der gesamten Informationssicherheit. Der Senat sieht keine Trennung der Handlungsfelder vor.

Zu 2a.:
Schwerpunkte des Handelns waren neben präventiven Maßnahmen um Umfeld der IT-Nutzung in der Pandemie, die reaktive Bewältigung von Sicherheitsvorfällen, die Unterstützung der Windows 10 Umstellung, die Bereitstellung der IKT-Basisdienste für die BSI-Zertifizierung des ITDZ und den Betrieb des CERT, die Durchführung eines Projektes für die Bereitstellung eines mandantenfähigen Werkzeuges zur Unterstützung des Informationssicherheitsmanagementprozesses (ISMS-Tool) in den Einrichtungen der Berliner Verwaltung mit dem Ziel den IKT-Basisdienst für das ISMS-Tool mit landeseinheitlich zu nutzenden Bausteinen nach dem BSI-Grundschutz 2021 bereitzustellen. Mit dem ITDZ wurde unter Beteiligung der Senatsverwaltung für Inneres und Sport unter Pandemiebedingungen eine Notfallstabsübung / Sicherheitsübung durchgeführt. Im Ergebnis des Plan-Projektes wurde das Umsetzungsprojekt (Build-Projekt) für einen Basisdienst PKI (public key infrastructure) als Grundlage einer sicheren und mit Vertrauensstellung agierenden Berliner E-Government-Infrastruktur erarbeitet und beauftragt. Weiterhin wurde für die Bereitstellung komplexer Informationssicherheitsdienstleistungen durch ein Cyber-Defense-Center Landesverwaltung zur Absicherung der eGovernment Dienstleistungen des Landes mit dem ITDZ eine Absichtserklärung mit dem Ziel der Bereitstellung als IKT-Basisdienst abgeschlossen.

3. Hat sich die zugrunde liegende Version der Informationssicherheitsleitlinie des Landes Berlin seit dem letzten Bericht geändert?

a) Wenn Ja, in welchen Punkten?

b) Wenn Nein, warum nicht?

c) Wie bewertet der Senat den geringen Umsetzungsgrad der zugunde liegenden Informationssicherheitsleitlinie?

d) Was bedeutet überhaupt „Umsetzungsgrad“? Bei welchem Umsetzungsgrad kann von guter IT-Sicherheit gesprochen werden? Was sind die Kriterien?

e) Welche Behörden und/oder Stellen haben die Leitlinie nur unzureichend umgesetzt (bitte benennen)? Woraus schließt der Senat das? Welche Sanktionen drohen diesen Verwaltungseinheiten?

f) Wie wird der Senat zur Verbesserung des Umsetzungsgrades beitragen?

Zu 3.:
Die dem Bericht zugrunde liegende Version der Informationssicherheitsleitlinie des Landes Berlin hat sich seit dem letzten Bericht nicht geändert.

Zu 3a.:
Antwort entfällt.

Zu 3b.:
Dem Senat standen nicht ausreichend personelle Ressourcen zur Fortschreibung zur Verfügung.

Zu 3c.:
Die Kernaspekte der Sicherheitsstrategie werden in der Leitlinie zur Informationssicherheit dokumentiert. Die Sicherheitsleitlinie ist von zentraler Bedeutung, da sie das sichtbare Bekenntnis der Leitungsebene zu ihrer Strategie enthält. Das bedeutet im Umkehrschluss, dass der Aufbau eines ISMS in den einzelnen Behörden gem. § 23 EGovG Bln noch nicht in ausreichendem Umfang erfolgt. Der Aufbau eines ISMS ist von zentraler Bedeutung mit dem Blick auf die Umsetzung und Steuerung des Informationssicherheitsprozesses. Aus dem geringen Umsetzungsgrad kann abgeleitet werden, dass eine gewünschte Standard-Absicherung der Informationssicherheit nach BSI IT-Grundschutz Kompendium mindestens unvollständig dokumentiert ist. Eine konkrete Ableitung des Sicherheitsniveaus mit Bezug auf konkrete IT-Infrastrukturen und IT-Systeme ist aus dem Umsetzungsgrad nicht ableitbar.

Zu 3d.:
Die Bewertung des Grades der Informationssicherheit basiert auf einem einheitlichen und länderübergreifend abgestimmten und strukturierten Bewertungsschema, das durch die/den Informationssicherheitsbeauftragten der einzelnen Behörden des Landes im Zuge der jährlichen Berichtserstattung eigenverantwortlich auszufüllen ist. Der Umsetzungsgrad ergibt sich auf der Basis der abgestimmten Kriterien zur Bewertung der Informationssicherheit einheitlich und automatisiert. Für die Bewertung, wie „gut“ der Umsetzungsgrad ist, wird der zugrundeliegende prozentuale Wert genommen. Gut im Sinne einer Schulnote (2) beginnt dann ab einem prozentualen Umsetzungsgrad von 95%. Liegt der Umsetzungsgrad unter 75% kann von einem ungenügenden Umsetzungsgrad gesprochen werden (Schulnote 5). Diese Bewertung liegt dem Fragenkatalog und der Festlegung durch den IT-Planungsrat zugrunde.

Zu 3e.:
Dem o.g. Bericht liegt eine Übersichtstabelle mit allen Umsetzungsgraden der Behörden bei. Daraus sind die einzelnen Werte ersichtlich. Behörden mit einem Umsetzungs-grad im Bereich unter 75% haben die Informationssicherheitsleitlinie unzureichend umgesetzt. Um die Anzahl der Behörden die zur Beantwortung der Frage benannt werden sollen zu minimieren, benennt der Senat alle Behörden, die einen Umsetzungsgrad von mindestens 75% und mehr erreicht haben. Das sind das ITDZ Berlin (100%), das Bezirksamt Reinickendorf (78,34%), das Landesamt für Gesundheit und Soziales (82,45%), das Landes Arbeitsgericht (82,18%), der Polizeipräsident Berlin (87,29%), das Sozialgericht (86,94%), die Justiz Vollzugsanstalten (81,20%) und die Senatsverwaltung für Wirtschaft Energie und Betriebe (81,76%). Alle anderen Behörden haben diesen Wert nicht erreicht. Der Senat hat keine Sanktionsmöglichkeiten. Es wird auch nicht als sinnvoll betrachtet, insbesondere finanzielle Sanktionen auszusprechen, wenn bekannt ist, dass vor allem die finanziellen Mittel der Behörden nicht ausreichen, um die Informationssicherheitsleitlinie umzusetzen.

Zu 3f.:
Gemäß den Standards des BSI wird der landesweite Informationssicherheits-managementprozess in einem kontinuierlichen Verbesserungsprozess gesteuert. Mit Unterstützung der Bereitstellung des ISMS-Tools zur Unterstützung der Prozess-dokumentation wird den Behörden ein Arbeitsmittel nach der Methodik des BSI in Verbindung mit landesweit einheitlichen Bausteinen zur Verfügung gestellt. Die kontinuierliche Wahrnehmung der Verantwortung der Behördenleitungen wird maßgeblich mittels einer enthaltenen Reporterstellung nach objektiven Vorgaben unterstützt. Eine weitere Stärkung der Informationssicherheit wird durch die Migration der verfahrensunabhängigen IKT erreicht. Die Migration führt zu einer Reduktion mannigfaltiger IKT-Instanzen in den Behörden. Nach der Migration wird eine regelmäßige Verifizierung des Informationssicherheitsniveaus erfolgen.

4. Im Bericht heißt es weiter, dass besonders große Defizite bei den finanziellen und personellen Ressourcen sowie im Notfallmanagement zu verzeichnen sind. Kann der Senat diese Mängel spezifizieren und nach jeweiliger Behörde sowie ungefähren Umfang der zusätzlich benötigten Ressourcen aufschlüsseln?

Zu 4.:
Für den zentral zuständigen Bereich der Informationssicherheit des Landes Berlin in der Abteilung V der Senatsverwaltung für Inneres und Sport wird aktuell eine Organisationsuntersuchung zur Personalbedarfsermittlung entsprechend dem Handbuch des BMI / Bundesverwaltungsamts durchgeführt, um die adäquate Stellenausstattung zu ermitteln. Das abschließende Ergebnis der Untersuchung wird voraussichtlich im März d.J. vorliegen.
Die benannten Defizite in den Verwaltungen des Landes Berlin können nicht im Detail aufgeschlüsselt werden. Die Defizite werden anhand des Umsetzungsgrades (Gesamtergebnis) bewertet. Die Stellungnahmen der Behörden, sofern erfolgt, liegen dem Jahresbericht als Anlage bei.
Der Umsetzungsgrad wird durch folgende Fragen ermittelt: Stehen ausreichend finanzielle Ressourcen zur Verfügung, um die infrastrukturellen, organisatorischen und technischen Maßnahmen umzusetzen? Stehen ausreichend personelle Ressourcen zur Verfügung, um die infrastrukturellen, organisatorischen und technischen Maßnahmen umzusetzen? Sind die Mittel für das ISMS im Haushalt klar ausgewiesen?

5. Weiter heißt es im Bericht, dass 86,96% der Behörden angeben, im Falle eines Angriffs nicht ausreichend für einen IKT-Notfall aufgestellt zu sein. Das erscheint besonders problematisch vor dem Hintergrund des Anstiegs von Angriffen von über 26%, während die Umsetzungsrate der geltenden Regelungen um lediglich 6 % angestiegen ist.

a) Was muss hier nach Meinung des Senats geschehen, um einer Ausweitung dieser Diskrepanz vorzubeugen und die Behörden bei der Abwehr von Angriffen besser zu unterstützen?
b) Liegen dem Senat im Übrigen weitergehende Erkenntnisse zu den Angreifern vor?
c) Hat der Senat bei der Begegnung von Angriffen auf Stellen des Bundes oder anderer Länder zugegriffen?
d) Wie funktioniert der regelmäßige Austausch zu Angriffen und möglichen Angriffsvektoren mit anderen (Sicherheits-)stellen?

Zu 5a.:
Zusammenfassend betrachtet muss eine Stärkung der Informationssicherheit geleistet werden, um dem erheblichen Anstieg von Angriffen entgegenzuwirken. Die zur Verfügung stehenden Ressourcen wurden von den Berliner Behörden zu 100%

ausgeschöpft. Dies bedeutet, dass für eine Stärkung der Informationssicherheit eine Aufstockung der Ressourcen erfolgen muss.

Zu 5b.:
Dem Senat liegen keine weitergehenden Erkenntnisse zu Angreifern vor.

Zu 5c.:
Der Senat wird bei der Begegnung von Angriffen durch das Berlin-CERT unterstützt. Das Berlin-CERT befindet sich im ständigen Austausch mit den CERT der Länder und dem CERT des Bundes im Verwaltungs-CERT-Verbund und nutzt die dadurch gewonnen Informationen, um den Senat zu unterstützen.

Zu 5d.:
Im Rahmen seiner Aufgabenwahrnehmung erfolgt - neben dem Anlass bezogenen - monatlich der regelmäßige Austausch zwischen dem Bereich IKT-Sicherheit der IKT-Steuerung jeweils mit dem CERT und dem IT-Sicherheitsbeauftragten des ITDZ. Bei diesem Austausch werden unter anderem die aktuelle Lage der Informationssicherheit, neue Angriffsmethoden und Angriffsvektoren sowie von aus anderen Institutionen und Gremien wie dem BSI, dem Verwaltungs-CERT-Verbund, der Allianz für Cybersicherheit übermittelte Themen erörtert und sofern erforderlich, weitere Maßnahmen zur Absicherung der Berliner Verwaltung abgeleitet.
Zu weiteren Themen gibt es zusätzlich monatlich einen Austausch mit dem betrieblich zuständigen Bereich im ITDZ.

Berlin, den 04. März 2021

In Vertretung

Sabine Smentek
Senatsverwaltung für Inneres und Sport