Abgeordnetenhaus BERLIN

Drucksache 18 / 24 683
Schriftliche Anfrage

18. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Burkard Dregger (CDU)

vom 26. August 2020 (Eingang beim Abgeordnetenhaus am 27. August 2020)

zum Thema:
Die (digitale) Sicherheit der Kritischen Infrastruktur

und **Antwort** vom 11. September 2020 (Eingang beim Abgeordnetenhaus am 14. Sep. 2020)

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 Burkard Dregger (CDU)
über
den Präsidenten des Abgeordnetenhauses von Berlin
über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 18 / 24 683
vom 26. August 2020
über Die (digitale) Sicherheit der Kritischen Infrastruktur

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

1. Wie viele Angriffe und wie viele versuchten Angriffe auf die Kritischen Infrastrukturen Berlins oder Teile davon wurden seit dem 01.01.2016 bis zur Beantwortung der Frage in Berlin verzeichnet (erbitte gesonderte Darstellung nach Art des Angriffs, Vollendung/Versuch, Art der kritischen Infrastruktur (z. Bsp. Hackerangriff) und Jahren)?

Zu 1.:
Die nach dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) gemeldeten Betreiber von Kritischen Infrastrukturen (KRITIS) haben die Verpflichtung, bei erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen KRITIS führen können oder geführt haben, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) darüber Meldung zu erstatten (§8b Absatz 4 Ziffer 2 BSIG). Es existiert keine landesgesetzliche Regelung, die eine Meldepflicht der KRITIS-Betreiber gegenüber den Berliner Landesbehörden vorschreibt.
Das BSI hat im Rahmen seiner Zentralstellenfunktion in Angelegenheiten der IT-Sicherheit der KRITIS-Betreiber zu der Fragestellung mitgeteilt, dass keine landesspezifischen Erfassungen und Auswertungen durchgeführt werden. Valide Erkenntnisse über Angriffe im Sinne der Fragestellung liegen dem Senat nicht vor.

2. Mit welchen Bundes- und/oder Landesbehörden kooperiert das Land Berlin bei Fragen der digitalen Sicherheit der Kritischen Infrastruktur in Berlin (z. Bsp. mit dem Cyber- und Informationsraum der Bundeswehr und/oder anderen) (erbitte gesonderte Darstellung nach Kooperationspartner und betroffene Infrastruktur)?

Zu 2.:
Auf Landesebene erfolgt ein fachlicher Austausch über die digitale Sicherheit Kritischer Infrastrukturen zwischen den Senatsverwaltungen und dem Landeskriminalamt und auf Bundesebene mit dem BSI sowie dem Bundeskriminalamt. Am 13. August 2018 schloss das BSI mit dem Land Berlin eine

Absichtserklärung zur vertieften Kooperation, die unter anderem den Austausch von Mitarbeiterinnen und Mitarbeitern aus dem Bereich Schutz Kritischer Infrastrukturen im Rahmen von Hospitationen beim BSI oder umgekehrt sowie den Austausch zu Prozessen des IT-Krisenmanagements und der Prävention von Cyberangriffen umfasst.

3. Welche Kritischen Infrastrukturen oder Teile davon werden in Berlin vom Land und welche von Privaten betrieben?

Zu 3.:
Die Bestimmung der Kritischen Infrastruktur im Kontext der Sicherheit in der Informationstechnik ist durch die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) geregelt. Sie betrifft die Sektoren Energie, Wasser, Ernährung, Informations- und Telekommunikationstechnik, Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr.
Die Betreiber kritischer Infrastrukturen haben nach § 8b Absatz 1 Satz 1 BSI-Gesetz gegenüber dem BSI eine Kontaktstelle zu melden. Die sich daraus ergebende vollständige Aufstellung der KRITIS-Betreiber im Kontext der Sicherheit in der Informationstechnik im Land Berlin ist durch das BSI aus Sicherheitsgründen eingestuft und kann vom Senat ohne das Einverständnis des BSI nicht nach außen gegeben werden. Dabei ist zu beachten, dass das parlamentarische Kontrollrecht insofern vom Deutschen Bundestag ausgeübt wird. Der Senat hat gleichwohl Kontakt mit dem BSI aufgenommen, sodass dem Fragesteller mit Einverständnis des BSI im Geheimschutzraum des Abgeordnetenhauses Einsicht in die vollständige Liste gewährt werden kann.
Einige offenkundige Landesbetriebe und Unternehmen, die in Berlin KRITIS betreiben, können gleichwohl genannt werden:
Landesbetriebe, die in Berlin KRITIS betreiben:

- Charité Universitätsmedizin Berlin
- Vivantes - Netzwerk für Gesundheit GmbH
- Berliner Verkehrsbetriebe (BVG) Anstalt des öffentlichen Rechts
- Berliner Wasserbetriebe Anstalt des öffentlichen Rechts
- Berliner Flughafen-Gesellschaft mbH, Tochter der Flughafen Berlin Brandenburg GmbH
- Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr
- Betrieb der Tunnel- und Verkehrstechnik der Bundesautobahn in Berlin sowie des Tunnels Tiergarten Spreebogen.

Unternehmen, die in Berlin KRITIS betreiben:

- Vattenfall Europe Sales GmbH (Vattenfall)
- Stromnetz Berlin GmbH (Stromnetz Berlin)
- Netzgesellschaft Berlin-Brandenburg mbH & Co. KG (NBB)

4. Zu welchen Kritischen Infrastrukturen wurden seit dem 01.01.2016 Gutachten oder Stellungnahmen betreffend potentielle Sicherheitsrisiken, insbesondere hinsichtlich der digitalen Infrastruktur mit welchen Ergebnissen erstellt und wer hat auf Seiten des Senats von diesen Gutachten jeweils wann Kenntnis erlangt?

Zu 4.:
Charité Universitätsmedizin Berlin:
Die digitale Infrastruktur der Charité wurde vom 17.06.2019 bis zum 21.06.2019 nach § 8a Absatz 1 Satz 1 BSIG geprüft.

Vivantes - Netzwerk für Gesundheit GmbH:
Durch die aktive Mitarbeit im Branchenarbeitskreis Medizinische Versorgung im Umsetzungsplan KRITIS und in verschiedenen Fach- und Arbeitsgruppen der Deutschen Krankenhausgesellschaft (DKG) und dem BSI hat sich Vivantes bereits frühzeitig bei der Festlegung geeigneter Anforderungen für technische und organisatorische Sicherheitsmaßnahmen in Krankenhäusern engagiert und die Entwicklung eines geeigneten branchenspezifischen Sicherheitsstandards gemäß § 8a Absatz 2 des BSI-Gesetzes zur Gewährleistung dieser Anforderungen mit gestaltet. Das BSI hat den im Juni 2019 von der DKG vorgelegten „Branchenspezifischen Sicherheitsstandard für Krankenhäuser“ („B3S“) geprüft und im Oktober 2019 die Eignung festgestellt.
Im Juni 2019 erbrachte Vivantes gemäß § 8a Absatz 1 des BSI-Gesetzes erstmalig den Nachweis zur Erfüllung der Anforderungen durch ein externes Sicherheitsaudit und hat die Ergebnisse dem BSI vorgelegt. Die Prüfung hat ein für Vivantes positives, über dem Branchendurchschnitt liegendes Ergebnis gezeigt.
Der Aufsichtsrat der Vivantes – Netzwerk für Gesundheit GmbH, in dem der Senator für Finanzen und die Senatorin für Gesundheit, Pflege und Gleichstellung vertreten sind, wird über den Status halbjährlich unterrichtet.

Berliner Verkehrsbetriebe (BVG) Anstalt des öffentlichen Rechts:
Im ersten Halbjahr 2019 wurde eine Prüfung nach dem branchenspezifischen Sicherheitsstandard (B3S) des Verbandes Deutscher Verkehrsunternehmen erfolgreich durchgeführt.

Berliner Wasserbetriebe Anstalt des öffentlichen Rechts:
Es liegen Zertifizierungen nach ISO 27001 ("Sicherheitsstandard für Informationssicherheitsmanagementsysteme") sowie die Erfüllung des branchenspezifischen Sicherheitsstandards B3S nach § 8a BSIG (sog. "KRITIS-Testat") vor.

Berliner Flughafen-Gesellschaft mbH, Tochter der Flughafen Berlin Brandenburg GmbH:
Für den Flughafen Berlin-Tegel wurde eine Stellungnahme als Bewertungsergebnis für die Nachweiserbringung nach § 8a BSIG bei dem Bundesamt für Sicherheit in der Informationstechnik eingereicht.

Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr:
(Lichtsignalanlagen-Infrastruktur einschl. Verkehrsregelungszentrale)
Es wurden Penetrationstests durchgeführt. Im Ergebnis sind zehn akute, fünf mittelbare sowie zehn latente Risiken festgestellt worden. Die zuständige Abteilung VI „Verkehrsmanagement“ der Senatsverwaltung für Umwelt, Verkehr und Klimaschutz hat von den vollständigen Ergebnissen der Penetrationstests seit 27.08.2020 Kenntnis erlangt.

Betrieb der Tunnel- und Verkehrstechnik der Bundesautobahn in Berlin sowie des Tunnels Tiergarten Spreebogen:
Gemäß § 8a Absatz 3 BSIG wurde eine Prüfung durch ein zertifiziertes Unternehmen im Juni 2020 durchgeführt. Die Ergebnisse der Prüfung (Abweichungen und Empfehlungen) sowie die Hinweise wurden in einem Maßnahmenplan zusammengefasst und sollen priorisiert innerhalb von 12 Monaten abgearbeitet werden. Da die Zuständigkeit Berlins für die Bundesautobahnen und anbaufreien

Bundesstraßen zum 01.01.2021 an den Bund bzw. die bundeseigene Gesellschaft (Autobahn GmbH) übergeht, sind die Ergebnisse einschließlich Maßnahmenplan an das Bundesministerium für Verkehr und digitale Infrastruktur weitergeleitet worden.

Vattenfall Europe Sales GmbH (Vattenfall), Stromnetz Berlin GmbH (Stromnetz Berlin), Netzgesellschaft Berlin-Brandenburg mbH & Co. KG (NBB):
Gemäß § 11 Absatz 1 a und 1b Energiewirtschaftsgesetz (EnWG) sind Energieversorgungsnetzbetreiber und Betreiber Kritischer Infrastrukturanlagen dazu verpflichtet, für einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die der Netzsteuerung dienen, zu sorgen. Die Regulierungsbehörde hat im Benehmen mit dem BSI einen Katalog von IT-Sicherheitsanforderungen erstellt und veröffentlicht. Setzen Netzbetreiber und Betreiber kritischer Infrastrukturen die Anforderungen dieses Sicherheitskatalogs um, wird vermutet, dass ein sicheres Energieversorgungsnetz betrieben wird. Der Katalog enthält zudem Regelungen zur regelmäßigen Überprüfung der Erfüllung der Anforderungen.
Sowohl Stromnetz Berlin und Vattenfall als auch NBB verfügen über eine entsprechende (Re-) Zertifizierung. Die erforderlichen Zertifizierungsnachweise werden gemäß IT-Sicherheitskatalog an die Bundesnetzagentur (BNetzA) geschickt. Dem Senat liegen keine Gutachten aus den Zertifizierungsverfahren vor. Stromnetz Berlin teilt mit, dass sie zusätzlich zu der gesetzlich vorgeschriebenen Zertifizierung Mitteilungen zu Sicherheitswarnmeldungen seitens des BSI zu potentiellen Sicherheitsrisiken klassifiziert und entsprechend Kritikalität durch Schutzmaßnahmen zur Umsetzung bringt.
NBB teilt mit, dass sie zusätzlich zu den gesetzlich vorgeschriebenen Maßnahmen in 2016/2017 eine Schwachstellen-Analyse der kritischen Infrastruktur durch einen Dritten vornehmen lassen hat. Die Analyse war seitens der NBB nur für den internen Gebrauch gedacht, daher wurde das Ergebnis nicht an Externe weitergegeben.

5. Inwiefern werden die Betreiber der Kritischen Infrastrukturen seitens des Senats dabei unterstützt, potentielle Sicherheitslücken, insbesondere hinsichtlich der digitalen Infrastruktur zu beseitigen und die Versorgung der Berliner Bevölkerung mit Kritischen Infrastrukturen langfristig uneingeschränkt zu sichern?

Zu 5.:
Die Zentrale Ansprechstelle Cybercrime für die Wirtschaft (ZAC) im **Landeskriminalamt Berlin** ist die zentrale Ansprechstelle für die Wirtschaft bei der Polizei Berlin für Fragen im Hinblick auf Gefahren durch Cyberkriminalität sowie zu IT-Sicherheitsvorfällen mit mutmaßlich kriminellem Hintergrund. Aufgabe dieser Zentralstelle ist es unter anderem, Wirtschaftsunternehmen (wie Betreibern von KRITIS) im Themenfeld Cybercrime kompetent zu beraten und damit zugleich sowohl im Vorfeld von Straftaten als auch im Schadensfall eine reibungslose Zusammenarbeit sicherzustellen.

Die **Senatsverwaltung für Wirtschaft, Energie und Betriebe** steht in ihrer Funktion als Energieaufsichtsbehörde in regelmäßigem Austausch mit Netzbetreibern zu Fragen der Sicherheit der Netze und über zukünftige Investitionen zur Modernisierung und Optimierung im Netzbereich. Zudem besteht eine enge Zusammenarbeit der Katastrophenschutzbehörden untereinander sowie mit Betreibern Kritischer Infrastrukturen, um die Versorgung der Berliner Bevölkerung zu sichern.

Die **Senatsverwaltung für Umwelt, Verkehr und Klimaschutz** ist zusammen mit dem Generalübernehmer für die Lichtsignalanlagen-Infrastruktur selbst Betreiber der Kritischen Infrastruktur für das Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr. Mit einem Projektteam aus externen IT-Dienstleistern, einem externen Informationssicherheitsbeauftragten, dem Generalübernehmer für die Lichtsignalanlagen-Infrastruktur, den zuständigen Signalbaufirmen sowie eigenen Mitarbeitenden wurde der Prozess der Erbringung des Konformitätsnachweises Ende 2018 gestartet. In Abstimmung mit dem zuständigen Bundesamt wird bis Ende 2020 erstmals dieser Konformitätsnachweis hinsichtlich der Vorgaben der Ersten Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017 (BSI-KritisV) erbracht. Das Projektteam wird in diesem Zusammenhang die geplanten oder bereits durchgeführten Mitigierungsmaßnahmen aller vorgefundenen Risiken inkl. derjenigen aus den Penetrationstests darlegen.

Berliner Flughafen-Gesellschaft mbH:
Durch das Land Berlin erfolgt mittelbar eine Unterstützung zur Verbesserung des Information Security Management System (ISMS).

Senatsverwaltung für Gesundheit, Pflege und Gleichstellung:
In den Jahren 2011 und 2012 wurden im Rahmen des Projekts „Risikoanalyse Krankenhaus-IT“ (RiKrIT) ein Leitfaden und eine Methode entwickelt, mit der kritische IT-Abhängigkeiten in einem Krankenhaus und daraus erwachsende Risiken für die Patientenversorgung und weitere wichtige Prozesse identifiziert und bewertet werden können. Der Leitfaden entstand aus einer Initiative des Berliner Senats. Das Vorhaben wurde unter Federführung des BSI und mit Beteiligung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe sowie des Unfallkrankenhauses Berlin (ukb) durch Auftragnehmer aus Industrie und Wissenschaft durchgeführt. Dieser Leitfaden steht seitdem allen Krankenhäusern bundesweit als Handlungsinstrument zur Verfügung. Damit wurden die Grundlagen geschaffen, nach denen die Krankenhäuser in eigener Verantwortung eine Risikoanalyse im IT-Bereich durchführen können.
Der Senat unterstützt die landeseigenen Berliner Krankenhäuser auf verschiedenen Wegen:

- Für die Charité dient ein erheblicher Teil der Maßnahmen im IT-Bereich auch der IT-Sicherheit. Investitionen in den IT-Bereich erfolgen aus dem (allgemeinen) investiven Zuschuss sowie für verschiedene Maßnahmen als einzeln veranschlagte bauliche Maßnahmen bzw. Beschaffungen aus dem Landeshaushalt.
- Der Senat wirkt gegenüber den landeseigenen Krankenhäusern auf die Qualitätssicherung und Weiterentwicklung des Risikomanagements hin.
- Im ersten Halbjahr des Jahres 2019 wurden in zwei Berliner Krankenhäusern Cyberübungen durchgeführt, in denen die Zusammenarbeit der IT-Sicherheit mit dem Krisenmanagement geübt wurde. Die Erkenntnisse aus den Übungen werden genutzt, um den anderen Berliner Krankenhäusern Hinweise zu geben, wie Sie die Vorsorge weiter ausbauen können.

Seit der Änderung des Landeskrankenhausgesetzes (LKG) im Jahr 2015 und der Einführung der Investitionspauschale liegt die Verantwortung sowohl für die Betriebs- als auch für die Investitionskosten nunmehr in einer Hand bei den Krankenhäusern selbst. Sie agieren damit eigenverantwortlich und können flexibel entsprechend ihrer selbstgesetzten Prioritäten zeitnah notwendige Investitionen realisieren - auch für Maßnahmen der IT-Sicherheit.

Im Rahmen des Krankenhausstrukturfonds II sind unter anderem Maßnahmen zur besseren Absicherung der IT-Sicherheit für unter die KRITIS-Verordnung fallende Krankenhäuser vorgesehen. Hier beteiligt sich das Land zusätzlich zum Einsatz der Investitionspauschale mit einem Kofinanzierungsanteil von 25 % der angemeldeten Gesamtkosten.

Charité Universitätsmedizin Berlin:
Die Charité wird in 2020 und 2021 bei der Abarbeitung von Maßnahmen, die sich aus der Prüfung durch die Berliner Datenschutzbehörde ergeben haben, unterstützt. Aus diesen Mitteln werden auch zusätzlich benötigte Sicherheitsmaßnahmen für die digitale Infrastruktur finanziert.

Vivantes - Netzwerk für Gesundheit GmbH:
Über das gesetzlich geforderte Maß hinaus hat Vivantes in 2019 den Fall eines Cyberangriffs auf einen Klinikstandort im Rahmen einer Stabsrahmenübung erprobt. Diese Stabsrahmenübung erfolgte auf Initiative und mit der Unterstützung der Senatorin für Gesundheit, Pflege und Gleichstellung. Die Überprüfung der bestehenden Prozesse und organisatorischen Maßnahmen des Störfall- und Notfallmanagements konnte erfolgreich abgeschlossen werden.

6. Welche Maßnahmen und Absprachen finden hinsichtlich der Sicherstellung der Versorgung mit Kritischen Infrastrukturen zwischen den diesbezüglichen Betreibern und dem Land Berlin sowie mit anderen Landes- oder Bundesbehörden statt?

Zu 6.:
Im Rahmen ihrer Ressortverantwortung treffen die Fachressorts eigenverantwortlich Absprachen mit den in ihren jeweiligen Zuständigkeitsbereich fallenden KRITIS-Betreibern vor dem Hintergrund der jeweils geltenden Fachgesetze. Im Rahmen der Koordinierungsfunktion der Senatsverwaltung für Inneres und Sport besteht mit den maßgeblichen Betreibern kritischer Infrastrukturen sowie den Sicherheitsbehörden Polizei Berlin und Berliner Feuerwehr regelmäßiger Kontakt. In dem von der Senatsverwaltung für Inneres und Sport moderierten Arbeitskreis Infrastrukturbetreiber tauschen sich die Betreiber untereinander, aber auch mit den Sicherheitsbehörden zu verschiedensten Themen aus. In mehreren Arbeitsgruppen wurden Themen wie die Sicherstellung von Kommunikationswegen, Kenntnisse über Ressourcen und Fähigkeiten, Abstimmung der Öffentlichkeitsarbeit in Krisenlagen sowie Ausarbeitung und Durchführung gemeinsamer Übungen vertieft. Ein engmaschiger Informationsaustausch fand auch während der Corona-Lage in regelmäßigen Telefonkonferenzen unter Moderation der Senatsverwaltung für Inneres und Sport und unter Beteiligung der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung sowie der Senatsverwaltung für Wirtschaft, Energie und Betriebe statt. Betreiber kritischer Infrastrukturen werden außerdem auch bei Übungen der Berliner Feuerwehr und der Polizei Berlin beteiligt.
Überregional engagieren sich verschiedene KRITIS-Betreiber in dem UP KRITIS. Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Ziel der Kooperation UP KRITIS ist es, die Versorgung mit kritischen Infrastrukturdienstleistungen in Deutschland aufrechtzuerhalten. Die am UP KRITIS beteiligten Organisationen arbeiten auf Basis gegenseitigen Vertrauens zusammen. Sie tauschen sich untereinander aus und lernen voneinander im Hinblick auf den Schutz Kritischer Infrastrukturen. Gemeinsam kommen alle Beteiligten so zu besseren Lösungen. Die Zusammenarbeit findet in Themen- und

Branchenarbeitskreisen statt. Darüber hinaus koordiniert das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) den Schutz kritischer Infrastrukturen. Das Bundesamt erarbeitet unter anderem Leitfäden zur Identifizierung kritischer Infrastrukturen und zum Risikomanagement und steht den Behörden beratend zur Seite.

7. Welche Maßnahmen betreffend die Mitarbeitenden der Betreiber Kritischer Infrastrukturen werden hinsichtlich der Ausschaltung möglicher Sicherheitsrisiken von den Betreibern jeweils ergriffen?

Zu 7.:
Es ist die eigenverantwortliche Verpflichtung der Betreiber Kritischer Infrastrukturen, durch Schulungen und Sensibilisierungen der Mitarbeitenden über Sicherheitsrisiken permanent aufzuklären sowie die sicherheitstechnischen Einrichtungen und Abläufe auf branchenspezifischen Stand der Sicherheitstechnik zu halten. KRITIS-Betreiber sind nach § 8a Absatz 3 BSI-Gesetz verpflichtet, mindestens alle zwei Jahre die Erfüllung der Anforderungen dieses Gesetzes auf geeignete Weise (z.B. durch Sicherheitsaudits, Prüfungen, Zertifizierungen) nachzuweisen.

8. Sind in Ansehung der jüngsten Erkenntnisse betreffend die Berliner Wasserbetriebe nach Ansicht des Senats die Kritischen Infrastrukturen hinreichend vor möglichen Angriffen, insbesondere vor Angriffen auf die digitale Infrastruktur der Kritischen Infrastrukturen geschützt? Wenn nein: warum nicht und was unternimmt der Senat diesbezüglich?

Zu 8.:
Die registrierten KRITIS-Betreiber sind verpflichtet, ihre branchenspezifischen Sicherheitsstandards für die IT-Sicherheit zu beachten und regelmäßig alle zwei Jahre den Stand der Technik nachweisen (z.B. durch Sicherheitsaudits, Prüfungen oder Zertifizierungen). Darüber hinaus wird die **Senatsverwaltung für Inneres und Sport** eine wissenschaftliche sektorenübergreifende Risikoanalyse gemeinsam mit den KRITIS-Betreibern vornehmen, um ein auf die Gegebenheiten der Metropole Berlin zugeschnittenes Informations- und Funktionsmodell zu erarbeiten. In einem einjährigen Projekt soll deshalb unter der Federführung der Senatsverwaltung für Inneres und Sport in Kooperation mit einer wissenschaftlichen Einrichtung eine mehrteilige Workshopreihe mit den Berliner Betreibern Kritischer Infrastrukturen geplant und durchgeführt werden. Das besondere Merkmal dieses Kooperationsprojektes ist, dass eine aktuelle Analyse der KRITIS-Situation mit einem Handlungskonzept erarbeitet werden soll.
Die Ausschreibung zu diesem Projekt ist erfolgt und nach Abschluss des Bieterverfahrens wird der Beginn des Vorhabens für Ende 2020 angestrebt.

Berlin, den 11. September 2020

In Vertretung

Torsten Akmann
Senatsverwaltung für Inneres und Sport