Senatsverwaltung für Inneres und Sport
SenInnDS III C 1 – 08825-1/2019-1-4

Berlin, 26. Februar 2020

9(0)223-2279
*Stephan.Elsner@seninnds.berlin.de*

**2748**

An die
Vorsitzende des Hauptausschusses
über
den Präsidenten des Abgeordnetenhauses von Berlin
über
Senatskanzlei – G Sen –

**Inanspruchnahme von externen Gutachten- und Beratungsdienstleistungen durch die Senatsverwaltung für Inneres und Sport**
**hier: Planung und Durchführung eines Kooperationsprojektes zur Cybersicherheit in Form einer Workshopreihe mit den Betreibern Kritischer Infrastrukturen im Land Berlin (betr.: Auflage A.21 zum Haushalt 2020/2021)**

**rote Nummer/n:** -

**Vorgang:** 51. Sitzung des Abgeordnetenhauses von Berlin am 12. Dezember 2019 Drucksache 18/2400

**Ansätze:**

| Kapitel 0500/54010 | | |
|---|---|---|
| abgelaufenes Haushaltsjahr: | 2019 | 20.000 € |
| laufendes Haushaltsjahr: | 2020 | 35.000 € |
| kommendes Haushaltsjahr: | 2021 | 70.000 € |
| Ist des abgelaufenen Haushaltsjahres: | 2019 | 57.379,71 € |
| Verfügungsbeschränkungen: | 2020 | 0,00 € |
| aktuelles Ist (Stand 29.01.2020) | 2020 | 5.735,93 € |

**Gesamtausgaben:** 100.000 €

Das Abgeordnetenhaus hat in seiner o.g. Sitzung unter anderem Folgendes beschlossen:
Auflage A.21 zum Haushalt 2020/2021
“Die Senatskanzlei und die Senatsverwaltungen und deren nachgeordnete Behörden und die Bezirksverwaltungen werden aufgefordert, den Hauptausschuss rechtzeitig vor Inangriffnahme der Ausschreibung von Gutachten- und Beratungsdienstleistungsaufträgen mit einem Bruttoauftragswert von mehr als 10.000 Euro zu unterrichten und zu begründen, warum die zu leistende Arbeit nicht von Dienststellen des Landes Berlin erledigt werden kann. In dem Fall, dass der Bruttoauftragswert 50.000 Euro überschreitet, ist die Zustimmung des Hauptausschusses des Abgeordnetenhauses von Berlin einzuholen.“

Beschlussvorschlag:
Der Hauptausschuss nimmt den Bericht zustimmend zur Kenntnis.

Hierzu wird berichtet:

## I. Sachverhalt

Die rasant voranschreitende Digitalisierung aller Lebensbereiche eröffnet insbesondere durch die Vernetzung ungeahnte Informations- und Kommunikationsmöglichkeiten für die

private Anwendung und revolutioniert Geschäfts- und Produktionsprozesse in der Wirtschaft. Nach vorsichtigen Schätzungen wird es im Jahre 2020 weltweit ca. 35 Milliarden vernetzter Geräte geben, ca. 800 Millionen allein davon in Deutschland. Damit einher geht eine enorme Zunahme des Datenwachstums, allein der mobile Datenverkehr wird in den nächsten zehn Jahren um das Siebenfache wachsen.

Aus sicherheitspolitischer Sicht ist allerdings auch zu konstatieren, dass sich durch dieses Wachstum die „Angriffsfläche" vergrößert hat und Cybersicherheit mittlerweile der entscheidende Faktor für eine erfolgreiche Digitalisierung ist.
Digitale Angreifer – gleich welcher Motivation – haben in den letzten Jahren die neuen technologischen Entwicklungen schnell adaptiert und Wege gefunden, die neuen technischen Möglichkeiten mit bekannten kriminellen Vorgehensweisen zu verbinden.
Die Cyber-Bedrohungslage ist sowohl international als auch national weiterhin angespannt. Dem jüngsten „Lagebericht zur IT-Sicherheit in Deutschland 2019" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Folge sind Infektionen mit Schadsoftware für private Anwender, staatliche Institutionen und Unternehmen nach wie vor die größte Gefahr im Cyberraum. Das BSI stellte in den letzten Jahren eine regelrechte Welle von Erpressungstrojanern (z.B. Mai 2017 „WannaCry"; „Emotet" in 2019) fest, bei der die angegriffenen Systeme mit automatisch nachgeladener Malware infiltriert und in der letzten Phase des Cyber-Angriffs deren Daten verschlüsselt werden, wobei gegen Zahlung eines Lösegelds – oft in der Krypto-Währung Bitcoin – die Entschlüsselung versprochen wird.

Dabei rückt aus innenpolitischer Sicht immer mehr der Schutz der informationstechnischen Systeme von Betreibern Kritischer Infrastrukturen in den Fokus, denn längst sind wesentliche Dienstleistungen im Bereich der Energie- und Wasserversorgung, des Transports und Verkehrs, der medizinischen und pflegerischen Versorgung sowie der Ernährung digitalisiert und damit angreifbar.
Cyber-Angriffe auf Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden, sind eine ernstzunehmende und reale Gefahr.

Auch wenn die Absicherung der „Lebensadern unserer Gesellschaft" in erster Linie die Aufgabe und spätestens seit dem Inkrafttreten des IT-Sicherheitsgesetzes im Jahre 2015 auch die gesetzliche Pflicht der Betreiber Kritischer Infrastrukturen (KRITIS) selbst ist, kann und muss der Staat hier flankierend und unterstützend zur Seite stehen. Störungen oder langanhaltende Ausfälle der Strom- oder Gasversorgung können sehr schnell Gefahren für die öffentliche Sicherheit und Ordnung verursachen, so dass der Staat mit gefahrenabwehrenden Maßnahmen reagieren muss. Professionelle Innenpolitik heißt in diesem Zusammenhang aber nicht nur Krisenmanagement, sondern auch Cybersicherheit bereits vor den Angriffen zu stärken, um bereits im Vorfeld Strukturen zu schaffen, die im Ernstfall funktionieren, also Reaktionszeiten verkürzen sowie Maßnahmen und Rollen im Krisenfall festlegen.
Als ein Beispiel eines professionellen Informationsmanagements ist die Einrichtung einer zentralen, behördlichen Kontaktstelle für das Land Berlin in der Senatsverwaltung für Inneres und Sport - Abt. III – zu nennen. Diese Kontaktstelle wird in enger Abstimmung mit den betroffenen Senatsressorts gemäß § 8 b BSI-Gesetz in der Fassung vom 24.07.2015 Informationen über sicherheitsrelevante Vorfälle bei Berliner KRITIS-Betreibern von und zum Bundesamt für Sicherheit in der Informationstechnik bündeln und austauschen.
Darüber hinaus wird diese Kontaktstelle ein Netzwerk zwischen den zuständigen Aufsichtsbehörden der Berliner KRITIS-Betreiber und den KRITIS-Unternehmen aufbauen und unterhalten, um die Zusammenarbeit in diesem Bereich zu verbessern und insbesondere Informationswege und Reaktionszeiten zu verkürzen.

Eine erfolgreiche Cyber-Abwehr kann jedoch nur gelingen, wenn die Schwachstellen bekannt sind und eine fundierte Risikoanalyse vorhanden ist.
Derzeit existiert für das Land Berlin keine wissenschaftlich fundierte Risikoeinschätzung zum Thema Cybersicherheit bei kritischen Infrastrukturen. Diese ist aber unverzichtbare Grundlage der weiteren Maßnahmen, zu denen u.a. die Erarbeitung eines auf die Gegebenheiten der Bundeshauptstadt zugeschnittenen Informations- und Funktionsmodell gehören muss.

Für die vernetzte Großstadt Berlin ist deshalb eine sektorenübergreifende Risikoanalyse zwingend erforderlich, die neben den sektoralen Risiken im KRITIS-Bereich auch die gegenseitigen Abhängigkeiten berücksichtigt.

Dazu soll in einem einjährigen Projekt unter der Federführung der Senatsverwaltung für Inneres und Sport in Kooperation mit einer der Situation in Berlin vertrauten wissenschaftlichen Einrichtung eine mehrteilige Workshopreihe mit den Betreibern Kritischer Infrastrukturen in Berlin geplant und durchgeführt werden. Im Rahmen der Workshop-Reihe sollen die genannten Projektpartner unter Koordinierung und Konsolidierung einer wissenschaftlichen Einrichtung ein Dokument entwickeln, das zur aktuellen Risikoanalyse im KRITIS-Bereich herangezogen werden kann. Dabei ist darauf zu achten, dass durch die voranschreitende, technische Weiterentwicklung, dieses Modell dynamisch und zukunftsfähig aufgestellt wird.

Anknüpfend an die Risikoanalyse soll in den Workshops ein Informations- und Funktionsmodell zwischen Behörden und KRITIS-Betreibern festgelegt werden, um im Falle eines Cyber-Vorfalls den schnellen und reibungslosen Informationsaustausch aller Beteiligten gewährleisten zu können.

**II. Begründung**

Die für das Gelingen dieses Projekts benötigte, wissenschaftliche Expertise zu dem Thema Schutz der informationstechnischen Systeme bei KRITIS-Betreibern im Land Berlin ist weder in der Senatsverwaltung für Inneres und Sport noch in anderen Senatsressorts in der erforderlichen Form vorhanden. Allerdings sind in Berlin eine Reihe von Hochschulen bzw. wissenschaftlichen Instituten ansässig, die als Projektpartner vorstellbar sind. Bei der Kostenschätzung wird die beabsichtigte Struktur des Kooperationsprojektes zugrunde gelegt. Danach wird der überwiegende Anteil durch Personalkosten auf Seiten des Projektpartners durch die wissenschaftliche Begleitung des Projekts entstehen. Weitere Kostenfaktoren sind u.a. die Sachkosten zur Durchführung der Workshopreihe.

**III. Finanzierung und Vergabe**

Die Maßnahme soll sich über ca. 12 Monate erstrecken und die Mittel für den geschätzten Auftragswert in Höhe von 100.000 Euro werden aus dem Kapitel 0500 / Titel 54010 bereitgestellt.
Die Vergabe soll im Rahmen einer Ausschreibung im 1. Quartal 2020 erfolgen.

In Vertretung

Sabine Smentek
Senatsverwaltung für Inneres und Sport