Abgeordnetenhaus BERLIN

Drucksache 19 / 11 637
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Christopher Förster (CDU)

vom 19. April 2022 (Eingang beim Abgeordnetenhaus am 21. April 2022)

zum Thema:
Security Observations Center

und **Antwort** vom 05. Mai 2022 (Eingang beim Abgeordnetenhaus am 06. Mai 2022)

Senatsverwaltung für Inneres, Digitalisierung und Sport

Herrn Abgeordneten Christopher Förster (CDU)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/11637
vom 19.04.2022
über Security Observations Center

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

1. Wann und durch wen wurde entschieden, das Security Observations Center (SOC) einzurichten?

Zu 1.:
Ein Security Operations Center (SOC) ist eine IT-Sicherheitsleitstelle mit vielfältigen Aufgaben, die weit über die Beobachtung (Observation) hinausgehen. Neben der Überwachung aller digitalen Netzwerke, Server, digitalen Geräte, Informationen und auch dem Datenfluss werden die Daten dahingehend aggregiert und korreliert, dass Abweichungen als Anzeichen möglicher Angriffe erkannt werden und darauf über das CERT reagiert wird.
Die Anforderung ein Security Operations Center (SOC) einzurichten ergab sich unter anderem aus der BSI-Auditierung des ITDZ Berlin. Der Beschluss dazu wurde Ende 2018 durch die Vorständin des ITDZ Berlin im Zuge der Genehmigung der Wirtschaftsplanung 2019 gefasst.

2. Wie hoch waren die Kosten für die Einrichtung des SOC? Bitte ggf. nach Haushaltsjahren und titelscharf aufschlüsseln.

Zu 2:
Die Einrichtungskosten für den Aufbau des SOC im ITDZ Berlin beliefen sich auf ca. 750.000 € und sind im Wesentlichen im Haushaltsjahr 2020 angefallen.

3. Welche konkreten Aufgaben hat das SOC?

Zu 3:
Das Security Operations Center (SOC) ist ein moderner Leitstand im Cyber Defence Center Landesverwaltung (CDC-LV) des ITDZ Berlin. Von hier aus erfolgt rund um die Uhr die Erkennung und Abwehr von Angriffen auf die zentrale IKT-Infrastruktur des Landes Berlin. Das umfasst das Berliner Landesnetz (zentrales Daten- und Kommunikationsnetz der Berliner Verwaltung) sowie die IKT in den beiden Rechenzentren des ITDZ Berlin. Als zentrale Stelle zur Bündelung von IKT-Sicherheitsereignissen entsteht im SOC ein Echtzeit-Lagebild für die zentrale IT-Sicherheit des Landes Berlin.

4. Gehört zur Arbeit des SOC auch die Sichtung und Bewertung öffentlich zugänglicher Informationen zu möglichen Bedrohungen?

Zu 4:
Nein. Diese Tätigkeiten werden in anderen Bereichen des CDC-LV vorgenommen.

5. Besteht eine Vernetzung des SOC zu den für die Aufgabenerfüllung relevanten Sicherheitsbehörden?

Zur 5:
Ja, diese Vernetzung ist über das Berlin-CERT gewährleistet.

6. Ergeben sich durch die aktuelle außenpolitische Lage neue oder veränderte Schwerpunkte in der Arbeit des SOC?

Zu 6:
Seit Beginn des Ukraine-Konflikts steht das ITDZ Berlin mit Bezug auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) kommunizierte IT-Sicherheitslage in verstärktem Austausch mit dem BSI und setzt alle Sicherheitshinweise und empfohlenen Maßnahmen im Zusammenhang mit dem Angriff auf die Ukraine um. Für die Überwachung der zentralen IKT des Landes Berlin wurde das Monitoring durch das SOC entsprechend angepasst und erhöht, erforderliche Einsätze sind durch Rufbereitschaften sichergestellt, die kurzfristig auch einen 24/7-Dienst ermöglichen (siehe dazu auch die Antworten auf die Fragen 16 und 17). Darüber hinaus sendet das Berlin-CERT fortlaufend Hinweise zur Informationssicherheit und aktuellen Lage an die Informationssicherheitsbeauftragten der Berliner Landesverwaltung und steht diesen als Ansprechpartner für Fragen in diesem Zusammenhang zur Verfügung.

7. Ist das SOC in der Lage, Angriffe auf die IT Infrastruktur des Landes Berlin auch in den Behörden abzuwehren, die nicht direkt durch das ITDZ betreut werden?

Zu 7:
Das ITDZ Berlin ist verantwortlich für die Sicherheit der zentralen IKT-Infrastruktur des Landes Berlin. Dazu zählt auch IKT, die bereits migriert wurde und vom ITDZ Berlin administriert wird, etwa ein Großteil des Netzes für Daten- und Telekommunikation des Bezirks Charlottenburg-Wilmersdorf. Für die IT-Sicherheit der dezentralen IKT sind die Behörden und Organisationen der Berliner Verwaltung selbst verantwortlich.
Durch die Leistungen des SOC wird im Zusammenwirken mit dem Berlin-CERT grundsätzlich die Kommunikation für alle Behörden über das Berliner Landesnetz geschützt.

8. Welche Befugnisse hat das SOC gegenüber der Hauptverwaltung, den Bezirken, Unternehmen und Privatleuten?

Zu 8:
Das SOC hat gegenüber den genannten Stellen keine Befugnisse. Es stellt Erkenntnisse und Empfehlungen für das Berlin-CERT als Grundlage zur Reaktion zur Verfügung. Diese Inhalte und Empfehlungen werden über die etablierten Meldewege das Berlin-CERT an die Informationssicherheitsbeauftragten der Berliner Behörden kommuniziert.

9. Wem untersteht das SOC und wer ist somit weisungsbefugt?

Zu 9:
Das SOC untersteht als Bestandteil des CDC-LV der Weisungshierarchie des ITDZ Berlin. Die Leistungen für die Berliner Verwaltung werden im Rahmen der IKT-Basisdienste IKT-Sicherheit erbracht.

10. Mit wie vielen VZÄ ist das SOC ausgestattet?

Zu 10:
Das SOC ist heute mit fünf Planstellen für IT-Security-Operatorinnen und -Operatoren (inkl. Gruppenleitung) ausgestattet.

11. Wie viele Stellen sind davon besetzt?

Zu 11:
Derzeit sind vier Stellen davon besetzt.

12. Wie sind die für das SOC zur Verfügung stehenden Stellen bewertet?

Zu 12:
Die Stellen als IT-Security-Operatorinnen und -Operatoren sind mit EG 9-11 TV-L bewertet, die Gruppenleitung mit EG 12 TV-L.

13. Ist die Besetzung der neu geschaffenen Stellen mit externen Bewerberinnen und Bewerbern oder mit bereits vom Land Berlin beschäftigten Personen erfolgt?

Zu 13:
Für die Besetzung der Stellen IT-Security-Operatorinnen und -Operatoren konnten sowohl interne Mitarbeitende des ITDZ als auch externe Bewerberinnen und Bewerber gewonnen werden.

14. Wie wird der Senat zukünftig sicherstellen, dass hochqualifiziertes Personal mit relevanten IT Kenntnissen in der erforderlichen Anzahl für den Öffentlichen Dienst im Land Berlin zur Verfügung steht?

Zu 14:
Stellenbewertungen und Stellenbesetzungen erfolgen nach dem geltenden Tarifrecht. Anforderungen die Qualifizierung und Spezialisierung zu Gunsten des öffentlichen Dienstes spezifisch vorzunehmen, sind im Tarifrecht zu regulieren.

15. Sofern es noch unbesetzte Stellen gibt, wann werden diese besetzt?

Zu 15:
Zurzeit liegen keine qualifizierten Bewerbungen für die unbesetzte Stelle vor. Die Stellenausschreibung muss deshalb in Kürze erneut veröffentlicht werden.

16. Ist das SOC im Schichtbetrieb tätig?

Zu 16:
Im Rahmen der aktuell vereinbarten Servicezeiten werktags, Mo.-Fr., von 07:00 bis 18:00 Uhr ist das SOC derzeit im Zweischichtbetrieb tätig.

17. Ist das SOC auch außerhalb der regulären Dienstzeiten der Berliner Verwaltung einsatzfähig?

Zu 17:
Aktuell erfolgt über das SOC ein automatisiertes, technisches 24/7-Monitoring aller relevanten, zentralen IKT-Systeme. Bei Bedarf und in Abhängigkeit der Sicherheitslage kann über Rufbereitschaften oder die Anordnung von Überstunden temporär auch ein 24/7-Betrieb gewährleistet werden. Bei Beauftragung durch das Land Berlin kann das ITDZ auch einen permanenten 24/7-Betrieb einrichten. Technik und Ausstattung des SOC wurden hierauf ausgelegt.

18. Gibt es eine Rufbereitschaft im SOC?

Zu 18:
Siehe Antwort zu Frage 17.

19. Auf welche Dauer ist das SOC ausgelegt?

Zu 19:
Das SOC ist als dauerhafter Bestandteil der IKT-Sicherheitsarchitektur geplant.

20. Welche Datenmenge fällt täglich in der gesamten Berliner Verwaltung an?

Zu 20:
Zu den täglich in der gesamten Berliner Verwaltung anfallenden Datenmengen liegen u.a. aus Gründen der Datenvermeidung und Datensparsamkeit keine Angaben vor.

21. Ist die geplante Analyse von 1 Terabyte Daten pro Tag ausreichend oder ist eine Kapazitätserweiterung notwendig?

Zu 21:
Die derzeit verarbeiteten 1 Terabyte an Daten pro Tag im Security Information and Event Management (SIEM) System stellt den Status Quo dar. Mit der Überwachung zusätzlicher Systeme wird diese Menge noch ansteigen. Dies wurde bei der Planung bereits berücksichtigt. Eine Kapazitätserweiterung ist aktuell noch nicht notwendig und müsste durch den Senat beauftragt werden.

22. Sollte eine Kapazitätserweiterung notwendig sein, in welchen Schritten ist diese geplant?

Zu 22:
Eine Kapazitätserweiterung wird vom jeweiligen Bedarf abhängig gemacht und wird voraussichtlich im Rahmen der Migration der IKT weiterer Behörden zum ITDZ notwendig.

23. Wird vom SOC auch eine konzeptionelle Gestaltung von Sicherheitsrichtlinien ausgehen?

Zu 23:
Nein.

24. Gibt es die Möglichkeit für andere Behörden des Landes Berlin, auf die Fähigkeiten und Kompetenzen des SOC zuzugreifen?

Zu 24:
Die Fähigkeiten und Kompetenzen des SOC wirken im Sinne der Antworten zu Fragen 7 und 8 für die Kommunikation im Berliner Landesnetz und die vom ITDZ betriebene IKT. Im Rahmen der Migration der verfahrensabhängigen IKT hin zum ITDZ werden sukzessive für weitere Behörden die Leistungen aus dem SOC vollumfänglich wirksam.

Berlin, den 5. Mai 2022

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport