

18. Wahlperiode

## Schriftliche Anfrage

des Abgeordneten **Stefan Ziller (GRÜNE)**

vom 13. November 2019 (Eingang beim Abgeordnetenhaus am 18. November 2019)

zum Thema:

**Rolle der Landesbevollmächtigten für Informationssicherheit bei den Emotet-Vorfällen in der Berliner Verwaltung**

und **Antwort** vom 03. Dezember 2019 (Eingang beim Abgeordnetenhaus am 09. Dez. 2019)

Herrn Abgeordneten Stefan Ziller (GRÜNE)  
über  
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort  
auf die Schriftliche Anfrage Nr. 18/21620  
vom 13. November 2019  
über Rolle der Landesbevollmächtigten für Informationssicherheit bei den Emotet-  
Vorfällen in der Berliner Verwaltung

---

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

1. Welche Rolle spielt die Landesbevollmächtigte für Informationssicherheit bei den aktuellen Emotet-Vorfällen in der Berliner Verwaltung?

Zu 1.:

Nach § 21 Abs. 4 E-Government-Gesetz Berlin (EGovG Bln) hat die IKT-Staatssekretärin die Aufgaben aus § 21 Abs. 4 E-GovG Bln an die Landesbevollmächtigte für Informationssicherheit (Landes-InfSiBe) übertragen. Die Bewältigung von Schadsoftware-Vorfällen ist dem in § 21 Abs. 4 EGovG Bln benannten Handlungsrahmen der "Unterstützung und Überwachung bei der Umsetzung der IKT-Sicherheits-Standards" zuzuordnen. Das erfolgt bei sicherheitsrelevanten Vorfällen in IKT-Systemen nach § 23 Abs. 2 mit Unterstützung des Computersicherheits-Ereignis- und Reaktionsteam (Berlin-CERT). Dazu wurde ein landesweit einheitlicher Meldeprozess zu IKT-Sicherheitsvorfällen etabliert. Die Landesbevollmächtigte erhält bei allen Sicherheitsvorfällen gemäß dem geltenden Meldeprozess zu IKT-Sicherheitsvorfällen zwecks Wahrnehmung der operativen Steuerung des behördenübergreifenden Informationssicherheitsprozesses vom Berlin-CERT die eingehenden Meldungen. Ihr obliegt die unmittelbare Information der IKT-Staatssekretärin. Das ist sowohl bei den sicherheitsrelevanten Vorfällen mit der Schadsoftware Emotet als auch bei den Vorfällen mit anderer Schadsoftware (z.B. im Bereich der Schulen) erfolgt.

Das weitere Vorgehen erfolgt nach der Methodik des BSI-Grundschutzkompendiums mit den Prozessbausteinen Detektion und Reaktion. Die Beschreibungen, Gefährdungslage, und Anforderungen sind im Prozess-Baustein DER.2.1 "Behandlung von Sicherheitsvorfällen" und auf Grund des Sicherheitsvorfalles mit der Schadsoftware Emotet zusätzlich im Prozess-Baustein DER.2.3 "Bereinigung weitreichender Sicherheitsvorfälle" enthalten. Das Vorgehen nach den Prozessbausteinen wird von der Bevollmächtigten bei IKT-Sicherheitsvorfällen aktiv durch Kommunikationsprozesse begleitet.

Die Bereinigung des Sicherheitsvorfalls mit der Schadsoftware Emotet am Kammergericht Berlin bzw. die Rückführung in den Produktivbetrieb dauern an. Die begonnene Umsetzung der Anforderungen aus den o.g. BSI-Bausteinen wird in regelmäßiger Abstimmung zwischen Berlin-CERT, behördlichem Informationssicherheitsbeauftragten und Landes-InfSiBe begleitet.

2. Welche Weisungsrechte gegenüber anderen Stellen der Berliner Verwaltung (auch Bezirke) hat die Landesbevollmächtigte für Informationssicherheit im Falle eines entsprechenden Angriffs/Befalls?

Zu 2.:

Die Befugnisse ergeben sich aus der gemäß der von der IKT-Staatsekretärin übertragenen Bevollmächtigung nach § 21 Abs. 2 Satz 2 Nr. 4 EGovG Bln. Diese beinhaltet folgende Befugnisse:

Die Bevollmächtigte

- hat zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden, ein Zutrittsrecht im Rahmen bestehender Regelungen und gesetzlicher Vorgaben,
- hat im Rahmen ihrer Tätigkeit ein zeitlich, auf die Dauer der wahrzunehmenden Aufgabe, begrenztes Zugriffsrecht auf alle betroffenen IT-Systeme und damit verarbeitete Daten. Je nach Art der Daten muss sie sich hierzu vorab mit dem Datenschutzbeauftragten abstimmen,
- führt Revisionen im Themenbereich der Informationssicherheit durch bzw. veranlasst Revisionen durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in ihrem Aufgabenbereich,
- vertritt die IKT-Staatssekretärin in relevanten Gremien des IT-Sicherheitsmanagements.

Aufgrund der Geschäftsverteilung des Senats sind zudem bei Vorfällen, die in Folge des in § 1 EGovG Bln benannten Geltungsbereichs außerhalb der Bevollmächtigung durch die IKT-Staatsekretärin liegen und Auswirkungen auf die Informationssicherheit der Berliner Verwaltung haben können, Vorfälle bezogen nach der Vorgehensweise entsprechend dem Prozess-Baustein DER.2.1 "Behandlung von Sicherheitsvorfällen" des BSI-Grundschutzkompendiums durch die Bevollmächtigte zu prüfen und ggf. präventive Maßnahmen mit dem Ziel der Minimierung bzw. Vermeidung von Risiken einzuleiten.

3. Wie bewertet der Senat den Status Quo angesichts der aktuellen Erfahrungen? Welche Änderungen von Abläufen und Kompetenzen empfehlen sich im Sinne der Verbesserung der IT-Sicherheit der Berliner Verwaltung?

Zu 3.:

Grundsätzlich werden die etablierten Regelungen und Prozesse als wirksam bewertet. Neben der regelmäßigen Prüfung der Regelungen finden die ereignisbezogenen Nachbereitungen zu Vorfällen Eingang in den kontinuierlichen Verbesserungsprozess des landesweiten Informationssicherheitsmanagement.

Dabei werden auch Potentiale für eine qualitative und quantitative Verbesserung identifiziert, so zum Beispiel die stetige Verbesserung der Kommunikation zu betroffenen Zielgruppen und auch adressatengerechte Darstellung der Inhalte sowie die Übertragung der gesammelten Schlussfolgerungen und Ergebnisse in die Regelungen und Richtlinien zur IKT-Sicherheit. Für ein derart anforderungsgerechtes Verwaltungshandeln ist eine Stärkung der Verwaltung mit Specialistinnen und Spezialisten erforderlich, die über Kompetenzen in Handlungsfeldern Informationssicherheit, Prozessgestaltung und Kommunikation zur Informationssicherheit, sowie Informationssicherheitssensibilisierung verfügen. Dazu werden die Stellenbesetzungsverfahren mit Inkrafttreten des Haushaltes 2020/2021 zeitnah begonnen.

4. Wie ist die Zusammenarbeit der Landesbevollmächtigten für Informationssicherheit mit dem ITDZ, Senatsverwaltungen, nachgeordneten Behörden sowie Bezirken organisiert?

Zu 4.:

In der Bestellung zu der oder dem Landesbevollmächtigten für Informationssicherheit (Landes-InfSiBe) wird zur Organisation ausgeführt:

Der oder die Landes-InfSiBe besitzt eine aufgabenbezogene unabhängige Stellung, ist aber gemäß § 21 Abs. 1 Satz 1 EGovG Bln bei der von der IKT-Staatssekretärin geleiteten Abteilung V der Senatsverwaltung für Inneres und Sport angesiedelt. Er oder sie berichtet in dieser Rolle der IKT-Staatssekretärin direkt. Die IKT-Staatssekretärin trägt weiterhin die Gesamtverantwortung für alle Belange der Informationssicherheit.

Es wird sichergestellt, dass die Wahrnehmung der Rolle der oder des Landes-InfSiBe in der Aufgabenwahrnehmung unterstützt wird und bei auftretenden Konflikten die Aufgabenwahrnehmung der Landes-InfSiBe vorrangig realisiert wird. Der Landes-InfSiBe verfügt über ausreichendes Wissen und Erfahrung auf dem Gebiet der Informationssicherheit und Informationstechnologie.

Die Leitung der Abteilung V unterstützt den oder die Landes-InfSiBe bei der Wahrnehmung der sich aus dieser Bestellung ergebenden Aufgaben. Dem oder der Landes-InfSiBe werden die erforderlichen Ressourcen zur Erfüllung dieser Aufgaben im verfügbaren Umfang zur Verfügung gestellt. Die Leitung der Abteilung V gewährleistet eine der Funktion angemessene Aus- und Fortbildung.

Mit der Bestellung werden folgende Verantwortlichkeiten und Aufgaben übertragen: Die Landes-InfSiBe verantwortet die operativen Einzelaufgaben zur Umsetzung von § 21 Abs. 2 Satz 2 Nr. 4 EGovG Bln. Zu den Aufgaben der Landes-InfSiBe gehören insbesondere:

- Die operative Steuerung des behördenübergreifenden Informationssicherheitsprozesses,

- die Erstellung der zentralen IKT-Sicherheitsarchitektur mit den Standards für die IKT-Sicherheit sowie weiterer Richtlinien zur Informationssicherheit,
- die enge Zusammenarbeit und Unterstützung des zentralen IKT-Notfallbeauftragten oder der zentrale IKT-Notfallbeauftragte, sowie Wahrnehmung von Aufgaben der Steuerung des behördenübergreifenden IKT-Notfallmanagements im Einzelfall,
- die Definition von IKT-Basisdiensten zur Informationssicherheit,
- die Überwachung der Umsetzung der IKT-Sicherheitsarchitektur und IKT-Sicherheits-Standards,
- die regelmäßige Berichterstattung über den Stand der Informationssicherheit,
- die Beratung der IKT-Staatssekretärin in allen Fragen der Informationssicherheit,
- die Unterstützung der Behörden bei der Umsetzung der IKT-Sicherheits-Standards,
- die fachliche Steuerung des ITDZ bzgl. der Informationssicherheit,
- die Zusammenarbeit mit dem Berlin-CERT bei IT-Sicherheitsvorfällen,
- die Steuerung von Maßnahmen zur Sensibilisierung und Schulung der Beschäftigten bezüglich Informationssicherheit.

Die Verantwortlichkeiten und Aufgaben aus der Bestellung werden im Zuge der gegenwärtigen Fortschreibung in die Informationssicherheitsleitlinie aufgenommen. Zur Organisation der Zusammenarbeit enthält die Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (Informationssicherheitsleitlinie – InfoSic-LL) weiterhin folgende Regelungen:

Die IKT-Sicherheitsarchitektur umfasst:

- die Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (InfoSic-LL),
- methodische und technisch-organisatorische Richtlinien zu einzelnen Aspekten der IKT-Sicherheit, die die InfoSic-LL durch Vorgabe standardisierter Rahmenbedingungen für wesentliche Aspekte der IKT-Sicherheit konkretisieren,
- IKT-Basisdienste für IKT-Sicherheit, die gemäß § 24 EGovG Bln vom ITDZ Berlin den Behörden zur verbindlichen Nutzung bereitgestellt werden sowie
- Standard-IKT-Sicherheitsbausteine für die verfahrensunabhängige IKT und definiert in diesem Sinne auch die IKT-Sicherheits-Standards.

Das Informationssicherheitsmanagement-Team (InfSiMa-Team) berät den Landesbeauftragten oder die Landesbeauftragte für Informationssicherheit zu strategischen oder behördenübergreifenden Aspekten der Informationssicherheit. Es besteht aus

- dem oder der Landesbevollmächtigten für Informationssicherheit (Vorsitz),
- den Behördlichen Informationssicherheitsbeauftragten,
- dem oder der Informationssicherheitsbeauftragten des ITDZ Berlin.

Darüber hinaus können weitere Teilnehmerinnen und Teilnehmer hinzugezogen werden. Den Informationssicherheitsbeauftragten der Verwaltung des Abgeordnetenhauses, des Rechnungshofs von Berlin und der Beauftragten für Datenschutz und Informationsfreiheit steht die Teilnahme frei.

5. Welche Informations- und Kontrollrechte hat die Landesbevollmächtigte für Informationssicherheit gegenüber ITDZ, Senatsverwaltungen, nachgeordneten Behörden sowie Bezirken?

Zu 5.:

Gemäß der von der IKT-Staatssekretärin übertragenen Bevollmächtigung nach § 21 Abs. 2 Satz 2 Nr. 4 EGovG Bln hat die Bevollmächtigte folgende Befugnisse/Kompetenzen:

Der bzw. die Landes-InfSiBe

- ist in allen für die Informationssicherheit relevanten Themen rechtzeitig und im angemessenen Umfang zu informieren (sowohl auf Nachfrage als auch unaufgefordert, soweit eine Relevanz für die Informationssicherheit besteht),
- ist bei Vorhaben und Änderungen, die die Informationssicherheit berühren können (z. B. neue IT-Projekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit, ...) frühzeitig in die Abstimmung und Umsetzung einzubeziehen,
- hat ein Anhörungsrecht bei allen Entscheidungen die ihren Verantwortungsbereich betreffen (z. B. bei der Initiierung von IT-Projekten, Beschaffung von Informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern),
- hat direktes Vortragsrecht gegenüber der IKT-Staatssekretärin,
- hat zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden, ein Zutrittsrecht im Rahmen bestehender Regelungen und gesetzlicher Vorgaben,
- hat im Rahmen ihrer Tätigkeit ein zeitlich, auf die Dauer der wahrzunehmenden Aufgabe, begrenztes Zugriffsrecht auf alle betroffenen IT-Systeme und damit verarbeitete Daten. Je nach Art der Daten muss sie sich hierzu vorab mit dem Datenschutzbeauftragten abstimmen,
- führt Revisionen im Themenbereich der Informationssicherheit durch bzw. veranlasst Revisionen durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in ihrem Aufgabenbereich,
- vertritt die IKT-Staatssekretärin in relevanten Gremien des IT-Sicherheitsmanagements,
- hat bei Vorfällen, die außerhalb des Geltungsbereichs dieser Bestellung liegen und Auswirkungen auf die Informationssicherheit der Berliner Verwaltung haben können, das Recht entsprechende Maßnahmen zu prüfen und ggf. einzuleiten.

Berlin, den 03. Dezember 2019

In Vertretung

Sabine Smentek  
Senatsverwaltung für Inneres und Sport