Stadtverordnetenversammlung
der
Landeshauptstadt
Potsdam

23/SVV/1316

Große Anfrage
öffentlich

IT-Sicherheitsvorfälle von 2019/2022

Einreicher:	*Datum*
Fraktion CDU	24.11.2023

geplanter Sitzungstermin	*Gremium*	*Zuständigkeit*
24.01.2024	Stadtverordnetenversammlung der Landeshauptstadt Potsdam	zur Kenntnis

Anlass des Auskunftsersuchens gem. § 29 Abs. 1 BbgKVerf.:

Die reibungslose Abwicklung allen Verwaltungshandelns ist die wesentliche Voraussetzung für die Erfüllung des Auftrags und der den Bürgerinnen und Bürgern geschuldete Dienstleistung. Die Arbeit der Verwaltung wird heutzutage wesentlich von IT-Systemen unterstützt und größtenteils erst ermöglicht. Dem Schutz dieser Systeme von innen oder außen ist daher höchste Priotität einzuräumen. Aufgabe der Stadtverordneten ist die Kontrolle der Verwaltung und ist als Verpflichtung anzusehen, insbesondere, wenn die Nichterfüllung zu erheblichen Nachteilen führt. Die vollständige Untersuchung der IT-Vorkommnisse ist daher geboten. Dazu gehört auch die beantwortung von Fragen, die aus Sicherheitsgründen besser nicht öffentlich beantwortet werden sollen.

Ergänzend zum Bericht zum IT-Sicherheitsvorfall vom 28. Dezember 2022 bis 30. März 2023 werden folgende Fragen gestellt:

1. Welche konkreten technischen und organisatorischen Maßnahmen zur Verbesserung der IT- Sicherheit wurden nach dem ersten Trennen der öffentlichen IT-Systeme der LHP (Lock Down 2019) getroffen?
2. Gab es hierzu Handlungsempfehlungen von dritter Seite und wenn ja, von wem und welche?
3. Wenn ja, inwieweit und welche dieser Handlungsempfehlungen wurden befolgt?
4. Wurde nach dem Lock Down 2019 das „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ (Version 2.0 vom 15.10.2019) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in der LHP umgesetzt? Wenn nicht, warum nicht, und wenn nur in Teilen, welche Teile und welche Teile nicht?
5. Lag Ende 2021 eine vollständige Übersicht der IT-Architektur der LHP inkl. deren Dokumentation vor?
6. Wurde eine solche Dokumentation von dritter Seite angemahnt oder angefordert?
7. Hat die LHP vorsorglich erhöhte Sicherheitsstandards z. B. für kritische Infrastruktur umgesetzt?
8. Welche Handlungsoptionen für das zweite Trennen der öffentlichen IT-Systeme der LHP (Lock Down 2022) lagen vor?
9. Warum haben die getroffenen technischen und organisatorischen Maßnahmen des Lock Down 2019 beim Lock Down 2022 nicht gegriffen?

10. Wurde nach dem Lock Down 2022 das „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ (Version 3.0 vom 31.03.2022) vom BSI in der LHP umgesetzt? Wenn nicht, warum nicht, und wenn nur in Teilen, welche Teile und welche Teile nicht?
11. Sollte weiterhin kein „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ vom BSI in der LHP geplant sein, werden die Checklisten „Weg in die Basis-Absicherung (WiBA)“ vom BSI beantwortet und umgesetzt? Wenn ja, bis wann? Wenn nicht, warum

In der Beantwortung der Fragestellungen wird davon ausgegangen, dass sich die Fragestellungen nicht auf das Jahr 2019 beziehen, sondern auf den Januar 2020. Im Jahr 2019 gab es keinen entsprechenden Sicherheitsvorfall.

Grundsätzlich kann ausgeführt werden, dass die LHP in den vergangenen Jahren erhebliche und wirksame Fortschritte im Bereich der IT-Sicherheit erreichen konnte. Neben organisatorischen Maßnahmen wie der Neuzuordnung des IT-Sicherheitsbeauftragten zum Bereich des Oberbürgermeisters, verbunden mit einer inhaltlichen Neubeschreibung und Prozessanpassungen betrifft dies auch die Dokumentation sowie verschiedenste technische Maßnahmen.

Die seit 2020 ergriffenen Maßnahmen haben bei der Behandlung verschiedenster Sicherheitslücken in genutzter Software und zuletzt bei der Behandlung der Bedrohungslage 2022/2023 ihre Wirkung erfolgreich unter Beweis stellen können. Zu keinem Zeitpunkt kam es zu einem erfolgreichen Angriff oder einer Kompromittierung von IT-Systemen.

Gleichzeitig muss aber auch festgehalten werden, dass sich die Betreiber von IT-Systemen und damit auch die LHP in einem ständigen Wettkampf mit Angreifern befinden, wobei diese in der Regel in jeder Hinsicht über umfassendere Ressourcen verfügen. Die Gewährleistung der IT-Sicherheit wird zunehmend auch die LHP fordern und herausfordern. Eine wichtige Maßnahme zur Behinderung der Bemühungen der Angreifer ist es, Informationen zu Maßnahmen der IT-Sicherheit nur sehr eingeschränkt und nach dem Vorsichtsprinzip außerhalb der IT-Organisation zu kommunizieren.

1. Welche konkreten technischen und organisatorischen Maßnahmen zur Verbesserung der IT- Sicherheit wurden nach dem ersten Trennen der öffentlichen IT-Systeme der LHP (Lock Down 2019) getroffen?

Der Abschlussbericht des Sicherheitsvorfalls im Jahr 2020 wurde durch einen externen Dienstleister der LHP erstellt. In diesem wurden die in der Beantwortung zu Frage 1 benannten Handlungsempfehlungen und Sofortmaßnahmen dokumentiert.

In der Umsetzung wurde die LHP durch die sich ab März 2020 anschließende Corona-Pandemie deutlich behindert. Dennoch konnten nahezu alle Maßnahmen umgesetzt werden.

Im Weiteren wird auf die Beantwortung der Kleinen Anfragen 23/SVV/0010, 23/SVV/0071, 23/SVV/0072 verwiesen.

Die Beantwortung des Status der Umsetzung der Handlungsempfehlungen und Sofortmaßnahmen wird durch den CISO der LHP als vertraulich klassifiziert und ist damit ausschließlich im nicht öffentlichen Teil zu behandeln. Sie werden mündlich vorgetragen.

2. Gab es hierzu Handlungsempfehlungen von dritter Seite und wenn ja, von wem und welche?

Seitens der LDA Brandenburg gab es im November 2020 Empfehlungen. Diese betrafen organisatorische Maßnahmen hinsichtlich der Zuordnung und Rolle des

Informationssicherheitsbeauftragten sowie die Verbesserung der Dokumentationen. Die Umsetzung dieser Maßnahmen wurde bereits vor Vorliegend des Schreibens der LDA eingeleitet (vgl. Antworten zu Frage 1). Ferner wird darauf hingewiesen, dass die Auswertung des Vorfalls und die Maßnahmen extern erstellt wurden.

3. Wenn ja, inwieweit und welche dieser Handlungsempfehlungen wurden befolgt?

Siehe Beantwortung zu Frage 1.

Ergänzend kann ausgeführt werden, dass die Empfehlungen von Dritter Seite in die Umsetzung von Maßnahmen stets einbezogen wurden. Bei der Behandlung von komplexen Sicherheitssituationen ist die LHP auf die Hinzuziehung externer Partner angewiesen. Dies wird als wesentlicher Faktor für die erfolgreiche Behandlung von entsprechenden Vorfällen betrachtet. Für die Entscheidungsfindung ist eine unabhängige Einschätzung eine wichtige Unterstützung.

4. Wurde nach dem Lock Down 2019 das „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ (Version 2.0 vom 15.10.2019) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in der LHP umgesetzt? Wenn nicht, warum nicht, und wenn nur in Teilen, welche Teile und welche Teile nicht?

Der Aufbau eines IT-Sicherheitsmanagements bzw. die Implementierung eines Information Security Management System (ISMS, englisch für „Managementsystem für Informationssicherheit“) ist ein kontinuierlicher Prozess. Dieser wurde ab dem 1. Quartal 2020 gemäß BSI-Vorgaben begonnen. Es wurden zu allen Bausteinen technische sowie organisatorische Maßnahmen umgesetzt. Die Bausteine des BSI Grundschutzes wurden gemäß Prioritäten, Schutzbedarf und Abhängigkeiten implementiert. Die Basis-Absicherung Kommunalverwaltung ist eine Empfehlung und Teilmenge davon. Jede Kommune muss für sich entscheiden, welche Anforderungen für Basis, Standard und Erweiterte Anforderungen umzusetzen sind.

Die LHP orientiert sich jederzeit an den aktuellen Vorgaben. Das trifft auch auf das IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung zu. Diese Vorgaben wurden mehr als erfüllt.

5. Lag Ende 2021 eine vollständige Übersicht der IT-Architektur der LHP inkl. deren Dokumentation vor?

Eine vollständige Übersicht der IT-Architektur im Sinne von aktuellen Netzwerkplänen und -Diagrammen sowie Verfahrensdokumentationen liegt seit Mitte 2020 vor und wird auch bei Veränderungen aktualisiert.

6. Wurde eine solche Dokumentation von dritter Seite angemahnt oder angefordert?

Es gab zu keinem Zeitpunkt eine entsprechende Forderung von dritter Seite. Seitens der LDA wurden die in der Antwort zur Frage 2 ausgeführten Empfehlungen ausgesprochen. Die LDA hat keine Unterlagen zur IT-Architektur angefordert. Auch gab es keine Forderungen zur Bereitstellung der Abschlussberichte.

7. Hat die LHP vorsorglich erhöhte Sicherheitsstandards z. B. für kritische Infrastruktur umgesetzt?

Die LHP unterliegt bisher nicht der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV).

Hinsichtlich der für die von der BSI-Kritisverordnung erfassten Sektoren benannte allgemeine Forderung, die IT-Sicherheit nach dem „Stand der Technik“ umzusetzen,

wird jedoch eingeschätzt, dass viele der bei der LHP implementierten Maßnahmen mindestens bereits diesem Anspruch genügen. Auch ist bei dieser Thematik darauf hinzuweisen, dass KRITIS ausschließlich auf die Verfügbarkeit der kritischen Dienstleistungen fokussiert.

8. Welche Handlungsoptionen für das zweite Trennen der öffentlichen IT-Systeme der LHP (Lock Down 2022) lagen vor?

Die gemeinsam mit der ZAC (Zentrale Ansprechstelle Cybercrime) Brandenburg, dem Polizeipräsidium Reutlingen und dem CERT (Computer Emergency Response Team) Brandenburg getroffene Lageeinschätzung am 29.12.2022 mündete in der dringenden Empfehlung an den Oberbürgermeister der Trennung sämtlicher Verbindungen der LHP zu allen externen Netzen. Grundlage dieser Lageeinschätzung waren die bekannten Ermittlungsstände der Polizeibehörden.

9. Warum haben die getroffenen technischen und organisatorischen Maßnahmen des Lock Down 2019 beim Lock Down 2022 nicht gegriffen?

Die Lagebilder in 2020 und 2022 waren nicht vergleichbar. In 2020 war der sogenannte Angriffsvektor bekannt. Auch handelte es sich damals um einen maschinellen Angriff.

Bei der Bedrohungslage 2022/2023 war hingegen nur gesichert, dass es eine sehr ernst zu nehmende Bedrohung für IT Systeme in der Stadt Potsdam gibt. Es war weiterhin nur allgemein bekannt, dass ein hochprofessioneller Angriff unmittelbar bevorsteht und ggfs. durch die Angreifer bereits vorbereitende Maßnahmen in der Zielumgebung des Angriffs ergriffen wurden bzw. dieser auch schon gestartet wurde.

Festzustellen ist, dass die nach 2020 ergriffenen Maßnahmen (siehe Antwort zu Frage 1) in erheblichem Maße dazu beigetragen haben, die Bedrohungslage 2022/2023 in, auch nach externer Einschätzung, hoher Professionalität zu behandeln. Dies betrifft neben der Organisation/Kommunikation auch die Dokumentation und die Systemzustände.

Die in 2023 implementierten zusätzlichen Maßnahmen haben zu einer weiteren deutlichen Verbesserung des Sicherheitsniveaus beigetragen. Bspw. ist es nunmehr möglich, dass Anomalien frühzeitig und ohne zeitliche Unterbrechung erkannt werden können um dann, ebenfalls sehr zeitnah, Maßnahmen einzuleiten.

10. Wurde nach dem Lock Down 2022 das „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ (Version 3.0 vom 31.03.2022) vom BSI in der LHP umgesetzt? Wenn nicht, warum nicht, und wenn nur in Teilen, welche Teile und welche Teile nicht?

In Bezug auf den angefragten Aspekt wird eine als vertraulich eingestufte und damit nicht öffentliche Dokumentation geführt. Gemäß interner und externer Vorgaben werden der Datenschutz sowie die Schutzziele der Informationssicherheit mit Hilfe von Datenschutzfolgeabschätzungen sowie Schutzbedarfsfeststellungen umgesetzt. Entsprechend des Schutzbedarfes und der bekannten Risiken werden Maßnahmen für Prozesse und Anwendungen gefordert und umgesetzt. Insgesamt werden alle 22 Bausteine des „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ in unterschiedlichem Erfüllungsstand umgesetzt.

11. Sollte weiterhin kein „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung“ vom BSI in der LHP geplant sein, werden die Checklisten „Weg in die Basis-Absicherung (WiBA)“ vom BSI beantwortet und umgesetzt? Wenn ja, bis wann? Wenn nicht, warum nicht?

Die 19 Checklisten „Weg in die Basis-Absicherung (WiBA)“ werden vollständig berücksichtigt und sind derzeit in unterschiedlichem Erfüllungsstand in Umsetzung.

Anlagen:
Keine