Stadtverordnetenversammlung der
Landeshauptstadt Potsdam

Kleine Anfrage

Drucksache Nr. (ggf. Nachtragsvermerk)

23/SVV/0010

Einreicher: Stadtverordneter Krämer, Fraktion Sozial.DIE LINKE öffentlich

Betreff:
Erneuter Cyberangriff auf Potsdam

Erstellungsdatum:	05.01.2023
Eingang Büro der SVV:	05.01.2023
weitergeleitet an das Büro OBM:	05.01.2023
Termin der Beantwortung:	26.01.2023
Terminverlängerung:	31.01.2023
Eingang der Beantwortung:	02.03.2023

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

Kurz vor dem Jahreswechsel zu 2023 ging die Potsdamer Stadtverwaltung – wie bereits im Januar 2020 – offline. Alle Systeme wurden herunterfahren, nachdem festgestellt worden war, dass das Rathaus zu wiederholten Mal Ziel eines Cyberangriffs geworden war. Grund dafür war eine Sicherheitslücke in der Serversoftware der Firma Citrix. Betroffen sind u.a. der Bürgerservice, die KfZ-Zulassungs-, und Fahrerlaubnisbehörde sowie der E-Mail-Verkehr von innen nach außen und umgekehrt. Auch städtische Unternehmen sind betroffen

Ich frage den Oberbürgermeister:

1. **Welche Schritte wurden seitens der LHP seit 2020 unternommen, um sich vor einen erneuten Angriff zu schützen?**

   Die Landeshauptstadt Potsdam hat ihre IT-Infrastruktur, wie auch zuvor, sukzessive weiter abgesichert. So wurde in der Verwaltung u.a. komplett auf das Betriebssystem Windows 10 umgestellt, fortlaufend Sicherheitsupdates eingepflegt, die Stelle des Informationssicherheitsbeauftragten neu beschrieben und entsprechend besetzt und aufgrund der Bedeutung direkt im Geschäftsbereich des Oberbürgermeisters im Bereich Informationssicherheit und Datenschutz (914) angesiedelt. Darüber hinaus konnte im November 2021 die neu geschaffene Stelle des IT-Architekten besetzt werden, um u.a. sichere Softwarearchitekturen für unternehmenskritische Anwendungen/Infrastrukturen zu schaffen. Durch die Mitgliedschaft im Zweckverband DIKOM, der TUIV AG und der Allianz für Cybersicherheit kann die LHP auf entsprechende Expertisen und Vernetzungsangebote zurückgreifen. Die Gesamtheit der ergriffenen Maßnahmen hat dazu geführt, das seither keine kriminellen Einzeltäter:innen oder Gruppen die IT-Infrastruktur der Landeshauptstadt Potsdam kompromittieren konnten.

Unterschrift

2. **Welche Erkenntnisse wurden bei der Schadensanalyse gewonnen?**

   Die Landeshauptstadt Potsdam konnte sich aufgrund der vorsorglichen Trennung zum Internet erfolgreich vor einem möglicherweise bevorstehenden Angriff schützen. Die IT-Infrastruktur der Landeshauptstadt Potsdam ist weder in Teilen noch in Gänze kompromittiert worden.

3. **Welche Lehren zieht die Stadt diesmal – nach bisherigen Stand – aus diesem Cyberangriff?**

   Die Landeshauptstadt Potsdam hat nach Information von Sicherheitsbehörden über eine mögliche Bedrohungslage sich für die vorsorgliche Trennung vom Internet entschieden und konnte sich somit erfolgreich vor einem möglicherweise bevorstehenden Angriff schützen. Die Landeshauptstadt Potsdam sieht sich darin bestärkt, dass die bereits zuvor getroffenen Maßnahmen und Investitionen in die IT-Sicherheit sowie die Anbindung des Themas direkt im Geschäftsbereich des Oberbürgermeisters der richtige Weg waren und sind. Die Landeshauptstadt Potsdam wird diesen Weg weitergehen, nach wie vor Investitionen in die IT-Sicherheit tätigen und dem Thema IT-Sicherheit insgesamt weiterhin oberste Priorität einräumen.

4. **Sind nach dem erneuten Angriff zusätzliche Investitionen in die IT-Sicherheut geplant, wenn ja welche?**

   Die Landeshauptstadt Potsdam wird zusätzliche und bereits geplante Investitionen tätigen. Hierzu zählt bspw. eine 24/7-Überwachung.

5. **Wird die LHP zur dauerhaften Gewährleistung der IT-Sicherheit künftig verstärkt mit externen Dienstleistern zusammenarbeiten?**

   Ja, die Landeshauptstadt Potsdam wird noch stärker mit externen Dienstleistern zusammenarbeiten.

Zuständigkeit: GB Zentrale Verwaltung