Stadtverwaltung Cottbus ·· Postfach 101235 · 03012 Cottbus

Stadtverordnetenversammlung Cottbus/Chóśebuz
Fraktion DIE LINKE
Erich Kästner Platz 1
03046 Cottbus/Chóśebuz

STADT COTTBUS
CHÓŚEBUZ

DER OBERBÜRGERMEISTER
WUŠY ŠOŁTA

Datum

24. Januar 2023

Geschäftsbereich/Fachbereich

Büro des Oberbürgermeisters
Datenschutz- und Informations-sicherheitsbeauftragter

Zeichen Ihres Schreibens

AN-04/23

Sprechzeiten

- nach Vereinbarung -

Ansprechpartner/in

Theodor Kubusch

Zimmer

214

Mein Zeichen

01-kub_-

Telefon

+ 49 (0) 355 / 612 - 21 26

Fax

+ 49 (0) 355 / 612 - 13 21 26

E-Mail

theodor.kubusch@cottbus.de

Anfrage AN-04/23 zur Stadtverordnetenversammlung am 25.01.2023 zum Thema "Maßnahmen zur IT-Sicherheit in der Stadtverwaltung"

Sehr geehrter Herr Loehr,
sehr geehrte Damen und Herren,

Ihre Fragestellungen vom 10.01.2023 beantworte ich wie folgt:

Vorbemerkungen

A. Vorab gestatte ich mir im Bezug zu den allgemeinen Maßnahmen der Verwaltung hinsichtlich der Struktur und des Betriebs eines Informationssicherheitsmanagementsystems nach BSI-Standard 200-1 auf meine Antwort zur Anfrage AN-32/22 vom 23.05.2022 zu verweisen.
B. Bezüglich der nachfolgenden Fragestellungen im Kontext zu einem Cyber-Angriff bei der Landeshauptstadt Potsdam und den damit einhergehenden präventiven Maßnahmen ist hier voranzustellen, dass der Stadt Cottbus/Chóśebuz und ihrem IT-Dienstleister darüber nur die Erkenntnisse aus der medialen Berichterstattung vorliegen. Aus taktischen Gründen der Notfallbewältigung und Ermittlungspraxis können gegenwärtig keine anderen Informationen erkundet werden.

zu 1.) **Würde die Stadtverwaltung in einem ähnlich gelagerten Fall ebenfalls mit einem solchen Shutdown reagieren müssen oder gibt es alternative Präventivmaßnahmen?**

Die Stadtverwaltung Cottbus/Chóśebuz müsste in einem ähnlich gelagerten Fall ebenfalls mit einem derartigen Shutdown rechnen, sofern die vorliegenden Erkenntnisse zur Lage in der Landeshauptstadt

Stadtverwaltung Cottbus
Neumarkt 5
03046 Cottbus

Konto der Stadtkasse
Sparkasse Spree-Neiße
IBAN:
DE06 1805 0000 3302 0000 21
BIC: WELADED1CBN

www.cottbus.de

Potsdam richtig gedeutet werden konnten. Diese Annahme beruht einerseits darauf, dass im Falle einer erkannten und hiernach sogar angedrohten Bedrohungslage der Schutz der Informationssysteme vorrangig zu betrachten ist. Hinsichtlich der Dauer einer solchen Außerbetriebnahme kann jedoch keine abstrakte Prognose getroffen werden. Andererseits wäre aufgrund der komplexen Vernetzungsstrukturen und Abhängigkeiten verschiedenster Akteure in den Verwaltungsprozessen auch eine Außerbetriebnahme von Entscheidungen anderer Institutionen abhängig. So erschiene es spekulativ auch nicht ausgeschlossen, dass im Falle einer solchen Bedrohungslage auch ein Ausschluss aus dem Landesverwaltungsnetz zur Folge haben könnte, sodass alle darüber betriebenen Dienste nicht mehr zur Verfügung stünden.

Ungeachtet dieser Szenarien ist jedoch nicht zu verhehlen, dass derartig gelagerte Angriffsbedrohungen (hier die sogenannte „Brute-Force-Attack“) weitestgehend durch Präventivmaßnahmen ausgeschlossen sein sollen, indem die Stadtverwaltung Cottbus/Chóśebuz derartig angreifbare Dienste restriktiv nach außen hin verfügbar hält. Die Gewährleistung einer solchen ausgewogenen und dennoch wirksamen Sicherheitskultur beruht auf standardisierten Prozessen zum Einsatz solcher Dienste (Systemhärtung).

Überdies betreibt die Stadt Cottbus/Chóśebuz in Zusammenarbeit mit ihrem IT-Dienstleister ein informelles Computer-Ereignis- und Reaktions-Team (CERT), welches regelmäßig Bedrohungslagen analytisch bewertet und in den erforderlichen Fällen durch Präventivmaßnahmen in die Feinspezifikationen der Dienste einfließen lässt.

zu 2.) **Wie ist die Stadtverwaltung auf mögliche Hackerangriffe – beispielsweise im Rahmen eines Erpressungsversuchs – vorbereitet?**

Aus technischer Sicht verfolgt die Stadtverwaltung Cottbus/Chóśebuz eine Präventionsstrategie, indem konventionelle Angriffe größtmöglich ausgeschlossen werden sollen. Hierzu orientieren sich sowohl IT-Dienstleister als auch die Verwaltung an den Anforderungen der IT-Grundschutz-Methodik (BSI-Standard 200-2; Standardabsicherung nach IT-Grundschutz-Kompendium) und, dort wo nötig, an den individuell abgeleiteten Maßnahmen aus dem Risikomanagement (BSI-Standard 200-3).

Eine Vorbereitung auf erweiterte und innovative Angriffe kann lediglich durch frühzeitige Detektion (Monitoring, CERT), Audits und Revisionen, agile Reaktionsmechanismen (Notfallmanagementsystem, BSI-Standard 200-4) einschließlich der erforderlichen Wiederherstellungsstrategien erfolgen. Dies erfolgt dem Grunde nach durch einen gegenwärtig bestehenden Aufbau eines Notfallmanagements bei dem IT-Dienstleister, der Entwicklung eines betrieblichen Kontinuitätsmanagements in der Verwaltung, welches sodann in einer gesonderten Notfallbewältigungsstrategie münden soll, der ISO/IEC-Zertifizierung des Rechenzentrums und Datensicherungsstrategien.

In Summe dieser Präventionsmaßnahmen erscheint es aus gegenwärtiger Sicht nicht denkbar, auf derartige mögliche Erpressungsversuche einzugehen, sondern vielmehr einen raschen Wiederanlauf mit geringem Informationsverlust (≤ 24 Stunden) anzustreben.

...3

zu 3.) **Wie sind für den Fall von Hackerangriffen die Daten der Bürgerinnen und Bürger vor unerlaubten Zugriffen geschützt?**

Das Informationssicherheits- und datenschutzrechtliche Gewährleistungsziel der „Vertraulichkeit“ wird durch eine Vielzahl verschiedener Maßnahmen in Abhängigkeit unterschiedlichster Angriffsszenarien und Verarbeitungsdienste verfolgt. Die Durchsetzung erfolgt durch technische und organisatorische Maßnahmen, die sich aus den unterschiedlichen (insgesamt 1.800) Anforderungen des IT-Grundschutz-Kompendiums ergeben.

Freundliche Grüße

im Auftrag

Theodor Kubusch