STADT COTTBUS
CHÓŚEBUZ

DER OBERBÜRGERMEISTER
WUŠY ŠOŁTA

Stadtverwaltung Cottbus/Chóśebuz · Postfach 101235 · 03012 Cottbus/Chóśebuz

AfD Fraktion
Herrn
Georg Simonek
Erich-Kästner-Platz 1
03046 Cottbus

Datum 23 . Mai 2022

Geschäftsbereich/Fachbereich
Büro des Oberbürgermeisters

Zeichen Ihres Schreibens

Sprechzeiten

Ansprechpartner/-in
Theodor Kubusch

Zimmer

Mein Zeichen

Telefon
0355 612 2126

Fax

E-Mail

Ihre Anfrage AN-32/22 zur Stadtverordnetenversammlung am 25.05.2022
Zur Thematik „IT-Sicherheit“

Sehr geehrter Herr Simonek,

Ihre Anfrage beantworte ich wie folgt:

Vorbemerkung

Die Stadt Cottbus/Chóśebuz betreibt eine Vielzahl an IT-Systemen in verschiedenen, voneinander unabhängigen IT-Verbünden. Im Wesentlichen umfasst dies die IT-Verbünde der

a) Stadtverwaltung Cottbus/Chóśebuz,
b) integrierten Regionalleitstelle Lausitz sowie
c) die Infrastrukturen der Schul-IT.

Darüber hinaus werden dedizierte IT-Verbünde in den Eigenbetrieben

d) Grün- und Parkanlagen der Stadt Cottbus sowie
e) Sportstättenbetrieb der Stadt Cottbus betrieben.

Zu den letzteren (d) und e)) liegen keine aussagekräftigen Erkenntnisse vor.

Für die unter Litera a) und b) benannten IT-Verbünde sind jeweils umfangreiche standardisierte Informationssicherheitsmaßnahmen etabliert. Für die Infrastrukturen der Schul-IT sind derartige Maßnahmen gegenwärtig nicht (dokumentiert) existent, jedoch sind solche durch Änderung der IT-Strategie im Schulbetrieb mit der Neuausrichtung bindend vorgesehen.

Stadtverwaltung Cottbus/Chóśebuz
Neumarkt 5
03046 Cottbus/Chóśebuz

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

...

Frage 1: Gab es bereits Hackerangriffe auf das IT-System der Stadt Cottbus/Chóśebuz?

Im Jahr 2016 war ein erfolgreicher Hackerangriff zu verzeichnen, der durch eine ungezielte Aktivität verursacht wurde. Gezielte Angriffe auf die Stadt Cottbus/Chóśebuz sind nicht bekannt.

Bei dem weitestgehend unbestimmten Begriff des „Hackerangriffs“ ist in Beantwortung der Fragestellung davon auszugehen, dass darunter böswillige Aktivitäten gemeint sein sollen, die versuchen, IT-Systeme der Stadt Cottbus/Chóśebuz einerseits gezielt, andererseits wahllos zu kompromittieren.

Zielstellung der Informationssicherheit ist es, derartige böswillige Angriffe präventiv (durch umfassende Detektions- und Reaktionsmaßnahmen) auszuschließen oder frühzeitig abwenden zu können. Festzustellen ist, dass der Stadt Cottbus/Chóśebuz gegenwärtig nur ein *erfolgreicher* Hackerangriff aus dem Jahr 2016 bekannt ist, wobei es sich dabei um eine ungezielte Aktivität handelte, die im Wesentlichen auf menschliches Fehlverhalten zurückzuführen war. Diese wurden infolgedessen zum Anlass genommen, um entsprechende Änderungen in der Sicherheitsstrategie einzuführen. Es ist somit davon auszugehen ist, dass bis auf diesen Einzelfall derartige Aktivitäten bisher ohne Erfolg blieben. Gezielte Hackerangriffe auf die IT-Systeme der Stadt Cottbus/Chóśebuz sind nicht bekannt.

Nachweisbar ist, dass es regelmäßig ziellose Aktivitäten gibt, die derartige böswillige Anstrengungen darstellen. Da in der nicht qualifizierbaren Einordnung derartiger Aktivitäten zum Begriff „Hackerangriff“ Definitionsprobleme bestehen, können keine quantifizierten Angaben über alle „böswilligen Aktivitäten“ gemacht werden. Diese sind schlichtweg nicht erfasst, da dies für die Beurteilung der Informationssicherheit irrelevant ist. So sind bspw. täglich eine überaus hohe Zahl böswilliger eingehender E-Mails zu verzeichnen, die weitestgehend durch Schutzsysteme „abgefangen“ werden. Die verbleibende Zahl eindringender Nachrichten, die es möglicherweise zum Ziel haben, Ransomware einzuschleusen, werden durch lokale Schutzmechanismen (Anti-Virensysteme, Monitoring, gehärtete/eingeschränkte Systemeinstellungen) und Sensibilisierungskampagnen verhindert.

Frage 2: Was veranlasst die Verwaltung, um Hackerangriffe abzuwehren?

Die Stadt Cottbus/Chóśebuz betreibt zur präventiven Abwendung umfassende Informationssicherheitsmaßnahmen in organisatorischer und technischer Ausführung nach den einschlägigen Standardisierungsprozessen. Zudem werden Sicherheitsmeldungen durch ein Computer-Ereignis- und Reaktions-Team ausgewertet und behandelt.

Die Stadt Cottbus/Chóśebuz betreibt, dort wo etabliert, umfassende Informationssicherheitsmaßnahmen nach den standardisierten Vorgehensweisen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), um derartige Hackerangriffe bereits im Vorfeld abwenden zu können. Dies umfasst insbesondere die verbindliche Anwendung der BSI-Standards 200-1 (Informationssicherheitsmanagement) und 200-2 (IT-Grundschutz-Methodik) sowie, dort wo nötig, 200-3 (Risikomanagement) unter Beachtung der Anforderungen des IT-Grundschutz-Kompendiums in der Standardabsicherung. Hierzu sind sämtliche internen und externen IT-Dienstleister durch entsprechende Weisungen (Dienstanweisung, Verträge zur Auftragsverarbeitung) verpflichtet.

Zudem betreibt die Stadt Cottbus/Chóśebuz auf Basis des BSI-Standards 200-2 und dem IT-Grundschutz-Kompendium umfassende Detektions- und Reaktionsmaßnahmen (Detektion von sicherheitsrelevanten Ereignissen, Behandlung von Sicherheitsvorfällen, Vorsorge für die IT-Forensik, Audits und Revisionen sowie in Ansätzen Maßnahmen des Notfallmanagements), worunter technische Sicherheitssysteme (bspw. Firewalls, Anti-Virenscanner u. ä.) als auch

organisatorische Regelungen (Sicherheitsbewertungen, Verhalten der Beschäftigten usw.) zu verstehen sind.

Überdies hat die Stadt Cottbus/Chóśebuz seit dem Jahr 2021 außerhalb der Linienorganisation ein – organisatorisch bisher nicht definiertes, aber faktisch etabliertes – Computer-Ereignis- und Reaktions-Team (CERT-CB) gebildet, welches Sicherheitsmeldungen anderer Institutionen (bspw. CERT-Bund, CERT-BB, Software-Hersteller/-innen u. ä.) entgegennimmt oder durch Monitoring selbst erkennt sowie entsprechend bewertet und präventiv behandelt. Zudem hat die Stadt Cottbus/Chóśebuz über die TUIV-AG ein landesweites kommunales CERT initiiert, welches in Kooperation mit dem Zentralen IT-Dienstleister des Landes Brandenburg aufgebaut werden soll.

Durch das CERT-CB wurden im Jahr 2021 neun Ereignisse als relevant eingestuft und im Vorfeld durch Gegenmaßnahmen behandelt. Im Jahr 2022 wurden bisher sechs derartige Sicherheitsmeldungen behandelt.

Vorausschauend ist die Verwaltung zur Verbesserung der Reaktionsmöglichkeiten seit 2021 bestrebt, ein Kontinuitätsmanagement (BCM; Business-Continued-Management) einzuführen. Hierzu besteht gegenwärtig die Anforderung, ein Verfahren zur Durchführung einer Business-Impact-Analyse (Auswirkungsanalyse) zu etablieren, woraus ein umfassendes Notfallmanagement abgeleitet werden muss.

Frage 3: Werden die Dokumentationen dazu ständig aktualisiert?

Die Stadt Cottbus/Chóśebuz sieht die Informationssicherheit als fortwährenden Entwicklungsprozess an, der regelmäßig den Gegebenheiten und Ständen der Technik anzupassen ist. Somit sind Dokumentationen zeitgemäß – in einer dafür vorgesehenen Fachanwendung – zu führen und bei wesentlichen Änderungen zu aktualisieren.

Maßnahmen des Informationssicherheitsmanagementsystems (ISMS) werden nach dem Konzept „PDCA“-Zyklus (Plan-Do-Check-Act; Planen-Ausführen-Überprüfen-Reagieren/Verbessern) implementiert, sodass die Sicherheitsmaßnahmen fortlaufend analysiert und aktualisiert werden. Die Änderungen werden in den dafür vorgesehenen Dokumentationen fortgeschrieben. Hierzu sind die jeweils zuständigen Beschäftigten angewiesen, ein zur Verfügung gestelltes ISMS-Tool einzusetzen, welches die Maßnahmen dokumentiert.

Frage 4: In welchen Zeiträumen werden die Beschäftigten der Stadtverwaltung zum Thema IT-Sicherheit geschult?

Beschäftigte der Stadtverwaltung Cottbus/Chóśebuz werden zum Zeitpunkt ihrer Einstellung einmalig zum Thema Informationssicherheit sensibilisiert. Es werden regelmäßig freiwillige Seminare zur „Cyber-Sicherheit“ angeboten. Zudem ergehen „Awareness“-Kampagnen per Intranet-News in gezielten Fällen.

Das IT-Grundschutz-Kompendium sieht für die Sensibilisierung der Beschäftigten zum Thema Informationssicherheit mehrere Möglichkeiten vor. Neben gängigen (allumfassenden) Schulungsmaßnahmen können dies individuelle (bereichsbezogene) Schulungskampagnen, als auch Aufklärung durch Handlungen, Workshops oder allgemeine Informationsvermittlung (Newsletter, Flyer etc.) sein.

Jede bei der Stadtverwaltung Cottbus/Chóśebuz neu eingestellte Person wird in einem lückenlosen Prozess auf Kernthemen der sicheren Nutzung der IT-Systeme (einmalig)

sensibilisiert. Danach existieren keine weiteren Pflichtschulungen. Zur Abdeckung des allgemeinen Schulungsbedarfs wird jährlich mindestens ein Schulungsangebot zur Informationssicherheit vorgehalten. Die Vorgesetzten der Bereiche sind durch Dienstanweisung verpflichtet, derartigen Schulungsbedarf zu ermitteln und anzumelden.

Hinsichtlich aktueller Informationssicherheitsthemen (spezifische Gefährdungslagen) finden sich regelmäßige Aufklärungsinformationen im Intranet der Stadt Cottbus/Chóśebuz.

Mit freundlichen Grüßen

Im Auftrag

gez.
Theodor Kubusch
Datenschutz- und Informationssicherheitsbeauftragter
der Stadt Cottbus/Chóśebuz