Az.: 10.24.35/13

CHEMNITZ
KULTURHAUPTSTADT
EUROPAS 2025

Datum 04.04.2022
Nr.: RA-062/2022

**Anfrage von Stadtratsmitgliedern - öffentlich**
(gemäß § 28 Abs. 6 SächsGemO in Verbindung mit der Geschäftsordnung für den Stadtrat der Stadt Chemnitz)

Fragesteller/in: Herr Toni Rotter (Fraktionsgemeinschaft BÜNDNIS 90/DIE GRÜNEN)
Vorname Name (Fraktion)

**Kurzbezeichnung: Sicherheit in der Stadtverwaltung Chemnitz - Cybersicherheitskonzept**

**Frage:**

Sehr geehrter Oberbürgermeister,

einerseits nimmt die, grundsätzlich zu begrüßende, Digitalisierung der SVC zu. Andererseits nehmen Attacken auf die digitale Infrastruktur der Kommunen zu, deren Hintergründe und Motivationen vielfältig sind. Zu nennen sind im Osten Deutschlands der Landkreis Anhalt-Bitterfeld[1] und die Kommune Suhl[3]. Letztere musste wegen des Ransomware-Angriffs den Katastrophenfall ausrufen. Nicht minder ist mit Blick auf die derzeitigen Aggressionen Russlands auch im digitalen Raum das Thema wieder von erhöhter Brisanz.

Daher stellen sich folgende Fragen an die Stadtverwaltung Chemnitz:

**1. Welche Handlungsschritte leiten sich für die SVC aus den Vorfällen in Suhl (Malsoftware) und Bitterfeld (Ransomware) ab?**

a) Welche Unterschiede gibt es, die einen Angriff in Chemnitz unwahrscheinlicher machen? Gibt es Checklisten, Methodik o.ä, um frühzeitig Angriffe und Datenabgriffe (zum Zweck der Erpressung) zu erkennen?

b) Würde auch in Chemnitz bei einem ähnlichen Vorfall der Katastrophenfall ausgelöst werden?

c) Welche Schritte würden eingeleitet werden, wenn persönliche Daten oder z.B. nicht-öffentliche Protokolle veröffentlicht werden? Wie werden Betroffene informiert und unterstützt?

d) Gibt es sichere, umfassende, funktionsgetestete Offline-Backups, die schnell und strukturiert wieder eingespielt werden können?

e) Gibt es Notfallpläne, ggf. sogar Notfallübungen?

**2. Wurden seitens der Stadt Chemnitz Sicherheitsgutachten (z. B. bei der TU Chemnitz) beauftragt oder unabhängige Penetrationtests beauftragt?**

a) Wie wird die Sicherheit gegen Angriffe durch Human Hacking / Social Engineering[2] eingeschätzt?

b) Wie häufig werden Mitarbeiter:innen geschult bzw. finden Belehrungen (Awareness-Schulungen) statt?

c) Gibt es angepasste Dienstvereinbarungen?

d) Hat Chemnitz eine:n IT-Sicherheitsbeauftragte:n und werden die Sicherheitsanforderungen für

kritische Infrastruktur nach dem §8 BSIG erfüllt?

**3. Zum 31.12.2019 waren 334 Notebooks im Bestand, Ende Februar 2021 sollten es fast 1.400 mobile Windows-Geräte sein.**

a) Sind diese Geräte, wenn sie in Homeoffice/Telearbeit genutzt werden, durch zwei-Faktor Authentifizierung abgesichert?
b) Greifen diese Geräte grundsätzlich über eine VPN-Verbindung auf das städtische Netzwerk zu?

c) Gibt es in der Chemnitzer Verwaltung noch Rechner auf Windows 8.1 oder älter, ohne erweiterten Support?

c) Wie wird der Einsatz von Open Source Betriebssystemen und/oder Programmen für kritische Strukturen eingeschätzt?

Mit freundlichen Grüßen
Toni Rotter

[1] Cyberangriff auf Landkreis Anhalt-Bitterfeld 2021
unter https://kommunalwiki.boell.de/index.php/Cyberangriff_auf_Landkreis_Anhalt-Bitterfeld_2021; Abruf 01.04.022

[2] „Die bekannteste Form des Social Engineering ist das Phishing – wörtlich: das Fischen nach Passwörtern. Durch häufig sehr echt wirkende E-Mails sollen Personen dazu gebracht werden, auf einen Link zu klicken und auf der ebenfalls gefälschten Zielseite Passwörter .." (Social Engineering – der Mensch als Schwachstelle. BSI Bund
unter https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html#:~:text=Die%20bekannteste%20Form%20des%20Social,ebenfalls%20gef%C3%A4lschten%20Zielseite%20Passw%C3%B6rter%20bzw.; Abruf 01.04.2022

[3] Cyberangriff auf Stadtverwaltung Suhl. Golem.: https://www.golem.de/news/malware-cyberangriff-auf-stadtverwaltung-suhl-2203-163788.html; Abruf 01.04.2022

**Die Ratsanfrage wurde elektronisch erstellt und enthält keine eigenhändige Unterschrift.**