OTTO-DIX-STADT GERA

OBERBÜRGERMEISTER

OTTO-DIX-STADT GERA • Stadtverwaltung • Postfach 11 64 • 07501 Gera

Fraktion BÜNDNIS 90/DIE GRÜNEN
Vorsitzenden Herrn Nils Fröhlich

- im Hause -

Ihr Ansprechpartner: Julian Vonarb
Dezernat für Allgemeine Verwaltung, Wirtschaft und Kultur
Geschäftsbereich des Oberbürgermeisters
Sitz: Kornmarkt 12, 07545 Gera
Zimmer: 117
Telefon: 0365 838 1001
Fax.: 0365 838 1005
E-Mail: Oberbuergermeister@gera.de
Aktenzeichen (bitte stets angeben):

Datum: 9. Mai 2022

T-Sicherheit in den digitalen Strukturen der Stadtverwaltung
e vom 01.04.2022

Herr Fraktionsvorsitzender Fröhlich,

Ihre oben genannte Anfrage möchte ich gern wie folgt beantworten:

1. **Wie viele Cyberangriffe gab es seit 2020 bis heute? (wir bitten um eine Übersicht mit Zeitpunkt, Art der Attacke, verursachter Schaden)**

Es wurden seit 2020 keine Angriffe als solche registriert. Ebenfalls wurden durch unsere Monitoringsysteme (Überwachungssysteme im Netzwerk) auch keine ungewöhnlichen Aktivitäten innerhalb unserer IT-Infrastruktur festgestellt, die auf einen erfolgreichen Angriff schließen lassen könnten. Über den zentralen E-Mail-Gateway werden monatlich ca. 120.000 Mails als Spam identifiziert. E-Mails stellen das größte Einfallsrisiko für potenzielle Angreifer dar und unterliegen aus diesem Grund unserer besonderen Aufmerksamkeit.

2. **Inwieweit gibt es ein Konzept zur IT-Sicherheit? Wann und von wem wurde dieses erstellt?**

Das IT-Sicherheitskonzept und die IT-Sicherheitsrichtlinie wurden 2010/2011 durch das Fachgebiet (FG) Organisation in Zusammenarbeit mit dem FG Information und Kommunikation erstellt. Allgemeine Aussagen zur IT-Sicherheit haben immer noch Gültigkeit. In der operativen Umsetzung wird die technische Entwicklung berücksichtigt.

3. **Wenn es bestehende Maßnahmen zur IT-Sicherheit gibt, inwieweit werden sie evaluiert und wie erfolgt diese Evaluation?**

Mit meiner Entscheidung zur Fortschreibung des Informationssicherheitskonzept vom 16.02.2022 werden die bestehenden Sicherheitsmaßnahmen evaluiert. Diese Evaluation erfolgt gemeinsam durch den IT-Sicherheitsbeauftragten (ISB), der Abteilung Digitalisierung und IT und externer Partner.

4. Inwieweit wird der IT-Grundschutz des BSI umgesetzt?

Bereits das IT-Sicherheitskonzept und die IT-Sicherheitsrichtlinie basierten auf den Empfehlungen zum IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). In der am 23.07.2020 erlassenen IT-Sicherheitsleitlinie ist die Umsetzung des BSI-Grundschutzes festgeschrieben.

5. Wer übernimmt die Aufsicht bei Fragen der Datensicherheit? (wir bitten um eine Übersicht ob extern/intern, stundenäquivalent oder eigene Stelle, bei welcher Qualifikation)

Es ist ein IT-Sicherheitsbeauftragter benannt, der Aufsicht bei Fragen der Datensicherheit wahrnimmt. Seit Januar 2020 wird die Stelle intern durch einen speziell ausgebildeten und zertifizierten Beschäftigten besetzt.

6. Inwieweit verfügt die Geraer Stadtverwaltung über eigenes IT-Fachpersonal? (wir bitten um eine Übersicht mit Abteilung, Anzahl des IT-Fachpersonals und der jeweiligen Qualifikation)

Dem Stellenplan ist zu entnehmen, dass die Abteilung Digitalisierung und IT für IT-Fachfragen innerhalb der Stadtverwaltung zuständig ist. Diese besteht aus 25 Beschäftigten, welche in verschiedene Teams aufgeteilt sind. Alle verfügen über entsprechende Fachkenntnisse und bilden sich stetig fort. Darüber hinaus werden den Beschäftigten fortlaufend Angebote zur weiteren bzw. tieferen Qualifikation unterbreitet.

7. Inwieweit erfolgt ein regelmäßiger Austausch mit anderen Kommunen über Maßnahmen der Informationssicherheit? (bitte um mindestens drei Beispiele: bzgl. der Kommune, Weg/Art der Kommunikation, konkret besprochenes Thema)

Der stattfindende, regemäßige Austausch war aufgrund der besonderen Situation in den vergangen 2 Jahren nur eingeschränkt möglich. Grundsätzlich findet ein interkommunaler Austausch in einer Ostthüringer und Westsächsischen Arbeitsgruppe statt die auch von regelmäßigen Treffen gekennzeichnet ist. Darüber hinaus gibt es einen regen Austausch im Rahmen der Digitalisierung von Verwaltungsleistungen und im Zusammenhang mit der regionalen Internetplattform mit nahezu allen größeren Landkreisen und Städten. Mit Weimar, Jena, Suhl und dem Wartburgkreis wird ein enger Austausch auf Arbeitsebene gepflegt.

8. Werden Kooperationen zur Erhöhung der IT-Sicherheit angestrebt? Wenn ja, welche?

Zur Erhöhung der IT-Sicherheit werden weitere Kooperationen angestrebt. Über die Kommunale Informationsverarbeitung Thüringen GmbH (KIV) deren Mitgesellschafter wir sind, die Mitgliedschaft im Zweckverband Kommunale Informationsverarbeitung Sachsen (KISA) und die enge Zusammenarbeit mit der Lecos GmbH werden bereits jetzt konkrete Maßnahmen zur Verbesserung der IT-Sicherheit umgesetzt. Diese Kooperationen sollen weiter ausgebaut werden.

9. Wie hoch ist der Anteil von Opensource-Software in der genutzten Verwaltungs-IT? (wir bitten um eine Übersicht mit Namen, Fierausgeber und Nutzungsgrund)

Im Zusammenhang mit der Umsetzung von Smart-City-Maßnahmen erhöht sich der Anteil der eingesetzten Open-Source Produkte. In den Umsetzungsrichtlinien des Bundesministeriums des Inneren, für Bau und Heimat ist festgelegt:

> *Open-Source- und Open-Knowledge-Ansätze sollen in den Modellprojekten umgesetzt sowie interoperable Lösungen und standardisierte Schnittstellen entwickelt und genutzt werden.*[1]

Darüber hinaus gab und gibt es immer wieder Bestrebungen und Versuche Open-Source Produkte zu implementieren. Im Bereich der den Arbeitsprozess unterstützenden Software kommen diese Produkte auch vermehrt zum Einsatz. Beispiele sind:

- Intranet auf Basis von Mediawiki
- Geracloud auf Basis von nextcloud
- Museumsbibliothek auf Basis von koha
- Videokonferenzsystem auf Basis von Big Blue Button
- spezielle Officeanwendungen aus dem LibreOffice Portfolio
- Content Management System für die Webseiten der Stadt - Joomla und Wordpress

Im kommerziellen und professionellen Umfeld ist Open-Source nicht mit „kostenlos" gleich zu setzen. Für den Einsatz werden teilweise Wartungs- und Pflegekosten erhoben, welche mit anderer proprietärer Software vergleichbar ist.
Die zur Unterstützung der Fachaufgaben eingesetzte Software (Fachanwendungen) unterliegt in großen Teilen speziellen Anforderungen durch gesetzliche Vorgaben. Vor allem Aufgrund der Verfügbarkeit gibt es nur wenig Spielraum für den Einsatz von Open-Source Software in diesen Bereichen.

10. Wie hoch sind die Gesamtausgaben für Maßnahmen der IT-Sicherheit im Haushalt? (bitte aufschlüsseln nach Gesamtvolumen und Anteil der Ausgaben für IT-Sicherheit)

Kosten für IT-Sicherheit lassen sich nicht explizit ausweisen und definieren. Jede Erneuerung und Aufrüstung der IT-Infrastruktur, der Software und auch der Arbeitsplatztechnik stellt auch eine Erhöhung der IT-Sicherheit dar, da so aktuelle Systeme im aktuellen Sicherheitslevel zum Einsatz kommen. Jedes Jahr wird für diese Maßnahmen ein höherer sechsstelliger Betrag in den Haushalt eingestellt und verausgabt.
Aufgrund der bekannten Haushaltssituation und der damit verbunden Zwänge, können regelmäßig nicht die Haushaltsmittel bereitgestellt werden, die zur Umsetzung der geplanten IT-Maßnahmen nötig sind. Diese Einschränkung beeinflusst auch Investitionen, die sich direkt oder indirekt auf die Erhöhung bzw. Sicherung der IT-Sicherheitsstandards auswirken. Darüber hinaus ist es für uns als öffentlicher Arbeitgeber eine besondere Herausforderung auf dem Arbeitsmarkt um gut ausgebildete, qualifizierte und motivierte Beschäftigte zu konkurrieren.

11. Welche Antivirenprogramme werden genutzt? Handelt es sich um käuflich zu erwerbende Lizenzen? (wir bitten um eine Übersicht mit jeweiligem Programm, Herausgeber, Kosten)

Wir setzen eine professionelle, zentral verwaltete Antivirensoftware ein. Diese Software arbeitet mit Suchalgorithmen unterschiedlicher Hersteller und kommt auf allen Windowsgeräten zum Einsatz.

---

[1] Bundesministerium des Innern, für Bau und Heimat Abteilung SW Stadtentwicklung, Wohnen, öffentliches Baurecht; https://www.smart-cities-made-in.de/foerdergegenstand/foerderfaehige-massnahmen/

Darüber hinaus wird das Produkt auch auf dem zentralen E-Mail-Gateway und der Webproxy genutzt. Unautorisiertes Verhalten von eingesetzten Linuxgeräten innerhalb unserer Infrastruktur wird durch besonders restriktiven Einsatz der lokalen Firewalls verhindert.

12. Wird noch das Antivirenprogramm „Kaspersky" des russischen Softwareunternehmens Kaspersky Lab genutzt? Wenn ja, in welchen Bereichen?

Nein, das Antivirenprogramm „Kaspersky" des russischen Softwareunternehmens Kaspersky Lab wird bei uns nicht genutzt.

13. Wurde das Antivirenprogramm „Kaspersky" durch ein anderes Programm ersetzt? Wenn ja, wann? (wir bitten um eine Übersicht mit Abteilung und Datum)

Das Antivirenprogramm „Kaspersky" ist in der IT-Infrastruktur der Stadtverwaltung auch in der Vergangenheit nicht eingesetzt worden.

14. Welche städtischen Einrichtungen und Strukturen mit kommunaler Beteiligung (z.B. des Verkehrs, der Energie- und Wärmeversorgung, ZVME, Rettungsdienste, Krankenhäuser, ÖPNV, Müllentsorgung, ...) sind digital zugänglich oder werden digital gesteuert? Wie werden diese vor Cyberangriffen geschützt? (wir bitten um eine Übersicht mit jeweiligen Sektoren und Schutzmaßnahmen)

Eigenbetriebe und Strukturen mit städtischer Beteiligung organisieren ihre IT-Dienste in eigener Zuständigkeit und Verantwortungen. Erkenntnisse darüber, welche digitalen Prozesse in diesen Einrichtungen etabliert, wie diese gesteuert werden und wie sich diese gegen Cyberangriffe schützen liegen uns nicht vor.

15. Wer ist zuständig, die Software zu aktualisieren, auf Sicherheitsvorfälle zu reagieren und Systemzustände zu überwachen? (wir bitten um eine Übersicht mit ob extern/intern, stundenäquivalent, Qualifikation)

Die Abteilung für Digitalisierung und IT im Haupt- und Personalamt überwacht fortlaufend die vertrauenswürdigen Updatequellen der jeweiligen Softwarehersteller. In weiten Teilen erfolgt die Installation der Updates über automatisierte Updatemechanismen. Die regelmäßige und anlassbezogene, d.h. auf das aktuelle Sicherheitsgeschehen abgestimmte, Updateinstallation stellt einen wesentlichen Bestandteil unsere IT-Sicherheitsstrategie dar.

16. Liegt ein Plan oder Konzept für den Fall vor, dass ein Bereich ungeplant ausfällt oder gehackt wurde? Wann und von wem wurde dieser/dieses erstellt? Inwieweit darf dies unter der Berücksichtigung von Sicherheitsaspekten beschrieben werden? (Bitte um Beschreibung so weit wie aus Sicherheitsgründen möglich, wenn Berichterstattung nicht möglich, bitte rechtliche Grundlage dafür nennen)

Im operativen Bereich wurden bereits Vorgehensweisen eruiert und erprobt. Im Zusammenhang mit dem Fortschreiben des IT-Sicherheitskonzeptes soll auch ein IT-Notfallplan erstellt werden, um auf die genannten Fälle strukturiert und standardisiert zu reagieren.

17. Inwieweit ist das Personal der Stadtverwaltung gegenüber digitalen Risiken sensibilisiert? (wir bitten um eine Übersicht mit jew. Personal, Abteilung und wie es sensibilisiert/geschult wird)

In 2020 und 2021 fanden drei Live-Hacking-Veranstaltungen im KuK statt, in denen eine große Anzahl von Beschäftigten sensibilisiert wurde. Anhand des Feedbacks der Beschäftigten kann auf einen beachtlichen Multiplikationseffekt geschlossen werden. Weitere Sensibilisierung erfolgt durch regelmäßige Hinweise auf digitale Gefahren im Intranet/SVG-Wiki.

In Anwendung von § 22 Abs. 2 Satz 2 der Geschäftsordnung des Stadtrates der Stadt Gera und seiner Ausschüsse erhält auch jede Fraktion im Stadtrat die Anfrage sowie diese Antwort zur Kenntnis.

Mit freundlichen Grüßen

Julian Vonarb
Oberbürgermeister