Landeshauptstadt Magdeburg

Stellungnahme der Verwaltung

öffentlich

Stadtamt	Stellungnahme-Nr.	Datum
Amt 12	S0053/25	11.02.2025

zum/zur

F0031/25 CDU/FDP – Stadtratsfraktion, Manuel Rupsch

Bezeichnung

IT-Sicherheit und Schutz vor Cyberangriffen in der Stadtverwaltung Magdeburg

Verteiler	Tag
Die Oberbürgermeisterin	25.02.2025

Am 10. Januar 2025 meldete die Landeshauptstadt Dresden einen umfassenden IT-Blackout: Parktickets konnten nicht mehr ausgestellt werden, die Zulassungsstelle, das Kita-Portal und Finanzbuchungen waren vollständig ausgefallen. Auch die „Dresden Cloud“ war lahmgelegt. Zu diesem Zeitpunkt fand zudem eine Bombenentschärfung statt. Ausgerechnet während dieses Vorfalls fiel auch die Website www.dresden.de aus, wodurch die Bürgerinnen und Bürger keine Informationen mehr erhalten konnten. Dieser Vorfall zeigt auf, wie anfällig die IT-Infrastruktur im Bereich der Verwaltung ist. Auch der Cyberangriff auf den Landkreis Anhalt-Bitterfeld verdeutlicht die Bedrohungslage und die Schwachstellen in der öffentlichen Verwaltung.

Laut securityheaders.com weist die Landeshauptstadt Magdeburg in der Kategorie „IT-Sicherheit“ die Bewertung „C“ auf, was nicht optimal ist. In der heutigen global vernetzten IT-Welt ist es nicht mehr die Frage, ob Städte von Cyberangriffen betroffen sein werden, sondern vielmehr, wann. Besonders im Bereich der Künstlichen Intelligenz beobachten wir einen signifikanten Anstieg an kriminellen Aktivitäten.

Die Verwaltung nimmt Stellung und beantwortet die Fragen wie folgt:

Aufgrund der weltweiten Cybersicherheitslage äußert sich die Verwaltung der Landeshauptstadt Magdeburg nicht öffentlich zu Details der IT-Sicherheit.

Für die Verwaltung können diesbezügliche Fragen jedoch gerne in einem direkten Gespräch der Fraktionen mit dem Informationssicherheitsbeauftragten, Herrn Matthias Schmitz, beantwortet werden.

Die KID Magdeburg GmbH (nachfolgend KID) beauftragt regelmäßige (quartalsweise) Scans aller öffentlich erreichbaren Server der KID. Die Ergebnisse werden analysiert und es werden, sofern relevant und möglich, entsprechende Härtungsmaßnahmen eingeleitet.

Die Gesamtbewertung der Scanergebnisse für die einzelnen Server ergibt sich hierbei aus sicherheitsgefährdenden Funden (z.B. Schwachstellen) sowie aus Abweichungen zu allgemeinen Empfehlungen, welche jedoch kein direktes Sicherheitsrisiko für das Stadtnetz darstellen.

Die im Scan von securityheaders.com für die Website www.magdeburg.de vermerkten Funde haben keine Sicherheitsrelevanz für das Stadtnetz.

1. **Wie viele IT-Angriffe gab es im vergangenen Jahr auf die Verwaltung der Landeshauptstadt Magdeburg?**

   Die folgenden Angaben beziehen sich ausschließlich auf Angriffsversuche, welche mittels Firewall durch die KID auf Netzebene detektiert wurden.

   Geblockte Angriffe:
   Ca. 500 pro Tag - ca. 180.000 pro Jahr
   (nicht mitgezählt sind Angriffe auf Applikationsebene, wie z. B. user/login-Versuche)

   Gebockte Spam/Phishing/Malware E-Mails:
   durchschnittlich ca. 40.000 pro Tag - ca. 14,6 Mio. pro Jahr

   Außerhalb dieser gab es im Jahr 2024 keine IT-Angriffe.

2. **Ist es möglich, die Herkunft der Angriffe zu lokalisieren? Gibt es Muster oder geografische Schwerpunkte?**

   keine Angaben möglich

3. **Wurden besonders schützenswerte Bereiche, wie beispielsweise das Amt 37, Ziel von IT-Angriffen?**

   Da das Stadtnetz vom öffentlichen Internet getrennt ist, gibt es bei Angriffsversuchen auf die Firewall keinen speziellen Bereich oder Amt, der angegriffen wird.

   Gezieltere Angriffe erfolgten im letzten Jahr nicht.

4. **Welche Maßnahmen ergreift die Stadt Magdeburg, um ihre IT-Infrastruktur bestmöglich zu schützen?**

   Zur Absicherung des Rechenzentrumbetriebs hält die KID als IT-Dienstleister der LH Magdeburg ein Informationssicherheitsmanagementsystem (ISMS) entsprechend ISO/IEC 27001 aufrecht und verbessert dieses fortlaufend. Die KID setzt in diesem Zusammenhang diverse Sicherheitsmaßnahmen um, die unter anderem als technische und organisatorische Maßnahmen vertraglich vereinbart sind.

   Die Stadtverwaltung selbst hat zusätzlich technische und organisatorische Maßnahmen im Einsatz, um die IT-Sicherheit zu erhöhen. Dazu gehören Schulungen, Richtlinien und Sicherheitslösungen. Die Stadt baut zurzeit ein eigenes ISMS nach ISO/IEC 27001 auf der Basis von IT-Grundschutz auf.

5. Welche finanziellen Mittel sind für die kommenden Jahre erforderlich, um einen umfassenden Schutz gegen Cyberangriffe sicherzustellen?

Informationssicherheit ist eine tragende Säule des laufenden Betriebs von IT-Systemen. Der Betrieb der IT-Systeme auf dem aktuellen Stand der Technik beinhaltet bereits Maßnahmen zum Schutz gegen Cyberangriffe. Konkrete Werte lassen sich nicht benennen, da die technische Entwicklung auch im Bereich der Informationssicherheit/Angriffsvektoren nur schwerlich für mehrere Jahre vorhergesagt werden kann. Grundsätzlich lässt sich festhalten, dass ein adäquates IT-Budget für einen zeitgemäßen IT-Betrieb notwendig ist und damit wesentliche Vorkehrungen gegen erfolgreiche Angriffe gegen die IT-Infrastruktur getroffen werden können. Grundsätzlich müssen IT-Budgets in den nächsten Jahren steigen, um sowohl Teuerungen der IT-Dienstleistungen als auch inhaltliche Erweiterungen der IT-Services abzudecken.

6. Welche Vorkehrungen trifft die Stadt Magdeburg, um einen ähnlichen Cyberangriff wie im Landkreis Anhalt-Bitterfeld zu verhindern?

Ein Cyberangriff nach Muster des Angriffs auf den Landkreis Anhalt-Bitterfeld (2021) ist in der Landeshauptstadt Magdeburg nicht möglich.

In der Landeshauptstadt Magdeburg sind verschiedene Sicherheitsmaßnahmen und -konzepte umgesetzt, welche im Landkreis Anhalt-Bitterfeld zum Zeitpunkt des Angriffs nicht bestanden, u. a.:

- Sicherung der Zugänge zum Stadtnetz über gesicherte Wege und konsequente Netztrennung zum Internet
- Vergabe administrativer Berechtigungen erfolgt bedarfsweise nach dem Prinzip der geringsten Privilegien

Borris