Landeshauptstadt Magdeburg

Stellungnahme der Verwaltung

öffentlich

Stadtamt	Stellungnahme-Nr.	Datum
Amt 12	S0358/21	23.08.2021

zum/zur

F0219/21
Fraktion FDP/Tierschutzpartei - Stadträtin Carola Schumann

Bezeichnung

IT-Sicherheit / Schutz vor Cyberangriffen

Verteiler	Tag
Der Oberbürgermeister	31.08.2021

Sehr geehrter Herr Oberbürgermeister,

der Landkreis Anhalt-Bitterfeld hat infolge eines Hackerangriffs auf das Computersystem der Kreisverwaltung mit einem Trojaner am 6. Juni 2021 den bundesweit ersten Cyber-Katastrophenfall ausgerufen. Die Verwaltung wurde durch die Attacke arbeitsunfähig, sodass keine Dienstleistungen für die Bürgerinnen und Bürger mehr angeboten und zum Beispiel keine Sozial- und Unterhaltsleistungen mehr ausgezahlt werden können bzw. konnten. Nach Aussagen von Expertinnen und Experten sei die kommunale IT-Infrastruktur in Deutschland allgemein nur unzureichend gegen Cyberangriffe geschützt.

Ich frage Sie daher:

1. Wie ist die Landeshauptstadt Magdeburg nach Ihrer Einschätzung auf mögliche Cyberangriffe bzw. die Abwehr von Hackerangriffen vorbereitet?

2. Mit welchen Maßnahmen und personellen Ressourcen werden die IT-Systeme der Stadtverwaltung und die zahlreichen gespeicherten Daten der Bürgerinnen und Bürger geschützt?

3. Sind aufgrund der sich häufenden Angriffe weitere Maßnahmen vorgesehen?

4. Wo ist der Schutz der IT-Technik der Landeshauptstadt angesiedelt?

5. Waren bereits Cyberangriffe auf das Computersystem der Stadtverwaltung zu verzeichnen?

   Wenn ja: Wie wurden diese abgewehrt und welche Auswirkungen hatten diese?

6. Auf welchem Stand ist die IT-Technik der Stadtverwaltung und entspricht diese den aktuellen Anforderungen an die IT-Sicherheit?

Wie folgt wird Stellung genommen:

1. Wie ist die Landeshauptstadt Magdeburg nach Ihrer Einschätzung auf mögliche Cyberangriffe bzw. die Abwehr von Hackerangriffen vorbereitet?
Die Bereitstellung und der Betrieb der IT-Infrastruktur der Verwaltung der Landeshauptstadt Magdeburg erfolgen seit 1999 durch die Kommunale Informationsdienste Magdeburg GmbH (KID) als beauftragtem IT-Dienstleister, welcher sich zu 100% in kommunalem Eigentum befindet. Diese betreibt am Standort Magdeburg ein eigenes Rechenzentrum für die Services und Fachverfahren der Landeshauptstadt. Der sichere Betrieb der IT-Landschaft der Landeshauptstadt wird dabei zentral wie dezentral durch eine mehrstufige hard- und softwarebasierte IT-Sicherheitsarchitektur und Datensicherungslösung gewährleistet. Im Rahmen der bestehenden Verträge mit der KID Magdeburg GmbH werden dafür auch die Konzeption und die Umsetzung der IT-Sicherheitsorganisation sowie die damit verbundenen Prozesse zur Informationssicherheit durch die KID abgebildet. Um durchgängig die Sicherheit der Daten während der Verarbeitung zu gewährleisten, hat die KID nationalen und internationalen Empfehlungen folgend seit 2004 ununterbrochen ein Informationssicherheitsmanagementsystem (ISMS) gemäß internationaler Norm ISO/IEC 27001 implementiert. Wesentlicher Bestandteil der Zertifizierung ist die fortlaufende Prüfung und Umsetzung technischer und organisatorischer Maßnahmen zum Schutz vor Cyberangriffen, Schadsoftware und unbefugtem Zugang zu Informationen im Betrieb der IT-Infrastruktur.

2. Mit welchen Maßnahmen und personellen Ressourcen werden die IT-Systeme der Stadtverwaltung und die zahlreichen gespeicherten Daten der Bürgerinnen und Bürger geschützt?
Grundlage des Schutzes vor unautorisiertem Zugriff auf die Daten der Bürgerinnen und Bürger bildet ein mehrstufiges IT-Sicherheits- und Datensicherungskonzept. Dieses stellt technisch und organisatorisch sicher, dass alle Informationen sicher gespeichert werden, damit die Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der Daten während des gesamten Verarbeitungsprozesses gewährleistet sind. Darüber hinaus wird durch ein mehrstufiges Backupsystem die sichere Aufbewahrung der Daten für den Fall einer Wiederherstellung gewährleistet. Die notwendigen fachlichen und personellen Ressourcen zum sicheren IT-Betrieb der Landeshauptstadt Magdeburg werden durch die KID Magdeburg GmbH im Rahmen der vereinbarten Services bereitgestellt.
Ergänzend werden in regelmäßigen Abständen externe IT-Sicherheitsunternehmen mit der Durchführung von Penetrationstests beauftragt, um mögliche Schwachstellen noch besser identifizieren und beseitigen zu können. Die Ergebnisse fließen in die Analysen und laufenden Maßnahmen zur Verbesserung der IT-Sicherheitsarchitektur und -infrastruktur ein.
Letztlich entscheidender Faktor beim Thema Informationssicherheit ist der mit den IT-Systemen agierende Mensch, weshalb für die Mitarbeiter KID Magdeburg GmbH laufende Sensibilisierungs-/Schulungsmaßnahmen eine unabdingbare Notwendigkeit darstellen.

3. Sind aufgrund der sich häufenden Angriffe weitere Maßnahmen vorgesehen?
Als Bestandteil des Informationssicherheitsprozesses für den sicheren Betrieb des Rechenzentrums ist die IT-Sicherheit von essenzieller Bedeutung. Mit dem stetigen quantitativen und qualitativen Wachstum an Schadsoftware und dem erhöhten Aufkommen von Cyberkriminalität werden auch die Maßnahmen zum Schutz vor den Bedrohungen für die Informationssicherheit immer komplexer. Die KID Magdeburg GmbH passt ihre IT-Sicherheitsstrategie in Zusammenarbeit mit der Landeshauptstadt und den Sicherheitsbehörden der Bundesrepublik fortlaufend den aktuellen Anforderungen an. Neben zahlreichen Standardmaßnahmen wie Virenschutz, Filtertechnologien, dem Einsatz von Firewalls neuester Generation im Zusammenspiel mit der regelmäßigen Aktualisierung der Software wird es immer wichtiger, schnellstmöglich auf erkannte Schwachstellen zu reagieren. Die KID Magdeburg GmbH partizipiert als Teilnehmer der Allianz für Cyber-Sicherheit (ACS) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aktuell und fortlaufend von Sicherheitswarnungen und kann zeitnah auf IT-Bedrohungen reagieren.

4. Wo ist der Schutz der IT-Technik der Landeshauptstadt angesiedelt?
Die IT-Infrastruktur und sowie der Schutz der IT-Technik der Landeshauptstadt wird vom IT Dienstleister KID Magdeburg GmbH am Standort Magdeburg betrieben.

5. Waren bereits Cyberangriffe auf das Computersystem der Stadtverwaltung zu verzeichnen? Wenn ja, wie wurden diese abgewehrt und welche Auswirkungen hatten diese?
Jede IT-Sicherheitsinfrastruktur ist permanent und fortlaufend einer Vielzahl von Cyberangriffen ausgesetzt. Dies trifft selbstverständlich auch auf die IT der Verwaltung der Landeshauptstadt zu.
Nahezu alle Cyberangriffe sind nicht zielgerichtet bezogen auf die Stadtverwaltung, sondern versuchen generell bekannte Schwachstellen in der IT-Infrastruktur auszunutzen. Durch das IT-Sicherheitskonzept der KID Magdeburg GmbH werden diese abgefangen und eliminiert.

6. Auf welchem Stand ist die IT-Technik der Stadtverwaltung und entspricht diese den aktuellen Anforderungen an die IT-Sicherheit?
IT-Sicherheit ist kein statischer Zustand, der einmal definiert bis zur Erneuerung der gesamten IT-Umgebung betrieben wird. Einer der Kernfaktoren dafür sind die regelmäßige Planung und Anpassung der IT-Technik und -Architektur. Die zyklische Erneuerung der IT-Technik und der damit verbundenen Planung der personellen und materiellen Ressourcen ist einer der Grundbausteine des Informationssicherheitsmanagementsystems der KID Magdeburg GmbH. Die regelmäßige Überprüfung des Standes der Technik im Rahmen der Zertifizierung des Rechenzentrums durch einen externe Prüforganisation stellt sicher, dass die aktuellen Anforderungen stets gegeben sind.

Dr. Trümper