Land **Burgenland**

Hans Peter Doskozil
Landeshauptmann

Frau Landtagspräsidentin
Mag.a Astrid Eisenkopf
Landhaus / Europaplatz 1
7000 Eisenstadt

Eisenstadt, 05. Dezember 2025

Sehr geehrte Frau Landtagspräsidentin!

Die von Herrn Landtagsabgeordneten Mag. Christian Sagartz, BA, gemäß Art. 44 L-VG iVm § 29 der GeOLT an mich gerichtete schriftliche Anfrage vom 24. Oktober 2025, Zl. 2100-0315, betreffend „IT-Sicherheit", beantworte ich schriftlich wie folgt:

1. Gab es seit 2022 Cyber-Angriffe auf die IT-Infrastruktur der Landesregierung Burgenland?
a. Falls ja: Wann, in welcher Form und in welchem Ausmaß?
b. Welche Systeme waren betroffen?
c. Welche unmittelbaren Maßnahmen wurden ergriffen?
2. Welche IT-Sicherheitsmaßnahmen bestehen derzeit im Amt der Burgenländischen Landesregierung?
a. Ist eine flächendeckende Zwei-Faktor-Authentifizierung implementiert?
b. Gibt es ein IT-Notfallhandbuch?
c. Bestehen funktionierende Backup- und Wiederherstellungsstrategien?
3. Welche Strukturen zur aktiven Überwachung und Abwehr von Angriffen sind eingerichtet?
a. Gibt es ein Security Operations Center (SOC) oder eine vergleichbare Einrichtung?
b. Werden externe Dienstleister für Cyber-Security beauftragt?
4. Welche präventiven Maßnahmen setzt die Landesregierung, um CyberAngriffe zu verhindern?
a. Gibt es verpflichtende Schulungen für Bedienstete?
b. Werden regelmäßig externe Sicherheitsüberprüfungen durchgeführt?
5. Welche Lehren wurden aus dem Kärntner Cyber-Angriff gezogen und auf Landesebene im Burgenland umgesetzt?

Zu den Fragen 1 bis 5:

Es gab keine erfolgreichen Cyberangriffe auf die Systeme der Landesregierung. Die IT-Infrastruktur wird – wie alle privaten und öffentlichen Organisationen - jedoch fortlaufend Ziel automatisierter Angriffsversuche, insbesondere durch Spam-Mails sowie durch regelmäßige Scans nach potenziellen Schwachstellen der extern erreichbaren Dienste. Diese Aktivitäten werden kontinuierlich überwacht und durch geeignete Sicherheitsmaßnahmen abgewehrt. In der IT-Infrastruktur der Landesregierung ist ein mehrstufiges Konzept mit moderner IT-

Sicherheitsmaßnahmen für Clients, Server und Netzwerke implementiert. Dazu zählen unter anderem die Anwendung eines Least-Privilege-Prinzips welches den Anwendern nur die notwendigsten Rechte gibt und nach dem Need-to-know-Prinzip zu begründen sind, ein Antiviren-System mit EDR/XDR-Funktionalität, eine State-of-the-Art-Firewall, die Umsetzung von Best Practices im Netzwerkdesign (z. B. Mikrosegmentierung), ein durchdachtes User-Tiering-Modell, Webfiltering durch Proxy-Server sowie eine verhaltensbasierte Analyse des Netzwerkverkehrs zur Erkennung von schädlichen Aktivitäten und Inhalten (Malicious Content). Diese Maßnahmen tragen maßgeblich zur Erhöhung der IT-Sicherheit und zum Schutz der Systeme vor Cyberangriffen bei. Für externe, öffentlich erreichbare Dienste erfolgt eine Zwei-Faktor-Authentifizierung (2FA) über das Stammportal des Landes mittels SMS, Authenticator-App oder ID-Austria. 2023 wurde das IT-Notfallhandbuch zur Ergänzung der bestehenden Richtlinien für IT-Sicherheit und Datenschutz erlassen. Die praktische Anwendung wurde in einem Cybersecurity-Planspiel beübt. Backup- und Wiederherstellungsstrategien sind Teil der IKT-Richtlinien und nutzen ein zentrales Service für Bandsicherungen im Rechenzentrum. Die größte Angriffsfläche innerhalb der IT-Infrastruktur stellen die Client-Geräte dar. Um diese gezielt zu schützen, wurde über einen Dienstleister ein MDR Service (Managed Detection and Response, d.h. eine 24/7-Überwachung) eingerichtet. Dabei werden Alarme für potenzielle Bedrohungen rund um die Uhr von einem Security-Center analysiert und nach einem technischen Regelwerk automatisch abgewehrt. Weiter wurde zum Schutz der mobilen Geräte (Smartphones) ein MDM (Mobile Device Management) eingeführt. Zusätzlich wird derzeit gemeinsam mit anderen Organisationen im „Haus Burgenland“ über die Digital Burgenland an der Ausschreibung für ein Security Operations Center (SOC) gearbeitet. Es werden regelmäßig externe Audits durch Dienstleister, sowie Schwachstellenscans, Penetrationstests und Lasttests durchgeführt, um die IT-Infrastruktur auf Sicherheitslücken und mögliche Angriffsvektoren zu überprüfen. Zudem gibt es Dienstleistungsverträge mit Experten der für die IT-Infrastruktur des Landes relevanten Hersteller um mit deren Fachwissen bei der Implementierung von Best-Practice-Vorgaben zu unterstützen und so die kontinuierliche Verbesserung der Sicherheitsmaßnahmen zu ermöglichen. Es finden verpflichtende Cybersicherheitsschulungen für alle Mitarbeiter statt. Die Schulungen werden über die Akademie Burgenland in Form eines E-Learning-Kurses angeboten. Darüber hinaus wird im Rahmen der Grundausbildung gezielt auf IT-Sicherheit mit Praxisbezug eingegangen, um den Mitarbeitern konkrete, praktische Tipps zur sicheren Nutzung der IT-Systeme zu vermitteln. Im November und Dezember d.J. werden zudem in Kooperation mit dem Bundesministerium für Inneres (Mitarbeiter*innen der NIS Behörde) spezielle Schulungen über die Akademie Burgenland in den Räumlichkeiten der Hochschule abgehalten. Im Rahmen des IKT-Expertennetzwerks der BLSG (Bund-Länder-Städte-Gemeinden) wurden der Angriff beim Land Kärnten analysiert und befunden, dass eine 24/7-Überwachung der Client-Geräte unbedingt erforderlich ist, um auch außerhalb regulärer Arbeitszeiten eine adäquate Reaktion auf Sicherheitsvorfälle gewährleisten zu können und schließlich das MDR Service implementiert. Dieses ermöglicht eine rund um die Uhr funktionierende Überwachung und Reaktion auf Sicherheitsvorfälle.

Mit freundlichen Grüßen

Landeshauptmann Mag. Hans Peter Doskozil

7000 Eisenstadt, Europaplatz 1 – Landhaus
Telefon +43 2682 600-2200, zum Ortstarif 057 600-2200
Fax +43 2682 600-2900, E-Mail hans-peter.doskozil@bgld.gv.at
Datenschutz: https://www.burgenland.at/datenschutz