Nr. 102-BEA der Beilagen zum stenographischen Protokoll des Salzburger Landtages
(3. Session der 16. Gesetzgebungsperiode)

Beantwortung der Anfrage

der Abg. Zweiter Präsident Dr. Huber, Klubobmann Egger MBA und Weitgasser an die Landesregierung (Nr. 102-ANF der Beilagen) – ressortzuständige Beantwortung durch Landeshauptmann Dr. Haslauer – betreffend EDV-Sicherheit im Land Salzburg

Hohes Haus!

Zur Beantwortung der Anfrage der Abg. Zweiter Präsident Dr. Huber, Klubobmann Egger MBA und Weitgasser betreffend EDV-Sicherheit im Land Salzburg vom 29. Jänner 2020 erlaube ich mir, Folgendes zu berichten:

Zu den Fragen 1 und 2:
Frage 1: Wurden in den Jahren 2016 bis 2020 die IT-Systeme des Landes Salzburg durch Cyberattacken angegriffen (Aufschlüsselung nach Jahren)?
Frage 2: Wie viele und welche IT-Systeme welcher Abteilungen wurden dabei angegriffen?

In den Jahren 2016 bis 2020 gab es keine erfolgreichen Cyberattacken auf die IT-Systeme des Landes Salzburg.
Angriffsversuche auf die IT-Systeme des Landes Salzburg und Versuche, z. B. durch Phishing- und SPAM Mail Attacken an Daten und Anwenderinformationen zu gelangen, gibt es jedoch laufend. Eine Aufschlüsselung der Angriffe ist nicht möglich, da diese Angriffe permanent und in großer Menge erfolgen (Details dazu siehe Beantwortung zu Punkt 3.)

Zu Frage 3: Welcher Schaden entstand dabei und wie hoch war dieser?

Es entstand noch kein Schaden durch Cyberattacken, jedoch wird der Aufwand (Personal- und Systemressourcen) für Präventivmaßnahmen und zur Abwehr von Angriffsversuchen überproportional höher.

Im Jahr 2019 mussten beispielsweise 950 Sicherheits-Schwachstellen (Fehlerhafte Softwarekomponenten der Hersteller, die potentiell von Angreifern ausgenutzt werden könnten) an zentralen IT-Komponenten behoben und ca. 1 Mio. Spam- und Phishing Mails monatlich abgewehrt werden (das sind in etwa 75 % des Mailverkehrs).

Zu Frage 4: Wie wird die Handlungsfähigkeit der Behörden und ihrer IT-Systeme bei großangelegten Cyberangriffen oder Elementarereignissen gewährleistet?

Aus Koordinierungssicht der für das Sicherheitsmanagement der Landesverwaltung zuständigen Dienststelle 0/15 stellt der Aspekt der IT/EDV-Sicherheit einen sicherheitsrelevanten Teilbereich dar, der vor allem auf die Fragen der Betriebs-, Ausfalls-, Daten- und Zugriffssicherheit fokussiert.

Wenngleich sich in der routinemäßigen Umsetzung bzw. Wahrnehmung der dabei verfolgten Sicherheitsziele die Fachgruppe 0/2 – Landesinformatik verantwortlich zeichnet, sind dem Referat Sicherheit und Katstrophenschutz vor allem die Teilbereiche „Betriebs- und Ausfallssicherheit“ im Interesse der behördlichen Einsatzkoordinierung- und -führung im Falle von Großschadens- und Katastrophenfällen ein besonderes Anliegen.

Redundante Datenleitungen zur Sicherstellung der EDV-basierten Kommunikationswege sowie Notstromversorgung mittels USV-Anlagen zur kurzfristigen und Notstromaggregate zur mittel- bis längerfristigen Stromversorgung im Falle des Ausfalls in Folge von Elementarereignissen oder gar eines Black Outs sind dazu die derzeit dem Stand der Technik entsprechenden Antworten.

Flächendeckende Redundanzen zu diesen Teilaspekten existieren auf Grund der Vielzahl der von der Landesverwaltung betriebenen Standorte derzeit nicht. Die Errichtung des in Planung befindlichen Dienstleitungszentrums sollte der Landesverwaltung aber die Möglichkeit bieten, diesem Erfordernis in einer neuen und vor allem zukunftsträchtigen Form gerecht zu werden.

Im Zusammenhang mit dem IT-Schutzsystem wird um Verständnis gebeten, dass Details/Produktnamen nicht öffentlich bekannt gegeben werden. Generell wird der Schutz der IT-Systeme des Landes u. a. durch folgende Vorkehrungen und Maßnahmen der Fachgruppe 0/2 – Landesinformatik gewährleistet:

- IT-Architektur:
  Beim Aufbau der IT-Systeme und Schnittstellen ist die IT-Sicherheit ein wesentliches Kriterium, einheitliche IT-Standards. IT-Systeme und Daten sind mehrfach redundant und ausfallsicher vorhanden. Im Organisationshandbuch der Fachgruppe 0/2 sind für alle Security-Belange die Prozesse unter Berücksichtigung von Risikobewertungen definiert.
- IT-Katastrophenvorsorge-Tests:
  Die Simulation eines Standortausfalls und andere mögliche Ausfallszenarien werden laufend geübt und anhand dieser Erkenntnisse werden ständig Verbesserungsmaßnahmen durchgeführt.
- Einsatz moderner und aktueller IT-Schutzkomponenten (z. B.: Firewalls, Virenscanner mit KI-Technologie, Cybersecurity Detection Technologie.
- Schulung der Anwender:
  Verhalten bei einem Virenvorfall, Phishing-Mails, Social Engineering, Umgang mit sensiblen Daten und Kennwörtern.

- Schwachstellenmanagement:
  Laufende Analyse der eingesetzten IT-Komponenten auf Hersteller-Schwachstellen, Fehlkonfigurationen, Angriffsversuche, etc. Risikobewertung, Maßnahmen zur Beseitigung von Schwachstellen, setzen von Präventiv- und Qualitätssicherungsmaßnahmen. Laufende, automatisierte Überprüfung der Eigenentwicklung auf neu bekannt gewordene Schwachstellen in den verwendeten Entwicklungssystemen.
- Präventionsmaßnahmen:
  Zusammenarbeit bei Cyberangriffen mit externen Spezialfirmen, Internet-Providern, Landes- und Bundesbehörden sowie der Polizei.
- Monitoring:
  Jährliche Security-Strategie Workshops sowie quartalsmäßige Security-Jour Fixes der Führungskräfte mit dem zentralen Security-Team werden abgehalten. Die Qualität und effiziente Prozess-Durchlaufzeit der Präventiv-Maßnahmen wird über einen international standardisierten Wert (Risc-Score-Card) von den Führungskräften überwacht.

Ich ersuche das Hohe Haus um Kenntnisnahme dieser Anfragebeantwortung.

Salzburg, am 11. März 2020

Dr. Haslauer eh.