BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2024 / 527 von Hannes Hänggi: «IT-Sicherheit in der Verwaltung: Wie gross ist die Abhängigkeit von Drittanbietern?»
2024/527

vom 11. Februar 2025

1. Text der Interpellation

Am 29. August 2024 reichte Hannes Hänggi die Interpellation 2024/527 «IT-Sicherheit in der Verwaltung: Wie gross ist die Abhängigkeit von Drittanbietern?» ein. Sie hat folgenden Wortlaut:

Mitten in den Sommerferien führte ein fehlerhaftes Update der US-Cybersicherheitsfirma «Crowdstrike» zu einem weltweiten Ausfall von Millionen Computern, die unter dem Betriebssystem Windows liefen. Betroffen waren auch kritische Infrastrukturen wie Spitäler und die Flugsicherung Skyguide. Zwar wurde der Fehler rasch behoben, er zeigte aber die Anfälligkeit und Fragilität unseres modernen Lebens, das ohne Computer nicht mehr denkbar wäre. Verdeutlicht wurde dies zudem durch den Cyberangriff auf die Baselbieter Steuerverwaltung kurz darauf, der aber mit «Crowdstrike» nichts zu tun hatte.

Der Kanton unternimmt viele Anstrengungen, die Gefahr durch Cyberangriffe möglichst klein zu halten und den Ausfall von Computersystemen möglichst zu verhindern. Durch die zunehmende Digitalisierung steigt die Anfälligkeit aber trotzdem.

Der Regierungsrat wird gebeten, folgende Fragen zu beantworten:

1. Waren im Kanton Basel-Landschaft Verwaltungseinheiten und Institutionen mit Beteiligungen des Kantons vom Computerausfall wegen «Crowdstrike» betroffen? Waren auch kritische Infrastrukturen betroffen?

2. Existieren in der Verwaltung redundante, diversitäre Systeme (z. B. mit anderen Betriebssystemen), um im Falle eines Ausfalls die wichtigsten Funktionen aufrechtzuerhalten?

3. Werden Software-Updates in der Verwaltung auf allen Computern gleichzeitig ausgeführt oder zeitverschoben, um allfällige Fehler erkennen zu können?

4. Wie stark ist die Abhängigkeit der im Kanton eingesetzten Software von Microsoft? Werden Alternativen geprüft?

5. Wie steht es um die digitale Souveränität in der Verwaltung? Gibt es Bestrebungen, die Abhängigkeiten von Drittanbietern bei IT-Produkten und -Dienstleistungen möglichst gering zu halten?

2. Einleitende Bemerkungen

Die Interpellation referenziert auf den weltweiten Ausfall von Windows-Systemen, welcher von einem Update der Software Crowdstrike ausgelöste wurde. Der Vorstoss adressiert dazu für die kantonale Verwaltung Basel-Landschaft wichtige Fragestellungen.

Der Regierungsrat begrüsst die Sensibilisierung und Unterstützung des Landrats für die Anliegen der Cybersicherheit. Mit den nachfolgenden Antworten wird auch dargelegt, mit welchen bereits etablierten oder geplanten Massnahmen adressierte Risiken minimiert werden.

3. Beantwortung der Fragen

1. *Waren im Kanton Basel-Landschaft Verwaltungseinheiten und Institutionen mit Beteiligungen des Kantons vom Computerausfall wegen «Crowdstrike» betroffen? Waren auch kritische Infrastrukturen betroffen?*

Die kantonalen Verwaltungseinheiten und Institutionen mit Beteiligungen nutzen die Software Crowdstrike nicht. Es waren damit keine Infrastrukturen dieser Einheiten und Beteiligungen von diesem spezifischen Problem betroffen.

2. *Existieren in der Verwaltung redundante, diversitäre Systeme (2. B. mit anderen Betriebssystemen), um im Falle eines Ausfalls die wichtigsten Funktionen aufrechtzuerhalten?*

Die Systemlandschaft und Prozesse der kantonalen Verwaltung BL sind darauf ausgerichtet Ausfallrisiken zu minimieren. Dazu gehören unter anderem redundante Rechenzentren, eine unabhängige Stromversorgung der wichtigsten Standorte und kritische Services welche unterschiedliche Technologien verwenden, um bei Störfällen verfügbar zu bleiben. Ein Beispiel für einen solchen Service mit parallel betriebenen (diversitären) Technologien ist die Kommunikation von Blaulichtorganisationen, welche beim Ausfall eines Systems auf eine alternative Lösung umgestellt werden kann.

Die operative Sicherstellung der Systemverfügbarkeit gehört zum festen Bestandteil des Tagesgeschäfts der Informatik-Organisation, beispielsweise die Durchführung von Backups, die Pflege von Firewallregeln oder das Einspielen von Sicherheitsupdates. In der Informatik- und Kommunikationstechnologie (IKT) kann ein Ausfall jedoch nie vollständig ausgeschlossen werden. Deshalb ist die Vorbereitung auf Sicherheitsereignisse und deren Bewältigung inklusive der Wiederherstellung der Leistungen ein wichtiger Bestandteil des IT Service Continuity Managements (ITSCM) und des Business Continuity Managements (BCM).

3. *Werden Software-Updates in der Verwaltung auf allen Computern gleichzeitig ausgeführt oder zeitverschoben, um allfällige Fehler erkennen zu können?*

Der Prozess für Systemveränderungen in der kantonalen Verwaltung BL folgt dem Best Practice-Ansatz von ITIL, dass Systemanpassungen erst nach einer Risikobeurteilung und erfolgreichen Tests in die produktiven Systemumgebungen eingespielt werden dürfen. Risikorelevante Updates von IKT-Basisleistungen werden zeitverschoben eingeführt. Dabei werden neue Funktionen zuerst in Pilotgruppen produktiv getestet, bevor ein Rollout an die gesamte Verwaltung erfolgt. Auch Fachanwendungen folgen grundsätzlich diesem Prinzip. Die Verantwortung für das Testen liegt bei denjenigen Dienststellen, welche die Fachanwendungen einsetzen.

Ein durch Systemveränderungen bedingtes, vollständiges Testen aller funktionalen und technischen Abhängigkeiten vor Inbetriebsetzung ist jedoch nicht für jede Veränderung praktizierbar. Die Vielzahl der notwendigen Testfälle in den komplexen und vielfach über die Grenzen einzelner Behörden und Kantone hinaus verknüpften Systeme und Datenströme

übersteigt die Ressourcen- und Zeitverhältnisse. Zeitverhältnisse werden im Besonderen exogen limitiert durch dringliche Sicherheitsupdates (Bedrohungslage) oder die Häufigkeit von Änderungen im Gesamtverbund aller vernetzten Systeme in unabhängig gesteuerten Behörden und Organisationen. Systemanpassungen insbesondere in verknüpften Systemen und Datenströmen können einmalig oder über die Zeit zu Schwachstellen und Fehlern führen, welche in den Tests nicht erkannt werden und auch nicht unmittelbar zu Problemen führen. Solche Risiken können mit einem systematischen Schwachstellen-Monitoring und mit Hilfe von regelmässigen Überprüfungen der operativen Systemumgebungen entdeckt werden. Limitierung von Zeit und Mitteln für die proaktive Durchführung von Tests und die nachträglichen Penetrationtests bedingen einen risikoorientierten Ansatz. Dabei werden Risikofähigkeit und Mittelbereitstellung periodisch im Rahmen des kantonalen Risikomanagements und der Aufgaben- und Finanzplanung austariert.

4. *Wie stark ist die Abhängigkeit der im Kanton eingesetzten Software von Microsoft? Werden Alternativen geprüft?*

Wie bei praktisch allen Verwaltungen und grossen privaten Unternehmen besteht auch in der kantonalen Verwaltung Basel-Landschaft eine Abhängigkeit von Microsoft. Umfang, Risiken, Alternativen und Massnahmen wurden im Rahmen des Regierungsratsbeschlusses[1] zur Einführung von Microsoft Cloud Diensten in der Verwaltung BL breit ermittelt und erwogen. In diesem Prozess befinden sich die meisten Kantone. Die Organisation digitale Verwaltung Schweiz (DVS) bündelt dabei Bestrebungen und Initiativen zur Bereitstellung von Alternativen. Aktuell bestehen noch keine etablierten Alternativen für die Betriebssysteme und Office-Pakete. Das sind jene Produkte von Microsoft, die aktuell noch als Lizenz erworben und auf eigener IT-Infrastruktur installiert und genutzt werden können. Open-Source Software als Alternative bietet dabei Chancen, löst aber das Problem der Abhängigkeit von externen Softwarelieferanten nicht grundsätzlich und kann neue Herausforderungen und Risiken mit sich bringen. Auch Open-Source Software muss abgestimmt, betrieben, gewartet und weiterentwickelt werden. Das dafür benötigte Knowhow muss intern aufgebaut oder extern sichergestellt werden. Open-Source-Software wird durch unterschiedliche Programmiererinnen und Programmierern aus der eigenen und externen Organisationen inklusive Drittanbietern weiterentwickelt. Das kann zu Herausforderungen bei der Qualitätssicherung und Kompatibilität führen. Eine zusätzliche indirekte Abhängigkeit der kantonalen Verwaltung BL von Microsoft besteht durch eine Vielzahl von anderen, spezialisierten Software-Produkten, welche ihrerseits Software-Produkten aus der Office Produktepalette von Microsoft einsetzen.

Aufgrund von Transparenz, Ressourcenverfügbarkeiten und aus Kostengründen können auf Open-Source basierende Systeme jedoch eine sinnvolle Alternative zu Standardprodukten sein. Der Einsatz einer Open-Source-Lösung wird einzelfallweise beurteilt. So werden in der kantonalen Verwaltung BL Open-Source-Lösungen bereits für einige Anwendungsfälle eingesetzt. Beispiele dafür sind die aktuelle Webseite des Kantons, das laufende Projekt zur Weiterentwicklung des iGov-Portals oder das für bestimmte Anwendungen eingesetzte Betriebssystem Linux. Seit dem 01.01.2024 ist zudem der Bund durch das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG)[2] verpflichtet, den Quellcode seiner selbst oder in seinem Auftrag entwickelten Software-Lösungen – vorbehältlich Rechtsansprüche Dritter – der Öffentlichkeit zur Verfügung zu stellen.

1 RRB 2024-1257

2 Publikation Bundeskanzlei Open Source: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-102670.html

5. *Wie steht es um die digitale Souveränität in der Verwaltung? Gibt es Bestrebungen, die Abhängigkeiten von Drittanbietern bei IT-Produkten und -Dienstleistungen möglichst gering zu halten?*

Der Begriff der digitalen Souveränität[3] bezieht sich in der Regel auf die Reduktion der Abhängigkeit von ausländischen Lieferanten und nicht auf die Unabhängigkeit von Drittanbietern an sich. Der Bundesrat hält in seiner Medienmitteilung[3] fest (Zitat:) «Unter «digitaler Souveränität» wird die Fähigkeit von Staaten verstanden, im digitalen Raum Kontrolle auszuüben. Eine vollkommene Kontrolle oder Souveränität ist aber keinesfalls erstrebenswert, da sie einer Abkapselung von der digitalen Welt gleichkäme». Die öffentlichen Verwaltungen sind Nutzerinnen von IKT-Produkten und nur in den wenigsten Fällen deren Produzentinnen. Die Eigenentwicklung von Software-Lösungen wird wo immer möglich vermieden[4]. Die Sicherstellung von Wirtschaftlichkeit, Unabhängigkeit, Qualität und Sicherheit über die gesamte Produkt-Lebensdauer spricht bei den allermeisten der hunderten, in der kantonalen Verwaltung BL eingesetzten Software-Produkte für eine externe Beschaffung und Betriebsunterstützung.

Die Abhängigkeit von Dritten wird zunehmend verstärkt. Im Besonderen durch die zunehmende Nutzung von Lösungen im Infrastruktur-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS) Bezugsmodell. Entscheide zur Produktentwicklung, Inbetriebsetzung von Funktionen und Verwendung von Daten die im Zusammenhang mit der Nutzung dieser Services entstehen, liegen nicht mehr im direkten Steuerungsbereich der nutzenden Organisation. Die Durchsetzung der Kontrolle und Steuerung muss über vertragliche Vereinbarungen erwirkt werden.

Die Reduktion der zunehmenden Risiken gegenüber Drittanbietern werden dabei in der Verwaltung BL im Rahmen von Entwicklungen, des Verfügbarkeitsmanagements, des Risikomanagements sowie des Beschaffungs- und Vertragsmanagements bewusst und kontinuierlich geführt und weiterentwickelt. Dabei werden im Besonderen bei Neu- und Ersatzbeschaffungen die Abhängigkeit und damit die Verfügbarkeitsrisiken unter Anwendung von Schutzbedarfsanalysen und Informationssicherheitskonzepten kritisch begutachtet. Bei Abschluss oder Erneuerung von Verträgen werden zudem kontinuierlich zusätzliche Auflagen eingearbeitet und – wo immer möglich – durchgesetzt.

Langfristig wird eine Stärkung der digitalen Souveränität nur im Verbund der Behörden aller Stufen zu bewältigen sein. Mit der Schaffung der digitalen Verwaltung Schweiz (DVS), als gemeinsame Organisation von Bund, Kantonen und Städten, wurde dazu eine wegweisende Entwicklung in Gang gesetzt. Unter anderem profitieren alle Mitglieder bereits von den gemeinsam erarbeiteten Vertragsbedingungen und Konditionen mit der Firma Microsoft Schweiz GmbH. Diese beinhalten insbesondere auch Verbesserungen im Bereich der Rechtssicherheit für die nutzenden Organisationen.

Weitere gemeinsame Massnahmen unter dem Dach der DVS sind mit dem gemeinsamen Kompetenzaufbau zu Cloud-Governance und einer Anschubfinanzierung zu Cloud- und Open Source-Projekten geplant[5]. In Ergänzung erstellt das Bundesamt für Informatik im geplanten Zeitraum zwischen 2025 und 2032 eine Swiss Governance Cloud Infrastruktur (SGC) für die Bundesverwaltung. Dazu sind auch Anforderungen der Kantone berücksichtigt worden und die Bereitstellung zur Nutzung der SGC durch die Kantone ist beabsichtigt.

---

[3] Vergleich dazu Medienmitteilung Bundesrat Source: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-102670.html

[4] Vergleich dazu SGS 140.5, Verordnung über die Informatik, §5 Abs.2 (https://bl.clex.ch/app/de/texts_of_law/140.51)

[5] Informationen zu den Cloud-Projekten der DVS unter: https://www.digitale-verwaltung-schweiz.ch/umsetzungsplan/agenda-dvs/institutionelle-grundlagen-fuer-cloud-dienste-der-verwaltung-schaffen

Die kantonale Verwaltung entwickelt das Risikomanagement inklusive dem Management und Überwachung von IKT-Lieferanten sukzessive weiter. Das beinhaltet unter anderem auch konkrete Auflagen in den Verträgen wie zum Beispiel das Recht auf Einsicht in Kontrollberichte oder die Durchführung risikoorientierter Audits.

Liestal, 11. Februar 2025

Im Namen des Regierungsrats

Der Präsident:

Isaac Reber

Die Landschreiberin:

Elisabeth Heer Dietrich