KANTON solothurn

Regierungsratsbeschluss

vom 22. August 2023

Nr. 2023/1249
KR.Nr. I 0166/2023 (FD)

Interpellation Marie-Theres Widmer (Die Mitte, Steinhof): Schutz unserer digitalen Verwaltungssysteme vor Cyberangriffen
Stellungnahme des Regierungsrates

---

1. Vorstosstext

Beim Hackerangriff auf den IT-Dienstleister Xplain AG im Mai 2023 ist eine grosse Menge an Daten gestohlen worden, darunter sensible Daten diverser Bundesstellen. Sie wurden im Darknet veröffentlicht. Der Kanton Solothurn wurde bisher von einer solchen Katastrophe verschont. Es stellen sich Fragen zur Sicherheit der digitalen Daten des Kantons Solothurn.

1. Grundsätzlich**:** Mit welchen Massnahmen schützt sich der Kanton vor der Cyberkriminalität? Gibt es schon Erkenntnisse aus dem Datenklau, sodass diese Massnahmen angepasst werden können?
2. Thema Mitarbeiter: Wie hoch wird das Bewusstsein (Awareness) der betroffenen kantonalen Mitarbeitenden betreffend Cybersicherheit eingeschätzt und wie soll dies erhöht/gefördert werden?
3. Zum Thema Cloud: Wo liegen die Daten des Kantons? Werden die Kompetenzen für die IT-Sicherheit vom Kanton selbst bereitgestellt oder werden sie eingekauft?
4. Thema sensible Daten: Wie ist der Umgang mit den sensiblen Daten geregelt? Gibt es Gedanken, sensible Daten nicht in der Cloud zu nutzen? Wie wird das kontrolliert?
5. Thema Zusammenarbeit mit sicherem nationalem Datenverbundsystem: Was ist angedacht und was wird schon umgesetzt?
6. Digitalisierungsstrategie und -schutz der Kantone: Gibt es einen Austausch zwischen den Kantonen? Wie wird verhindert, dass die Kantone Fehler wiederholen, die andere Kantone schon gemacht haben? Falls kein Austausch vorhanden ist: könnte der Kanton sich vorstellen, sich in diese Richtung zu engagieren?

2. Begründung

Im Vorstosstext enthalten.

3. Stellungnahme des Regierungsrates

3.1 Vorbemerkung

Das Amt für Informatik und Organisation (AIO) ist zuständig für die Verwaltung sowie die Gerichte. Die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz, die selbständigen öffentlich-rechtlichen Anstalten sowie die kantonalen Schulen (Ausbildungsbereiche) sind in dieser Beantwortung nicht enthalten. Sie verfügen aber über gleichwertige Massnahmen und Prozesse.

Der Schutz der kantonalen Verwaltung vor Cyberkriminalität erfordert einiges an Massnahmen, Prozessen und Organisation, um die Sicherheit der Unternehmensdaten und -systeme zu gewährleisten. Die Bedrohungslandschaft entwickelt sich ständig weiter. Das AIO und seine Partner informieren sich daher laufend über aktuelle Entwicklungen, um zusätzliche Massnahmen zu ergreifen, um sich vor Cyberkriminalität zu schützen.

3.2 Zu den Fragen

3.2.1 Zu Frage 1:

Grundsätzlich: Mit welchen Massnahmen schützt sich der Kanton vor der Cyberkriminalität? Gibt es schon Erkenntnisse aus dem Datenklau, sodass diese Massnahmen angepasst werden können?

Die Informationssicherheit ist ein zentrales Element in der kantonalen Verwaltung. Entsprechend ist das Thema auch in der Verwaltung verankert. Im Bericht «Finanzaufsichtsrevision 2022 AIO» schreibt die kantonale Finanzkontrolle folgendes: Mit der ISO-Zertifizierung nach 27001 hat das AIO einen Meilenstein erreicht und die Basis für eine umfassende «Informationssicherheit» geschaffen. Ebenso liegen Leitlinien wie auch das Konzept «Informationssicherheit» vor, worin auch die Rollen der Departemente, Dienststellen und Fachanwender beschrieben wird. Da Fachanwender die Dateneigner sind, kommt ihnen die Verantwortung für die Informations- und Datensicherheit sowie das BCM (Business Continuity Management) zu.

Das Amt für Informatik und Organisation ist die zentrale Anlaufstelle. Neben gängigen technologischen Aspekten wie diverse, mehrstufige Sicherheitssysteme in allen IT-Bereichen wurde auch ein Informationssicherheitsmanagement-System (ISMS) aufgebaut und eingefügt, welches durch die ISO / IEC 27001 Zertifizierung seine Wirksamkeit belegt. Mit dem ISMS wird sichergestellt, dass sowohl technische, organisatorische, managementbezogene und rechtliche Anforderungen abgedeckt werden.

Der Bereich Informationssicherheit wird fortlaufend aktuell gehalten, sowohl technologisch wie auch personell. Aktivitäten und Massnahmen werden den Bedrohungslagen angepasst. Dies unabhängig von einzelnen Sicherheitsvorfällen. Das Thema «Datenklau» ist dabei nur ein Element von vielen anderen.

Vom Datenabzug bei der Firma Xplain AG ist der Kanton Solothurn nur indirekt betroffen. Es gibt keine Geschäftsbeziehung oder Verträge mit der Firma. Im Datenabzug erscheint trotzdem auch der Kanton Solothurn. Grund dafür ist, die Zusammenarbeit der Polizei Kanton Solothurn mit dem Polizeikonkordat Nordwestschweiz (PKNW). Dem Konkordat gehören die Kantone Aargau, Basel-Landschaft, Basel-Stadt, Bern und Solothurn an. Im Moment laufen entsprechende Auswertungen und Analysen, warum der Kanton Solothurn im Datenauszug erwähnt wird.

3.2.2 Zu Frage 2:

Thema Mitarbeiter: Wie hoch wird das Bewusstsein (Awareness) der betroffenen kantonalen Mitarbeitenden betreffend Cybersicherheit eingeschätzt und wie soll dies erhöht/gefördert werden?

Das AIO führt bereits seit sieben Jahren Awareness Kampagnen für die kantonale Verwaltung durch. Dabei sind Phishing Mails einer der wichtigsten Faktoren. Mehrmals pro Jahr erhalten die Mitarbeitenden der kantonalen Verwaltung Phishing Mails verschiedenster Arten mit verschiedenen Schwierigkeitsgraden, um den Umgang mit solchen Angriffen zu üben. Auch wurde ein Phishing Reporting Service eingeführt, mit welchem Mitarbeitende verdächtige Mails prüfen lassen können, um sicherzustellen, ob diese gut- oder bösartig sind.

Weiter wird das Bewusstsein der Mitarbeitenden zusätzlich geschärft, in dem laufend verschiedenste Awareness Massnahmen durchgeführt werden. Aktuelle Massnahmen sind (Liste nicht abschliessend):

- Phishing Kampagnen (oben beschrieben)
- Informationssicherheits-Quiz
- Tipps & Tricks laufend im Intranet
- Einzelschulungen
- Vorstellungen in Gruppen
- Informationsanlässe
- Passwort-Assessments
- eLearnings zu verschiedenen Informationssicherheitsthemen

Laut Auswertung der aktuellen Awareness Kampagne hat sich das Bewusstsein im laufenden Jahr stark verbessert. Vergleicht man diese Werte mit bekannten Benchmarks, ist das Bewusstsein der Mitarbeitenden innerhalb der kantonalen Verwaltung als leicht höher als der Durchschnitt in anderen Organisationen einzustufen.

3.2.3 Zu Frage 3:

Zum Thema Cloud: Wo liegen die Daten des Kantons? Werden die Kompetenzen für die IT-Sicherheit vom Kanton selbst bereitgestellt oder werden sie eingekauft?

Grundsätzlich liegen die Daten des Kantons in den eigenen Rechenzentren. Es gibt nur ganz wenige Anwendungen, welche in der Cloud betrieben werden. Dies ist abhängig vom Schutzbedarf der zu bearbeitenden Daten. Die Verwaltung hat vor längerer Zeit das Merkblatt «Cloudservices» erarbeitet. Diese beschreibt, welche Daten in welcher Art von Cloud bearbeitet werden können und welche nicht. Ebenfalls ist beschrieben, was ein Cloud-Service Provider sicherstellen muss, wenn Daten der kantonalen Verwaltung Solothurn bearbeitet werden müssen.

Die Kompetenzen für die IT-Sicherheit werden grundsätzlich durch den Kanton bereitgestellt. Im AIO gibt es dafür die Abteilung «Informationssicherheit / QS», welche über entsprechende Kompetenzen verfügt. Situationsweise müssen bei Beschaffungen im Sicherheitsbereich, dem Testen von Anwendungen auf Schwachstellen, in Projekten, bei Expertisen und Analysen etc. zusätzlich externe Firmen für Dienstleistungen beigezogen werden. Eine Abdeckung nur mit internen Ressourcen ist nicht möglich und auch nicht sinnvoll. Die Bedrohungen sind dynamisch und wir müssen umgehend auf diese reagieren. Dies erfordert die Zusammenarbeit mit externen Spezialisten.

3.2.4 Zu Frage 4:

Thema sensible Daten: Wie ist der Umgang mit den sensiblen Daten geregelt? Gibt es Gedanken, sensible Daten nicht in der Cloud zu nutzen? Wie wird das kontrolliert?

Für alle Vorhaben in denen Daten digital bearbeitet werden, wird in der kantonalen Verwaltung eine Schutzbedarfsanalyse erstellt. Diese definiert den Schutzbedarf in Bezug auf Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit der Daten und Systeme. Wird ein er-

höhter Schutzbedarf festgestellt, müssen Risikoanalysen und Informationssicherheits- und Datenschutz (ISDS) Konzepte erstellt werden. Diese werden, vor der Freigabe, mit der kantonalen Datenschutzstelle abgestimmt und beinhalten Massnahmen zum Umgang mit den schützenswerten Daten.

Das Merkblatt «Cloudservices» gibt aktuell vor, wie mit sensiblen Daten in der Cloud umgegangen wird bzw. was ein Cloud-Service Provider erfüllen muss, um definierte Daten bearbeiten zu dürfen. Weitere Themen zum Umgang mit Daten in der Cloud sind in Erarbeitung. Auch in diesem Bereich wird eng mit anderen Kantonen zusammengearbeitet.

3.2.5 Zu Frage 5:

Thema Zusammenarbeit mit sicherem nationalem Datenverbundsystem: Was ist angedacht und was wird schon umgesetzt?

Das sichere Datenverbundsystem (SDVS) besteht aus dem sicheren Datenverbundnetz (SDVN) und dem Datenzugangssystem (DZS). Das SDVS soll die Vernetzung zwischen 40 Standorten des Bundes, 36 Anschlusspunkten der Kantone und 44 Betreiberinnen von kritischen Infrastrukturen breitbandig auch im Fall einer länger andauernden Strommangellage, bei Stromausfall oder beim Ausfall der kommerziellen Kommunikationsnetze während mindestens zwei Wochen sicherstellen sowie die Integrität und den Schutz gegenüber Cyberattacken wesentlich verbessern. Vom Bundesamt für Bevölkerungsschutz (BABS) ist geplant, dass dem SDVN die betreffenden Einsatzorganisationen wie die Einsatzzentralen der Kantonspolizeien, die kantonalen Führungsstäbe sowie Betreiber von kritischen Infrastrukturen angeschlossen werden.

In der Verwaltung sind die Organisationen Amt für Militär und Bevölkerungsschutz (AMB), die Polizei Kanton Solothurn sowie das AIO im Projekt involviert. Die Projektleitung für die Einführung ist im AMB angesiedelt. An einer Informationsveranstaltung vom BABS in Solothurn wurde über den provisorischen Zeitplan informiert. So sollen bis 2025 alle Kantone an das Netz angeschlossen sein. Anschliessend erfolgt dann die Ablösung des veralteten Meldesystems «Vulpus» über das SDVN. Dieses Teilvorhaben soll in Zusammenarbeit mit der Polizeiinformatik Schweiz umgesetzt werden. Es ist zu rechnen, dass weitere Anwendungen vom Bund auf das SDVN migriert werden. Eine Detailplanung liegt dazu aber noch nicht vor.

3.2.6 Zu Frage 6:

Digitalisierungsstrategie und -schutz der Kantone: Gibt es einen Austausch zwischen den Kantonen? Wie wird verhindert, dass die Kantone Fehler wiederholen, die andere Kantone schon gemacht haben? Falls kein Austausch vorhanden ist: könnte der Kanton sich vorstellen, sich in diese Richtung zu engagieren?

Aktuell besteht die Zusammenarbeit in diesem Bereich auf verschiedenen Ebenen. Wöchentlich werden die aktuellen Informationen seitens Bund zur Situation im Cyberraum Schweiz und international im «Weekly Cyber Situation Briefing» des NCSC (Nationale Zentrum für Cybersicherheit) abgeglichen und informiert. Proaktive Operationen zum Schutz, werden auf Grund dieser aktuellen Informationen direkt ausgeführt und umgesetzt. Weiter besteht eine enge Zusammenarbeit der Kantone und Bundesstellen im Bereich Cyber innerhalb der DVS (Digitale Verwaltung Schweiz). Die spezifische Arbeitsgruppe «Informations- und Cybersicherheit» innerhalb der DVS definiert Best Practice-Regeln für den Schutz digital gespeicherten Daten. Sie beurteilt Sicherheitsaspekte von neuen oder sich abzeichnenden Tendenzen im IKT-Bereich, schlägt risikominimierende Massnahmen vor und stellt Empfehlungen zur Minderung von Informatiksicherheits-Risiken bereit. Im Krisenfall werden innerhalb der Gruppe «Task Forces» einberufen. Damit wird eine kompetente Beratung der involvierten Organisationen sichergestellt, nötigenfalls mit Einbezug der betroffenen Lieferanten. Eine weitere enge Zusammenarbeit besteht mit dem Si-

cherheitsverbund Schweiz (SVS). Die «nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» zeigt auf, wie diese gesetzten Ziele zur Verbesserung der Cyber-Resilienz erreicht werden sollen. Die Verabschiedung der NCS erfolgte im April 2018. Sie zeigt in sechs definierten Handlungsfelder die nötigen Massnahmen für Bund und Kantone auf. Ein grosser Teil dieser in den Handlungsfelder definierten Massnahmen wurden bereits umgesetzt. Der genaue Stand des Umsetzungsgrades ist im «Jahresbericht zum Stand der Projekte im Umsetzungsplan der Kantone zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2018–2022» zu entnehmen. Dieser ist öffentlich unter https://www.svs.admin.ch/de/themen-/cybersicherheit/cybersicherheit-kantone.html#441_1612790888827 (zuletzt abgerufen am 19. Juli 2023) einsehbar.

Grundsätzlich ist zu betonen, dass im Bereich der Zusammenarbeit und Informationsaustausch in den letzten Jahren enorme Fortschritte erzielt wurden. Die Kantone haben die Massnahmen für den Schutz ihrer Verwaltung und der Bevölkerung vor Cyberrisiken stark ausgebaut. Der Schutz vor Cyber-Risiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Alle «Akteure» tragen die Verantwortung, sich gemeinsam vor diesen Bedrohungen auf allen Ebenen adäquat zu schützen.

Andreas Eng
Staatsschreiber

Verteiler

Finanzdepartement
Amt für Informatik und Organisation
Parlamentsdienste
Traktandenliste Kantonsrat