KANTON solothurn

Regierungsratsbeschluss

vom 30. März 2021

Nr. 2021/472
KR.Nr. K 0018/2021 (FD)

Kleine Anfrage Christoph Scholl (FDP.Die Liberalen, Selzach): Ist der Kanton Solothurn im Bereich Cyber-Sicherheit auf die anstehenden Herausforderungen vorbereitet? Stellungnahme des Regierungsrates

---

1. Vorstosstext

Das Thema Cyber-Sicherheit gewinnt mit der zunehmenden Digitalisierung und gerade mit der aktuellen Homeoffice-Pflicht deutlich an Bedeutung. Entsprechend ist es wichtig, dass Unternehmen und auch die öffentliche Verwaltung angemessene Bemühungen betreiben, um die Sicherheit der IT-Systeme zu gewährleisten.

In diesem Zusammenhang stellen sich verschiedene Fragen:
1. Wie beurteilt der Regierungsrat die Situation im Bereich Cyber-Sicherheit bei den IT-Systemen des Kantons Solothurn im Vergleich zu anderen Kantonen?
2. Werden heute regelmässig externe Überprüfungen der technischen Sicherheit vorgenommen (Penetration Testing)? Falls ja, wie lautet das Urteil durch die Überprüfenden? (Es wäre hilfreich eine [selbstverständlich zensierte] Version des Berichtes zu erhalten.)
3. In welchen Bereichen sieht der Regierungsrat in Bezug auf das Thema der Cyber-Sicherheit den höchsten Handlungsbedarf, und welche Massnahmen zur Erhöhung der Cyber-Sicherheit sind geplant?

2. Begründung

Im Vorstosstext enthalten.

3. Stellungnahme des Regierungsrates

3.1 Vorbemerkungen

Cyber-Risiken prägen den heutigen Alltag. Für Aufsehen sorgten in jüngster Zeit breit angelegte Angriffswellen, die weltweit zu grossen Schäden führten, aber auch gezielte und oft politisch motivierte Angriffe auf staatliche Infrastrukturen zum Zweck der Spionage oder Sabotage.

Um den Cyber-Risiken aktiv entgegenzutreten und die Sicherheit des Landes vor den Bedrohungen aus dem Cyber-Raum zu wahren, hat der Bundesrat an seiner Sitzung vom 18. April 2018 die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018-2022 (NCS II) verabschiedet. Die Strategie baut auf den Arbeiten der ersten NCS (2012-2017) auf, weitet diese wo nötig aus und ergänzt sie mit neuen Massnahmen, um der heutigen Bedrohungslage zu entsprechen. Sie wurde zusammen mit der Wirtschaft, den Kantonen und den Hochschulen erarbeitet und bildet die Basis für die nötigen gemeinsamen Anstrengungen zur Minderung der Cyber-Risiken.

Die Strategie sieht vielfältige Massnahmen vor zu Ausbau und Entwicklung der Cyber-Sicherheit. Sie reichen vom Aufbau von Kompetenzen und Wissen und der Förderung der internationalen Kooperation über die Stärkung des Vorfall- und Krisenmanagements sowie der Zusammenarbeit bei der Cyber-Strafverfolgung bis hin zu Massnahmen der Cyber-Abwehr durch die Armee und den Nachrichtendienst des Bundes (NDB).

Die beschriebenen Massnahmen will der Bund in Zusammenarbeit mit den Kantonen, der Wirtschaft und der Gesellschaft umsetzen. Die beabsichtigte Wirkung der NCS betrifft die ganze Schweiz und damit auch den Kanton Solothurn.

3.2 Zu den Fragen

3.2.1 Zu Frage 1:

Wie beurteilt der Regierungsrat die Situation im Bereich Cyber-Sicherheit bei den IT-Systemen des Kantons Solothurn im Vergleich zu anderen Kantonen?

Der Sicherheitsverbund Schweiz (SVS) beschäftigt sich mit sicherheitspolitischen Themen, die Bund und Kantone gemeinsam betreffen. In Zusammenarbeit mit Vertretern der Kantone erarbeitete eine Arbeitsgruppe des SVS basierend auf der NCS II den Umsetzungsplan der Kantone. Die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und –direktoren (KKJPD) verabschiedete den Umsetzungsplan der Kantone im April 2019. Der Umsetzungsplan ist ein Anhang der NCS II und auf die spezifischen Bedürfnisse der Kantone abgestimmt. Die KKJPD beauftragte den SVS, zusammen mit den kantonalen Vertretern die erforderlichen Schritte einzuleiten, um die Massnahmen der kantonalen Umsetzungsplanung zur Nationalen Cyber-Strategie 2018–2022 zu realisieren.

In der ersten Jahreshälfte 2020 haben alle Kantone an einer Erhebung der IKT-Resilienz (Widerstandsfähigkeit bei einem Cyber-Angriff) im Rahmen des Umsetzungsplans der Kantone zur NCS II teilgenommen. Analysiert wurden die minimalen Anforderungen in Bezug auf relevante Prozesse, Aufgaben und Kompetenzen, was ein wertvoller Schritt und Beitrag zur Verbesserung der Cyber-Sicherheit in den Kantonen und in der Schweiz darstellt.

Die Auswertung liefert über alle Kantone hinweg ein grundsätzlich positives Bild über die Cyber-Sicherheit und insbesondere über die IKT-Resilienz in den Kantonen, wenngleich mit bestehendem Verbesserungspotenzial in ausgewiesenen Funktionen (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen). Die Detailanalyse ermöglicht eine nuancierte Perspektive auf Teilbereiche der IKT-Resilienz, die bereits erfolgreich verbessert wurden und auf andere Bereiche, in denen noch Nachholbedarf besteht. Für den Kanton Solothurn ergab sich Verbesserungsbedarf in den Bereichen Passwort-Richtlinien, Mindestvorkehrungen für die Notfallbewirtschaftung sowie Sensibilisierung von Mitarbeitenden. Die neuen Passwort-Richtlinien wurden deshalb verschärft, im Bereich Sensibilisierung wurden die Umsetzungen (Kampagnen, Infos, Schulungen) verstärkt angegangen.

Mit RRB Nr. 2020/1659 vom 24. November 2020 hat der Regierungsrat zudem das Konzept „Informationssicherheit der kantonalen Verwaltung“ verabschiedet. Das Konzept dient als Grundlage für ein einheitliches Sicherheitsmanagement innerhalb der Verwaltung des Kantons Solothurn. Das Konzept hat zum Ziel ein unternehmensweites Informationssicherheitsmanagementsystem, ein einheitliches Vorgehen und einen umfassenden Sicherheitsstandard im Bereich der Informationssicherheit etablieren und unterhalten zu können. Informationssicherheit soll gewährleistet sein in Bezug auf die Sicherheit und den Schutz aller Daten, elektronischen Informationen und der zu ihrer Bearbeitung benötigten Systeme, Prozesse sowie der Infrastruktur für den Geschäftsbetrieb der kantonalen Verwaltung. Das Konzept wurde von der Abteilung Informationssicherheit / QS des Amtes für Informatik und Organisation erarbeitet.

Das AIO ist seit 1997 ISO 9000 zertifiziert und dokumentiert damit, den erhöhten Anforderungen an ein wirksames Qualitätsmanagement zu entsprechen. Mit der angestrebten Zertifizierung nach ISO 27000 möchte das AIO seine Prozesse und Dienstleistungen weiter verbessern und sich noch stärker für die Sicherheit von Informationen, Daten und Systemen einsetzen.

3.2.2 Zu Frage 2:

Werden heute regelmässig externe Überprüfungen der technischen Sicherheit vorgenommen (Penetration Testing)? Falls ja, wie lautet das Urteil durch die Überprüfenden? (Es wäre hilfreich eine [selbstverständlich zensierte] Version des Berichtes zu erhalten.)

Ja, Audits und Penetrationstests im IKT-Bereich werden regelmässig durch spezialisierte Firmen durchgeführt. So sind Penetrationstests u.a. zwingend für Systeme, welche Schnittstellen mit dem Internet aufweisen und mindestens erhöhten Schutzanforderungen zu genügen haben. Die Audits werden vom Amt für Informatik und Organisation, aber auch von der Kantonalen Finanzkontrolle in Auftrag gegeben. Die Berichte sind nicht öffentlich. Sie werden aber gegenüber der Kantonalen Finanzkontrolle vollständig offengelegt und besprochen. Diese überprüft auch regelmässig die Umsetzung der festgestellten Punkte.

Die letzten Audits wurden in den Bereichen Firewall, Home-Office-Zugang und eTax durchgeführt. Die Audits zeigen das erwartete Bild. Der Kanton Solothurn erzielte auf einer 100er Skala gute 82.25 Punkte. Bei kantonalen Verwaltungseinheiten wird ein Wert zwischen 78 und 88 Punkten als gut betrachtet. Die Punkte mit einer hohen Kritikalität wurden und werden soweit möglich und nötig behoben. Sämtliche Massnahmen werden im AIO bewirtschaftet und regelmässig mit der Finanzkontrolle besprochen. Auch in diesem Jahr sind weitere Audits und Penetrationstests geplant.

Die seit dem Jahr 2016 gültigen „Allgemeine Geschäftsbedingungen des Kantons Solothurn über die Informationssicherheit und den Datenschutz bei der Erbringung von Informatikdienstleistungen (AGB ISDS)“ wurden kürzlich überarbeitet. Diesbezüglich wurde von der Beauftragten für Information und Datenschutz festgehalten, dass der Kanton Solothurn wohl eine der besten (und strengsten) Sicherheits-AGBs von allen Kantonen habe.

3.2.3 Zu Frage 3:

In welchen Bereichen sieht der Regierungsrat in Bezug auf das Thema der Cyber-Sicherheit den höchsten Handlungsbedarf, und welche Massnahmen zur Erhöhung der Cyber-Sicherheit sind geplant?

Die kantonale Verwaltung und deren Infrastruktur sollen vor Cyber-Risiken effektiv geschützt sein. Der Schutz vor Cyber-Risiken ist eine Querschnitts- und Verbundaufgabe, die nur gemeinsam erfüllt werden kann. Staat, Wirtschaft und Bevölkerung tragen gemeinsam Verantwortung und sind angehalten, mit ihrem Verhalten und ihren Massnahmen die Wohlfahrt zu sichern und die Widerstandsfähigkeit gegenüber Cyber-Risiken zu erhalten.

Um die Cyber-Sicherheit in der kantonalen Verwaltung zusätzlich zu erhöhen, sind in allen Dienststellen verantwortliche Personen zu bezeichnen, welche über entsprechendes Know-how verfügen und sich dem Thema Informationssicherheit annehmen. Mit dem Konzept „Informationssicherheit der kantonalen Verwaltung“ wurde die dafür nötige Basis erarbeitet. Ein Information Security Management System wird aufgebaut und die Rolle des/der Informationssicherheitsverantwortlichen in den Dienststellen eingeführt. Damit soll gewährleistet werden, dass die Prozesse der Informationssicherheit bekannt gemacht und auch angewendet werden. Mit der Einführung in den Dienststellen wird noch in diesem Jahr gestartet im Rahmen zweier Pilotprojekte im Departement des Innern sowie im Bau- und Justizdepartement.

Andreas Eng
Staatsschreiber

Verteiler

Finanzdepartement
Amt für Informatik und Organisation
Parlamentsdienste
Traktandenliste Kantonsrat