KANTON solothurn

Regierungsratsbeschluss

vom 1. März 2022

Nr. 2022/274
KR.Nr. I 0017/2022 (FD)

Interpellation Richard Aschberger (SVP, Grenchen): Ist der Kanton gewappnet für Cyberangriffe? (26.01.2022)
Stellungnahme des Regierungsrates

---

1. Vorstosstext

Cyberangriffe mehren sich, nehmen fast schon exponentiell zu und können gravierende Folgen nach sich ziehen. Bei Privatunternehmen sind laut aktuellen Umfragen in der Schweiz und in Deutschland die Cyberangriffe unterdessen die grösste Sorge. Aktuell gibt es diverse Grosskonzerne, welche darunter leiden (Emil Frey Gruppe, CPH Gruppe etc.), und die damit einhergehenden Probleme werden an Zulieferer oder Endabnehmer/Kunden weitergegeben.

Der Kanton Solothurn selbst sowie die von ihm „gelenkten" Unternehmen müssen mit Angriffen rechnen. Daher bitte ich um die Beantwortung der folgenden Fragen:

1. Gab es in den letzten Jahren Cyberangriffe auf den Kanton oder seine kontrollierten Firmen/Anstalten (beispielsweise Blaulichtorganisationen, Pensionskasse Kanton Solothurn [PKSO], Solothurner Spitäler [SoH], Solothurnische Gebäudeversicherung [SGV], Schulen etc.)?
2. Gibt es neue Baustellen seit der Pandemie in Bezug auf Sicherheit bei Login via Homeoffice?
3. Sind Projekte in Planung, welche gezielt Cyberrisiken angehen und falls ja, hat das Platz in laufenden Budgets?
4. Gibt es betriebliche Kontinuitätsmanagements (BCM) für den Kanton und seine kontrollierten Firmen/Anstalten?
5. Wie viele und in welchem Umfang (CHF) vergibt der Kanton bei diesem Thema Aufträge an externe Firmen?

2. Begründung (Vorstosstext)

Im Vorstosstext enthalten.

3. Stellungnahme des Regierungsrates

3.1 Vorbemerkungen

Das Amt für Informatik und Organisation (AIO) ist der Erbringer von Informatikdienstleistungen für die Verwaltung. Gemäss der vom Regierungsrat festgelegten Informations- und Kommunikationstechnik Strategie 2021 – 2026 umfasst der Bereich Verwaltung nebst der Kernverwaltung auch die Polizei Kanton Solothurn und die Gerichte. Mit der Pensionskasse Kanton Solothurn besteht ein separates Service Level Agreement für die Erbringung von Informatikdienstleistungen und die Informationssicherheit. Die Antworten auf die Fragen im Vorstosstext beschränken sich auf diese Bereiche.

Nicht zuständig ist das AIO demgegenüber für die Solothurner Spitäler AG, die Fachhochschule Nordwestschweiz und die selbständigen öffentlich-rechtlichen Anstalten sowie für den Informatik-Einsatz zu Unterrichtszwecken an den kantonalen Schulen. Es ist davon auszugehen, dass auch in diesen Organisationen entsprechende Prozesse und Schutzmassnahmen bestehen.

Das Thema Informationssicherheit / Cybersicherheit ist seit Jahren im Brennpunkt der Informationstechnologie und seit einiger Zeit auch im Fokus der Öffentlichkeit. Angriffe finden rund um die Uhr statt und treffen sowohl renommierte Unternehmen als auch die öffentlichen Verwaltungen. Nebst Angriffen auf Schwachstellen in Hard- und Software erfolgen auch gezielte Phishing Angriffe (auf elektronischem Weg durchgeführte Betrugsversuche). Gerade bei dieser Art von Angriffen ist der Mensch als Anwender der Informatikmittel die grosse „Schwachstelle". Das AIO und auch die Verwaltung sind sich dieser Problematik schon seit längerem bewusst, entsprechend wird seit Jahren gezielt in technische, organisatorische und schulische Massnahmen investiert.

Seit 2019 wurde und wird mit folgenden Massnahmen den Cyberrisiken begegnet:

- Die Leitlinie „Informationssicherheit der kantonalen Verwaltung Solothurn" wurde erstellt und vom Regierungsrat mit RRB 2019/823 vom 21. Mai 2019 beschlossen.

- Das Konzept „Informationssicherheit der kantonalen Verwaltung" wurde erstellt und vom Regierungsrat mit RRB 2020/1659 vom 24. November 2020 beschlossen.

- Der Zugriff auf das private E-Mail Postfach vom geschäftlichen Arbeitsplatz aus wurde verunmöglicht. Der Kanton hat diese Massnahme im Jahr 2020 als 11. Kanton umgesetzt.

- Das AIO hat im Jahr 2020 die Stabsabteilung Informationssicherheit aufgebaut. Diese ist direkt dem Chef AIO unterstellt und umfasst 300 Stellenprozente. Sie kümmert sich um alle Themen rund um die Informationssicherheit. Seit dem 1. Dezember 2021 wird die Stabsabteilung geführt vom Gesamtverantwortlichen für die Informationssicherheit.

- Diverse Prozesse wurden neu eingeführt und optimiert und der Sicherheitsbereich ausgebaut. Dieser umfasst Bereiche wie Analysen, Monitoring, Überwachung usw.

- Massnahmen im Bereich Awareness (Bewusstsein) wurden erarbeitet und eingeführt. Dabei steht die Sensibilisierung der Mitarbeitenden für die Informationssicherheit im Vordergrund. Zur Förderung der Awareness und zu Schulungszwecken werden bereits seit dem Jahr 2017 die Mitarbeitenden mit fiktiven Phishing-Angriffen auf die Problematik aufmerksam gemacht und entsprechend sensibilisiert. Seit 2018 finden regelmässig Awareness-Kampagnen statt und seit 2021 steht den Mitarbeitenden auch eine Webseite mit Fragen rund um die Informationssicherheit zu Schulungszwecken zur Verfügung. Mitarbeitende können sich auf der Startseite des Intranets bei den AIO-Direktlinks über den Stand der Informationssicherheit informieren.

- Ebenfalls im Jahr 2017 wurde die Passwortstärke der Mitarbeitenden-Zugänge mittels einem Audit geprüft. Als Folge wurde das Dokument „Umgang mit Passwörtern" überarbeitet.

- Das AIO strebt die Zertifizierung nach der Norm ISO 27001 an, eine international führende Norm für Informationssicherheits-Management-Systeme und damit die wichtigste Zertifizierung im Bereich der Cybersicherheit. Die bestehende Zertifizierung nach ISO 9001 genügt den heutigen Anforderungen an einen Erbringer von

Informatikdienstleitungen nicht mehr. Die neue Norm umfasst die Einführung eines Informationssicherheits-Management-Systems (ISMS), welches die Regeln und Methoden festlegt, mit denen sich die Informationssicherheit sicherstellen, steuern, kontrollieren und kontinuierlich verbessern lässt. Die Zertifizierung ist für November 2022 geplant und aktuell auf Kurs.

3.2 Zu den Fragen

3.2.1 Zu Frage 1:

Gab es in den letzten Jahren Cyberangriffe auf den Kanton oder seine kontrollierten Firmen/Anstalten (beispielsweise Blaulichtorganisationen, Pensionskasse Kanton Solothurn [PKSO], Solothurner Spitäler [SoH], Solothurnische Gebäudeversicherung [SGV], Schulen etc.)?

Zugriffsversuche auf die Informatiksysteme der kantonalen Verwaltung erfolgen im Sekundentakt. In den meisten Fällen sind es automatisierte Angriffsversuche auf bereits bekannte Schwachstellen, die dank den bestehenden Sicherheitsvorkehrungen rechtzeitig erkannt werden.

Es kam unter anderem zu folgenden Sicherheitsvorfällen: „Cryptolocker Befall" (Verschlüsselungssoftware), Malware-Infektionen auf Workstations, Angriffe auf Schwachstellen in Betriebssystemen, Datenbank-Software und Fachanwendungen sowie „Distributed Denial of Service (DDoS) Attacken", die gezielt die Nichtverfügbarkeit eines Dienstes oder Servers herbeizuführen beabsichtigen.

Keiner dieser Vorfälle hat Schaden verursacht, die Sicherheitssysteme und Prozesse haben stets funktioniert und die Angriffe konnten rechtzeitig abgewehrt werden. Nachfolgende zwei DDoS Angriffe im Jahr 2021 wurden an das Nationale Zentrum für Cybersicherheit gemeldet:

22.06.2021 ein DDoS Angriff; Location: Russian Federation

07.09.2021 ein DDoS Angriff; Location: Russian Federation

3.2.2 Zu Frage 2:

Gibt es neue Baustellen seit der Pandemie in Bezug auf Sicherheit bei Login via Homeoffice?

Die Verwaltung stellte bereits vor der Covid-19 Pandemie sogenannte Remote-Zugänge für die Arbeit im Homeoffice zur Verfügung, der Fernzugriff auf die Systeme übers Internet wird seit 15 Jahren ermöglicht. Diese jahrelange Erfahrung hilft beim Umgang mit Cyberrisiken. Deshalb wurde von Anfang an zwingend auf einen 2. Faktor (2FA) gesetzt beim Remote-Zugang. 2FA bezeichnet den Identitätsnachweis eines Anwenders mittels einer Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten. Im Jahr 2019 wurde eine spezialisierte Firma beauftragt, ein Audit in diesem Bereich durchzuführen. Die Ergebnisse dieses wie auch der anderen Audits werden stets mit der Finanzkontrolle besprochen.

Die Herausforderungen, die es infolge der vermehrten Homeoffice-Nutzung während der Pandemie zu bewältigen gab, betrafen vorwiegend die personellen Ressourcen und die Kosten. So mussten im Jahr 2020 innert weniger Tage mehrere Hundert Remote-Zugänge eingerichtet und freigeschaltet werden. Dies zeigt sich konkret in der stark ansteigenden Zahl von SMS, welche die Benutzer bei jedem Fernzugriff für den 2. Faktor zugestellt bekamen. Wurden im Jahr 2019 noch etwas über 50'000 SMS versendet, waren es im Jahr 2021 bereits über 320'000 SMS.

3.2.3 Zu Frage 3:

Sind Projekte in Planung, welche gezielt Cyberrisiken angehen und falls ja, hat das Platz in laufenden Budgets?

Aktuell laufen diverse Aufträge und Projekte, welche die Informationssicherheit der kantonalen Verwaltung betreffen. Dies sind zum einen die Einführung eines ISMS, die ISO 27001 Zertifizierung sowie Optimierungen in den Bereichen Awareness und technische Massnahmen sowie bei bestehenden Prozessen. Weitere Optimierungen in den Bereichen Automatisierung, Penetration Testing, Update und Patching-Prozesse sind aufgegleist.

Die ISO 27001 Zertifizierung bedingt viele Massnahmen, Richtlinien und Prozesse, welche neu geschaffen oder wo nötig optimiert werden. Der Aufwand fällt im Globalbudget des AIO an. Sicher ist bereits jetzt, dass das neue Globalbudget 2023-2025 höher ausfallen wird. Nebst Kosten im Informationssicherheitsbereich entstehen höhere Kosten beim Software- und Personalaufwand aber auch beim Life-Cycle-Management der bestehenden Plattformen.

Die Einführung der Informationssicherheit in den Dienststellen wird nicht übers Globalbudget des AIO erfolgen. Gemäss Konzept „Informationssicherheit der kantonalen Verwaltung" sollen in den Departementen die hierfür notwendigen Ressourcen geschaffen werden. Zurzeit laufen entsprechende Pilotprojekte im Finanzdepartement, Bau- und Justizdepartement sowie im Departement des Innern. Schätzungen gehen von insgesamt 4-6 Stellen aus.

3.2.4 Zu Frage 4:

Gibt es betriebliche Kontinuitätsmanagements (BCM) für den Kanton und seine kontrollierten Firmen/Anstalten?

Es sind viele technische Massnahmen für den kontinuierlichen Betrieb der Infrastrukturen der kantonalen Verwaltung vorhanden. Dies sind zum Beispiel zwei redundante Rechenzentren, Netzwerksysteme, Speichersysteme, Hochverfügbarkeits-Cluster in der Virtualisierungs-Umgebung, Datensicherungsprozesse usw. Ein spezifisches BCM Konzept für das AIO befindet sich aktuell im Aufbau. Gemäss dem Konzept „Informationssicherheit der kantonalen Verwaltung" ist das AIO verantwortlich für die Verwaltung des BCM hinsichtlich Informatik und Infrastruktur. Demgegenüber sind die Dienststellen verantwortlich für die BCM-Aufgaben bezüglich der Prozesse, Räumlichkeiten und Ressourcen.

3.2.5 Zu Frage 5:

Wie viele und in welchem Umfang (CHF) vergibt der Kanton bei diesem Thema Aufträge an externe Firmen?

Dies kann nicht pauschal beziffert werden. Wie bereits erwähnt, laufen aktuell Projekte im Bereich Informationssicherheit / Qualitätssicherung. Allfällige finanzielle Mittel sind dabei im Mehrjahresprogramm Informatik (MJP) und/oder im Globalbudget des AIO enthalten. In Fachanwendungen, wo besonders schützenswerte Daten bearbeitet werden, werden situativ Sicherheitstests (Penetration Tests) durchgeführt. Die Durchführung wird an externe Firmen vergeben, welche über das notwendige Wissen verfügen. In erster Priorität werden neue Anwendungen, die übers Internet erreichbar sind, solchen Tests unterzogen. Im Schnitt sind das 2-4 Fachanwendungen pro Jahr. Die Kosten betragen Fr. 10'000.00 bis Fr. 20'000.00 und sind im MJP enthalten. Das AIO lässt zudem jedes Jahr 1-2 Audits in verschiedenen Bereichen (Netzzugänge, Homeoffice-Zugang, Firewall, Netzwerkzonierung usw.) durchführen.

Dieser jährliche Posten in der Höhe von Fr. 20'000.00 bis Fr. 30'000.00 ist ebenfalls im Globalbudget enthalten. Zentral ist auch der Unterhalt der verschiedenen Hard- und Softwarekomponenten im Rahmen des Life-Cycle-Managements. Auch dieser erfolgt über die MJP und wird dort ausgewiesen.

Andreas Eng
Staatsschreiber

Verteiler

Finanzdepartement
Amt für Informatik und Organisation
Parlamentsdienste
Traktandenliste Kantonsrat