KANTON
LUZERN

Regierungsrat

Luzern, 31. Oktober 2023

ANTWORT AUF ANFRAGE A 6

Nummer:	A 6
Protokoll-Nr.:	1093
Eröffnet:	26.06.2023 / Justiz- und Sicherheitsdepartement i.V. mit Finanzdepartement

Anfrage Estermann Rahel und Mit. über die Cybersicherheit der öffentlichen Verwaltung und der Infrastruktur im Kanton Luzern

Einleitung

Die Cybersicherheit im Kanton Luzern wird auf der Basis der Nationalen Cyberstrategie NCS II umgesetzt. Diese beruht auf Eigenverantwortlichkeit und föderalistischen Prinzipen. Sie wird als gemeinschaftliche Aufgabe von Gesellschaft, Wirtschaft und staatlichen Institutionen auf allen drei Staatsebenen angesehen. Konkrete Fragen betreffend Zustand, Organisation und Vorkommnisse mit Bezug zu den kantonalen IT-Infrastrukturen können wir aufgrund der hohen Sensitivität dieses Themenbereichs im Rahmen einer öffentlichen parlamentarischen Anfrage nicht im Detail beantworten.

Unser Rat wird aber bezüglich der Resilienz der Informations- und Kommunikationstechnik (IKT), dem aktuellen Reifegrad und über allfällige Vorkommnisse bei den kantonalen Infrastrukturen und den im Kanton als kritisch eingestuften Infrastrukturen regelmässig vertraulich orientiert. Wir stellen dabei fest, dass die IT-Sicherheitsorganisationen aller Unternehmen und Institutionen infolge der weltweit immer stärker zunehmenden Anzahl Cyberangriffe mit immer professionellerer Ausprägung vor immer grössere Herausforderungen gestellt werden. Unser Kanton bildet hier keine Ausnahme.

Zu Frage 1: Über welche Standards, Zuständigkeiten, Arbeitsstellen und Systeme verfügt der Kanton Luzern für eine sichere Speicherung von digitalen Daten und Systemen?

Die im März 2022 von unserem Rat beschlossene und seither in Umsetzung befindliche Informations- und Informatiksicherheitsstrategie gewährleistet die sichere Speicherung von digitalen Daten und Systemen. Konkret adressieren dabei die an den internationalen Sicherheitsstandard ISO 27001/27002 angelehnten Schutzmassnahmen die aktuellen Cyberrisiken. Organisatorisch sind die Departemente für die Absicherung ihrer Fachanwendungen (Departementsinformatik) zuständig, während die Dienststelle Informatik für die Absicherung der Rechenzentren, Server- und Datenbanksysteme, Netzwerke sowie für die eingesetzten Konzernapplikationen zuständig ist (Konzerninformatik). Zur spezifischen Adressierung von IT-

Sicherheit und Informationsschutz in den Departementen und Gerichten sind die jeweiligen Informations- und Informatiksicherheitsbeauftragen verantwortlich. Auf der technischen Seite werden Überwachungs- und Scanningsysteme betrieben, welche sowohl Konzernanwendungen als auch Anwendungen der Departemente auf bekannte Schwachstellen hin überprüfen.

Zu Frage 2: Gemäss Informationen aus der Branche haben in der Schweiz rund 50'000 Server gravierende Sicherheitslücken – davon 21'000 Bildungs-Server, 10'000 Behörden-Server und 10'000 Server des Gesundheitswesens. Wie schätzt der Kanton Luzern die Lage im eigenen Kanton ein? Sind ihm eigene Sicherheitslücken oder Angriffe auf die öffentliche Infrastruktur bekannt? Waren dabei Personendaten betroffen?

Zu konkreten Sicherheitslücken und Angriffen auf eigene oder öffentliche Infrastrukturen im Kanton äussern wir uns aufgrund der hohen Sensibilität des Themas nicht öffentlich. Bezüglich der Identifikation von neuen Sicherheitslücken sind unsere Fachleute regelmässig im Informationsaustausch mit dem nationalen Zentrum für Cybersicherheit (NCSC). Dies betrifft die allgemeine Lage sowie Vorkommnisse in uns betreffenden Sektoren wie beispielsweise das Bildungswesen. Hinweise des NCSC respektive dringende Handlungsempfehlungen zur Behebung von gravierenden Sicherheitslücken setzen wir um, sobald diese vom NCSC kommuniziert werden. Darüber hinaus befolgen wir dringende Handlungsempfehlungen der Hersteller unserer Produkte.

Zu Frage 3: Das nationale Zentrum für Cybersicherheit (NCSC) ermahnt die Betreiber unsicherer Server, bessere Massnahmen zu ergreifen. Wie nimmt der Kanton seine Sorgfaltspflicht für seine Dienststellen, aber auch für Schulen oder ausgelagerte Organisationen (Spitäler, Wasser- und Energieversorgung usw.) wahr? Wie erfolgt die Zusammenarbeit mit dem NCSC und mit anderen Kantonen?

Die Behandlung und Bewältigung derartiger Technologierisiken, zum Beispiel unsichere Server, erfolgt verwaltungsintern im Rahmen des strategisch aufgebauten Technologierisiko-Managements. Dieses umfasst die Konzern- und Departementsinformatik (vgl. Antwort zu Frage 1) und damit sämtliche Informatikmittel der kantonalen Verwaltung inklusive kantonale Schulen. Hier finden eine regelmässige Zusammenarbeit und ein regelmässiger Austausch mit dem NCSC statt, fallweise auch ein kantonsübergreifender Austausch auf Expertenlevel.

Sofern nicht schon durch den Bund wahrgenommen, nimmt der Kanton die Beratung und Unterstützung gegenüber den als kritisch eingestufte Unternehmen und Institutionen (so genannte kritische Infrastrukturen) wahr. Dieser Austausch soll infolge der erhöhten Gefahr aus dem Cyberraum verstärkt werden. Seit April 2022 nimmt die Stelle des kantonalen Cyberkoordinators innerhalb des Justiz- und Sicherheitsdepartements diese Aufgabe wahr. Die entsprechenden Aufbauarbeiten sind im Gang. Die Stelle soll periodisch die aktuelle Resilienz der Informations- und Kommunikationstechnologien und den Cyber-Reifegrad der kritischen Infrastrukturen auf Kantonsgebiet überprüfen. Zeigen die Auswertung entsprechende Defizite, beispielsweise bei spezifisch definierten Minimalstandards des Bundes oder anderen branchenüblichen Sicherheitsstandards, soll das betroffene Unternehmen respektive die betroffene Institution mittels konkreten Handlungsempfehlungen durch den Cyberkoordinator unterstützt werden. Hier findet eine regelmässige Absprache und Austausch mit dem NCSC

und/oder den verantwortlichen Bundesämtern wie unter anderem dem Bundesamt für Energie statt.

Zu Frage 4: Für Erstaunen sorgte kürzlich, dass durch einen Angriff auf die private Software-Firma Xplain heikle Daten von Bundesstellen betroffen waren und schliesslich im Darknet veröffentlicht wurden. Mit welchen externen Anbietern arbeitet der Kanton Luzern in seiner Datenverwaltung zusammen? Nach welchen Grundsätzen erfolgt diese Zusammenarbeit zur Datenverwaltung (beispielsweise Auswahl des Anbieters, Verschlüsselung oder Aufteilung von Datensätzen zur Risikominimierung usw.)?

Im Rahmen der Umsetzung der Informations- und Informatiksicherheitsstrategie wurden die Mindeststandards für externe IT-Dienstleister angehoben. Je nach Klassifikation der vom externen IT-Dienstleister verarbeiteten und gespeicherten Daten sind Sicherheitszertifizierungen wie etwa ISO 27001 zwingend, respektive muss ein gleichwertiger Nachweis erbracht werden. Analoge Mindeststandards kommen im Bereich Datenschutz zur Anwendung. Auf der technischen Seite befindet sich ein Prozess zur «sicheren Bereitstellung von Testdaten» und «Daten-Anonymisierung» im Aufbau. Diese zwei Ansätze dienen somit der Risikominimierung von sensitiven Daten während der Entwicklungs- und Umsetzungsphase.

Zu Frage 5: Wie steht der Kanton Luzern zur auf Bundesebene diskutierten Meldepflicht für Cyberattacken auf kritische Infrastrukturen sowie zur weitergehenden Meldepflicht für Schwachstellen und Sicherheitslücken?

Der Kanton Luzern unterstützt die Meldepflicht für kritische Infrastrukturen und die entsprechende Erweiterung auf Schwachstellen und Sicherheitslücken. Dank der erweiterten Meldepflicht werden die betroffenen Unternehmen verpflichtet, sich sowohl über Schwachstellen zu informieren als auch ihre IT-Umgebung (inklusive eingesetzter Software) permanent zu überprüfen. Das ist aus Sicht des Kantons ein vertretbarer Mehraufwand mit Blick auf den damit verbundenen Sicherheitsgewinn für alle.

Zu Frage 6: Viele Gemeindeverwaltungen verfügen über sehr knappe Ressourcen und sind durch die Situation herausgefordert – besonders, weil sie genauso über viele schützenswerte Personendaten verfügen. Unterstützt der Kanton die Gemeinden in der Gewährleistung der Cybersicherheit auf ihren eigenen kritischen Infrastrukturen und Datenbanken?

Der Cyberkoordinator hat im Herbst 2022 eine Datenerhebung zum aktuellen Stand der Cybersicherheit bei allen 80 Luzerner Gemeinden und ihren externen IT-Dienstleistern durchgeführt. Die vertraulichen Resultate wurden unserem Rat präsentiert. Der Kanton respektiert die Gemeindeautonomie auch im Bereich der Cybersicherheit und wir sind der Auffassung, dass die Gemeinden diese Aufgabe in Eigenverantwortung lösen müssen. Zugleich sind wir uns der sehr knappen Ressourcen in einigen Gemeindeverwaltungen bewusst und wollen daher, wo sinnvoll und für den Kanton finanziell vertretbar, Synergien schaffen. Beispielsweise stellen wir interessierten Gemeinden das durch die Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) in Auftrag gegebene eLearning «eCyAd» zum Thema

Informations- und Cybersicherheit kostenlos zur Verfügung. Parallel sensibilisiert der Cyberkoordinator die Gemeinden bei entsprechenden Anlässen in enger Koordination mit dem Verband Luzerner Gemeinden.