KANTON
LUZERN

Regierungsrat

Luzern, 12. Dezember 2023

ANTWORT AUF ANFRAGE A 20

Nummer: A 20
Protokoll-Nr.: 1291
Eröffnet: 11.09.2023 / Finanzdepartement

Anfrage Howald Simon und Mit. über das Abwehren von Cyberattacken in der kantonalen Verwaltung durch neue Technologien

Vorbemerkung
Die kantonale Verwaltung ist, so wie die gesamte Wirtschaft, aufgrund der weltweit steigenden Anzahl von Cyberangriffen mit immer professionellerer Ausprägung vor zunehmende Herausforderungen gestellt. Deshalb hat die Verwaltung des Kantons Luzern in den letzten Jahren bedeutende Investitionen in die Informations- und IT-Sicherheit getätigt, um mit der steigenden Bedrohungslage Schritt halten zu können.

Konkrete Fragen zum Zustand und zur Organisation der kantonalen IT-Infrastrukturen sowie zu konkreten Vorkommnissen können wir aufgrund der hohen Sensitivität dieses Themenbereichs im Rahmen einer öffentlichen parlamentarischen Anfrage nicht im Detail beantworten. Ergänzend verweisen wir an dieser Stelle deshalb auch auf die Antwort zur Anfrage Estermann Rahel über die Cybersicherheit der öffentlichen Verwaltung und der Infrastruktur im Kanton Luzern (Anfrage A 6).

Zu Frage 1: Mit welchen Vorkehrungen schützt sich die kantonale Verwaltung vor Cyberattacken? Mit welchen Vorkehrungen werden neue Angriffsversionen erkannt? Wie wird vorausschauend in die Informationssicherheit investiert?

Mit folgenden Vorkehrungen werden Cyberattacken, neue Angriffsversionen und vorausschauende Investitionen in die Informationssicherheit getätigt:
- Die Dienststelle Informatik und die Sicherheitsorgane der kantonalen Verwaltung stehen in regelmässigem Austausch mit dem Nationalen Zentrum für Cybersicherheit NCSC, den Verwaltungen, den Hochschulen und der Wirtschaft, insbesondere auch in Bezug auf neue Angriffsversionen sowie allfällige durch das NCSC und durch Experten empfohlene technische und organisatorische Gegenmassnahmen. Dazu gehören unter anderem Weiterbildungen im Bereich «Cyber Threat Intelligence».
- Die Strategie und der Investitionsbedarf in Cybersicherheit richten sich nach den Bedrohungsformen und den damit verbundenen Risikoeinschätzungen. Die Vorkehrungen gegen Cyberattacken orientieren sich an internationalen Sicherheitsstandards ISO 27001/27002.

Zu Frage 2: Wie sieht die Statistik der letzten Jahre bezüglich unspezifischer und bösartiger Cyber-attacken in der kantonalen Verwaltung aus? Wie viele Attacken hat es gegeben, wie viele waren erfolgreich, welche Systeme, Informationen und Daten waren betroffen?

Zu konkreten Cyberattacken in der kantonalen Verwaltung können wir uns nicht öffentlich äussern (vgl. Vorbemerkung). Wir unterstützen jedoch die Meldung kritischer Infrastrukturen für Cyberangriffe (vgl. Vollmachtschreiben vom 5. April 2022 an das EFD) und der Kanton Luzern befolgt auch die entsprechenden Empfehlungen.

Zu Frage 3: Welche Lösungsansätze sind aus Sicht des Regierungsrates die sichersten, um die sensiblen Daten der kantonalen Verwaltung auf höchstem Niveau zu schützen?

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. ISO 27001/27002 regelt die benötigten Prozesse, Kontrollen und Schutzmassnahmen in den Bereichen Technik, Technologie, Betrieb, Organisation und Personal (Schulung, Sensibilisierung). Die Massnahmen sind risikobasiert (Risikoanalyse) und schaffen die Grundlage, um die ständig steigenden Anforderungen an die Informationssicherheit bewältigen zu können. Die PDCA (Plan, Do, Check, Act)-Methode stellt eine kontinuierliche Verbesserung des ISMS (Information Security Management System) nach ISO 27001/27002 sicher und dient der laufenden Verbesserung der Maturität der Schutzmassnahmen. Mit diesem Lösungsansatz lassen sich die sensiblen Daten der kantonalen Verwaltung auf höchstem Niveau schützen.

Zu Frage 4: Wird zur Abwehr von Hackerattacken das Scion-Protokoll eingesetzt? Falls nicht, weshalb nicht?

Das SCION-Protokoll (Scalability, Control and Isolation On Next Generation Networks) ist im Prinzip ein neues Routing-Protokoll, welches im Wesentlichen Verbesserungen gegenüber bestehenden Protokollen in den Eigenschaften Pfadkontrolle, Zuverlässigkeit und Sicherheit bietet. Es wurde an der ETH Zürich entwickelt und von der Firma Anapaya in der Schweiz vermarktet. Das derzeit im Internet verwendete Routing-Protokoll wurde 1989 erfunden und heisst BGP (Border Gateway Protocol). Das SCION-Protokoll ist daher als Weiterentwicklung primär für den Einsatz im weltweiten Internet konzipiert. Zurzeit wird SCION (SCION Association, Verein mit Sitz in Luzern) in der Schweiz von Providern wie Swisscom, Sunrise und VTX Telecom in eigenen Netzen angeboten. Dort wird es als geschlossenes Netz zur Verbindung von Standorten einer Organisationseinheit wie zum Beispiel dem Secure Swiss Finance Network (SSFN) oder dem HIN Vertrauensraum und/oder zur Anbindung von Remote-Arbeitsplätzen eingesetzt. Das SCION-Protokoll wird zurzeit weder im kantonalen Verwaltungsnetz LUnet noch für die Anbindung ans Internet verwendet. Stattdessen werden verschiedene bewährte Methoden, Technologien und Praktiken zur Abwehr von Hackerangriffen eingesetzt. Das Internet selbst unterstützt das SCION-Protokoll nicht. Zudem wird SCION von den grossen Herstellern von Netzwerkkomponenten im Kern noch nicht unterstützt. LUnet als kantonales Verwaltungsnetz verfügt über keine «öffentlichen» Verbindungen und wird vollständig und geschlossen vom Kanton Luzern mit

eigenen Netzwerkkomponenten betrieben. Ein Einsatz des SCION-Protokolls innerhalb des LUnet ist daher zurzeit nicht notwendig. Weil das SCION-Protokoll in Bezug auf die bereits realisierten Schutzmassnahmen für das Kantonsnetzwerk keinen zusätzlichen Schutz bietet, spielt diese neue Technologie in unserer Sicherheitsstrategie noch keine Rolle. Wir beobachten jedoch weiterhin die Entwicklung sowohl der Sicherheitstechnologie als auch die neuen Bedrohungsszenarien.

Zu Frage 5: Gibt es verwaltungsnahe Organisationen (LUKS, Lups, LUKB usw.) und andere Kantone, welche die neuen Technologien (wie zum Beispiel das Scion-Protokoll) bereits im Einsatz haben?

Zurzeit ist das SCION-Protokoll bei verwaltungsnahen Organisationen sowie in anderen Kantonen noch nicht produktiv im Einsatz. Der Bund beziehungsweise der Bereich Digitale Transformation und IKT-Steuerung (DTI) der Bundeskanzlei sowie die Dienststelle Informatik des Kantons Luzern beschäftigen sich proaktiv mit dem SCION-Protokoll. Sie stehen in Kontakt mit den relevanten Stakeholdern, der ETH Zürich und den führenden Providern in der Schweiz und verfolgen aufmerksam die Verbreitung und Weiterentwicklung des SCION-Protokolls. Die Digitale Verwaltung Schweiz (DVS) gestaltet die strategische Steuerung und Koordination der Digitalisierungsaktivitäten von Bund, Kantonen und Gemeinden. Die Zusammenarbeitsorganisation prüft zusammen mit der Firma Anapaya mögliche Pilotprojekte für Anwendungen von SCION in der öffentlichen Verwaltung. Dabei werden sowohl das kantonale Verwaltungsnetzwerk LUnet als auch das Netzwerk KOMBV-KTV, welches die Kantone mit dem Bund verbindet, als ausreichend geschützt beurteilt. Zusammenfassend beurteilen wir das SCION-Protokoll als vielversprechende Technologie mit Potential.

Zu Frage 6: Wie hoch wären die prozentualen und absoluten Mehrkosten beim Einsatz von neuen Technologien (wie zum Beispiel des Scion-Protokolls)?

Die Dienststelle Informatik (DIIN) setzt aktuelle und etablierte Technologien ein. Wir gehen davon aus, dass sich auch in diesem Bereich die Technologien weiterentwickeln werden und somit auch zukünftig Mehrkosten entstehen.

Zu Frage 7: Wie stehen aus Sicht des Regierungsrates alle bisherigen Aufwendungen im Verhältnis zur Zielerreichung (Informationssicherheit und Datenschutz der kantonalen Verwaltung, potenzielle Schadenssumme)?

Wir beurteilen die getätigten Aufwendungen im Verhältnis zur Zielerreichung als angemessen und verhältnismässig. Der risikobasierte und adaptive Ansatz ist im bestehenden Umfeld zweckmässig. Trotzdem arbeiten wir weiterhin mit unseren Fachexperten zusammen, um regelmässig neue Entwicklungen auf Seiten der Bedrohungslage zu erkennen, Handlungsbedarf hinsichtlich von Strategieanpassungen im Bereich der Vorkehrungen zu identifizieren sowie rechtzeitig allfällige Finanzierungsschritte in die Wege zu leiten. Dies zur Absicherung der Zielsetzungen auf den Gebieten Informationssicherheit und Datenschutz in finanzieller, rechtlicher und politischer Hinsicht.