KANTON LUZERN

Regierungsrat

Luzern, 3. Juli 2018

ANTWORT AUF ANFRAGE A 524

Nummer:	A 524
Protokoll-Nr.:	695
Eröffnet:	19.03.2018 / Finanzdepartement i.V. mit Justiz- und Sicherheitsdepartement

Anfrage Meyer Jörg und Mit. über den Schutz vor Cyber-Angriffen

Einleitung
Wir begrüssen es, dass die Anfrage die Thematik der Cyberrisiken aufnimmt und dieses wichtige Thema somit in den Fokus der Öffentlichkeit tritt. Gleichzeitig gilt es einleitend festzuhalten, dass wir Fragen betreffend die IT-Sicherheitsinfrastrukturen und -Organisation im Rahmen einer öffentlichen parlamentarischen Anfrage – gerade zum Schutz der kantonalen IT – nicht im Detail beantworten werden.

Alle in der Anfrage explizit erwähnten Organisationen (Kanton, Spitäler, Schulen, Gemeinden), welche grösstenteils über eigene IT Infrastrukturen verfügen, stehen im Bereich von Cyber-Risiken vor der gleichen Herausforderung. Auch wenn die technische Umsetzung weitgehend dezentral erfolgt, ist es wichtig, im Verbund den Erfahrungsaustausch zu fördern. Dazu haben wir, wie später ausgeführt wird, auch entsprechende Gremien. Mittel- und längerfristig streben wir eine weitere Bündelung der Kräfte an, damit auch kleinere Organisationseinheiten (z. B. einzelne Gemeinden) von den Anstrengungen der grösseren Einheiten – wie zum Beispiel vom Kanton mit seinen 800 Servern und 10'000 Arbeitsplätzen oder vom Luzerner Spital mit seinen sehr vielen besonders schützenswerten Personendaten – profitieren können. Die dazu notwendige Diskussion, insbesondere über die Staatsebenen hinweg, wird noch zu führen sein.

Zu Frage 1: Wie beurteilt er die Bedrohungslage und den Stand der Sicherheitsvorkehrungen generell und bezogen auf den Kanton?

Kantonale Verwaltung
Grundsätzlich beurteilen wir die aktuelle Bedrohungslage – auch aufgrund der Einschätzung der *Melde- und Analysestelle für Informationssicherung* (MELANI) – als weiterhin akut. In letzter Zeit wurden denn auch vermehrt Angriffe auf Infrastrukturen der öffentlichen Hand publik. Dabei können nicht nur gezielte Angriffe negative Auswirkungen auf die kantonale Infrastruktur haben. Vielmehr stellt beispielsweise auch Ransomware (Verschlüsselung von Daten) generell immer eine Gefahr für die Informatikmittel der öffentlichen Hand dar.

Die kantonale Verwaltung ist für aktuelle Gefahren gut gerüstet und sie orientiert sich an branchenüblichen und anerkannten «best practices». Wir stellen fest, dass sich die Kadenz neuer Angriffsmethoden stetig erhöht. Es gilt daher insbesondere neue Formen zu erkennen und geeignete Schutzmassnahmen abzuleiten. Mit der Einführung flächendeckender eGovernment-Lösungen und der generellen Digitalisierung entstehen zudem neue Angriffsvektoren. Diesen Veränderungen müssen wir entsprechend Rechnung tragen.

Auswirkungen bekannter Angriffsmethoden werden mit Hilfe technischer und organisatorischer Massnahmen minimiert. Diese benötigen jedoch ständige Justierungen und Verbesserungen, um auf die sich ändernde Bedrohungslage reagieren zu können. Technische Hilfsmittel sind beispielsweise der Einsatz von Sicherheits-Gateways, welche die E-Mail-Kommunikation oder das Browsen im Internet überwachen und gegebenenfalls die Verbindungen blockieren.

In der kantonalen Verwaltung wurden im Jahr 2017 durch diesen Sicherheits-Gateway automatisiert nahezu 90 Prozent der ankommenden E-Mails gefiltert, ohne dass diese auf die eigentliche E-Mail Infrastruktur gelangten. Diese E-Mails kamen entweder von nicht vertrauenswürdigen Absendern, sie stellten eine Bedrohung dar (Spam, Viren, Phishing) oder enthielten unerwünschte Inhalte. In Zahlen bedeutet dies, dass fast 46 Millionen E-Mails automatisch blockiert wurden. Falls in den übrigen 5,5 Millionen zugestellten E-Mails bisher unbekannte Schadsoftware enthalten sein sollte, greifen weitere Massnahmen, um die Ausführung und Ausbreitung der Schadsoftware zu verhindern.

Der beste Weg, eine Cyber-Attacke zu erkennen oder den Ausbruch einer Schadsoftware zu verhindern, ist der Mensch. Die Mitarbeiterinnen und Mitarbeiter entsprechend auszubilden und zu sensibilisieren stellt deshalb die grösste Herausforderung dar. Speziell in einem Umfeld, bei dem sich die Spezialgebiete und Fähigkeiten der Mitarbeitenden stark unterscheiden und die Abhängigkeiten komplex sind, bieten sich für Angreifer unterschiedlichste Möglichkeiten für einen Angriff an. Die Dienststelle Informatik publiziert deshalb mehrmals pro Jahr einen IT-Sicherheits-Newsletter sowie eine Awareness-Kampagne, welche aktiv auf den Bildschirmen der Mitarbeiterinnen und Mitarbeiter eingeblendet wird. Zudem ist eine flächendeckende Schulung mit einem e-Learning in Vorbereitung, welche im Herbst 2018 durchgeführt wird.

Zu Frage 2: Wie beurteilt er die Bedrohungslage und den Stand der Sicherheitsvorkehrungen bezogen auf die Gemeinden, Spitäler (Luzerner Kantonsspital, Luzerner Psychiatrie usw.), Alters- und Pflegezentren, Sozialberatungsstellen, Schulen usw.?

Kantonale Schulen und Volksschulen
Die Mehrheit der Luzerner Schulen sind über das Swisscom Projekt «Schulen ans Internet» mit dem Internet verbunden. Alle kantonalen Schulen und ungefähr die Hälfte der Volksschulen profitieren von den Sicherheitsvorkehrungen, welche die Swisscom zur Verfügung stellt. An den kantonalen Schulen werden die Geräte von der Dienststelle Informatik betreut. Sie profitieren daher zusätzlich von Sicherheitsmechanismen der zentralen Informatik des Kantons Luzern.

Die Bedrohungslage wird auch bei den Schulen als akut beurteilt. Neben den technischen Massnahmen setzt man bei den Schulen sehr stark auf die Awareness der einzelnen Benutzerinnen und Benutzer. Die Awareness-Schulung bildet im Zusammenhang mit dem vermehrten Einsatz von privaten Geräten (BYOD) im Schulumfeld die Grundlage für die Sensibilisierung im Bereich Datenschutz und Datensicherheit.

Luzerner Kantonsspital
Das Gesundheitswesen gehört gemäss IBM Security Report seit dem Jahr 2015 zu den am meisten von Cyberangriffen betroffenen Sektoren. Entsprechend stuft das Luzerner Kantonsspital das Thema Cyberrisiken als eines der Top IT-Risiken für das Spital ein. Als Gegenmassnahme werden laufend unterschiedliche technische Massnahmen zur Schadensprävention etabliert. Zusätzlich arbeitet auch das Luzerner Kantonsspital mit Fachinstitutionen wie MELANI zusammen. Um der rasant steigernden Gefahr von Cyberrisiken angemessen zu begegnen, hat das Luzerner Kantonsspital entsprechende Fachspezialisten zur Ausarbeitung einer Cyber-Defense-Strategie beauftragt. Dabei sollen zusätzliche technische

Massnahmen zur frühzeitigen Erkennung und Behebung von Schwachstellen geprüft werden. Der Variantenentscheid wird noch in diesem Jahr erwartet.

Luzerner Psychiatrie
Die Luzerner Psychiatrie stuft die Thematik Cyberrisiken in ihrem Risikomanagement als ein Hauptrisiko im operativen Bereich ein. Die Bedrohungslage verändert sich täglich und bedarf einer hohen Aufmerksamkeit und Flexibilität. Die technischen Vorkehrungen innerhalb der Luzerner Psychiatrie werden laufend aktualisiert und erweitert. Diese Anpassungen basieren immer auf den Empfehlungen und Erfahrungen der Hersteller und MELANI. Weiter betreibt die Luzerner Psychiatrie ein standardisiertes Risikomanagement, zu dem auch der Bereich Cyber-Risk gehört. Das schliesst aber nicht aus, dass die Luzerner Psychiatrie – wie andere Unternehmen auch – mit neuen unbekannten Angriffstechniken angegriffen werden kann. Bisher hat sie noch keine Schäden erlitten.

Gemeinden und deren Institutionen
Sofern die Gemeinden und deren Institutionen nicht auf die kantonale Infrastruktur zurückgreifen, liegt die Verantwortung für Sicherheitsvorkehrungen gegen Cyber-Attacken in den jeweiligen Zuständigkeitsbereichen.

Das kantonale Netzwerk, welches einen Grossteil der Gemeinden untereinander vernetzt, wird im laufenden Jahr so umgestaltet, dass die Gemeinden über diese Schnittstelle gegenseitig geschützt werden. Dies entbindet die Gemeinden jedoch nicht davon, ebenfalls entsprechende Schutzvorkehrungen zu treffen. Die Sicherheitsverantwortlichen der Gemeinden wurden denn auch im Rahmen verschiedener Veranstaltungen des kantonalen Führungsstabes über die Themen Cybercrime, aktuelle Bedrohungslage im Cyberspace und Schutz vor Cyberbedrohungen informiert und sensibilisiert.

Zu Frage 3: Wie viele Angriffe erfolgten in den letzten zwölf Monaten auf die genannten Institutionen, und wie entwickelt sich die Situation? Wurden auch schon Lösegelder bezahlt?

Kantonale Verwaltung
Die kantonale Verwaltung ist immer wieder Angriffen ausgesetzt. Ein grosser Teil der Angriffe zielt jedoch nicht direkt auf die Verwaltung. Vielmehr werden diese Angriffe breit gestreut, um eine möglichst grosse Angriffsfläche automatisiert ausnutzen zu können. Unsere etablierten Massnahmen haben dazu geführt, dass in den letzten zwölf Monaten und auch davor keine nennenswerten Schäden in der IT-Infrastruktur der kantonalen Verwaltung entstanden sind. Wenige Angriffe zielten auf einzelne Mitarbeiterinnen und Mitarbeiter ab. Diese Angriffe wurden von den Mitarbeitenden gemeldet oder von den Systemen erkannt und verhindert.

Die Möglichkeit, dass einzelne Angriffe nicht detektiert wurden, besteht jedoch in allen Organisationen. Dies ist nicht zuletzt deshalb möglich, weil die IT einem starken Wandel ausgesetzt ist und immer neue Angriffsvektoren entstehen (vgl. auch Antwort zu Frage 1). Das Beispiel Deutscher Bundestag zeigt, dass auch mit sehr viel mehr Aufwand (Infrastruktur und Personal) ein Angriff von professionell agierenden Angreifern nicht ganz ausgeschlossen oder verhindert werden kann.

Die kantonale Verwaltung hat bis heute keine Lösegeldzahlungen entrichtet und sie würde es – basierend auf den Empfehlungen von MELANI – grundsätzlich auch in Zukunft nicht machen.

Kantonale Schulen und Volksschulen
Im kantonalen Schulumfeld werden immer wieder Angriffe durch die technischen Massnahmen detektiert oder durch aufmerksame Personen gemeldet. Bisher ist es auch bei den kantonalen Schulen zu keinen Schäden gekommen.

Luzerner Kantonsspital
Das Luzerner Kantonsspital hat in den vergangenen zwölf Monaten trotz permanenter Cyberangriffe keine Schäden erlitten und auch kein Lösegeld bezahlt.

Luzerner Psychiatrie
Die Luzerner Psychiatrie ist immer wieder Angriffen ausgesetzt. Diese sind üblicherweise nicht gezielt oder dediziert auf die Institution gerichtet. In der Regel werden Bedrohungen unbewusst ausgelöst und nachfolgend durch die Sicherheitssysteme isoliert. Betroffene PC-Arbeitsplätze werden umgehend komplett ausgetauscht und in der Folge von der ICT neu aufbereitet. Auch die Luzerner Psychiatrie hat bisher kein Lösegeld bezahlt und sie will es auch in Zukunft nicht tun.

Zu Frage 4: Wie arbeitet der Kanton (z. B. die Polizei) zu diesem Thema mit den genannten Institutionen zusammen, und was geschieht konkret bei einem effektiven Angriff? Gibt es zum Beispiel Schulungen, Merkblätter usw.?

Kantonale Verwaltung
Der Kanton Luzern arbeitet direkt mit der MELANI als assoziiertes Mitglied zusammen. Die Dienststelle Informatik, die Luzerner Polizei, das Luzerner Kantonsspital und die Luzerner Psychiatrie sind Mitglied in den jeweiligen Gruppen. Dadurch erhält der Kanton Luzern wichtige nachrichtendienstliche Erkenntnisse über aktuelle Bedrohungslagen im Cyberraum und empfohlene dringliche Massnahmen.

Ferner hat sich der Kanton Luzern zu einem Informatiksicherheits-Roundtable (IT-Sicherheits-Roundtable) mit anderen Kantonen und staatsnahen Institutionen zusammengeschlossen, um laufend und gemeinsam aktuelle Strategien, Trends und Technologien zu beurteilen. Auch die Luzerner Polizei und das Luzerner Kantonsspital sind Mitglied dieses IT-Sicherheits-Roundtables.

Weiter organisiert die Schweizerische Informatikkonferenz (SIK) im Rahmen der Arbeitsgruppe Informatiksicherheit mehrere Austauschsitzungen im interkantonalen Umfeld. Der Kanton Luzern ist massgeblich an der Organisation dieser Austauschsitzungen beteiligt.

Die Dienststelle Informatik sensibilisiert die Mitarbeiterinnen und Mitarbeiter der kantonalen Verwaltung laufend im Rahmen von Awareness-Schulungen sowie mit eigens für die kantonale Verwaltung erarbeiteten Merkblättern.

Luzerner Polizei
Die Luzerner Polizei ist im Rahmen ihrer Zuständigkeit schweizweit mit anderen Ermittlungsstellen und der Bundeskriminalpolizei fedpol vernetzt und tauscht sich laufend über Ermittlungserkenntnisse aus. Ferner ist die Luzerner Polizei auch im Rahmen der Erarbeitung der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) im Sicherheitsverbund Schweiz (SVS) vertreten und berät über die Umsetzung der NCS 2.0 in den Kantonen. Daraus werden sich Massnahmen ergeben, die der Kanton Luzern beziehungsweise die Verwaltung umzusetzen haben werden. Eines der wichtigen Ziele der NCS 2.0 ist die Vernetzung und weitere Verbesserung der schweizweiten Zusammenarbeit bei der Bewältigung von Cyberlagen.

An der jährlich stattfindenden Cyber-Landsgemeinde nehmen Vertreterinnen und Vertreter der Dienststelle Informatik (DIIN) und der Luzerner Polizei in wichtigen Arbeitsgruppen aktiv Einsitz.

Ferner finden unter dem Lead der Bundeskriminalpolizei jährliche IT-Ermittler Tagungen statt, in denen Ermittlungstaktiken und Ermittlungstechnologien mit anderen Ermittlungseinheiten kantonaler Polizeikorps und der Bundeskriminalpolizei ausgetauscht werden. Ebenso partizipieren oft auch ausländische Ermittlungseinheiten – meist aus dem süddeutschen Raum – an diesen Anlässen.

Für den Schutz der polizeilichen Systeme und der Einsatzleitzentrale der Luzerner Polizei liegt die Zuständigkeit bei der Luzerner Polizei. In enger Absprache mit der Dienststelle Informatik setzt die Luzerner Polizei zur Erhöhung der Ausfallsicherheit und zur Verhinderung des Risikos von Cyber-Angriffen auf die sensiblen Systeme der Polizei laufend Massnahmen um.

Im Rahmen der Sicherheitsverbundsübung 2014 (SVU14)[1] wurden alle kantonalen Führungsstäbe damit beauftragt, ihre Informations-, Kommunikations- und Führungssysteme bezüglich Sicherheit, Verfügbarkeit und Integrität zu analysieren. Erkenntnisse aus dieser Analyse wurden in die Umsetzungsplanung aufgenommen (z. B. Verbesserung der Energieautonomie des Sicherheitsfunksystems POLYCOM).

Ein den gesamten Kanton betreffender Cyberangriff mit entsprechenden Auswirkungen auf die Landesversorgung und die kritische Infrastruktur des Kantons würde im Aufwuchsverfahren letztlich zur Einsetzung des kantonalen Führungsstabs führen. Der kantonale Führungsstab koordiniert nebst den üblichen Einsatzabschnitten auch Massnahmen, welche die Spitäler und Gemeinden betreffen.

Das Schweizerische Polizeiinstitut (SPI) hat im Rahmen der Neukonzeption der Cybercrime-Ausbildung für Polizistinnen und Polizisten ein mehrstufiges Kompetenzmodell erarbeitet. Derzeit wird das Grundmodul in allen Polizeikorps mittels eLearning mit dem Ziel geschult, die Grundkompetenzen zur wirksamen Bekämpfung der Cyberkriminalität flächendeckend zu vermitteln.

Kantonale Schulen und Volksschulen
Im Projekt Schulen ans Internet finden jährlich mindestens zwei Veranstaltungen statt, an denen sich die Verantwortlichen des Kantons mit Themen wie Datensicherheit und Datenschutz auseinandersetzen. Da an den Schulen vermehrt Privatgeräte eingesetzt werden, sind die Probleme breiter gefächert als in der kantonalen Verwaltung. Dies führt zu höherem Informationsbedarf.

Luzerner Psychiatrie
Die Mitarbeiterinnen und Mitarbeiter der Luzerner Psychiatrie werden insbesondere im Rahmen ihrer Einführung und anschliessend laufend über interne Meldungen sensibilisiert. Zudem ist bei der Luzerner Psychiatrie ein umfassendes Datenschutz- und Datensicherheitskonzept in Arbeit.

[1] https://www.svs.admin.ch/content/svs-internet/en/dokumentation/_jcr_content/contentPar/downloadlist/downloadItems/291_1457012635497.download/Internet_SVS_Schlussbericht_SVU_14_de_140416.pdf

Zu Frage 5: Welche Möglichkeiten sieht die Regierung zur Unterstützung und Stärkung der Cyber-Sicherheit der eigenen Infrastruktur wie auch derjenigen der genannten Institutionen? Gibt es Möglichkeiten im Rahmen einer schweizerischen oder zentralschweizerischen Zusammenarbeit (z. B. Beratung, Strafverfolgung)?

Cyberbedrohungen können nur gemeinsam bewältigt werden. Daher fokussiert sich die schweizerische Polizeilandschaft auf die Schaffung eines oder mehrerer nationaler Cyber-Kompetenzzentren. Entsprechende Konzepte befinden sich auf nationaler Stufe in Ausarbeitung. Nebst der Herausforderung der grundlegenden Organisation solcher Kompetenzzentren wird die Rekrutierung geeigneter Fachkräfte eine Herausforderung für die öffentliche Hand darstellen.

Auch die Zentralschweizerische Polizeikommandantenkonferenz (ZPKK) hat Ende 2017 Massnahmen in Auftrag gegeben, die polizeiliche Informatiksicherheit zu verbessern. Eine spezialisierte Arbeitsgruppe bearbeitet diese Thematik.

Die kantonale Verwaltung legt schon seit mehreren Jahren den Fokus auf die Informatiksicherheit. Mit der Überarbeitung der Informatiksicherheitsverordnung (SRL Nr. 26b) im Jahr 2016 wurden die rechtlichen Vorgaben aktualisiert und damit die Grundlagen geschaffen, die Infrastruktur und die Informationen entsprechend ihrer Klassifizierung besser schützen zu können. Die Informatiksicherheitsverordnung macht bindende Vorgaben in unterschiedlichen Disziplinen, so ist beispielsweise das regelmässige Überprüfen der getroffenen Massnahmen vorgeschrieben.

Weiter haben wir den Personalbestand für die Informatiksicherheit zur technischen Umsetzung und zur Unterstützung der Departemente seit 2015 von 100 auf 400 Stellenprozente erhöht. Zudem kann die Dienststelle Informatik bei speziellen Fragestellungen auf externe Spezialisten zurückgreifen.

Nicht mehr zeitgemässe Massnahmen und Infrastrukturen werden laufend durch neue, aktuelle ersetzt. Damit wir zusätzlich auf neue Bedrohungen reagieren können, erweitern wir – solange es wirtschaftlich sinnvoll ist – die Massnahmen laufend. Damit bei Projekten der Schutz vor Cyberattacken genügend gewichtet wird, werden die Prozesse aktuell überarbeitet und die Informatiksicherheit noch mehr eingebunden. Bei den laufenden Projekten «Digitaler Kanton» und «eGovernment» ist die Sicherheit ein zentrales Thema. Hier werden zukünftig neue, zusätzliche Massnahmen nötig werden, um die Informationen der Bürgerinnen und Bürger entsprechend zu schützen. Insgesamt investiert die Dienststelle Informatik jährlich rund eine Million Franken in die Erneuerung sowie den Einsatz von neuen IT-Sicherheits-Werkzeugen und -Methoden, um mit der Entwicklung der Gefahrensituation Schritt halten zu können.

Wie bereits bei der Antwort auf Frage 4 erwähnt, werden die Massnahmen in den zuständigen Fachgremien besprochen und abgeglichen. Somit findet ein reger Austausch statt.

Kantonale Schulen und Volksschulen
Die kantonalen Schulen profitieren von den Bestrebungen der zentralen Informatik in diesem Thema. Die Volksschulen werden jährlich an einer Veranstaltung für die technischen Betreuer über die Sicherheitsvorkehrungen informiert. Weiter plant die Dienststelle Volksschulbildung mittels einer Awareness-Kampagne, die Lehrpersonen im Bereich Datensicherheit zu unterstützen.

Luzerner Psychiatrie
Die Luzerner Psychiatrie verfügt über einen allgemeinen Sicherheitsbeauftragten (SIBE), es fehlt ihr aber heute noch ein spezifischer Sicherheitsbeauftragter (SIBE) für die Informatik. Die notwendigen Sicherheitsmassnahmen werden daher durch den Leiter Informations- und

Kommunikationstechnik (ICT) beziehungsweise die bestehenden Mitarbeiterinnen und Mitarbeiter der ICT sichergestellt.