KANTON NIDWALDEN
REGIERUNGSRAT
PROTOKOLLAUSZUG
Dorfplatz 2, Postfach 1246, 6371 Stans
Telefon 041 618 79 02, www.nw.ch

Stans, 29. November 2022
Nr. 653

Justiz- und Sicherheitsdirektion. Finanzdirektion. Parlamentarische Vorstösse. Interpellation von Landrat Dominik Steiner, Ennetbürgen, betreffend Cyber-Risiken und der Umgang damit im Kanton Nidwalden. Beantwortung

1 Sachverhalt

1.1

Mit Schreiben vom 23. Mai 2022 übermittelte das Landratsbüro dem Regierungsrat die Interpellation von Landrat Dominik Steiner, Ennetbürgen, betreffend Cyber-Risiken und dem Umgang damit im Kanton Nidwalden.

Der Interpellant ersucht diesbezüglich um die Beantwortung von sieben Fragen. Zu den einzelnen Fragen wird auf die nachfolgenden Erwägungen verwiesen.

1.2

Das Landratsbüro hat die Interpellation geprüft und festgestellt, dass sie Art. 53 Abs. 4 des Gesetzes über die Organisation und die Geschäftsführung des Landrates (Landratsgesetz, LRG; NG 151.1) entspricht. Zur Interpellation ist binnen sechs Monaten Stellung zu nehmen (vgl. § 108 Abs. 2 des Reglements über die Geschäftsordnung des Landrates [Landratsreglement, LRR; NG 151.11]).

1.4

Der Regierungsrat hat die Justiz- und Sicherheitsdirektion mit der Beantwortung der Anfrage beauftragt. Die Justiz- und Sicherheitsdirektion hat die Landwirtschafts- und Umweltdirektion, die Finanzdirektion, das Informatikleistungszentrum Ob- und Nidwalden (ILZ) sowie die Koordinationsstelle Notorganisation zum Mitbericht eingeladen.

2 Erwägungen

2.1

Der Interpellant verweist darauf, dass sich die Bedrohungslage durch gezielte Cyber-Angriffe negativ verändert habe. Dies zeigten verschiedene erfolgreiche Hackerangriffe der näheren Vergangenheit. Gerade auch in der Schweiz seien in den letzten 3 bis 5 Jahren namhafte Firmen betroffen gewesen. Zudem seien auch kritische Infrastrukturen vermehrt Ziel von Angriffen geworden.

Der Interpellant weist auch darauf hin, dass auf Bundesstufe diesbezüglich die Nationale Cyberstrategie überdacht und konsolidiert worden sei und insbesondere die Erweiterung des Nationalen Zentrums für Cybersicherheit (NCSC) in ein Bundesamt für Cybersicherheit angekündigt worden sei.

Die Schweiz befindet sich mitten in einem tiefgreifenden Digitalisierungsprozess. Dieser Prozess eröffnet grosse Chancen, birgt aber auch Risiken. Die wachsende Digitalisierung des

Alltags macht die Schweiz zunehmend abhängiger und damit verwundbarer gegenüber Störungen, Ausfällen und Missbräuchen dieser Technologien. Die rasante technologische Entwicklung, die immer stärkere Vernetzung und – im Fall von kriminellen Aktivitäten – die heterogene Täterschaft, die immer professioneller wird, bergen grosse Risiken für den Staat, die Gesellschaft und die Wirtschaft. Zeitliche und räumliche Einschränkungen für Cyber-Angriffe gibt es kaum. Sie überschreiten territoriale Grenzen und dies in einem hochdynamischen Umfeld mit kurzen Innovationszyklen. Cyber-Angriffe sind deshalb auch nicht per se zu verhindern. Eine absolute Sicherheit gibt es nicht. So ist auch ein vollständiger Schutz vor Cyber-Risiken mit verhältnismässigen Massnahmen nicht erreichbar.

Cybersicherheit ist auch kein Zustand, sondern ein stetiger Prozess. Deshalb schenkt der Kanton Nidwalden grösste Beachtung auf die Degradationsfähigkeit (in einem Notbetrieb die Funktionalität grundsätzlich erhalten und dabei auf die nicht unbedingt nötigen oder nur schwer zu schützenden Funktionen verzichten), der Resilienz (das System zu befähigen, externe Störungen zu verkraften und wieder in den Ursprungszustand zurückzukehren) und dem ganzheitlichen Managementprozess zur frühen Erkennung von Cyberrisiken.

Für die "Cyber-Sicherheit" der kantonalen Verwaltung ist das ILZ verantwortlich. Gestützt auf Art. 13 Abs. 1 der Vereinbarung über das Informatikleistungszentrum der Kantone Obwalden und Nidwalden (NG 152.2) stellt das ILZ durch organisatorische und technische Massnahmen sicher, dass die Datenschutzbestimmungen des Bundes und der Vereinbarungskantone eingehalten werden und die Datensicherheit jederzeit gewährleistet ist. Verantwortlich für die Vorsorge im Bereich Cybersicherheit für die kantonale Verwaltung ist somit das ILZ. Dieses behält die Übersicht über die wichtigsten Cyberrisken für unseren Kanton und leitet daraus die aktuelle Bedrohungslage ab. Es prüft neben dem aktuellen Schutz des Kantons vor Cyber-Risiken den künftigen Handlungsbedarf, wenn die Bedrohungslage und deren Entwicklung sich verändern.

2.2

Der Regierungsrat nimmt wie folgt zu den gestellten Fragen Stellung:

1. *Welche Erwartungen auf strategischer Ebene formuliert die Nidwaldner Regierung an den Bund, ein allfälliges Bundesamt für Cybersicherheit und an das zivil-militärische Zusammenwirken bzw. das Zusammenwirken zwischen Wirtschaft und Verwaltung?*

Der Schutz vor Cyber-Risiken ist eine Querschnitts- und Verbundsaufgabe, die nur gemeinsam und koordiniert zu erfüllen ist. In der immer stärker vernetzten Welt ist ein Zusammenwirken sämtlicher Ebenen im Bereich der Cybersicherheit von grosser Bedeutung. Dabei ist es wichtig, dass sowohl sämtliche föderalen Ebenen der Verwaltung (Bund, Kantone und Gemeinden) als auch die zivilen und militärischen Organisationen, die Wirtschaft und die Verwaltung einen guten Informationsaustausch pflegen.

Der Kanton Nidwalden will gemeinsam mit dem Bund, den Kantonen, den Gemeinden und den Partnern die Widerstandsfähigkeit gegen Cyberrisiken zum Nutzen der Bevölkerung, der Wirtschaft und der eigenen Mitarbeitenden stärken. Der Kanton Nidwalden will sich schützen vor Cyberrisiken. Digitalisierung als strategischer Schwerpunkt des Regierungsrates setzt Cybersicherheit voraus.

Die NCS 2018-2022 («Umsetzungsplan der Nationalen Strategie zum Schutz der Schweiz vor Cyber Risiken [NCS] 2018–2022») wurde von Bund, Kantonen und Wirtschaft gemeinsam entwickelt. So nahm auch der Kanton Nidwalden zu dieser Strategie Stellung. Diese auch für die Kantone aussagekräftige nationale Strategie dient dem Kanton Nidwalden für die Erarbeitung der kantonsspezifischen Strategie.

Der Kanton Nidwalden erwartet vom Bund, dass er die nationale Einschätzung über die aktuelle und künftige Bedrohung aktiv und frühzeitig kommuniziert und die auf seiner Stufe getroffenen oder geplanten Massnahmen darlegt. Dies ermöglicht es dem Kanton, rechtzeitig die strategischen Risiken zu erkennen, die künftige Entwicklung abzuschätzen, diese dem bestehenden Sicherheitsdispositiv gegenüberzustellen und anschliessend den Handlungsbedarf auf kantonaler Ebene zu bestimmen.

2. *Wie antizipiert die Nidwaldner Regierung die generelle und aktuelle Lage hinsichtlich Cyber-Risiken in Bezug auf die kritische Infrastruktur der öffentlichen Hand auf Stufe Gemeinde und Kanton:*
   a. *Verwaltung*
   b. *Energie-, Wärme- und Wasserversorgung*
   c. *Abwasseraufbereitung*
   d. *Führungsorganisation*
   e. *Kommunikation*
   f. *Erbringer eines öffentlichen Leistungsauftrages*
   g. *Etc.*

Vorbemerkungen:
Der Kanton Nidwalden passt in den jeweiligen Lagen die Handlungsfelder an und leitet daraus Massnahmen ab, um den Schutz des Kantons zu stärken.

Die nationalen Cyber-Schutz-Strategien und die Organisation des Bundes unterteilen die Aufgaben und Zuständigkeiten beim Cyber-Schutz in drei Bereiche:
– «Cyber-Sicherheit»;
– «Strafverfolgung von Cyber-Kriminalität»;
– «Cyber-Defence».

Wie bereits ausgeführt, ist für die "Cyber-Sicherheit" der kantonalen Verwaltung und der weiteren Kunden das ILZ verantwortlich. Gestützt auf Art. 13 Abs. 1 der Vereinbarung über das Informatikleistungszentrum der Kantone Obwalden und Nidwalden (NG 152.2) stellt das ILZ durch organisatorische und technische Massnahmen sicher, dass die Datenschutzbestimmungen des Bundes und der Vereinbarungskantone eingehalten werden und die Datensicherheit jederzeit gewährleistet ist. Im Rahmen dieser Vorsorgetätigkeit arbeitet das ILZ in erster Linie mit Informations- und Kommunikationstechnologien. Bei Sicherheitsvorfällen oder aktuellen notwendigen Cyberschutzmassnahmen spricht sich das ILZ mit dem Regierungsrat ab.

Für den Bereich «Strafverfolgung von Cyber-Kriminalität» sind der Bund und die Kantone zuständig. Die strategischen Vorgaben und Ziele der Regierung an die Kantonspolizei und die Staatsanwaltschaft werden in dieser Beantwortung berücksichtigt. Die Arbeiten der Kantonspolizei und der Staatsanwaltschaft des Kantons Nidwalden sind sowohl auf strategischer als auch operativer Ebene weit fortgeschritten und betreffen den gesamten Bereich der «Strafverfolgung von Cyber-Kriminalität». Zu nennen sind in diesem Zusammenhang insbesondere die Zusammenarbeit und Vernetzung der Kantonspolizei und der Staatsanwaltschaft im Cyberboard sowie im «Netzwerk für die Ermittlungsunterstützung in der digitalen Kriminalität» (Nedik).

Auch sind Geltungsbereich und Ausübung der Strafrechtspflege durch die Strafverfolgungsbehörden des Bundes und der Kantone in der Schweizerischen Strafprozessordnung (StPO; SR 312.0) bereits geregelt. In der NCS II gibt es ein spezielles Handlungsfeld «Strafverfolgung». Die Umsetzung der in der NCS II definierten vier Massnahmen sind im NCS 2018–2022 enthalten. Da es sich bei der Bekämpfung der Cyberkriminialität um eine Verbundsaufgabe der Strafverfolgungsbehörden des Bundes und der Kantone handelt, wurde mit dem sogenannten Cyberboard eine Koordinationsplattform der betroffenen Organisationen des Bundes und der Kantone geschaffen. In diesem Cyberboard werden sowohl die strategischen wie auch operativen Initiativen der Strafverfolgungsbehörden zusammengefasst.

Für den Bereich «Cyber-Defence» ist ausschliesslich der Bund zuständig. Daher ist dieser Bereich nicht Gegenstand der Beantwortung.

(a) Gemäss Vereinbarung über das Informatikleistungszentrum der Kantone Obwalden und Nidwalden (NG 152.2) hat das ILZ den Grundauftrag, die Informatikdienstleistungen für die kantonale Verwaltung zu erbringen. Es erarbeitet dabei im Rahmen der Vorgaben der Regierung Richtlinien für den Einsatz von Informatiksystemen im Kanton. Der Regierungsrat des Kantons Nidwalden hat in den Weisungen über die Nutzung von Informatikmitteln (Informatikweisungen) zudem den Schutz der Informatiksysteme der kantonalen Verwaltung weiter präzisiert und dem ILZ die Zuständigkeit für die Umsetzung der Informationssicherheit zugewiesen. Gleichzeitig wird darin auch der Grundsatz der Eigenverantwortung geregelt: jeder, der ein Informatiksystem verwendet, ist für den gesetzmässigen, zweckmässigen, sorgfältigen und verhältnismässigen Einsatz verantwortlich, insbesondere hinsichtlich des Umgangs mit internen und vertraulichen Daten.

(b) Das Elektrizitätswerk Nidwalden (EWN) hat für den Umgang mit seinen IT-Systemen und für allfällige Vorfälle ein mehrstufiges Konzept entwickelt. Es besteht aus:
- Betriebskonzept IT-Systeme
- IT-Sicherheitskonzept (wird aktuell implementiert)
- Cyber Incident Response Process
- IT-Notfallhandbuch (Entwurf liegt vor)

Im Normalbetrieb gibt das «Betriebskonzept IT-Systeme» die Grundzüge vor. Ziel ist es, damit Verantwortlichkeiten, Störungsmanagement und Benutzeranliegen im Zusammenhang mit den IT-Systemen des EWN schnell und mit den richtigen Ansprechpersonen / Partnern / Lieferanten sowie den richtigen Werkzeugen zu beheben. Im Weiteren werden die Kompetenzen, Einsatzgebiete wie auch Kommunikationswege aufgezeigt.

Ergänzend legt das EWN einen «Cyber Incident Response Process» fest. Darin wird die Reaktion auf einen Cybervorfall als Plan, der nach einem Cyberangriff umgesetzt wird, festgehalten. IT-Fachleute nutzen ihn, um auf Sicherheitsvorfälle zu reagieren. Ein klar definierter Plan für die Reaktion auf einen Vorfall kann den Schaden eines Angriffs begrenzen, die Kosten senken und die Zeit für die Behebung einer Sicherheitsverletzung verkürzen.

Um im Störungsfall (Auswirkungen eines Cyberangriffs) vorbereitet zu sein, erstellt das EWN ein «IT-Notfallhandbuch» (Entwurf liegt vor). Dieses Dokument regelt den Ablauf und die Anforderungen, welche bei einem Totalverlust der IT-Infrastruktur in den Anlagen des EWN vorzunehmen sind, um den Notfall zu bewältigen.

Parallel hat das EWN im Rahmen eines Business Continuity Managements (BCM) ein Krisenmanagement-Projekt gestartet. Ziel davon ist es, mittels Handbücher und Checklisten die Hauptprozesse im Krisenfall (u. a. IT-Ausfall) aufrecht zu erhalten.

(c) Bezüglich Störungen oder Ausfall von wichtigen Aggregaten von Abwasserreinigungsanlagen (ARA) ist aufgrund der fortschreitenden Digitalisierung im Bereich von Abwasserreinigungsanlagen auch der Cybersicherheit gebührend Rechnung zu tragen. Der Bundesrat hat mit der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie 2018-2022) den Teilsektor Abwasser als Bestandteil der kritischen Infrastrukturen festgelegt. Gemäss dem Strategiepapier des Bundes gilt es, kritische Infrastrukturen vor Cyber-Sabotage zu schützen.

In Nidwalden sorgen drei Abwasserreinigungsanlagen dafür, dass das anfallende Abwasser gereinigt wird. Alle drei ARAs wurden durch das Amt für Umwelt (AFU) zur Thematik Cybersicherheit sensibilisiert. Dabei wurde auf das entsprechende Weiterbildungsangebot hingewiesen und auf das Handbuch "Step by Step" vom Juni 2019 beziehungsweise das Register

"Cybersicherheit in OT (PLS) und IT (ICT)" verwiesen. Es handelt sich dabei um Empfehlungen des Amtes für Umwelt.

(d) Die Führungsorganisation des Kantons, namentlich der Kantonale Führungsstab (KFS), nutzt die Informatikmittel der kantonalen Verwaltung. Diese werden wiederum durch das ILZ zur Verfügung gestellt. Für den Unterhalt wie auch die Sicherheit der Geräte und Systeme ist das ILZ zuständig. Seitens KFS gibt es keine Antizipation im Sinne von sich auf die zukünftige Lage einzustellen. Übungszenarien des Kantons mit Unterstützung des ILZ, das im KFS zusammen mit der Verwaltung trainiert, gibt es nicht. Der KFS ist – wie der Rest der Verwaltung – darauf angewiesen, dass das ILZ auf mögliche Sicherheitsrisiken hinweist.

(e) Bezüglich Kommunikation stellt das ILZ folgende IT Services mit Hilfe von externen Providern sicher: Internet und Telefonie (Fixnet – Voice-over-IP [VOIP] und Mobilverbindungen). Der Internetzugang wird mit zwei verschiedenen Providern (Green/Swisscom) sichergestellt, Voice-over-IP und Mobilekommunikation durch Verträge mit der Swisscom.

Wichtig erscheint, dass umsichtig beziehungsweise auf der Zeitachse weit vorausgeplant wird (Themen wie "Sicheres Datenverbundsystem" SDVS, "Sicheres Datenverbundnetz" SDVN+, "Mobile Breitbandkommunikation" MBK, usw.).

Gemeinden und Kanton, insbesondere deren Blaulichtorganisationen und der Zivilschutz, verfügen mit Polycom über ein von der kantonalen Informatik getrenntes nationales Sicherheitsfunknetz. Bezüglich der Telefonienetze bestehen zwei Kanäle: Die Verwaltungstelefonie wird über die internen kantonalen Netzwerke abgewickelt, die Notrufverbindungen laufen über ein getrenntes Netzwerk der Swisscom. Hinsichtlich der Netzwerkstrategie des Bundes werden Redundanz- oder Folgelösungen für eine sichere Behörden- und Verwaltungskommunikation geplant oder sind teilweise in der Umsetzung. Der Regierungsrat unterstützt diese Umsetzungen explizit.

(f) siehe obige Bemerkungen.

3. *Welche Pläne verfolgt die Nidwaldner Regierung hinsichtlich Risikostrategie durch Cyber-Risiken und mit welchen Massnahmen (Notfallpläne, Technische Massnahmen, etc.) und Mitteln (Ressourcen, Organisationen, etc.) sollen die Risiken und Schäden verhindert werden können?*

Der Kanton Nidwalden verfügt über keine übergeordnete Cyberrisikostrategie. Der aktuelle Schutz des Kantons vor Cyber-Risiken leitet sich aus der aktuellen Lage und der Einschätzung deren Entwicklung ab. Erfolgreiche Cyber-Angriffe lassen sich mit verhältnismässigen Massnahmen nicht verhindern. Es geht im Rahmen der Risikoabwägungen deshalb darum, das potenzielle Schadensausmass möglichst klein zu halten, jederzeit einen minimalen Betrieb der Infrastrukturen sicherzustellen und das System zu befähigen, rasch wieder den Ursprungszustand herzustellen. Deshalb schenkt der Kanton Nidwalden grösste Beachtung auf die Degradationsfähigkeit, der Resilienz und dem ganzheitlichen Managementprozess zur frühen Erkennung von Cyberrisiken.

Das Cyberrisiko wird durch das ILZ und die Notorganisation des Kantons Nidwalden beobachtet und beurteilt, um die Regierung bei Fragen betreffend die Cyberrisiken konsistent und vorausschauend zu beraten.

Ganz grundsätzlich nimmt der Kanton gegenüber der Bevölkerung eine unterstützende Rolle ein. Er sorgt dafür – unter Berücksichtigung des Angebots des Bundes, dass die Bevölkerung in der Lage ist, eigenverantwortlich zu handeln. Hier sind die Regierung beziehungsweise der Kanton auf übergeordneter Stufe gefordert, indem sie Angebote zum Beispiel in den Themen

Aus- und Weiterbildung schaffen oder für Ereignisfälle geeignete Krisenorganisationen vorhalten.

4. Gibt es eine Deckung allfälliger Schäden durch ein Cyber-Ereignis und welche Schäden sind durch diese Versicherung gedeckt?

Das ILZ hat sowohl eine Betriebshaftpflicht- als auch eine Cyberversicherung. Allerdings beschränken sich diese auf das ILZ. Aktuell laufen im ILZ Abklärungen, wie die Versicherungssituation für den Verwaltungsinformatikbereich zwischen ILZ und den Kunden geregelt sein muss, damit eine Abdeckung garantiert werden kann und damit sowohl für das ILZ als auch seine Kunden klar ist, welche Bereiche versicherungstechnisch wie gedeckt werden müssen.

Seitens des Kantons besteht eine Betriebshaftpflichtversicherung. Eine spezielle Cyberversicherung wurde bisher nicht abgeschlossen. Die Finanzverwaltung ist diesbezüglich im Austausch mit dem ILZ und der Betriebshaftpflichtversicherung.

Das EWN hat die Versicherung solcher Schäden geprüft und bisher abgelehnt. Die Schäden würden zum grössten Teil nicht dem EWN entstehen, sondern als indirekte Schäden bei den Strombezügern. Diese würden durch die Versicherung nicht gedeckt. Im Zuge der Überlegungen, welche Partner bei der fachlichen Gegenreaktion auf einen Cyber-Angriff beigezogen werden sollen, wird erneut geprüft, ob die Versicherer einen Mehrwert bieten können.

5. Wie werden im Krisen- oder Ereignisfall wesentliche Miliz- oder andere Unterstützungselemente (wie der Zivilschutz oder andere Miliz- oder Teilzeitfunktionäre) rasch und sicher in die Prozesse und Systeme der Verwaltung integriert?

Bei einem Grossteil der Ereignisse können die IT-Systeme uneingeschränkt genutzt werden. Bereits heute werden Daten, Lagebilder, Berichte, usw. praktisch ausschliesslich digital bearbeitet und zur Verfügung gestellt.

Im Rahmen der vergangenen Einsätze zeigte sich, dass es nicht möglich ist, die geltenden Informatikweisungen in Einklang mit den operationellen Bedürfnissen der Milizeinsatzeinheiten des Kantons zu bringen. Die Koordinationsstelle Notorganisation und das ILZ sind beauftragt, eine Lösung zu erarbeiten, wie die Informatikweisungen und die operationellen Bedürfnisse der Krisenorganisation in Übereinstimmung gebracht werden können.

Der Regierungsrat hat dem ILZ die Zuständigkeit für die Vorsorge und Umsetzung der Informationssicherheit zugewiesen. Sollte ein Cyberangriff die IT der Verwaltung treffen, so würde das ILZ aktuell je nach Schweregrad in Zusammenarbeit mit Experten der Cyberversicherung und den Kunden den Fall bearbeiten. Bei den übrigen Szenarien (Angriff auf Wasserversorgung etc.) stehen die entsprechenden betroffenen Stellen in der Verantwortung. Dem ILZ kommt in diesen Fällen allenfalls eine beratende oder unterstützende Rolle zu (je nach Krisen- oder Ereignisfall).

6. Welche durch das ILZ getroffenen Massnahmen, hinsichtlich Cyber-Ereignissen wurden bereits getroffen und wie und in welchen Abständen werden diese auf ihre Effektivität überprüft?

Wie bereits in Ziff. 3 ausgeführt, betreibt das ILZ ein umfassendes Informationssicherheitsmanagementsystem (ISMS). Dieses beinhaltet einen grossen Katalog von sogenannten Controls, die die Sicherheitsdefinitionen für die Informatiksysteme umfassen. Darin werden diverse Sicherheitseinstellungen für Geräte (Server, Notebooks, PCs, Drucker etc.) aber auch Regeln für den Umgang mit den Systemen definiert. Sie basieren aktuell mehrheitlich auf den weltweit anerkannten Vorgaben des Bundesamtes für Sicherheit in der Informatik (BSI), Deutschland. Die Aktualisierung und Umsetzung der Controls wird im ILZ jährlich zweimal geprüft (intern und extern durch die Firma SGS, Genf), das Ergebnis in vertraulichen Berichten festgehalten

und dem Verwaltungsrat zur Kenntnis vorgelegt. Zusätzlich werden halbjährlich die im Internet exponierten Services (Webseiten, Applikationsservices) mit sogenannten Webpenetrationtests durch extern beauftragte Spezialisten auf ihre Sicherheit hin geprüft. Neue wichtige Services werden vor der Produktionsaufnahme zusätzlich auf die Sicherheit getestet. Im Weiteren werden in jährlich definierten Paketen spezielle Prüfungspakte (Server, Clients, Datenbanken etc.) mit einer externen IT Spezialistenfirma geprüft und mit Berichten entsprechend dokumentiert.

7. *Welche Massnahmen hinsichtlich einer erfolgreichen Sensibilisierung auf Cyber-Risiken, der Mitarbeitenden der öffentlichen Hand (Kanton, Gemeinden, Erbringer von Drittleistungen wie Wärmeverbundsorganisationen sowie öffentlich-rechtliche Anstalten), wurden bereits angedacht oder stehen in der Umsetzung?*

Das ILZ betreibt mehrstufige Sensibilisierungsmassnahmen für die Mitarbeitenden der angeschlossenen Kunden. So erscheint beispielsweise seit März 2022 ein monatliches Sicherheitsbulletin im Intranet des Verwaltungsnetzes mit aktuellen, aber grundlegenden Artikeln zum Thema Sicherheit. Im Herbst/Winter 2022/2023 wird zudem ein Security-Assessment für alle Mitarbeiter durchgeführt werden, mit dem die Mitarbeitenden mit einem Verwaltungslogin konkret in Bezug auf die Einhaltung von Securityaspekten geprüft werden. Mit Ergebnissen ist per 1. Quartal 2023 zu rechnen. Die gleichzeitige Aufschaltung eines eLearning Bereichs zum Thema Security ist Bestandteil der Herbstkampagne.

Das EWN führt zweimal pro Jahr ein E-Learning durch, um die Cyber-Risiken zu schulen. Ergänzt wird die Schulung mit unangekündigten «Attacken» durch einen externen Spezialisten. Die zuletzt im Februar 2022 durchgeführte Attacke brachte sehr gute Resultate: Niemand der EWN-Mitarbeitenden fiel auf die Phishing-Attacke herein.

Im Rahmen der Vorprüfung des Ausbauprojektes der ARA Aumühle hat zudem das Amt für Umwelt in der kantonalen Gesamtstellungnahme vom 29. September 2020 darauf hingewiesen, dass die Bauherrschaft (Abwasserverband Aumühle) im Rahmen des Vorprojektes Massnahmen nennen soll, um die Resilienz für die Cybersicherheit bei der ARA Aumühle zu verbessern und die Auswirkungen der neuen Systeme auf die Resilienz für die Cybersicherheit zu dokumentieren. Die Bauherrschaft hat an einer gemeinsamen Besprechung vom 18. Januar 2021 bestätigt, dass die Cybersicherheit bei der ARA Aumühle bereits innerhalb des laufenden Betriebes berücksichtigt sei.

2.3 Fazit

Der Kanton Nidwalden ist als Teil der Schweizerischen Eidgenossenschaft auch Teil der nationalen Cyber-Schutz-Strategien. Um den spezifischen Anforderungen des Cyber-Schutzes für den Kanton Rechnung zu tragen, orientiert sich der Kanton an den Einschätzungen der aktuellen und künftigen Bedrohungslage. Das ILZ und die Koordinationsstelle Notorganisation stehen in engem Kontakt mit dem Zentrum für Cybersicherheit, um die aktuelle Cyber-Lage und -bedrohung auszutauschen und wahrscheinliche Entwicklungen und Tendenzen antizipieren zu können.

Beschluss

Dem Landrat wird beantragt, von der Beantwortung der Interpellation von Landrat Dominik Steiner, Ennetbürgen, betreffend Cyber-Risiken und der Umgang damit im Kanton Nidwalden Kenntnis zu nehmen.

Mitteilung durch Protokollauszug an:
- Landrat Dominik Steiner, Ennetbürgen
- Landratssekretariat
- Elektrizitätswerk Nidwalden EWN
- InformatikLeistungsZentrum Ob- und Nidwalden (ILZ)
- Landwirtschafts- und Umweltdirektion (elektronisch)
- Finanzdirektion (elektronisch)
- Justiz- und Sicherheitsdirektion (elektronisch)

REGIERUNGSRAT NIDWALDEN

Landschreiber Armin Eberli