Regierungsrat des Kantons Uri

Auszug aus dem Protokoll
24. Januar 2017

Nr. 2017-40 R-362-28 Interpellation Adriano Prandi, Altdorf, zu «Datensicherheit in der Kantonalen Verwaltung»; Antwort des Regierungsrats

I. Ausgangslage

Am 16. November 2016 hat Landrat Adriano Prandi, Altdorf, eine Interpellation zu «Datensicherheit in der Kantonalen Verwaltung» eingereicht.

Landrat Adriano Prandi stellt fest, dass Cyberspionage und Angriffe auf öffentliche Verwaltungen, Banken, Spitäler, Industriebetriebe und Soziale Medien heute Realität sind. In den vergangenen Halbjahresberichten der Melde- und Analysestelle Informationssicherung Bund (MELANI) sei mehrmals über verschiedene solche Fälle berichtet worden. Dabei sei Prävention eine äussert wichtige Komponente im Kampf gegen Cyber-Spionage. Die Ziele der Angreifer seien vielfältig. Neben Informationsgewinn oder Verfügbarkeitsstörung von Systemen seien vielfach wirtschaftliche Aspekte der Grund für Angriffe. Der Interpellant stellt fest, dass der Austausch von Daten auf elektronischem Weg weiter zunehmen werde. Es sei deshalb wichtig, dass die kantonale Verwaltung ihre Daten gut schützt. Dies müsse zentral an einem Ort erfolgen und durch diejenige Stelle innerhalb der kantonalen Verwaltung wahrgenommen werden, die diesbezüglich die grösste Kompetenz hat.

Gestützt auf Artikel 127 ff. der Geschäftsordnung des Landrats (GO; RB 2.3121) stellt Landrat Adriano Prandi vier Fragen zur Datensicherheit der kantonalen Verwaltung.

II. Vorbemerkungen

Der Regierungsrat ist sich bewusst, dass die Datensicherheit und der sichere Umgang mit sensitiven Daten durch die Anwendenden enorm wichtig sind. Er hat diesbezüglich bereits verschiedene Massnahmen getroffen. Alle Informatiktätigkeiten innerhalb der kantonalen Verwaltung orientieren sich an einem IT-Leitbild und einer IT-Strategie, die vom Informatiklenkungsausschuss verabschiedet und abschliessend vom Regierungsrat freigegeben wurden. Die in diesen Dokumenten vorgegebenen Regeln und Informationen gelten für alle Direktionen der kantonalen Verwaltung, die Gerichte, die Kantonsbibliothek, die Leitung und Administration des bwz uri und der Kantonalen Mittelschule. Davon ausgenommen sind jedoch weitere öffentliche Anstalten wie z. B. die Urner Kantonalbank, das Kantonsspital Uri, die Sozialversicherungsstelle Uri usw. Diese betreiben eine eigene Informatikumgebung. Ebenfalls hat das Amt für Informatik (AfI) keinen direkten Einfluss auf das IT-Sicherheitsverhal-

ten und die IT-Umgebungen der nicht in der Kantonsinformatikumgebung gehosteten Urner Gemeinden.

Im IT-Leitbild steht zum Thema Sicherheit inhaltlich Folgendes geschrieben:

«Im Rahmen des zeitgemässen und branchenüblichen Möglichen wird alles, was angemessen ist, unternommen, um eine dauernde Gewährleistung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten/Informationen sicherzustellen.
Die IT-Strategie enthält die Organisation der Informatik und ergänzt, vertieft und strukturiert diese übergeordneten, sicherheitsrelevanten Aussagen wie folgt:

1. *Die ganzheitliche Betrachtung aller sicherheitsrelevanten Bereiche wird wie folgt strukturiert und mit Massnahmen sichergestellt:*
   - *Organisatorische Sicherheitsmassnahmen*
   - *Logische Sicherheitsmassnahmen*
   - *Physische Sicherheitsmassnahmen*
2. *Das AfI verfolgt die Entwicklung der IT-Sicherheitstechnologien stets und hält die entsprechende Umgebung auf dem Stand der Technik und sensibilisiert die Mitarbeitenden.*
3. *Die Durchsetzung der Informationssicherheit wird als eine Führungsaufgabe aller Stufen betrachtet.*
4. *Die Einhaltung der relevanten Anforderungen und Vorschriften der Informationssicherheit und des Datenschutzgesetzes werden periodisch durch interne oder externe Organe überprüft. Bei Projekten mit Datenschutzrelevanz wird jeweils der Datenschutzbeauftragte beigezogen.»*

III. Zu den gestellten Fragen

1. Wie schützt sich die kantonale Verwaltung vor Angriffen aus dem Netz?

Innerhalb der kantonalen Verwaltung zeichnet das Amt für Informatik (AfI) thematisch für den informatisierten Schutz der Daten verantwortlich. Das AfI gewährleistet mit verschiedenen Informatikprogrammen die Datensicherheit. Weiter hat es zum selben Zweck mehrere technische Vorkehrungen getroffen. Schliesslich hängt die Datensicherheit aber auch von den anwendenden Personen ab, die Daten erstellen, bearbeiten, speichern und archivieren. Nachfolgend sind verschiedene Massnahmen aufgelistet, mit denen die Datensicherheit gewährleistet wird:

- Risikomanagement
  Aufbauend auf einem vormaligen IT-Sicherheitskonzept wurde im Jahr 2012 zusammen mit der Firma SwissInfosec ein Risikomanagement-Tool (ISMS) eingeführt, das sich an den Standard von ISO 27001/2 anlehnt. Dieses ISMS wurde zur Visualisierung von Informationsrisiken aufgebaut und gibt aktuell und nachvollziehbar das Risikomanagement mit den getroffenen Massnahmen wieder. Auf demselben Programm wurde im Jahr 2013 das flächendeckende, interne Kontrollsystem (IKS) der kantonalen Verwaltung Uri implementiert.

- Schulung und Sensibilisierung

Einschlägige Studien belegen, dass mehr als 80 Prozent aller Vorfälle im Zusammenhang mit Datenverlust auf unwissende oder ungeschulte Mitarbeitende zurückzuführen sind. Dies verdeutlicht, dass nicht nur Technik und Informatik unsere Daten schützen, sondern jeder einzelne Mitarbeitende in der Thematik Informationssicherheit geschult und sensibilisiert werden muss.

Deshalb werden alle Neueintretenden zu einem halbtägigen IT-Grundlagenkurs aufgeboten, der durch einen Mitarbeiter des AfI intern durchgeführt wird. Auch hat der Regierungsrat am 18. August 2015 beschlossen, mittels einer vom AfI zur Verfügung gestellten eLearning-Plattform für alle Mitarbeitenden mit einem Kantons-Account eine IT-Sicherheits-Kampagne durchzuführen. Das Ziel dieser Informations- und IT-Sicherheits-Ausbildung war es, die Aufmerksamkeit zu fördern, unbewusste Handlungen im Umgang mit Daten vermeiden, Aufklärung anhand von Beispielen zu betreiben, vor Social Engineering[1] zu warnen, das Verständnis für Risikomassnahmen zu fördern, Weisungen und Verhalten in Erinnerung zu rufen, Hilfe und Ansprechpartner zu kennen, die Eigenverantwortung und richtiges Verhalten bei Risiken und Vorfällen zu fördern. Insgesamt lässt sich feststellen, dass diese Kampagne zur Stärkung der IT- und Informationssicherheit in der Verwaltung beigetragen hat.

Die Mitarbeitenden werden zudem laufend übers Intranet unter dem Newsportal auf aktuelle Informationen und Ankündigungen wie System-/Softwareupgrades, kritische Ransomware- oder Virenwarnungen hingewiesen. Im Intranet sind auch alle wichtigen Dokumente zur IT-Sicherheit (IT-Leitbild, IT-Strategie, Weisungen, Konzepte, Verhaltensregeln, IT-Notfallhandbuch, Kontaktdaten zum Helpdesk, Pikettnummer usw.) aufgeschaltet.

- Logisch-/technische Massnahmen
  Der Betrieb der Informatikumgebung und der Sicherheitskomponenten der Verwaltung wird allgemein nach der «Best Practice Methode» betrieben. Der Datenschutz und die Integrität wird durch ein ActiveDirectory-Konzept mit Clients, Gruppen und Benutzerauthentifizierung und die Anwendungsberechtigungen sichergestellt. Für die Anmeldung am Kantonsnetz werden per Policies komplexe Passwörter verlangt. Auch ist es nicht ohne weiteres möglich, von ausserhalb den Räumlichkeiten der kantonalen Verwaltung auf die Kantonsnetzwerke zuzugreifen. Dies ist nur mittels einem sogenannten Fernzugriff möglich, der extra beantragt werden muss und eine «2-Faktoren Authentifizierung» (Username/Passwort und Secure-PIN), VPN und eine verschlüsselte Verbindung (SSL) voraussetzt.

  Aktionslogs sind in verschiedenen Bereichen und Anwendungen verfügbar.

  Das Datensicherungskonzept (Backup) ist sehr granular aufgebaut und ermöglicht es, die einzelnen Daten sehr rasch wiederherzustellen. Ein Diskbackup an verschiedenen Standorten (Altdorf-Werkhof Flüelen) wird mit einer Bandstation an einem Drittstandort ergänzt.

  Die Systemverfügbarkeit wird durch redundante Systemkomponenten und eine virtualisierte Serverumgebung unter Berücksichtigung der Wirtschaftlichkeit möglichst hochgehalten. Kernanwendungen und allgemeine Software werden ausschliesslich mit der automatisierten Software-

[1] www.melani.admin.ch/melani/de/home/themen/socialengineering.html

verteilung auf dem aktuellsten Release- oder Patchstand gehalten. Die Server werden monatlich an den sogenannten Patchdays aktualisiert. Das gesamte Netzwerk wird mittels eines Monitoring Tools aktiv überwacht.

Das Kantonsnetzwerk ist zentral mittels Firewall und einer demilitarisierten Zone (DMZ) von der Umwelt abgesichert. Der gesamte Internetverkehr wird über einen überwachten Proxyserver geleitet. Gewisse Inhalte können nicht empfangen oder gesendet werden. Der Mailverkehr des Exchange Servers läuft ebenfalls über eine Sicherheits-Appliance, welche die Mails auf Malware prüft und Spam aussortiert. Eine Lösung für Mailverschlüsselung ist bedarfsgerecht verfügbar. Ein mehrstufiger Malwareschutz mit unterschiedlichen Produkten ist implementiert.

- Physische Massnahmen
  Das AfI betreibt zwei örtlich getrennte Rechenzentrumsräume im Raum Altdorf. Diese Räume werden durch Zutrittskontroll-/Schliessanlagen elektronisch überwacht und sind nur für die AfI-Mitarbeitenden zugänglich. Brandschutz, Unterbrechungsfreie Stromversorgungen (USV) und Klima-/Löschanlagen, Einbruchsalarmanlagen sowie Serverraumüberwachungskameras gehören zur Ausstattung.

  Das sehr leistungsfähige Kantonsnetzwerk mit einem 10 Gbit/s Backbone ist als Netzwerkring Siegwarthaus-Brikermatte-Werkhof Flüelen-Werkhof Göschenen aufgebaut. Bei einem Ausfall eines Rechenzentrums (Feuer, Wasser, Sabotage) kann dadurch innerhalb wenigen Stunden ein Notfallbetrieb aufgenommen werden. Eine Rücksicherung der Daten wäre in einem solchen Desaster-Fall nicht notwendig, da mit unserem Storage-Metrocluster die Daten immer in beiden Rechenzentren gleichzeitig aktuell gehalten werden.

2. Wie wird sichergestellt, dass die IT-Sicherheit ein höchstmögliches Niveau und Qualität hat und auch laufend aktualisiert wird?

Das AfI trägt die Hauptverantwortung für den gesamten operativen Informatik-Einsatz und damit für die eingesetzten Sicherheitssysteme in der kantonalen Verwaltung Uri. Durch die zentrale Verantwortlichkeit für IT-Budget, Projekte und Beschaffungen können die Sicherheitsanforderungen bereits früh im Beschaffungsprozess eingebracht werden.

Der Regierungsrat ist sich bewusst, dass die innerhalb der kantonalen Verwaltung für die Gewährleistung der Datensicherheit zur Verfügung stehenden Ressourcen schweizweit eher gering sind. Die Mitarbeitenden des AfI sind jedoch bestrebt, durch die Mitarbeit in interkantonalen Gremien zu nutzbringendem Fachwissen und hilfreichen Kontakten zu kommen. Mitarbeitende des AfI sind deshalb in folgenden Gremien aktiv vertreten:

- *Schweizerische Informatik Konferenz (SIK; www.sik.ch/)*
  Die Arbeitsgruppe Informatiksicherheit der SIK ist ein Fachgremium von Spezialisten der IT-Sicherheit und der Informatikrevision, das den Erfahrungsaustausch pflegt. Soweit zweckmässig und nützlich, werden zu den aufgeworfenen Fragen unter dem Blickwinkel des Information Security Management Systems (ISMS, ISO 27001/2) Best Practice Regeln erarbeitet.
- *Zentralschweizer Informatik Konferenz (ZIK)*

Die Vorsteher der Informatikämter LU, UR, SZ, OW, NW und ZG treffen sich minimal drei Mal pro Jahr zu aktuellen Themen und Erfahrungsaustausch.

- *Datenschutzbeauftragter Kanton Uri (www.ur.ch/de/verwaltung/verwaltungorg/?amt_id=996)*
  Wird bei datenschutzrelevanten Themen angefragt oder beigezogen.
- *Sicherheitsverbund Schweiz mit Nationaler Strategie zum Schutz von Cyber-Risiken*
  Der Bundesrat hat am 27. Juni 2012 die «Nationale Strategie der Schweiz vor Cyber-Risiken» und am 15. Mai 2013 deren Umsetzungsplan verabschiedet. Die NCS mit ihren 16 Massnahmen fokussiert insbesondere auf die frühzeitige Erkennung vor Cyber-Risiken sowie auf eine Stärkung der Widerstandsfähigkeit der kritischen Infrastrukturen.
- *Melde- und Analysestelle Informationssicherung Bund MELANI*
  Seit 2014 ist das AfI Mitglied im geschlossenen Kundenkreis.
- *SwissInfosec GRC Toolbox (www.infosec.ch/tools/software-grc)*
  Als Lizenzmitglied Teilnahme an den ISMS-Praxis-Foren.
- *ERFA IT-Sicherheit Zentralschweiz*
  Die ERFA-Gruppe basiert darauf, dass die Teilnehmer der ERFA ihre Erfahrungen an andere Verwaltungen oder Firmen weitergeben und von den Erfahrungen anderer Verwaltungen und Firmen profitieren. Nebst öffentlichen Verwaltungen sind viele private Firmen (CSS, Suva, KSLU, RUAG, Pilatus, Emmi, Schindler, L&G, HSLU, LU-Polizei, Maxon usw.) vertreten.
- *Zusammenarbeit mit spezialisierten Informatik-Partnerfirmen.*
- *Diverse IT-Sicherheits-News-Listen und Internet-Foren.*

3. Wurden in der Vergangenheit spezialisierte Firmen beauftragt, die Sicherheit zu testen, indem man sie versuchen liess, ins System einzudringen?

Erstmals wurde im März 2009 eine externe Firma damit beauftragt, einen Security-Check und einen «Eindringungsversuch» auf die Systemumgebung der kantonalen Verwaltung Uri durchzuführen. Zwischenzeitlich wurden weitere Security Assessments oder Audits durchgeführt. Im November 2014 wurde eine Netzwerkanalyse mit einem führenden Produkteanbieter und im April 2015 letztmals ein Angriff auf die öffentlich erreichbaren Anwendungen der kantonalen Verwaltung durch eine IT-Sicherheitsfirma inszeniert. Im Juni 2015 erfolgte im Rahmen des Sicherheitsverbunds Schweiz eine Erhebung in allen Kantonen zur Reduzierung der Cyberrisiken.

Durch das Bestimmen des jeweils gegenwärtigen Stands der Sicherheit und dem Ausmachen von potenziellen Schwachstellen konnten eben Letztere behoben werden. Die Angriffsfläche und das Angriffsfenster für erfolgreiche Attacken sowie Einbrüche wurden durch diese Audits jeweils minimiert. In unserer grösseren und durch stetige Veränderungen (Ergänzungen, Releases, Updates usw.) begriffenen IT-Systemumgebung mit einer Vielzahl von Anwendungen ist es unerlässlich, Sicherheitsaudits in nicht allzu grossen Zyklen wiederholend durchzuführen.

4. Wurde in Erwägung gezogen, für das WLAN- und Extranet Login ein zweistufiges Authentisierungsverfahren mit PIN-Code (per SMS) einzuführen?

Das Wireless Netzwerk (WLAN) der kantonalen Verwaltung ist logisch in drei Bereiche mit unterschiedlicher Funktionalität unterteilt:

- Uri-intern: Dies ist das interne WLAN für unsere mobilen Geräte. Wenn der Notebook/Tablet beim Start nicht mit einem Netzkabel verbunden ist, wird er sich mit dem WLAN URI-intern verbinden, und die Mitarbeitenden können mit der gewohnten Arbeitsplatzumgebung arbeiten.
- Uri-Byod («bring your own device»): Für alle internen und privaten Geräte (Smartphone), die nicht über das ActiveDirectory verwaltet werden. Mit dieser Verbindung ist nur ein Internet-Zugang möglich. Eine Verbindung auf Daten der kantonalen Verwaltung ist nicht möglich.
- Uri-Guest: Für Gäste, Besucher der kantonalen Verwaltung. Der Internet-Zugang ohne Verbindung auf das Netzwerk der kantonalen Verwaltung ist durch dieses Profil möglich. Der Benutzername und das Kennwort wird von den Direktionen/Ämtern vergeben und ist nur einen Tag gültig.

Vom WLAN, das vom Landrat oder von externen Gästen benutzt werden kann, ist es nicht möglich, auf das Kantonsnetzwerk und die darin vorhandenen Daten zuzugreifen, da es logisch vom Kantonsnetz getrennt ist. Aus diesem Grund macht es hier keinen Sinn, erhöhte Sicherheitsanforderungen umzusetzen.

Mit der Frage nach dem Extranet-Login gehen wir davon aus, dass der Interpellant auf die Sitzungs-Applikation für den Zugriff auf die Landrats-/Regierungsrats-Sitzungsunterlagen Bezug nimmt. Diese Extranet-Anwendung (www.ur.ch/extranet) wird wie die Homepage des Kantons Uri (www.ur.ch/) im Outsourcing betrieben und liegt im Verantwortungsbereich der Standeskanzlei. Diese plant im Jahr 2017 für alle Anwenderinnen/Anwender die Zwei-Faktoren-Authentifizierung für den Extranet-Datenzugriff (ähnlich dem Fernzugriff auf die Verwaltungsdaten) einzuführen, sofern die Ratsleitung dem zustimmt. Das heisst, dass bei jedem Zugriff auf das Extranet den Benutzerinnen und Benutzern ein Code per SMS auf das Mobiltelefon zugestellt werden muss, bevor das Login erfolgen kann. Diese Lösung ist zwar weniger benutzerfreundlich, aber sie erfüllt die IT-Richtlinien der kantonalen Verwaltung.

Mitteilung an Mitglieder des Landrats (mit Interpellationstext); Mitglieder des Regierungsrats; Rathauspresse; Standeskanzlei; Amt für Informatik und Finanzdirektion.

Im Auftrag des Regierungsrats
Standeskanzlei Uri
Der Kanzleidirektor