Beschluss Nr. 305/2025
Schwyz, 15. April 2025 / ju

Postulat P 15/24: Fertig mit den Ausreden – Cybersicherheit jetzt!
Beantwortung

1. Wortlaut des Postulats

Am 25. November 2024 haben Kantonsrat Lorenz Ilg und vier Mitunterzeichner folgendes Postulat eingereicht:

«Gutes Timing: Am heutigen Abstimmungssonntag scheint die Webseite unseres Kantons Schwyz www.sz.ch seit spätestens 11:15, kurz nach Schliessung der Abstimmungs-Urnen, down, also offline zu sein. Ebenfalls offline waren die Webseiten folgender Gemeinden in unserem Kanton: Altendorf, Küssnacht, Lachen, Reichenburg, Tuggen, Wangen.

Es ist ein geringer Trost, dass noch ein paar andere Städte & Gemeinden in der Schweiz, so wie z.B. Baden, Aarau, Brugg etc. offline sind. Offenbar hat der Internetprovider Backslash AG aus dem Kanton Thurgau ein Problem: dessen Webseite ist ebenfalls nicht erreichbar.

Wir Grünliberalen haben xmal nachgefragt, was der Kanton für die Cybersicherheit und gegen Cyberattacken unternehme - vielleicht ist es jetzt Zeit, einzusehen: zu wenig?! Dabei geht uns Cybersecurity alle an: auch den Kanton Schwyz. Dazu gehört u.a. auch die sorgfältige Auswahl und Prüfung sämtlicher IT-Dienstleister, was über das Verfassen von Pflichtenhefter und anschliessend ordentliche Beschaffung über öffentliche Ausschreibungen erfolgt.

Art des Angriffes: Gemäss Bundesamt für Cyber Sicherheit (BACS) https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/ddos-2024-11-24.html und Aargauer Zeitung https://www.aargauerzeitung.ch/aargau/aarau/angriff-ausgerechnet-am-wahlsonntag-deshalb-sind-diverse-gemeinde-websiten-aktuell-nicht-erreichbar-ld.2702130 sei der Internet-Dienstleister, die Firma Backslash AG, von einer DDOS-Attacke betroffen. Wenn dem so wäre, dann werden die Webseiten wohl in ein paar Stunden oder Tagen wieder online sein. Wenn dem aber nicht so wäre, dann könnten allenfalls auch Daten vom nicht genügend gesicherten RZ abgeflossen sein, ähnlich wie im Fall der Firma Xplain (deren Software im Kanton SZ bei der Polizei höchstwahrscheinlich ebenfalls im Einsatz ist).

Nicht von der DDoS-Attacke betroffen scheint die Webseite des Wahl- und Abstimmungssystems des Kantons zu sein, mindestens waren die Resultate über https://kanzlei.sz.ch/app/publication/de/24-11-2024/issues abrufbar.

CyberSecurity jetzt! Der Kanton Schwyz macht zu langsam vorwärts mit dem Auf- und Ausbau der IT-Infrastruktur, insbesondere auch mit der Cybersicherheit. Wenn per Ende 2024 auch noch das analoge Radio abgeschaltet sein wird, wird die Bevölkerung dereinst nur noch über DAB+ (Digital terrestrisches Radio) sowie online über die Homepage informiert werden können. Es ist nicht vorstellbar, wie die Bevölkerung im 21. Jahrhundert in Krisensituationen (z.B. bei einer Pandemie wie Corona, einem Hochwasser oder drohenden Bergsturz wie in Brienz) informiert werden soll, wenn dann auch noch die Webseite des Kantons Schwyz offline ist?! Wir sind einerseits immer mehr abhängig von dieser digitalen Infrastruktur, ohne diese jedoch genügend zu schützen. Dieser Larifari in der Digitalisierung muss ein Ende haben, weshalb wir die Regierung endlich zum Handeln auffordern!

Antrag: Der Regierungsrat wird daher beauftragt eine vollständige Auslegeordnung der gesamten IT-Infrastrukur sowie eine Analyse zur Cybersicherheit derselben vorzunehmen und konkrete Vorschläge und verbindliche Massnahmen zu unterbreiten, wo und wie die Cybersicherheit deutlich erhöht werden könnte. Ziel muss es sein möglichst rasch eine hinreichende hohe Sicherheit zu erreichen und gleichzeitig eine maximale hohe Verfügbarkeit der IT-Infrastruktur, insbesondere auch der Webseite des Kantons, zu erreichen.

Wir danken dem Regierungsrat für die zügige Bearbeitung. Besten Dank für die Unterstützung für eine sichere IT-Infrastruktur.»

2. Antwort des Regierungsrates

2.1 Ausgangslage

Am Abstimmungssonntag vom 24. November 2024 hat eine unbekannte Täterschaft die Internetseite des Kantons Schwyz (www.sz.ch) mit einer DDoS-Attacke angegriffen (DDoS: Distributed Denial of Service = Verweigerung des Dienstes). Ziel eines DDoS-Angriffs ist, die Verfügbarkeit einer Website oder von anderen Internetdiensten zu beeinträchtigen. Dies erfolgt mit einer massiven Anzahl von gleichzeitigen Anfragen auf die gleiche Internetadresse. Die Website des Kantons Schwyz – in Verantwortung der Staatskanzlei – und auch Webseiten von Gemeinden und Kantonen, die vom gleichen externen Web-Dienstleister betrieben werden, waren dadurch nur noch zeitweise erreichbar. Die kantonseigene Infrastruktur wurde nicht angegriffen. Durch diverse technische Massnahmen des Amts für Informatik mit Unterstützung des Bundesamts für Cybersicherheit, dem Web-Dienstleister und dessen Internetbetreiber sowie der Kantonspolizei konnte die Überlastung noch am Sonntag reduziert und am Montag abgewehrt werden. Am Nachmittag des 25. Novembers 2024 war die Website des Kantons wieder uneingeschränkt verfügbar. Am 27. November 2024 erfolgte ein erneuter DDoS-Angriff, der rasch abgewehrt werden konnte. Während der DDoS-Attacke wurden keine anderen Systeme des Kantons attackiert oder beeinträchtigt. Auch sind keine Daten abgeflossen. Der DDoS-Angriff wird strafrechtlich verfolgt. Ein genereller Schutz vor DDoS-Attacken ist nicht realisierbar. Zwar erlauben schnelle Reaktionszeiten und adaptive Filtersysteme eine wirksame Abwehr, jedoch bleibt bei der öffentlichen Zugänglichkeit der Webseite stets ein Restrisiko für diesen spezifischen Angriffsvektor. Dieses Risiko gilt es aus Sicht des Regierungsrates als transparente, bürgernahe Verwaltung auch in Kauf zu nehmen.

2.2 Haltung des Regierungsrats

Die Informationssicherheit hat für den Regierungsrat hohe Priorität. Das zuständige Finanzdepartement und das Amt für Informatik passen die kantonale IT laufend an die neuen Bedrohungen an und nutzen dazu bewährte Methoden. Dies erfolgt einerseits im Rahmen der Umsetzung des Informationssicherheits-Management-Systems (ISMS) zur Verbesserung der Informationssicherheit der kantonalen IT-Infrastruktur, der Netzwerksicherheit und von Fachapplikationen. Andererseits überprüfen das zuständige Finanzdepartement und das Amt für Informatik die Informationssicherheit regelmässig und nehmen dort, wo nötig, die erforderlichen Anpassungen zur Verbesserung vor.

2.2.1 Laufende Massnahmen

Aktuell werden unter anderem, aber nicht abschliessend, folgende Massnahmen zur Verbesserung der Informationssicherheit durch das Amt für Informatik durchgeführt:

- die Einführung eines externen Security Operation Centers für die 24/7 Überwachung der kantonalen IT-Infrastruktur und des kantonalen Netzwerks (Ausgabenbewilligung Kantonsrat pendent);
- die Verbesserung des Zugriffsschutzes mittels breiterer Anwendung von Multifaktor-Authentisierung;
- die Inbetriebnahme von Komponenten, um Webanwendungen auf der kantonalen IT-Infrastruktur noch besser vor Angriffen zu schützen;
- die Durchführung von Penetration-Tests (simulierte Hackerangriffe) der kantonalen IT-Infrastruktur sowie von Fachapplikationen;
- die Durchführung von regelmässigen ordentlichen und ausserplanmässigen Wartungsfenster bei Verfügbarkeit von Patches für Zero-Day-Angriffe (Ausnutzung unbekannter Sicherheitslücken);
- die Durchführung von Sensibilisierungskampagnen in der kantonalen Verwaltung betreffend Phishing und weiteren Cyberangriffen;
- Etabliertes Computer Security Incident Response Team (Computer-Sicherheitsvorfall-Reaktionsteam) des Amts für Informatik zusammen mit der IT der Kantonspolizei für die systematische und koordinierte Bearbeitung von Security-Vorfällen;
- regelmässiger Austausch mit dem Bundesamt für Cybersicherheit.

2.2.2 Regelmässige, selektive Audits

In den vergangenen 24 Monaten wurden folgende Bereiche geplant und/oder auditiert und anschliessend Optimierungsmassnahmen definiert und umgesetzt:

- Penetration Test einer Fachanwendung (Frühling 2023);
- Security Audit eines Basisdienstes (Herbst 2023);
- Penetration Test eines Basisdienstes (Frühling 2024);
- Web Application Penetration Test einer Fachanwendung (Frühling 2024);
- Web Application Penetration Test einer Fachanwendung (Herbst 2024);
- Externer Zugriff auf Basisdienste (ab Frühling 2025).

Das Amt für Informatik führt diese Massnahmen in Eigenleistung und mit Unterstützung von externen Experten durch. Zudem wurde eine zusätzliche Cybersecurity-Stelle im Amt für Informatik per 2025 geschaffen, um die Kapazitäten zu erhöhen.

2.2.3 Optimierung der Cybersicherheit als kontinuierlicher Verbesserungsprozess

Die Ziele des Postulats, die Verbesserung der Cybersicherheit, werden mit den ergriffenen Massnahmen bereits erfüllt. Auch nach Abschluss der oben erwähnten Massnahmen wird die kantonale IT laufend an neue Bedrohungen angepasst. Eine externe Analyse ist nach der Inbetriebnahme des Security Operation Center und des Informationssicherheits-Management-Systems zielführend und im Anschluss an die Umsetzung dieser beiden Grossprojekte bereits vorgesehen. Eine stete Adaption ist in diesem Umfeld mit dynamischen Bedrohungen auch notwendig und es besteht dauerndes Optimierungspotenzial. Diesbezüglich zeigen sich auch zusätzliche Herausforderungen bei dezentralen (Fach-)Lösungen, welche über die Jahre aufgebaut wurden. Der Regierungsrat ist entsprechend auch bestrebt, ganzheitliche Ansätze voranzutreiben. Entsprechend hat er auch per 1. März 2025 die Verordnung über die Informationstechnologie vom 1. September 2015 (IT-Verordnung, ITV, SRSZ 143.113) zu einem grossen Teil revidiert und insbesondere in den Bereichen Informationssicherheit, IT-Beschaffung und IT-Steuerung verbesserte Grundlagen geschaffen.

2.2.4 Kommunikation mit der Bevölkerung

DDoS-Angriffe können grundsätzlich jederzeit vorkommen und die Verfügbarkeit von Websites bzw. von Internetdiensten beeinträchtigen. Die Auswirkungen können durch technische Massnahmen reduziert werden. Eine vollständige Abwehr ist aktuell aber nur mit Unterstützung des Internetbetreibers und weiterer Stellen möglich. Der Kanton unterhält neben der eigenen Website auch diverse Social-Media-Kanäle, um mit der Bevölkerung kommunizieren zu können. In Krisensituationen, bei welchen auch der Internetzugang der Bürger nicht mehr funktionieren würde, kommen die Notfalltreffpunkte in den Gemeinden und Bezirken zum Einsatz. Die üblichen Kommunikationsmittel des Bevölkerungsschutzes sind weiterhin vorhanden und bedingen keine operative Webseite.

2.3 Fazit

Der Regierungsrat erachtet die Durchführung einer vollständigen Auslegeordnung der gesamten IT-Infrastruktur sowie die Analyse zur Cybersicherheit als nicht zielführend. Der notwendige interne und externe Ressourcenbedarf für diese Auslegeordnung und Analyse wird auf rund 100 interne Personentage und Fr. 200 000.-- bis Fr. 350 000.-- externe Expertenunterstützung geschätzt (exklusive Bearbeitung allfälliger Befunde). Mit den aktuellen Massnahmen werden die Ziele des Postulats bereits erfüllt. Die Durchführung einer vollständigen externen Auslegeordnung, die externe Analyse der Cybersicherheit und das Aufzeigen von konkreten Vorschlägen und verbindlichen Massnahmen verzögert die bereits ergriffenen Massnahmen und zeigt potenziellen Angreifern Ansatzpunkte auf. Aus diesem Grund beurteilt der Regierungsrat das Postulat in seiner Wirkung als kontraproduktiv und beantragt daher, es nicht erheblich zu erklären.

Ebenso wenig zielführend erachtet der Regierungsrat die Tonalität des vorliegenden Vorstosses. Die im Postulat dargelegten, nicht zutreffenden Vermutungen und Unterstellungen sind nicht sachgemäss und eines ordentlichen, konstruktiven politischen Prozesses nicht würdig.

Beschluss des Regierungsrates

1. Dem Kantonsrat wird beantragt, das Postulat P 15/24 nicht erheblich zu erklären.

2. Zustellung: Mitglieder des Kantonsrates.

3. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatsschreiber; Sekretariat des Kantonsrates; Departemente; Amt für Informatik.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun
Staatsschreiber