Anfrage NEOS – eingelangt: 12.6.2024 – Zahl: 29.01.567

Anfrage der LAbg. Fabienne Lackner, NEOS

Herrn Landesrat MMag. Daniel Zadra

Herrn Landesrat Christian Gantner

Landhaus

6900 Bregenz

Bregenz, am 12.06.2024

Anfrage gem. § 54 der GO des Vorarlberger Landtages:
Cybersicherheit - Wie gut ist das Land aufgestellt, wenn es um den Schutz vor Cyberangriffen geht?

Sehr geehrte Herrn Landesräte,

die Digitalisierung hat nicht nur neue Möglichkeiten geschaffen, sondern auch die Kriminalität in Teilen in den virtuellen Raum verlagert. Mit dem Aufkommen des World Wide Webs, von Smartphones und Computern hat die Cyberkriminalität floriert und sogar zu einem Riesengeschäft entwickelt. Besonders alarmierend sind Beispiele wie die russischen Cyberangriffe auf die US-Regierung, wobei ausländische Geheimdienstmitarbeiter Zugang zu Finanzdaten und Passwörter erhielten. Genauso sind US-Unternehmen gefährdet, wie der Slack-Angriff auf Uber zeigt. Dabei erhielt ein Hacker den vollständigen Zugang zum Unternehmen, einschließlich E-Mail-Systeme und Cloud-Speicher.[1]

Bundeskanzler Olaf Scholz sieht eine Zeitenwende durch den russischen Angriff auf die Ukraine.[2] Seither zeigen digitale Angriffe auf ukrainische Infrastrukturen und regierungsnahe Unternehmen einen „Krieg im Netz". Die Wirtschaftskammer schließt nicht aus, dass es durch die Auseinandersetzung zwischen Russland und Ukraine zu Kollateralschäden in Österreich kommen kann.[3] Selbst das EU-Parlament wurde bereits mehrfach gehackt, ebenso wie die EU-Kommission.[4]

Wenngleich in anderer Form, aber Österreich blieb von der digitalen Bedrohung nicht verschont. 2022 wurde das Bundesland Kärnten Opfer eines Hackerangriffs. Eine internationale Gruppe forderte fünf Millionen Euro Lösegeld für eine Entschlüsselungssoftware. Auch hier der Verdacht einer russischen Beteiligung.[5] Anfang dieses Jahren erlebten gleich mehrere niederösterreichische Einrichtungen ähnliche Angriffe.[6] Selbst das Innenministerium erklärt auf seiner Website vor der allgegenwärtigen Gefahr durch Cyberbedrohungen.[7]

Die Internetkriminalität ist zu einer der größten Herausforderungen für die Sicherheit Österreichs geworden. Das unterstreicht die Studie „Cybersecurity in Österreich". Die Anzahl und Qualität der Cyberangriffe nehme zu. Deepfakes und Desinformationskampagnen würden sich rasant entwickeln. Die Statistik alarmierend: Jeder sechste Angriff auf ein Unternehmen war erfolgreich, jedes 3. Unternehmen hat zumindest einmal eine Lösegeld bei einem Ransomware-Angriff bezahlt. 54% der befragten Unternehmen waren in den letzten 12 Monaten Opfer

[1] https://arcticwolf.com/resources/blog-de/eine-kurze-geschichte-der-cyberkriminalitat/
[2] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Informationen-und-Empfehlungen/Cyber-Sicherheitslage-fuer-die-Wirtschaft/gravierende-Cyber-Risiken/Ukraine_Konflikt/ukraine_konflikt_node.html
[3] https://www.wko.at/it-sicherheit/bedrohungslage-aufgrund-des-kriegs-in-der-ukraine
[4] https://www.tagesschau.de/ausland/europa/eu-parlament-hackerangriff-101.html
[5] https://www.derstandard.at/story/2000136355061/cyberangriff-auf-kaernten-die-wichtigsten-fakten-zum-aktuellen-fall
[6] https://www.noen.at/niederoesterreich/chronik-gericht/cyber-kriminalitaet-in-niederoesterreich-gab-es-mehrere-hacker-angriffe-408900874
[7] https://www.bmi.gv.at/magazin/2023_09_10/12_Cybersicherheit.aspx

von Desinformationskampagnen, 42% sogar mehrmals. Zwei Drittel fürchten, dass Cyberangriffe auf ihre Dienstleister Auswirkungen auf sie selbst haben könnten.[8] Besonders besorgniserregend ist der Anstieg an Angriffen auf Krankenhäuser und Pflegeeinrichtungen.

Die Kriminalstatistik zeigt also klar, dass Hackerangriffe nicht nur häufiger werden, sondern zudem erhebliche Schäden verursachen. Es ist dringend notwendig, dass die Gesellschaft, die Behörden und Institutionen für die Gefahren der Cyberkriminalität sensibilisiert werden. Die entscheidende Frage ist daher: Wie gut ist Vorarlberg darauf vorbereitet?

Vor diesem Hintergrund stelle ich hiermit gemäß § 54 der Geschäftsordnung des Vorarlberger Landtages folgende

ANFRAGE

1. Wie schätzt die Landesregierung die aktuelle Bedrohungslage in Bezug auf Cyberkriminalität und Cyberspionage in Vorarlberg ein?
2. Wie viele Cyber-Angriffe (DDoS-Angriffe, Phishing E-Mails usw.) auf IT-Systeme der Landesverwaltung und landeseigener Betriebe gab es seit 2019? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbestand)
3. Welche Maßnahmen hat das Land Vorarlberg seit 2019 ergriffen, um Cyberangriffe auf das IT-System der Landesverwaltung und landeseigener Betriebe zu erkennen und abzuwehren sowie präventive Maßnahmen gegen Cyberkriminalität?
4. Welche Fortbildungsmaßnahmen werden Landesbediensteten im Umgang mit Cyberkriminalität seit angeboten und wie viele Teilnehmer:innen waren seither zu verzeichnen? Falls es keine Fortbildungsmaßnahmen gibt, warum nicht?
5. Welche Kooperationen zwischen dem Land Vorarlberg und den Gemeinden gibt es im Falle eines Cyber-Angriffs auf eine Vorarlberger Gemeinde? Falls keine vorgesehen sind, wieso nicht?
6. In wie vielen Fällen haben derartige Angriffe zu einer Beeinträchtigung des Betriebsablaufes geführt? (Bitte aufschlüsseln nach Jahr und Landesbehörde)
7. In wie vielen Fällen konnten die konkreten Angreifer ermittelt werden? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbestand)
8. Ist seit Beginn des Kriegs in der Ukraine eine Zunahme an Cyberangriffen zu verzeichnen?
9. Welche Folgen hatte der mögliche Cyberangriff mit Blick auf den Zugang der Daten für Dritte oder den Verlust von Daten und wie hoch schätzen sie den finanziellen Schaden ein, der durch Cyber-Angriffe bereits entstanden ist? (Bitte um Angabe pro Jahr)
10. Welche Initiativen, die das Thema Cyber-Security sowie verwandte Themen betreffen, unterstützt das Land Vorarlberg und in welcher Höhe?
11. Laut Medienberichten ist als Antwort auf die wachsende Bedrohung „Cyberkriminalität“ die Errichtung eines Cybercrime-Trainingscenters in Bregenz geplant – wie ist der Umsetzungsstand und wie viele Teilnehmer:innen sollen daran pro Kalenderjahr teilnehmen?
12. Wie viele Experten und Fachkräfte stehen der Polizei in Vorarlberg zur Verfügung, die sich mit der Abwehr von Cyberkriminalität beschäftigen?

[8] https://kpmg.com/at/de/home/insights/2024/04/cybersecurity-studie-2024.html

Für die fristgerechte Beantwortung dieser Anfrage bedanken wir uns im Voraus!

Mit freundlichen Grüßen

LAbg. Fabienne Lackner

Beantwortet: 2.7.2024 – Zahl: 29.01.567

Landesrat
MMag. Daniel Zadra

Vorarlberg
unser Land

Frau
LAbg. Fabienne Lackner
Landtagsklub NEOS
Im Hause

Im Wege der Landtagsdirektion

Bregenz, am 02. Juli 2024

Betreff: LT-Anfragebeantwortung, Zl. 29.01.567; Cybersicherheit: Wie gut ist das Land aufgestellt, wenn es um den Schutz vor Cyberangriffen geht?

Sehr geehrte Frau LAbg. Lackner,

ich erlaube mir, Ihre Anfrage vom 12.06.2024 (29.01.567: Cybersicherheit: Wie gut ist das Land aufgestellt, wenn es um den Schutz vor Cyberangriffen geht?) gemäß § 54 der Geschäftsordnung des Vorarlberger Landtags im Einvernehmen mit Landesrat Christian Gantner im Folgenden zu beantworten. Zugleich weise ich darauf hin, dass die Fragen 8, 11 und 12 außerparlamentarisch beantwortet werden, da die Angelegenheiten der Sicherheitspolizei in Gesetzgebung und Vollziehung Bundessache darstellen und nicht vom Interpellationsrecht des Vorarlberger Landtages umfasst sind.

1. **Wie schätzt die Landesregierung die aktuelle Bedrohungslage in Bezug auf Cyberkriminalität und Cyberspionage in Vorarlberg ein?**

Grundsätzlich teilt das Amt der Vorarlberger Landesregierung die Sicht des BKA: Cybersicherheit gewinnt immer mehr an Bedeutung und stellt eine der obersten Prioritäten und eine gemeinsame Verantwortung für Staat, Wirtschaft, Wissenschaft und Gesellschaft dar. Näheres findet sich im Bericht Cybersicherheit für das Jahr 2022.
Im Augenblick scheinen die sogenannten Ransomware-Angriffe, die noch 2022 Schlagzeilen machten, zurückzugehen, jedoch steigt die Bedrohung durch internetbasierte Erpressung und Online-Betrug an. Alte Schwachstellen werden weiterhin ausgenutzt, und es besteht ein anhaltendes Risiko durch Sicherheitslücken in populärer Software und weit verbreiteten Technologien.

Amt der Vorarlberger Landesregierung
Landhaus, Römerstraße 15, 6901 Bregenz, Österreich | www.vorarlberg.at | www.vorarlberg.at/datenschutz
daniel.zadra@vorarlberg.at | T +43 5574 511 26000 | F +43 5574 511 926095

2. **Wie viele Cyber-Angriffe (DDoS-Angriffe, Phishing E-Mails usw.) auf IT-Systeme der Landesverwaltung und landeseigener Betriebe gab es seit 2019? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbestand).**

Im angefragten Zeitraum kam es zu keinen Vorfällen, die nennenswerte Auswirkungen auf die Aufgabenerfüllung des Amtes der Vorarlberger Landesregierung hatten.
Im Jahr 2024 wurde ein Vorfall mit Caller-ID Spoofing verzeichnet. Interne Systeme waren dabei nicht betroffen, sondern es wurden Privatpersonen von einer fingierten Telefonnummer aus angerufen, die dem Amt der Vorarlberger Landesregierung zugeordnet war. Gemeinsam mit dem Telefonanbieter und der Polizei wurden Maßnahmen gesetzt, um die negativen Auswirkungen zu reduzieren.
Als „landeseigen" im Sinne dieser Anfrage gelten unselbständige, dem Land als Rechtsträger unmittelbar zuzuordnende Betriebe wie etwa der Landesforstgarten, das Umweltinstitut oder das Hochbauamt. Diese Betriebe waren im angefragten Zeitraum keinen Cyberattacken ausgesetzt.

3. **Welche Maßnahmen hat das Land Vorarlberg seit 2019 ergriffen, um Cyberangriffe auf das IT-System der Landesverwaltung und landeseigener Betriebe zu erkennen und abzuwehren sowie präventive Maßnahmen gegen Cyberkriminalität?**

Die Landesbehörden investieren in technologische und organisatorische Abwehrmaßnahmen und entwickeln diese kontinuierlich weiter. Diese Maßnahmen umfassen unter anderem:

- Aktiver Austausch innerhalb der CyberSecurity Branche wie z.B. Cert.at, govCert.at, Bundesländeraustausch im IT-Sec Bereich, aktives Mitglied Austrian Trust Circle, Teilnahme an Security-Konferenzen
- Aktive Überwachungsmaßnahmen wie z. B. Überwachungen von Meldungen von data breaches (pwned), Newslettern oder RSS-Feeds
- Aktives Patchmanagement der IT-Systeme
- Härtungsmaßnahmen zur Absicherung von Systemen
- Spam/Phishing-Schutz an den zentralen Mailing-Systemen und Schulung der Mitarbeiter zur Identifikation und Abwehr von Phishing-E-Mails
- Firewall-Systeme nach aktuellem Stand der Technik zur Netzwerksegmentierung und Überwachung des Netzwerkverkehrs mittels IDS
- Einsatz von MDM für die Verwaltung und Absicherung von mobilen Geräten
- Absicherung von externen Zugängen mittels MFA-Mechanismen
- Schulung der IT Benutzer:innen mit privilegierten Rechten
- IT-Sicherheit-Richtlinie
- Lieferantenmanagement der IT-Zulieferer und vertragliche Einbindung

4. **Welche Fortbildungsmaßnahmen werden Landesbediensteten im Umgang mit Cyberkriminalität seit angeboten und wie viele Teilnehmer:innen waren seither zu verzeichnen? Falls es keine Fortbildungsmaßnahmen gibt, warum nicht?**

Alle Mitarbeitenden, die Zugang zu den IT-Systemen haben, müssen verpflichtend das eLearning IT-Sicherheit und das eLearning Korruptionsprävention absolvieren. Zudem steht allen

Mitarbeitenden über das vConnect Portal ein einfacher Zugangspunkt zu Verfügung, bei dem die wichtigsten Themen zur IT-Sicherheit behandelt werden. Im Zuge der Einführung des eLearning wurde eine Phishing-Simulation mit einer anschließenden Awareness-Kampagne durchgeführt.

5. **Welche Kooperationen zwischen dem Land Vorarlberg und den Gemeinden gibt es im Falle eines Cyber-Angriffs auf eine Vorarlberger Gemeinde? Falls keine vorgesehen sind, wieso nicht?**

Im Falle eines Cyber-Angriffs steht den Gemeinden das Knowhow des Amt der Vorarlberger Landesregierung zur Verfügung. Vertreterinnen und Vertreter von IKT-Nutzer:innen aus dem Behördenbereich und der öffentlichen Verwaltung können über das govCert in aktiven Informationsaustausch eingebunden werden. Die Teilnehmer:innen erhalten Zugriff auf einschlägige Dokumente und können an IT-Sec Workshops, Schulungen und Security-„Stammtischen“ partizipieren.

6. **In wie vielen Fällen haben derartige Angriffe zu einer Beeinträchtigung des Betriebsablaufes geführt? (Bitte aufschlüsseln nach Jahr und Landesbehörde)**

Es wurde keine nennenswerten Beeinträchtigungen durch Angriffe verzeichnet.

7. **In wie vielen Fällen konnten die konkreten Angreifer ermittelt werden? (Bitte aufschlüsseln nach Jahr, Landesbehörde und Straftatbestand)**

Dem Amt der Vorarlberger Landesregierung ist kein erfolgreicher Cyberangriff bekannt.

8. **Ist seit Beginn des Kriegs in der Ukraine eine Zunahme an Cyberangriffen zu verzeichnen?**

Beim Landeskriminalamt Vorarlberg ist keine derartige Steigerung bekannt.

9. **Welche Folgen hatte der mögliche Cyberangriff mit Blick auf den Zugang der Daten für Dritte oder den Verlust von Daten und wie hoch schätzen sie den finanziellen Schaden ein, der durch Cyber-Angriffe bereits entstanden ist? (Bitte um Angabe pro Jahr)**

Im Amt der Vorarlberger Landesregierung ist kein erfolgreicher Cyberangriff registriert worden.

10. **Welche Initiativen, die das Thema Cyber-Security sowie verwandte Themen betreffen, unterstützt das Land Vorarlberg und in welcher Höhe?**

Das Amt der Vorarlberger Landesregierung steht in ständigem Austausch mit Akteur:innen der Cybersecurity-Branche sowie mit den anderen Bundesländern. Es ist etwa Mitglied des Austrian Trust Circle, bei cert.at sowie govCert.at und nimmt regelmäßig an Security-Konferenzen teil, um auf dem letzten Stand der Dinge zu bleiben.

11. **Laut Medienberichten ist als Antwort auf die wachsende Bedrohung „Cyberkriminalität“ die Errichtung eines Cybercrime-Trainingscenters in Bregenz geplant – wie ist der Umsetzungsstand und wie viele Teilnehmer:innen sollen daran pro Kalenderjahr teilnehmen?**

Die Implementierung des Cybercrime-Trainingscenters (CCTC) erfolgt im Rahmen der Kriminaldienstreform 2.0 im Landeskriminalamt Vorarlberg als neue Organisationseinheit und dient der Stärkung der Grundkompetenz von Polizeibeamtinnen und Polizeibeamten im Bereich „Cybercrime“. Derzeit findet eine Evaluierung der möglichen Standorte für die Errichtung des Cybercrime-Trainingscenters statt und es werden die zukünftigen Trainer des CCTC bereits ausgebildet. Es ist geplant, dass jede Beamtin und jeder Beamte nach Absolvierung der Polizei-Grundausbildung das Modul im CCTC absolviert. Zudem werden alle derzeitigen – mit Sonderverwendungen in diesem Bereich betrauten Beamtinnen und Beamten – sowie an dieser Thematik Interessierte, das CCTC-Modul absolvieren.

12. **Wie viele Experten und Fachkräfte stehen der Polizei in Vorarlberg zur Verfügung, die sich mit der Abwehr von Cyberkriminalität beschäftigen**?

Im Landeskriminalamt Vorarlberg stehen aktuell sieben Fachkräfte zur Verfügung, die im Bereich Cybercrime bzw. IT tätig sind. Des Weiteren verfügen die Bezirke über insgesamt zwölf Beamtinnen und Beamte, die neben ihrer Tätigkeit auf den Polizeiinspektionen als Bezirks-IT-Ermittler im Einsatz sind. Zwei weitere Beamt:innen sind beim LSE als IT Sachbearbeiter tätig.

Mit freundlichen Grüßen

MMag. Daniel Zadra
Landesrat