

Schwyz, 18. Januar 2024

Kleine Anfrage KA 34/23: Lehren aus dem Cyberangriff auf den Bezirk March
Beantwortung

1. Wortlaut der Kleinen Anfrage

Am 22. Dezember 2023 haben die Kantonsräte Michael Fedier und Dr. Michael Spirig folgende Kleine Anfrage eingereicht:

«In einer beunruhigenden Entwicklung zeigt sich die digitale Infrastruktur des Bezirks March anfällig für Cyberangriffe. Dieser Umstand kommt trotz wiederholter Warnungen und Anträge der Grünliberalen Partei (GLP) sowie den Empfehlungen des Nationalen Zentrums für Cybersicherheit (NCSC). Die anhaltende Störung der EDV-Systeme der Sekundarschulen seit dem 13. Dezember wirft nicht nur Fragen zur Sicherheit auf, sondern löst Verunsicherung bei Bevölkerung und Institutionen aus. Was wenn persönliche oder Firmendaten im Netz auftauchen? Wie steht es um die Ausbildungsqualität im Analogschulbetrieb und wie wirkt sich das auf die Bearbeitungsdauer von Baugesuchen aus? Alles in allem verdeutlicht dies auch das Versäumnis, angemessene Präventivmassnahmen zu ergreifen.

Detaillierte Informationen zu Sicherheitslücken werden normalerweise von den betroffenen Organisationen aus Sicherheitsgründen nicht veröffentlicht. Der Bezirk March sowie die Schulbehörden verwenden Software, welche jedoch bekanntermassen auch in anderen Bezirken im Kanton eingesetzt werden und möglicherweise als Einstiegspunkt für Cyber Angriffe diene. Auch der Kanton setzt auf Software für sein Content Management System (CMS) und den sogenannten «Online Schalter», welche nachweislich Sicherheitslücken haben und in den Städten Baden und Aarau erst gerade Ziel von Cyberangriffen wurden.

Für uns Grünliberale ist es jetzt umso mehr an der Zeit, dass effektive Massnahmen ergriffen werden, um die digitale Sicherheit zu gewährleisten. Die jüngsten Vorfälle verdeutlichen, dass Prävention und eine proaktive Herangehensweise entscheidend sind, um sich gegen die ständig wachsende Bedrohung durch Cyberangriffe besser zu schützen.

Wir bitten den Regierungsrat daher dringlich um die Beantwortung der folgenden Fragen:

1. *Welche Gemeinden und Bezirke sowie welche Einheiten vom Kanton haben das gleiche oder ähnlich gefährdete Systeme?*
2. *Was unternimmt der Kanton um gegen die nun aufgedeckten Sicherheitslücken in den anderen Bezirken und Gemeinden, sowie bei sich selbst, um präventiv vorzubeugen?*
3. *Weshalb wurde nicht reagiert, als das NCSC laut March Anzeiger vom 21. Dezember von einem bevorstehenden Angriff gewarnt hat? Hat der Kanton ebenfalls solche Warnungen bekommen?*

Für die Beantwortung der Fragen bedanken wir uns im Voraus.»

2. Antwort des Finanzdepartements

2.1 Vorbemerkungen

Am Samstag, 9. Dezember 2023 erhielten die Kontaktpersonen des Amtes für Informatik (AFI) vom NCSC per E-Mail die Meldung, dass beim Bezirk March ein Ransomware-Angriff stattfindet und eine mögliche Verschlüsselung bevorsteht. Zeitgleich meldete sich das NCSC telefonisch bei der Einsatzleitzentrale der Kantonspolizei Schwyz (Kapo), um über den Vorfall zu informieren. Beide Kommunikationswege führten dazu, dass sich innerhalb kurzer Zeit einerseits die Kapo, wie auch der Leiter AFI bei den verantwortlichen Personen des Bezirks March meldeten und über den Vorfall informierten sowie dringende Massnahmen empfahlen. Als präventive Massnahme seitens Kanton wurde die Verbindung des Bezirksnetzes zum Kantonsnetzwerk getrennt, um eine laterale Bewegung des Angreifers in andere Netze zu unterbinden.

2.2 Welche Gemeinden und Bezirke sowie welche Einheiten vom Kanton haben das gleiche oder ähnlich gefährdete Systeme?

Die Gemeinden und Bezirke betreiben ihre IT-Infrastruktur im Sinne der Autonomie der Gemeinwesen selbst. Berührungspunkte zum Kanton existieren nur in einzelnen Applikationen, welche vom AFI betrieben und über das Kantonsnetzwerk zur Verfügung gestellt werden. Insofern kann keine Aussage gemacht werden, welche Systeme von anderen Organisationen verwendet werden. Der Fokus sollte auch nicht auf ein spezifisches System gelegt werden. Um sich optimal vor Cyberangriffen zu schützen, müssen sämtliche Systeme in die Sicherheitsüberlegungen einbezogen werden.

2.3 Was unternimmt der Kanton um gegen die nun aufgedeckten Sicherheitslücken in den anderen Bezirken und Gemeinden, sowie bei sich selbst, um präventiv vorzubeugen?

Beim Kanton wurden bei diesem Vorfall keine Sicherheitslücken aufgedeckt, das kantonale System wurde nicht kompromittiert. Gemäss dem heutigen Wissensstand ist der Eintrittspunkt des Angreifers beim Bezirk March noch nicht eindeutig festgestellt. Eine der schwerwiegendsten Sicherheitslücken betrifft die fehlende Multifaktorauthentifizierung im Verwaltungs- und Schulumfeld. Der Kanton verlangt beim Zugriff auf interne Ressourcen von extern bereits seit Jahren einen zweiten Faktor. Diese Regelung wird im kommenden Jahr weiter verschärft und im Sinne eines Zero-Trust-Ansatzes auch auf den internen Zugriff ausgeweitet.

Das AFI hat die Gemeinden und Bezirke im Rahmen eines Meetings zum Vorfall informiert und die Empfehlung ausgesprochen, dass sie sich für den Zugang zum geschlossenen Kundenkreis des NCSC (Cyber Security Hub) anmelden sollen. So können die Verantwortlichen zeitnah vom NCSC kontaktiert werden und erhalten die wichtigsten Informationen hinsichtlich der aktuellen Bedrohungslage direkt von den Spezialisten des Bundes.

Selbstverständlich soll dieser Vorfall auch genutzt werden, um Verbesserungen in der aktuellen Struktur weiter zu forcieren. Eine mögliche Verbesserung besteht insbesondere in der Triage zentraler Informationen. Dazu erarbeitet das AFI zusammen mit der Fachgruppe Informatik des Verbandes Schwyzer Gemeinden und Bezirke (VSZGB) entsprechende Massnahmen. Weiter hat das AFI bereits vor dem Cyberangriff auf den Bezirk March mit der Aktualisierung der Netzwerksicherheitsrichtlinie (NSP) begonnen und wird die Anforderungen für die Gemeinden und Bezirke, welche eine Verbindung zum Kantonsnetzwerk haben, verschärfen. Eine weitere Massnahme aus der NSP sieht den Ausbau von Sicherheitskomponenten zu Drittnetzen mittels zusätzlicher Firewall-Technologie vor. Im ersten Quartal 2024 wird das Kantonsnetzwerk zudem durch eine spezialisierte Firma auditiert, anschliessend folgen gezielte Audits bei den Gemeinden und Bezirken.

Es wäre zudem wünschenswert, wenn der Bezirk March nach der Aufarbeitung des Vorfalls seine Erkenntnisse mit den anderen Schwyzer Gemeinden und Bezirken sowie dem AFI teilen würde, damit alle Gemeinwesen ihre Strukturen optimieren können.

2.4 Weshalb wurde nicht reagiert, als das NCSC laut March Anzeiger vom 21. Dezember von einem bevorstehenden Angriff gewarnt hat? Hat der Kanton ebenfalls solche Warnungen bekommen?

Wie bereits einleitend erwähnt, erfolgte die Reaktion des Kantons umgehend nach Erhalt der Meldung des NCSC. Die verantwortlichen Personen beim Bezirk March wurden innert kürzester Zeit über den Vorfall informiert. Auf Empfehlung des AFI hat der Bezirk March noch am gleichen Tag eine spezialisierte Firma für die Vorfallsbewältigung aufgeboden. Das AFI hat seinerseits seinen Vertragspartner im Rahmen eines Incident Response & Forensic Agreement eingesetzt und mit der Analyse des Kantonsnetzwerks beauftragt. Sämtliche involvierten Organisationen standen kontinuierlich im Austausch. Die Zuständigkeit für die Handhabung sowie Bewältigung des Vorfalls lag jedoch zu jedem Zeitpunkt beim Bezirk March.

3. Zustellung

Fragesteller; Kantonsratspräsident; Fraktionspräsidenten; Mitglieder des Regierungsrates; Staatschreiber; Sekretariat des Kantonsrates; Beauftragter für Information und Kommunikation; Finanzdepartement; Amt für Informatik; Medien.

Finanzdepartement des Kantons Schwyz

Der Departementsvorsteher:

Herbert Huwiler, Regierungsrat

Zustellung an die Medien: 18. Januar 2024