Regierungsrat des Kantons Schwyz

Beschluss Nr. 147/2025
Schwyz, 18. Februar 2025 / jh

Security Operations Center (SOC)
Ausgabenbewilligung des Kantonsrates

1. Ausgangslage und Handlungsbedarf

Ein Security Operations Center (SOC) ist eine zentrale Einheit, die für die Überwachung, Erkennung, Analyse und Reaktion auf IT-Sicherheitsvorfälle zuständig ist. In einem SOC arbeiten Experten mit spezialisiertem Fachwissen, um Bedrohungen rund um die Uhr zu identifizieren und abzuwehren. Es dient als operative Schaltzentrale für Cybersicherheit, die dabei hilft, Systeme und Daten gegen Angriffe zu schützen, Schwachstellen zu minimieren und schnell auf Sicherheitsvorfälle zu reagieren. Das Herzstück bildet dabei das Security Incident & Event Management (SIEM), welches Sicherheitsereignisse und Sicherheitsvorfälle aus den verschiedensten Quellen (Server, Firewall etc.) aggregiert, analysiert und Massnahmen daraus ableitet.

Die kantonale Verwaltung bewältigt aktuell ihre IT-Sicherheitsmassnahmen ohne ein dediziertes SOC. Das bedeutet, dass Bedrohungen oft in einem aufwendigen und fehleranfälligen Prozess manuell identifiziert und überprüft werden müssen. Angesichts der zunehmenden Komplexität und Häufigkeit von Cyberangriffen gelangt dieser Ansatz zunehmend und rasch an seine Grenzen. Da keine dezidierten Ressourcen vorhanden sind, um verdächtige Aktivitäten umfassend zu überwachen und schnell darauf zu reagieren, bestehen zunehmend massgebende Risiken. Dies insbesondere, da eine lückenlose Überwachung rund um die Uhr, etwa in der Nacht und am Wochenende, nicht gewährleistet werden kann. Die Einführung eines SOC schafft hier konkret Abhilfe und zusätzliche Sicherheit.

Der Aufbau eines eigenen SOC würde für das Amt für Informatik (AFI) eine erhebliche Herausforderung darstellen. Der Hauptgrund liegt im ausgesprochen hohen Ressourcenbedarf. Ein SOC erfordert hochspezialisierte Sicherheitsexperten, hochmoderne und dezidierte Technologien sowie Infrastruktur und einen 24/7-Betrieb. Wenn das AFI ein eigenes SOC aufbauen und betreiben würde, wären dafür mindestens fünf Vollzeitstellen erforderlich. Dies würde jährliche Personalkosten von mindestens 0.7 Mio. Franken verursachen. Zusätzlich kämen weitere Ausgaben für Hardware, Software und Lizenzen hinzu. Angesichts dieser Faktoren ist die Zusammenarbeit mit ei-

nem Managed Security Service Provider (MSSP) die ideale Lösung, um diese fehlenden, begehrten Ressourcen kurzfristig und nachhaltig zu beschaffen. Aufgrund des Mengeneffekts auf Seiten des MSSP fallen in der Summe erheblich geringere Anschaffungs- und Betriebskosten an. Gleichzeitig folgt der Kanton Schwyz der Vorgehensweise anderer Kantone, die ebenfalls, und aus denselben Gründen, hybride oder externe SOC-Betriebsmodelle umsetzen. Ein weiterer Vorteil eines MSSP im Vergleich zu einem internen Betrieb besteht darin, dass Erkenntnisse aus einer Vielzahl unterschiedlicher IT-Systeme verschiedener Kunden generiert werden können, welche wiederum zur Erhöhung der Sicherheit für die gesamte Kundschaft beitragen.

2. Projektbeschrieb

Ein SOC, das durch einen Managed Security Service Provider (MSSP) bereitgestellt wird, zeichnet sich durch eine zentrale Überwachungsplattform aus. Diese Plattform sammelt und analysiert in Echtzeit Sicherheitsdaten aus verschiedenen Quellen wie Netzwerken, Endgeräten und Cloud-Diensten, um eine umfassende Sicherheitsüberwachung zu gewährleisten. Dabei steht die lückenlose Verfügbarkeit im Mittelpunkt: Der MSSP garantiert eine durchgehende Überwachung und Reaktion, auch nachts, an Wochenenden und Feiertagen. Fortschrittliche Technologien und Automatisierungen ermöglichen es, Bedrohungen frühzeitig zu erkennen und zu priorisieren, wobei ein erfahrenes Analystenteam eingehende Alarme bewertet, Risiken analysiert und schnell auf kritische Sicherheitsvorfälle reagiert. Diese Reaktionsfähigkeit wird durch automatisierte Workflows und vordefinierte Abläufe im Rahmen von Best Practices unterstützt, die eine effiziente und zeitnahe Bearbeitung gewährleisten.

Ein von einem MSSP bereitgestelltes SOC kann auf die individuellen Bedürfnisse der kantonalen Verwaltung zugeschnitten werden. Dabei berücksichtigt es branchenspezifische Anforderungen aus dem Verwaltungsumfeld und entsprechende Compliance-Vorgaben. Ein weiteres wichtiges Merkmal ist die Transparenz: Regelmässige Berichte und Dashboards geben dem AFI einen klaren Überblick über den Sicherheitsstatus, aufgetretene Vorfälle und eingeleitete Massnahmen. Darüber hinaus ist die Architektur des SOC flexibel skalierbar, sodass sie mit den konstant wachsenden Anforderungen Schritt halten kann. Neben der reaktiven Bearbeitung von Sicherheitsvorfällen bietet das SOC auch proaktive Dienstleistungen wie Schwachstellenmanagement, Bedrohungsjagd (Threat Hunting) und strategische Sicherheitsberatung. Dies stellt sicher, dass die kantonale Verwaltung nicht nur auf Vorfälle vorbereitet ist, sondern auch potenziellen Risiken aktiv begegnet. Ein weiterer zentraler Aspekt ist die Unterstützung bei der Einhaltung regulatorischer Vorgaben. Das SOC hilft der kantonalen Verwaltung dabei, Vorschriften und Standards wie ISO 27001 (Informationssicherheits-Managementsystem), das Gesetz über die Öffentlichkeit der Verwaltung und den Datenschutz vom 23. Mai 2007 (ÖDSG, SRSZ 140.410), die Verordnung über die Informationstechnologie vom 1. September 2015 (ITV, SRSZ 143.113), aber auch Vorgaben aus dem Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020 (Informationssicherheitsgesetz, ISG, SR 128) zu erfüllen, indem es sicherstellt, dass die Informationssicherheit für die kantonale Verwaltung gestärkt wird und alle Massnahmen dokumentiert und überwacht werden. Indes sieht das Projekt keine Auslagerung von besonders schützenswerten Daten vor. Die Informationen der Bürger verbleiben weiterhin in den kantonalen Infrastrukturen und dabei besser vor Cyberbedrohungen geschützt.

3. Gemeinsame Beschaffung mit Gemeinden und Bezirken

Vor dem Hintergrund der deutlich überwiegenden Vorteile eines durch einen MSSP bereitgestellten SOC hat das AFI die entsprechenden Leistungen in einem offenen Verfahren ausgeschrieben. Dabei soll nicht nur der Kanton Leistungen beziehen können, sondern auch für andere öffentliche Institutionen im Kanton die entsprechenden Voraussetzungen geschaffen werden, um die Sicherheit im Verbund zu erhöhen. Das Vorhaben zur Beschaffung einer SOC-Lösung wurde im April

2024 an einer Sitzung der Fachgruppe Informatik des Verbands Schwyzer Gemeinden und Bezirke (VSZGB) den zuständigen Vertretern präsentiert. Ein Vertreter des Rechenzentrums Einsiedeln sowie des Bezirks March waren aktiv im erweiterten Projektteam eingebunden und haben massgeblich an der Evaluation des geeignetsten Anbieters mitgewirkt. Die Gemeinden, Bezirke, Schulen und Anstalten im Kanton können, unabhängig von der kantonalen Beschaffung, separat einen Bezugsvertrag abschliessen und von den Vergabekonditionen profitieren. Es besteht für die weiteren Bedarfsstellen indes keine Verpflichtung zum Bezug dieser Leistungen.

4. Finanzielle Auswirkungen

Die nachfolgenden Kosten ergeben sich aus dem verbindlichen Angebot der InfoGuard AG, welche im Wettbewerb das vorteilhafteste Angebot unterbreitete. Die Vergabe ist – auch im Interesse der weiteren potenziellen Bezüger (vgl. Ziffer 3) – bereits im Januar 2025 erfolgt, wobei ein Bezug durch die kantonale Verwaltung dem Vorbehalt der kantonsrätlichen Ausgabebewilligung unterliegt. Die einmaligen Kosten setzen sich aus einer Pauschale von Fr. 38 000.-- für die Inbetriebnahme und einem Stundenpaket von 500 Stunden von Fr. 90 000.-- für die Anbindung der Systeme an das SOC. Für die Anbindung an das IT-Service-Management (ITSM) und das Schwachstellenmanagement werden zusätzlich insgesamt Fr. 43 080.-- veranschlagt. In der Summe ergibt dies einmalige Kosten von Fr. 171 080.-- (exklusive Mehrwertsteuer).

Die jährlich wiederkehrenden Kosten setzen sich einerseits aus einem Pauschalbetrag von Fr. 148 600.-- für den Betrieb des SOC, einem Pauschalbetrag von Fr. 1200.-- für die Anbindung an das ITSM und einem Pauschalbetrag von Fr. 49 000.-- für den Betrieb des Schwachstellenmanagements zusammen. Die jährlichen Kosten belaufen sich in der Summe somit auf rund Fr. 198 800.-- (exklusive Mehrwertsteuer).

Gegenstand der Vergabe war eine Vertragsdauer von vier Jahren mit einer zweimaligen optionalen Verlängerung um ein weiteres Jahr. Während der initialen Phase von vier Jahren werden das SOC sowie die externen Leistungen evaluiert und mit den zugehörigen Bedürfnissen abgeglichen. Sollte sich Anpassungsbedarf ergeben, wird erneut ein offenes Ausschreibungsverfahren durchgeführt. Alternativ werden die Leistungen über sechs Jahre bezogen, weshalb vorliegend eine Ausgabenbewilligung für die einmaligen Aufbaukosten sowie die Betriebskosten für sechs Jahre von insgesamt rund Fr. 1 475 000.-- (inklusive Mehrwertsteuer) beantragt wird.

5. Behandlung im Kantonsrat und Referendum

5.1 Zuständigkeit und Ausgabenbremse

Gemäss § 28 Abs. 1 Bst. a des Gesetzes über den kantonalen Finanzhaushalt vom 20. November 2013 (FHG, SRSZ 144.110) ist der Kantonsrat für die vorliegende Ausgabenbewilligung zuständig. Sie gilt gemäss § 87 Abs. 2 der Geschäftsordnung des Kantonsrates vom 17. April 2019 (GOKR, SRSZ 142.110) als angenommen, wenn mindestens 60 Mitglieder des Kantonsrates zustimmen.

5.2 Referendum

Gemäss §§ 34 Abs. 2 Bst. c und 35 Abs. 1 Bst. b der Kantonsverfassung vom 24. November 2010 (KV, SRSZ 100.100) unterstehen Ausgabenbeschlüsse über neue einmalige Ausgaben von mehr als 5 Mio. Franken und Ausgabenbeschlüsse über neue jährlich wiederkehrende Ausgaben von mehr als Fr. 500 000.-- dem obligatorischen oder fakultativen Referendum. Der vorliegende Beschluss hat einen Ausgabenbeschluss von 1.475 Mio. Franken für sechs Jahre zum Gegenstand und unterliegt somit nicht dem obligatorischen oder fakultativen Referendum.

Beschluss des Regierungsrates

1. Dem Kantonsrat wird beantragt, die beiliegende Ausgabenbewilligung anzunehmen.

2. Zustellung: Mitglieder des Kantonsrates.

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

Im Namen des Regierungsrates:

Regierungsrat Kanton Schwyz

Michael Stähli
Landammann

Dr. Mathias E. Brun
Staatsschreiber