



Kantonsratsbeschluss

betreffend Beitrag des Kantons Zug zur Unterstützung des Aufbaus einer zentralen Informations- und Anlaufstelle für KMU im Kontext der Cybersicherheit (ITSec4KMU)

Bericht und Antrag des Regierungsrats
vom 24. August 2021

Sehr geehrte Frau Präsidentin
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen eine Vorlage zum Kantonsratsbeschluss betreffend Beitrag des Kantons Zug zur Unterstützung des Aufbaus einer zentralen Informations- und Anlaufstelle für KMU im Kontext der Cybersicherheit (ITSec4KMU) und erstatten Ihnen dazu nachstehenden Bericht, den wir wie folgt gliedern:

| | |
|--|-----------|
| 1. In Kürze | 2 |
| 2. Ausgangslage | 2 |
| 3. ITSec4KMU im Überblick | 2 |
| 4. Anfälligkeit gegen Cyberangriffe | 4 |
| 5. Projektumfang und -abgrenzungen | 4 |
| 6. Projektziele | 5 |
| 7. Rollout und zeitliche Umsetzung | 5 |
| 8. Wirtschaftliche Machbarkeit | 6 |
| 9. Rechtliche Machbarkeit | 6 |
| 10. Fazit Machbarkeitsanalyse | 6 |
| 11. Kanton Zug als idealer Standort | 7 |
| 12. Keine Konkurrenzierung der Privatwirtschaft | 8 |
| 13. Breit abgestütztes Projekt | 8 |
| 14. Einbindung ins Projekt Zug+ | 8 |
| 15. Vorfinanzierung über Lotteriefonds | 9 |
| 16. Allgemeinverbindlicher Kantonsratsbeschluss | 9 |
| 17. Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen | 9 |
| 17.1. Finanzielle Auswirkungen auf den Kanton | 9 |
| 17.2. Finanzielle Auswirkungen auf die Gemeinden | 10 |
| 17.3. Anpassungen von Leistungsaufträgen | 10 |
| 18. Zeitplan | 10 |
| 19. Antrag | 11 |

1. In Kürze

Im Rahmen des Programms Zug+ beantragt der Regierungsrat die Beteiligung an den Aufbaukosten einer zentralen Informations- und Anlaufstelle für kleine und mittlere Unternehmen (KMU) im Kontext der Cybersicherheit (ITSec4KMU) in der Höhe von gesamt-haft 1,385 Millionen Franken. Damit wird die Widerstandsfähigkeit der KMU gegenüber Angriffen aus dem Cyberspace gefördert und somit das Rückgrat der Schweizer Wirtschaft gestärkt. Die KMU werden motiviert, sich mit dem Thema Cybersicherheit auseinander zu setzen, minimale Grundschutzmassnahmen umzusetzen oder diese Dienstleistungen von Drittanbietenden in Anspruch zu nehmen. Sie werden damit auf die kommenden Gefahren aus dem Cyberraum bestmöglich vorbereitet.

2. Ausgangslage

Die fortschreitende Digitalisierung bringt nicht nur zahlreiche Annehmlichkeiten mit sich, sondern führt auch zu neuen Risiken, zum Beispiel im Hinblick auf Straftaten im Internet (Cyberkriminalität). Immer häufiger werden kleine und mittlere Unternehmen (KMU) Opfer eines Cyberangriffes, da grössere Unternehmen normalerweise mehr in ihre IT-Sicherheit investieren und entsprechend besser gegen Angriffe geschützt sind. Ein Cyberangriff kann für die Opfer einen finanziellen Verlust bedeuten, rufschädigend sein oder ein Unternehmen im schlimmsten Fall gar zur Geschäftsaufgabe zwingen. Für KMU sind Cyberangriffe noch immer eine abstrakte und wenig fassbare Gefahr und viele sind zu wenig geschützt. KMU-Gelder fliessen aufgrund einer Kosten-Nutzen-Abwägung und aufgrund des unsicheren Eintretens eines Vorfalls hauptsächlich in andere Bereiche. Dabei hilft nur schon die Umsetzung minimaler Cybersecurity-Grundschutzmassnahmen, wie zum Beispiel der richtige Umgang mit Passwörtern oder die regelmässige Sicherung der Daten (Backups), damit sich ein KMU vor Angriffen schützen kann bzw. besser auf diese vorbereitet ist.

Aktuell kann das Informations- und Aufklärungsbedürfnis der KMU bezüglich Cybersicherheit nicht gedeckt werden, wie unter anderem eine repräsentative Umfrage von gfs-Zürich vom 1. Dezember 2020 zeigt (vgl. Beilage 1). Aus diesem Grund ist der Aufbau eines Awareness-Zentrums im Kontext von Cybersicherheit für KMU vorgesehen. ITSec4KMU hat das Ziel, die Widerstandsfähigkeit von KMU gegenüber Angriffen aus dem Cyberspace im Kanton Zug und landesweit zu fördern und somit das Rückgrat der Wirtschaft zu stärken. KMU sollen motiviert werden, sich mit dem Thema Cybersicherheit auseinander zu setzen, minimale Grundschutzmassnahmen umzusetzen oder diese Dienstleistungen von Drittanbietenden in Anspruch zu nehmen. Dank einer dezentralen Organisation, einer Zusammenarbeit mit lokalen Verbänden, Organisationen und Fachhochschulen in der ganzen Schweiz sowie einer überwiegend öffentlichen Trägerschaft erreicht ITSec4KMU eine einzigartige physische Nähe zu KMU, ohne dabei eine Konkurrenz zu privatwirtschaftlichen Dienstleistungen darzustellen.

3. ITSec4KMU im Überblick

Das Angebot von ITSec4KMU setzt sich aus den drei Bereichen «Plattform», «Netzwerk» und «eigene Angebote» zusammen.

Die **Plattform** (Webseite) dient als zentrales Präsentations-, Informations- und Kommunikationsmedium. Darauf werden verschiedene Inhalte präsentiert, die für KMU im Zusammenhang mit Cybersicherheit relevant sind:

- Best-Practice-Leitfäden und Hilfsmittel, die KMU in ihrem Unternehmen einsetzen können, um so einen Grundschutz vor Cyberangriffen zu erreichen,

- Informationen zur KMU-Sicherheitslage und zu den Top-Sicherheitsrisiken, damit sich KMU vor aktuellen Gefahren bestmöglich schützen können, zum Beispiel Warnung vor Phishing-E-Mails von bestimmten Adressen,
- ein Veranstaltungskalender, der KMU Informations- und Schulungsanlässe aufzeigt,
- eine Verlinkung zur Meldestelle des Nationalen Zentrums für Cybersicherheit (NCSC), bei dem KMU Angriffsversuche melden können und eine erste Unterstützung bei nicht zeitkritischen Vorfällen erhalten,
- eine Übersicht von lokalen Sicherheitsdienstleistungsunternehmen, falls ein KMU die Cybersicherheit extern auslagern möchte,
- First-Level Support, falls ein KMU von einem Cyberangriff betroffen ist und unmittelbare Unterstützung benötigt sowie
- ein fachliches Quiz zur spielerischen Auseinandersetzung mit dem Thema.

Das **Netzwerk** setzt sich, neben den KMU selbst, aus verschiedenen Akteuren zusammen, die im Bereich Cybersicherheit für KMU in der Schweiz aktiv sind. Dies umfasst Verbände und Institutionen, den Bund und die Kantone, Fachhochschulen und Universitäten, sowie Unternehmen im Service- und Sicherheitsdienstleistungsbereich. Ziel des Netzwerks ist es, mittels auf Branchen und Gruppen abgestimmten Veranstaltungen der Netzwerkpartnerinnen und -partner, den Austausch und die Transparenz im Themenbereich zu fördern und so möglichst viele KMU zu erreichen und von der Bedeutung des Themas überzeugen zu können. Grundlage für ein funktionierendes Netzwerk stellt der niederschwellige Zugang zu den Informationen dar, wie er von ITSec4KMU sichergestellt wird.

Der letzte Bereich des Leistungsangebotes besteht in **eigenen Angeboten**, welche als gezielte Ergänzungen zu bereits vorhandenen Hilfestellungen erstellt werden. Die eigenen Angebote beinhalten ausgewählte Awareness- und Präventionsveranstaltungen, die gemeinsam mit den Netzwerkpartnerinnen und -partnern umgesetzt werden können, ein Monitoring der Medienlandschaft und ein Awareness-Siegel für KMU als Anreiz für KMU, sich mit dem Thema Cybersicherheit langfristig auseinander zu setzen.

ITSec4KMU wird bezüglich Rechtsform als Verein geführt werden. Die Verfolgung eines ideellen Zwecks, die Verwendung eines Gewinns im Sinne des Vereinszwecks, sowie die flexible Gestaltungsmöglichkeit der Mitgliederbeitragsstruktur vereinfacht die finanzielle Unterstützung durch den Bund und Kantone und erlaubt auch Verbänden und KMU die Aufnahme als Mitglied unter Entrichtung von Mitgliederbeiträgen. Zusätzlich zu den Erträgen durch Mitgliederbeiträge wird ITSec4KMU als Verein auch Einnahmen über eigene Angebote wie z.B. Awareness-Veranstaltungen erzeugen. Es ist geplant, zu Beginn der Projektumsetzung einen neuen Verein mit dem Namen «Cybersicherheit KMU Schweiz» zu gründen. In diesem werden die Aktivitäten (Plattform, Netzwerk, eigene Angebote) von ITSec4KMU umgesetzt und betrieben. Das Präsidium des neu gegründeten Vereins wird durch eine Vertretung der Hochschule Luzern, des Kantons Zug oder der Wirtschaft bekleidet. ITSec4KMU ist auch ein Präventionsprojekt; die Zuger Polizei wird daher in geeigneter Weise in die Vereinsstruktur miteinbezogen werden. Für die Zeit nach der Aufbauphase (inkl. Anschubfinanzierung) ist Vereinsstruktur noch zu klären. Mit § 1 Abs. 2 des Kantonsratsbeschlusses betreffend Beitrag des Kantons Zug zur Unterstützung des Aufbaus einer zentralen Informations- und Anlaufstelle für KMU im Kontext der Cybersicherheit (ITSec4KMU), wonach der Regierungsrat die Einzelheiten der Organisation von ITSec4KMU regelt, wird die hierzu nötige Rechtsgrundlage geschaffen.

Da ITSec4KMU nur erfolgreich sein kann, wenn bestehende Initiativen gebündelt werden und die im Themengebiet aktiven Player mit einer Stimme sprechen, werden frühzeitig mögliche Synergien mit bestehenden Organisationen, Verbänden und Vereinen gesucht. Eine mögliche

Zusammenarbeit könnte sich beispielsweise aus einem Zusammenschluss des neu gegründeten Vereins «Allianz Digitale Sicherheit Schweiz» (ADSS)¹, der unter anderem ein Label für IT-Sicherheitsdienstleister herausgibt, mit dem zu gründenden Verein für die Umsetzung von ITSec4KMU («Cybersicherheit KMU Schweiz») ergeben. Entsprechende Gespräche sind in Gange. Zwingende Voraussetzung für eine Zusammenführung der Aktivitäten in einen neuen oder bestehenden Verein ist der Sitz im Kanton Zug.

Detailinformationen können dem Abschlussbericht Vorarbeiten ITSec4KMU (inkl. Anhänge) vom 18. Dezember 2020 entnommen werden (vgl. Beilage 2). Um den Bericht und Antrag übersichtlich zu halten, wird nachfolgend auch auf die Kapitel dieses Abschlussberichts verwiesen.

4. Anfälligkeit gegen Cyberangriffe

Mit mehr als drei Millionen Beschäftigten bilden KMU das Rückgrat der Schweizer Wirtschaft. Zahlreiche Befunde zeigen, dass KMU in Bezug auf Angriffe aus dem Cyberspace nur ungenügend geschützt sind und bereits ein einzelner Angriff, zum Beispiel mittels Ransomware, ein KMU in seiner Existenz bedrohen kann. Wie eine Studie von Cisco zeigt, sind 43 Prozent aller Cyberangriffe gegen KMU gerichtet (vgl. Beilage 3). In der Schweiz waren im Jahr 2020 ein Viertel aller KMU mit bis zu 49 Mitarbeitenden von einem Cyberangriff betroffen (gfs-Zürich, 2020). Zugleich kann das Informations- und Aufklärungsbedürfnis der KMU aktuell nicht gedeckt werden (vgl. Beilage 1).

Aus diesem Grund hat der Kanton Zug die Erhöhung der Widerstandsfähigkeit gegen Cyberangriffe bei KMU in den Fokus gestellt, sich mit diversen Stakeholdern, unter anderem den Verantwortlichen vom Bund, abgesprochen und entsprechende Arbeiten initiiert. Unter der Leitung von Prof. René Hüsler (Direktor Departement Informatik der Hochschule Luzern) wurde im Zeitraum vom November 2019 bis April 2020 eine erste Skizze eines Businessplans für die Ausgestaltung eines Awareness-Zentrums im Kontext von Cybersicherheit für KMU ausgearbeitet. Am 18. Dezember 2020 wurde der angereicherte Businessplan für das Awareness-Zentrum fertiggestellt. Dieser beschreibt die organisatorische Ausgestaltung, die zu erbringenden Leistungen, die Marktanalyse, Marketing- und Kommunikationsaktivitäten sowie das Finanzierungsmodell des Zentrums (vgl. Beilage 2).

Wie Interviews mit KMU aus verschiedenen Branchen und mit diversen Verbänden sowie Behördenvertreterinnen und -vertretern zeigten, die im Rahmen der Ausarbeitung des Businessplans durchgeführt wurden, besteht ein grosses Bedürfnis für eine zentrale Informationsquelle für Sicherheitsthemen sowie für eine Community mit Möglichkeiten zum Austausch mit anderen KMU sowie Dienstleistungsanbietenden. Diese Bedürfnisse werden von den heutigen Akteurinnen und Akteuren noch nicht gesamtheitlich abgedeckt – umso wichtiger ist die Umsetzung des ITSec4KMU-Projektes. Die nötigen Vorarbeiten und Grundlagen für die Realisierung dieses Leuchtturmprojektes für den Kanton Zug sind somit bereits erbracht (vgl. zum Ganzen Beilage 2, Kapitel 2. Ausgangslage und Zielsetzung; Kapitel 5.1. KMU und Bedürfnisse; Kapitel 5.2. Marktbeurteilung und Alleinstellungsmerkmale des Vereins und Kapitel 5.3. Angestrebte Zusammenarbeiten).

5. Projektumfang und -abgrenzungen

Das Angebot von ITSec4KMU setzt sich, wie in Kapitel 4 «ITSec4KMU im Überblick» (Beilage 2) aufgezeigt, aus den drei Bereichen «Plattform», «Netzwerk» und «eigene

¹ <https://www.digitalsecurityswitzerland.ch/>

Angebote» zusammen. Um die Machbarkeit zu klären und die Bedürfnisse der verschiedenen Akteurinnen und Akteure im Markt abzuholen, wurden diverse Gespräche mit Verbänden und Behörden geführt. Neben dem NCSC und sowie im Speziellen MELANI (Melde- und Analysestelle Informationssicherung Bund) beurteilen digitalswitzerland, die Zuger Wirtschaftskammer, der Gewerbeverband des Kantons Zug, economiesuisse, asut, der Innovationspark Zentralschweiz, Swico und die Information Security Society Switzerland (ISSS), Mount10 (Swiss Cyber Defence DNA) sowie die Fachkonferenz Architektur und Life Science (FTAL) das Projekt als positiv und haben ihre Unterstützung in der weiteren Projektarbeit zugesichert.

Hervorzuheben ist, dass ITSec4KMU keine eigenen Dienstleistungen anbietet, welche in Konkurrenz zur Privatwirtschaft stehen. ITSec4KMU fördert die Privatwirtschaft und erschliesst neue Absatzmärkte für Unternehmen.

Wie in Kapitel 3 bereits erwähnt, wird im Moment eine mögliche Zusammenarbeit mit dem neu gegründeten Verein ADSS, die unter anderem ein CyberSeal für IT-Dienstleistende initiiert, geprüft, da diese Aktivität einen Teilbereich von ITSec4KMU darstellt (vgl. detaillierte Beschreibung des Projektumfangs und des Leistungsangebots in Beilage 2, Kapitel 4. Leistungsangebot).

6. Projektziele

ITSec4KMU fördert die Widerstandsfähigkeit von Schweizer KMU gegenüber Angriffen aus dem Cyberspace landesweit und stärkt somit das Rückgrat der Schweizer Wirtschaft. KMU werden motiviert, sich mit dem Thema Cybersicherheit auseinander zu setzen, minimale Grundschutzmassnahmen umzusetzen oder diese Dienstleistungen von Drittanbietenden in Anspruch zu nehmen. Die KMU in der Schweiz wissen, was bei einem erfolgreichen Angriff zu tun ist und an wen sie sich im Notfall wenden können. Durch das zentrale Awareness-Zentrum wird der Wirtschaftsstandort Schweiz als Ganzes gefördert und ist auf die kommenden Gefahren aus dem Cyberraum bestmöglich vorbereitet.

7. Rollout und zeitliche Umsetzung

ITSec4KMU soll phasenweise auf die ganze Schweiz ausgerollt werden, wobei folgende drei Teilphasen vorgesehen sind (Projektstart Mitte 2022):

- In der ersten Phase wird die Plattform aufgebaut und die Netzwerkpartnerinnen und -partner aus der deutschsprachigen Schweiz werden angesprochen. Ziel ist, die Plattform bis Ende 2022 live zu stellen. Dies stellt denn auch den eigentlichen Startschuss für den Betrieb des Vereins dar.
- In der zweiten Teilphase wird die französischsprachige Schweiz angesprochen. Dazu gehört auch der Ausbau der Plattform betreffend sprachliche Anpassungen. Diese Teilphase soll Mitte 2023 abgeschlossen sein.
- In der letzten Teilphase wird die Plattform weiter ausgebaut und das Netzwerk auf die italienische Schweiz ausgeweitet. Nach Beendigung dieser Phase ist die gesamte Schweiz abgedeckt, so dass ITSec4KMU Ende 2023 in den Vollbetrieb übergehen kann.

(Vgl. zum Ganzen Beilage 2, Kapitel 8. Planung Startphase sowie Anhang E; die Termine in dieser Beilage basieren auf einem Projektstart Anfang 2021 und wurden nicht auf den heutigen Stand aktualisiert)

8. Wirtschaftliche Machbarkeit

Eine detaillierte Planung der Kosten wurde aufgrund des Projektauftrags für die Startphase erarbeitet. Die Kosten ab Ende 2023 stellen eine Schätzung dar. Die Zielgenauigkeit der dafür vorgenommenen Annahmen hängt stark davon ab, wie viele Mitglieder aus der öffentlichen Hand und der Institutionen sich am Projekt beteiligen werden. Ziel ist, dass ab 2027 die laufenden Kosten von ITSec4KMU primär durch Einnahmen aus den eigenen Angeboten (Veranstaltungen, Workshops, Schulungen, etc.) sowie über Beteiligungen / Unterstützungen von Verbänden und Institutionen zu decken und (erst) sekundär durch Beiträge der öffentlichen Hand (Bund und Kantone).

Die tabellarische Übersicht der Kosten für den Kanton Zug stellt sich wie folgt dar:
Kantonsbeiträge an einmalige Projektkosten (in Franken):

| | 2022 | 2023 |
|---------|---------|---------|
| Aufwand | 800 000 | 325 000 |

Die einmaligen Projektkosten (Startphase) setzen sich wie folgt zusammen (Annahmen):

| | |
|-------------------|--|
| Personalkosten | 205 000 Franken (inkl. Sicherstellung Ressourcen 2021) |
| Plattform | 305 000 Franken |
| Netzwerk | 350 000 Franken |
| Eigene Angebote | 125 000 Franken |
| Vorprojektkosten | 65 000 Franken |
| Marketing | 45 000 Franken |
| Sonstiger Aufwand | 30 000 Franken |
| Total | 1 125 000 Franken |

Kantonsbeiträge in Vollbetriebsphase (in Franken):

| | 2024 | 2025 | 2026 |
|---------|--------|--------|--------|
| Aufwand | 50 000 | 50 000 | 50 000 |

Vgl. zum Ganzen auch Beilage 2, Kapitel 7 (Kosten und Finanzierung inkl. Anhänge A–D), wobei die Termine in dieser Beilage auf der Basis eines Starts des Projektes Anfang 2021 festgelegt und nicht auf den heutigen Stand aktualisiert wurden. Die obenstehenden tabellarischen Zusammenstellungen sowie die standardisierte Finanztabelle in Kapitel 16.1 berücksichtigen hingegen die aktuellen Daten.

9. Rechtliche Machbarkeit

Die Vorlage ist verfassungskonform und vereinbar mit internationalen Verpflichtungen der Schweiz. Die rechtliche Machbarkeit ist weder auf Kantons- noch auf Bundesebene eingeschränkt, was durch laufenden Austausch mit den entsprechenden Behörden sichergestellt wurde.

10. Fazit Machbarkeitsanalyse

Die wirtschaftliche Bedeutung der Resilienz von KMU gegenüber Angriffen aus dem Cyberspace ist unbestritten. Dies wurde von öffentlichen Institutionen (zum Beispiel NCSC) und diversen Verbänden und Vereinen (z. B. digitalswitzerland) und privaten Sicherheitsdienstleistenden (z. B. secnovum, SMESEC) erkannt. Das Resultat daraus ist, dass

heute eine Vielzahl an Initiativen existiert, welche die Cybersicherheit von KMU in der Schweiz erhöhen möchten.

Keine der betrachteten Initiativen von Seiten der Verbände und Vereine sowie von privaten Sicherheitsdienstleistenden erreicht jedoch die physische Reichweite oder den hohen Vernetzungsgrad zwischen den relevanten Akteurinnen und Akteuren, wie dies ITSec4KMU mit seinem dezentralen Netzwerk anstrebt. Auf Seite der Institutionen hat das NCSC nach eigenen Angaben nicht die Kapazität, sich in gleichem Ausmass der Cybersicherheit von KMU anzunehmen, wie dies ITSec4KMU beziehungsweise dem zu gründenden Verein «Cybersicherheit KMU Schweiz» mit seinem spezialisierten Leistungsangebot möglich ist. Das dezentrale Netzwerk, die Koordination und Führung durch Fachhochschulen und weiteren Institutionen, sowie eine überwiegend öffentliche Trägerschaft verschaffen dem Verein «Cybersicherheit KMU Schweiz» eine einmalige Marktstellung: Mit dem Netzwerk erreicht der Verein «Cybersicherheit KMU Schweiz» physische Nähe zu KMU im ganzen Land, dank der Koordination und Führung durch Fachhochschulen und weiteren Institutionen verfügt der Verein über eine grösstmögliche fachliche Kompetenz, und die überwiegend öffentliche Trägerschaft ermöglicht Transparenz bezüglich wirtschaftlicher Interessen.

11. Kanton Zug als idealer Standort

Gemäss den Legislaturzielen 2019–2022 des Kantons Zug soll die Sicherheit im virtuellen Raum gestärkt werden. Der Aufbau einer Plattform für Cybersicherheit für KMU ermöglicht der Zuger Wirtschaft einerseits direkten Zugang zu aktuellen Sicherheitslösungen. Die Unternehmen können sich so präventiv mit den Gefahren und Risiken der Digitalisierung auseinandersetzen und beispielsweise Ausfälle in den Betrieben mit geeigneten Massnahmen verhindern, wodurch die Sicherheit des Wirtschaftsstandorts Zug gestärkt wird. Es handelt sich somit um eine aktive Unterstützung der Unternehmen im Kanton, ohne dabei direkt in die Wirtschaft einzugreifen oder gar mit ihr in eine Konkurrenzsituation zu treten. Andererseits kann sich der Kanton Zug dank der Zusammenarbeit mit den wichtigsten Akteurinnen und Akteuren aus Wissenschaft und Wirtschaft sowie der Unterstützung des NCSC national im Themengebiet positionieren und von den Partnerschaften profitieren.

In Übereinstimmung mit der Digitalstrategie treibt der Kanton Zug die Digitalisierung der Verwaltung voran und will für die Wirtschaft ein vertrauenswürdiger Partner sein, der den digitalen Raum aktiv mitgestaltet. Das Projekt ITSec4KMU trägt zur Umsetzung dieses Ziels bei: Es erlaubt dem Kanton Zug eine Vorreiterrolle im Cybersecurity-Bereich wahrzunehmen, eine der Hauptvoraussetzungen für Vertrauen in digitale Leistungen und neue Technologien.

Als Kanton mit einer hohen IT-Affinität und einem fast doppelt so hohen Anteil an IT-relevanten Arbeitsplätzen im Vergleich zum Schweizer Durchschnitt, ist der Kanton Zug als Standort für ein Zentrum zur Verbesserung der IT-Sicherheit von KMU prädestiniert. Zudem ist Zug mit seinem Potenzial an Fintech, Blockchain/DLT-Kompetenzen und bestehenden Cybersecurity-Unternehmen ein idealer Ort für die Koordination eines solchen Zentrums. Mit dem Tech-Cluster Zug besteht ein attraktives Gefäss für die physische Infrastruktur von ITSec4KMU. ITSec4KMU ermöglicht es dem Kanton Zug, das Dienstleistungsangebot der bereits heute im Kanton Zug ansässigen Hochschule Luzern mit dem renommierten Departement Informatik auszubauen (Medienmonitoring, Ausbildungsangebote, z. B. «eBanking – aber sicher!»).

Dank des Zentrums entstehen im Kanton Zug zusätzliche Arbeitsplätze. Einerseits aufgrund des Zentrums (Verein «Cybersicherheit KMU Schweiz») selbst, andererseits aufgrund neuer Absatzkanäle für die IT-Provider im Kanton, die KMU unterstützen, die sich nicht selbst mit dem Thema Cybersicherheit auseinandersetzen (können) und auf externe Spezialistinnen und

Spezialisten zurückgreifen. Auch im Bereich der Sensibilisierung für das Thema sowie bei der Durchführung von Schulungen ergeben sich Aufträge für Unternehmen im Kanton Zug, indem zum Beispiel die Dienstleistungen der bereits heute im Kanton ansässigen Hochschule Luzern mit dem renommierten Departement Informatik ausgebaut werden können. So kann die Weiterentwicklung von ITSec4KMU vorangebracht werden und die Bedeutung des Standorts Zug als Sitz des Vereins «Cybersicherheit KMU Schweiz» wird gefestigt. Dieses innovative Projekt wird für den Kanton Zug Signalwirkung haben. Es weist starke Synergien für die lokale Wirtschaft auf und stellt für die KMU auch ein Präventionsprojekt dar.

12. Keine Konkurrenzierung der Privatwirtschaft

ITSec4KMU ist eine unabhängige Plattform zur Förderung der Schweizer Cybersicherheit. Zu keinem Zeitpunkt stellen die Dienstleistungen von ITSec4KMU eine Konkurrenz zur Privatwirtschaft dar. ITSec4KMU soll die KMU im Kanton Zug stärken und den IT-Providern des Kantons neue Absatzkanäle ermöglichen, indem die Plattform bei der Vermittlung von Dienstleistungen zwischen den KMU und den IT-Providern des Kantons unterstützt. Ziel ist einerseits, dass lokale Unternehmen lokale Dienstleistungen bei den IT-Provider im Kanton Zug beziehen und dass andererseits IT-Provider mit spezifischen Fähigkeiten und Dienstleistungen über die Kantonsgrenzen hinweg Kundinnen und Kunden gewinnen und ihre Dienstleistungen vertreiben können.

13. Breit abgestütztes Projekt

Das Projekt ITSec4KMU wurde in der Konzeptions- und Entstehungsphase von der Departementsleitung des eidgenössischen Finanzdepartements sowie vom Delegierten des Bundes für Cybersicherheit als wertvoll beurteilt. Es ist ein Vorhaben, das der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken dient und einen Bereich abdeckt, den der Bund mit dem NCSC selbst nicht umsetzen kann. Dem Kanton Zug ermöglicht das Vorhaben somit eine grosse Wirkung in einem für den Kanton zentralen Themengebiet. Zudem hat ITSec4KMU die Möglichkeit, niederschwellig mit weiteren Bundes- und Kantonsbehörden zusammenzuarbeiten, was für ein Unternehmen aus der Privatwirtschaft aufgrund von Interessenkonflikten schwierig ist.

14. Einbindung ins Projekt Zug+

Mit dem Projekt Zug+ soll der Kanton Zug unter anderem so positioniert werden, dass er auch in Zukunft erfolgreich bleibt. In diesem Zusammenhang erarbeitete der Regierungsrat Projekte, für welche Machbarkeitsanalysen erstellt wurden. Für ITSec4KMU wurde auf fundierter Basis ein Businessplan erarbeitet, welcher zeigt, dass das Bedürfnis der KMU für eine zentrale Anlaufstelle rund um Informationssicherheit und Awareness vorhanden ist.

Der Kantonsrat hat am 6. Mai 2021 vom Zwischenbericht des Regierungsrats vom 26. Januar 2021 zum Programm Zug+ Kenntnis genommen (Vorlage Nr. 3195.1 - 16510²). In diesem Bericht wurde unter anderem über den Umfang und den Zwischenstand des Projekts ITSec4KMU informiert.

² https://kr-geschaefte.zug.ch/dokumente/9368/3195-1-16510_Nachtragskredit_2_Budget-2021.pdf

15. Vorfinanzierung über Lotteriefonds

Die Vorarbeiten sowie die Erstellung des Businessplans wurden vom Regierungsrat mit Mitteln aus dem Lotteriefonds vorfinanziert. Diese Anschubfinanzierung belief sich auf total 110 000 Franken. Die Staatswirtschaftskommission hat dieses Vorgehen ablehnend zur Kenntnis genommen, da es sich gemäss ihrer Einschätzung um eine Zweckentfremdung des Lotteriefonds handelt (Vorlage Nr. 3163.3 - 16457³). Der Regierungsrat wird diesen Betrag dem Lotteriefonds wieder gutschreiben.

16. Allgemeinverbindlicher Kantonsratsbeschluss

Zur finanziellen Unterstützung des Kantons am Aufbau einer zentralen Informations- und Anlaufstelle für KMU im Kontext der Cybersicherheit (ITSec4KMU) im Sinne einer Anschubfinanzierung besteht heute keine genügende Rechtsgrundlage. Nicht einschlägig ist insbesondere § 4 Abs. 1 des Gesetzes über die Wirtschaftspflege im Kanton Zug (Wirtschaftspflegegesetz) vom 4. Juli 2013 (BGS 915.1), wonach der Kantonsrat mit einfachem Beschluss über den Beitritt von regionalen, nationalen und internationalen Trägerschaften, Plattformen und Institutionen im Wirtschaftsbereich entscheidet, der jährliche Kosten von mehr als 100 000 Franken zur Folge hat. Vorliegend handelt es sich nicht um ein Engagement, welches der Vernetzung dient. Es steht vielmehr die Unterstützung des Aufbaus einer neuen Informations- und Anlaufstelle für KMU im Zusammenhang mit Cybersicherheit Raum. Die Beteiligung am Aufbau dieser Stelle fällt damit nicht in den Anwendungsbereich von § 4 Abs. 1 Wirtschaftspflegegesetz. Bei dieser Ausgangslage ist eine genügende Rechtsgrundlage in Form eines allgemeinverbindlichen Kantonsratsbeschlusses nach Art. 34 Abs. 1 der Kantonsverfassung (BGS 111.1) zu schaffen.

17. Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen

17.1. Finanzielle Auswirkungen auf den Kanton

Die Beiträge des Kantons Zug belaufen sich bis ins Jahr 2026 auf gesamthaft 1,385 Millionen Franken. Davon betreffen 1,125 Millionen Franken Beiträge an die einmaligen Projektkosten in den Jahren 2022 und 2023 sowie im Jahr 2022 die in Kapitel 15 erwähnte Gutschrift an den Lotteriefonds von 110 000 Franken (Vorfinanzierung). Die Kantonsbeträge in der Vollbetriebsphase belaufen sich in den Jahren 2024–2026 auf jeweils 50 000 Franken.

Die erste Projektphase wird in der Verantwortung und unter der Leitung des Departements Informatik, Prof. Dr. René Hüsler, durchgeführt und somit agiert das Departement Informatik als Destinatär für die Summe von 1,235 Millionen Franken. Der Kanton Zug wird mit dem Departement Informatik der Hochschule Luzern eine entsprechende vertragliche Vereinbarung zu den Meilensteinen abschliessen. Die Beträge von jeweils 50 000 Franken im Vollbetrieb ab 2024 werden dem spätestens im Jahr 2023 gegründeten Verein «Cybersicherheit KMU Schweiz» überwiesen werden.

³ https://kr-geschaefte.zug.ch/dokumente/9204/3136-3-16457_Budget-2021_Zusatzbericht.pdf

| A | Investitionsrechnung | 2022 | 2023 | 2024 | 2025 |
|----------|---|-------------|-------------|-------------|-------------|
| 1. | Gemäss Budget oder Finanzplan: bereits geplante Ausgaben | | | | |
| | bereits geplante Einnahmen | | | | |
| 2. | Gemäss vorliegendem Antrag: effektive Ausgaben | | | | |
| | effektive Einnahmen | | | | |
| B | Erfolgsrechnung (nur Abschreibungen auf Investitionen) | | | | |
| 3. | Gemäss Budget oder Finanzplan: bereits geplante Abschreibungen | | | | |
| 4. | Gemäss vorliegendem Antrag: effektive Abschreibungen | | | | |
| C | Erfolgsrechnung (ohne Abschreibungen auf Investitionen) | | | | |
| 5. | Gemäss Budget oder Finanzplan: bereits geplanter Aufwand | 350 000 | 50 000 | 50 000 | 50 000 |
| | bereits geplanter Ertrag | | | | |
| 6. | Gemäss vorliegendem Antrag: effektiver Aufwand | 910 000 | 325 000 | 50 000 | 50 000 |
| | effektiver Ertrag | | | | |

17.2. Finanzielle Auswirkungen auf die Gemeinden

Diese Vorlage hat keine finanziellen Auswirkungen auf die Gemeinden.

17.3. Anpassungen von Leistungsaufträgen

Diese Vorlage hat keine Anpassungen von Leistungsaufträgen zur Folge.

18. Zeitplan

| | |
|--------------------|--|
| 30. September 2021 | Kantonsrat, Kommissionsbestellung |
| Okt./Nov.2021 | Vorberatende Kommission |
| Dezember 2021 | Kommissionsbericht vorberatende Kommission |
| Januar 2022 | Beratung Staatswirtschaftskommission |
| Januar 2022 | Bericht Staatswirtschaftskommission |
| 3. März 2022 | Kantonsrat, 1. Lesung |
| 31. März 2022 | Kantonsrat, 2. Lesung |
| 8. April 2022 | Publikation Amtsblatt |
| 7. Juni 2022 | Ablauf Referendumsfrist |
| 8. Juni 2022 | Inkrafttreten (ohne Volksabstimmung) |
| 27. November 2022 | Allfällige Volksabstimmung |
| 28. November 2022 | Inkrafttreten (bei Volksabstimmung) |

Aufgrund der bereits vorgenommenen Abklärungen betreffend Machbarkeit sowie wegen der Dringlichkeit wird auf eine externe Vernehmlassung verzichtet.

19. Antrag

Gestützt auf die vorstehenden Ausführungen beantragen wir Ihnen, auf die Vorlage Nr. 3285.2 – 16690 einzutreten und ihr zuzustimmen.

Zug, 24. August 2021

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Martin Pfister

Der Landschreiber: Tobias Moser

Beilagen nur elektronisch verfügbar:

- Beilage 1: Schlussbericht «Digitalisierung und Cyber-Sicherheit in kleinen Unternehmen» vom 1. Dezember 2020
- Beilage 2: Abschlussbericht Vorarbeiten ITSec4KMU vom 18. Dezember 2020
- Beilage 3: Cisco-Bericht «Sicherheitsgrundlagen für KMU»