



Kantonsratsbeschluss

betreffend Finanzierung der Konzeption, der Umsetzung und des Betriebs eines kantonalen Kompetenzzentrums für Cybersicherheit (KKC) sowie einer strategischen Partnerschaft mit der Eidgenössischen Technischen Hochschule Zürich (ETH) und der Hochschule Luzern (HSLU) im Bereich Cybersicherheit

Bericht und Antrag des Regierungsrats
vom 8. Juli 2025

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen eine Vorlage zum Kantonsratsbeschluss betreffend Finanzierung der Konzeption, des Aufbaus und des Betriebs des Kompetenzzentrums für Cybersicherheit sowie einer strategischen Partnerschaft mit der ETH und der HSLU im Bereich der Cybersicherheit. Den dazugehörigen Bericht legen wir Ihnen wie folgt vor.

Inhalt

1. In Kürze	3
2. Ausgangslage	3
2.1. Cyberbedrohungen im digitalen Zeitalter	3
2.2. Legislaturziel «Stärkung der Sicherheit im virtuellen Raum»	4
3. Ziel und Auftrag des Kantonalen Kompetenzzentrums Cybersicherheit (Säule 1)	6
3.1. Ziel und Leistungsauftrag	6
3.2. Strategische Grundsätze mit ihren Wirkungsfeldern und Messung des Erfolges	9
4. Leistungsspektrum und Betriebsmodell des KKC (Säule 1)	13
4.1. Organisation	13
4.2. Einbindung in den politischen Willensbildungs- und Entscheidungsprozess	14
4.3. Lagebild Cybersicherheit und strategische Handlungsfelder	14
4.4. Leistungsspektrum zur Stärkung der Cybersicherheit	14
5. Partnerschaften mit Hochschulen (Säule 2a)	16
5.1. Partnerschaft mit der ETH Zürich	16
5.1.1. Partnerschaft mit dem Zurich Information Security and Privacy Center (ZISC)	16
5.1.1.1. Nutzen für den Kanton Zug	16
5.1.1.2. Themenfelder der Zusammenarbeit	17
5.1.2. Partnerschaft mit der SCION-Association	17
5.1.2.1. Nutzen für den Kanton Zug	18
5.1.2.2. Themenfelder der Zusammenarbeit	18
5.2. Partnerschaft mit der Hochschule Luzern (HSLU)	19
5.2.1. Nutzen für den Kanton Zug	19
5.2.2. Themenfelder der Zusammenarbeit	20

6. Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen	21
6.1. Umsetzungskonzept	21
6.2. Finanzielle Auswirkungen auf den Kanton	22
6.2.1. Aufbau- und Betriebskosten Kantonales Kompetenzzentrum Cybersicherheit (Säule 1)	22
6.2.2. Projektförderung (Säule 1)	23
6.2.3. Partnerschaften (Säule 2a)	23
6.2.4. Gesamtkosten (Säule 1 und 2a)	24
6.3. Finanzierung aus Mehrerträgen der OECD-Mindeststeuer	24
6.4. Finanzielle Auswirkungen auf die Gemeinden	25
6.5. Anpassungen von Leistungsaufträgen	25
6.6. Mehrwert für den Kanton Zug	25
7. Zeitplan	25
8. Antrag	26

1. In Kürze

Die fortschreitende Digitalisierung führt zu wachsenden Cyberbedrohungen, die nicht nur Unternehmen und staatliche Institutionen, sondern auch zunehmend die Bevölkerung betreffen. Der Kanton Zug ist davon stark betroffen: Mit 815 gemeldeten Fällen im Jahr 2024 erreichte die Cyber-Wirtschaftskriminalität einen neuen Höchststand. Angriffe wie Phishing, Schadsoftware oder Identitätsdiebstahl zeigen, dass digitale Sicherheit ein zentrales gesellschaftliches Anliegen geworden ist.

Als Antwort darauf hat der Kanton Zug die Cybersicherheitsinitiative Zug (CSI) ins Leben gerufen, ein schweizweit einzigartiges Vorhaben, das dem Kanton die Positionierung als Leuchtturmstandort für digitale Sicherheit ermöglicht. Herzstück davon bildet das Kantonale Kompetenzzentrum für Cybersicherheit (KKC). Dieses verfolgt vier Hauptaufträge:

1. Das KKC hilft gezielt besonders **vulnerablen Anspruchsgruppen innerhalb der Bevölkerung**.
2. **Kleine und mittlere Unternehmen** werden vom KKC unterstützt, ihre **Cyberresilienz zu erhöhen**.
3. Das KKC fördert die **Vernetzung und Koordination** von privaten und öffentlichen Partnern.
4. Die Potentiale der Cybersicherheit für die Erhöhung der **Attraktivität des Wirtschafts- und Forschungsplatzes Zug** werden vom KKC gezielt genutzt.

Die Initiative folgt einem mehrsäuligen Modell, in dem Forschung, Anwendung und Wirtschaft eng zusammenarbeiten. Partner wie die Eidgenössische Technische Hochschule Zürich (ETH), die Hochschule Luzern (HSLU), das Nationale Testzentrum für Cybersicherheit (NTC) sowie Unternehmen und Organisationen aus der Privatwirtschaft bilden gemeinsam eine starke Brücke zwischen Wissenstransfer und praktischer Umsetzung. Durch diese gezielte Zusammenarbeit und strategische Steuerung entsteht eine nachhaltige Cybersicherheitsstrategie für den Kanton.

Ein zentraler Umsetzungspartner ist dabei die Zuger Polizei, die bereits im Rahmen ihres Leistungsauftrags Präventionsarbeit leistet. Diese wird im Sinne einer «bürgernahen Polizei» weiter ausgebaut und spielt eine wichtige Rolle in der Sensibilisierung der Bevölkerung im Bereich der digitalen Sicherheit.

Der Kanton Zug nutzt diese Initiative nicht nur zur Gefahrenabwehr, sondern auch zur Stärkung seiner wirtschaftlichen Wettbewerbsfähigkeit sowie zur Förderung digitaler Resilienz und positioniert sich als führender Standort für digitale Sicherheit und setzt schweizweit neue Standards.

2. Ausgangslage

2.1. Cyberbedrohungen im digitalen Zeitalter

Die fortschreitende Digitalisierung durchdringt zunehmend alle Lebens- und Arbeitsbereiche und bringt neben erheblichen Chancen auch wachsende Risiken mit sich. Die Schweiz, und mit ihr der Kanton Zug, sieht sich einer zunehmend komplexen und dynamischen Bedrohungslage im Cyberraum ausgesetzt. Jüngste Vorfälle gravierender Datendiebstähle sowie Betriebsunterbrüche bei Behörden, öffentlichen Institutionen und bundesnahen Unternehmen machen in aller Deutlichkeit sichtbar: Cyberangriffe stellen eine reale, ernstzunehmende und akute Gefährdung der öffentlichen Sicherheit und der Funktionsfähigkeit zentraler Infrastrukturen dar und können nicht nur Schäden im virtuellen Raum verursachen, sondern auch durch die Abhängigkeit von Versorgungs-, Verkehrs- und Produktionsinfrastrukturen von vernetzten Informatikmitteln zu erheblichen, gegebenenfalls nicht umkehrbaren Schäden in der physischen Welt führen. Die

zunehmende Bedeutung von Robotik und KI-gestützten autonomen Systemen in Verkehr, Fertigung oder Logistik verschärfen diese Bedrohung zusätzlich.

Während sich bewährte Schutzkonzepte im analogen Raum bislang als verlässlich erwiesen haben, zeigt die sich zuspitzende Bedrohungslage im virtuellen Raum, verursacht durch kriminelle, ideologisch motivierte oder staatlich gelenkte Akteure, dass auch im digitalen Umfeld robuste, wirkungsvolle und nachhaltig finanzierbare Schutzmechanismen etabliert werden müssen. Die rasante technologische Entwicklung und die zunehmende Abhängigkeit von digitalen Prozessen machen den Handlungsbedarf zusätzlich dringlich.

Das Ausmass dieser Herausforderung lässt sich eindrücklich anhand der aktuellen Kriminalitätsstatistik belegen: Im Jahr 2024 registrierte die Zuger Polizei im Bereich der Cyber-Wirtschaftskriminalität 815 Delikte. Der höchste je verzeichnete Wert. Bereits im Vorjahr wurde ein markanter Anstieg um 90 Prozent auf 730 Fälle festgestellt. Diese Entwicklungen zeigen nur die bekannten Fälle ohne Dunkelziffer und verdeutlichen den Handlungsdruck auf kantonaler Ebene, sowohl hinsichtlich Prävention als auch hinsichtlich der Reaktionsfähigkeit staatlicher Stellen.

Cyberbedrohungen betreffen dabei längst nicht mehr ausschliesslich Unternehmen oder staatliche Institutionen. Auch die Bevölkerung ist zunehmend den Gefahren digitaler Angriffe ausgesetzt, sei es durch Phishing, Schadsoftware, Identitätsdiebstahl, sogenannte «Enkeltricks» oder Betrugsversuche über soziale Netzwerke. Dies sind nur einige Beispiele für die vielfältigen Gefahren. Die Anforderungen an digitale Resilienz, Datenschutz und Aufklärung steigen entsprechend. Es braucht deshalb eine breit abgestützte Strategie zur Stärkung der Cybersicherheit, in die auch Präventionsmassnahmen, Informationskampagnen und die Förderung digitaler Kompetenzen einfließen.

Sicherheit ist ein fundamentales Gut und Bedürfnis der Gesellschaft und bildet eine unverzichtbare Grundlage aller privaten, geschäftlichen und staatlichen Interaktionen. Der Kanton will die Sensibilisierung und Eigenverantwortung seiner Bürgerinnen und Bürger fördern und damit für angemessene Sicherheit sorgen. Angesichts der Komplexität moderner Gesellschafts-, Wirtschafts- und Politikformen kann hierbei nur ein methodisch ausgereifter, integraler Ansatz einen ausreichenden Nutzen bei vertretbaren Kosten schaffen.

2.2. Legislaturziel «Stärkung der Sicherheit im virtuellen Raum»

Im Rahmen des Legislaturziels zur «**Stärkung der Sicherheit im virtuellen Raum**» will der Kanton Zug seine Fürsorgeverantwortung im Bereich der digitalen Kriminalität wirksam wahrnehmen. Die Sicherheitsdirektion hat deshalb gemeinsam mit der Finanzdirektion ein abgestimmtes Modell zur nachhaltigen Stärkung der digitalen Sicherheit im Kanton Zug erarbeitet: Die Cybersicherheitsinitiative Zug (CSI) umfasst wichtige Grundpfeiler zur Sensibilisierung und Abwehr der Gefahren aus dem Cyberspace. Ein zentrales Element der Umsetzung des Legislaturziels 132 «Stärkung der Sicherheit im virtuellen Raum» ist der Aufbau und Betrieb eines **Kantonales Kompetenzzentrums Cybersicherheit (KKC)**. Dieses wirkt mit einem vierfachen Leistungsauftrag, welcher die besonders vulnerablen Anspruchsgruppen «Bevölkerung» und «kleine/mittelständische Unternehmen» (KMUs) abdeckt, für eine geeignete Vernetzung und Koordination mit Partnern in einem «Hub für Cyber- und Informationssicherheit» sorgt und die Chancen der Cybersicherheit für den Wirtschafts- und Forschungsplatz Zug in enger Abstimmung mit übergeordneten Strukturen und Abläufen auf Bundesebene berücksichtigt. Zudem werden die Projektarbeiten, welche die Zuger Polizei im Rahmen des Legislaturziels bereits vorgenommen hat, in die Cybersicherheitsinitiative überführt und angepasst.

Das nachfolgend abgebildete Säulenmodell stellt sicher, dass alle relevanten Stakeholder ihre spezifischen Stärken in einem koordinierten Rahmen einbringen. Das Kantonale Kompetenzzentrum Cybersicherheit ist der Säule 1 zugeordnet, während die Partnerschaft KKC/Hochschulen unter Säule 2a angegliedert ist (grün markiert). Dazu stellt der Regierungsrat diesen Antrag für einen Kantonsratsbeschluss. Die Partnerschaft zwischen dem NTC und der ETH

wird unter 2b angegliedert. Dazu wird ein separater Antrag für einen Kantonsratsbeschluss gestellt.

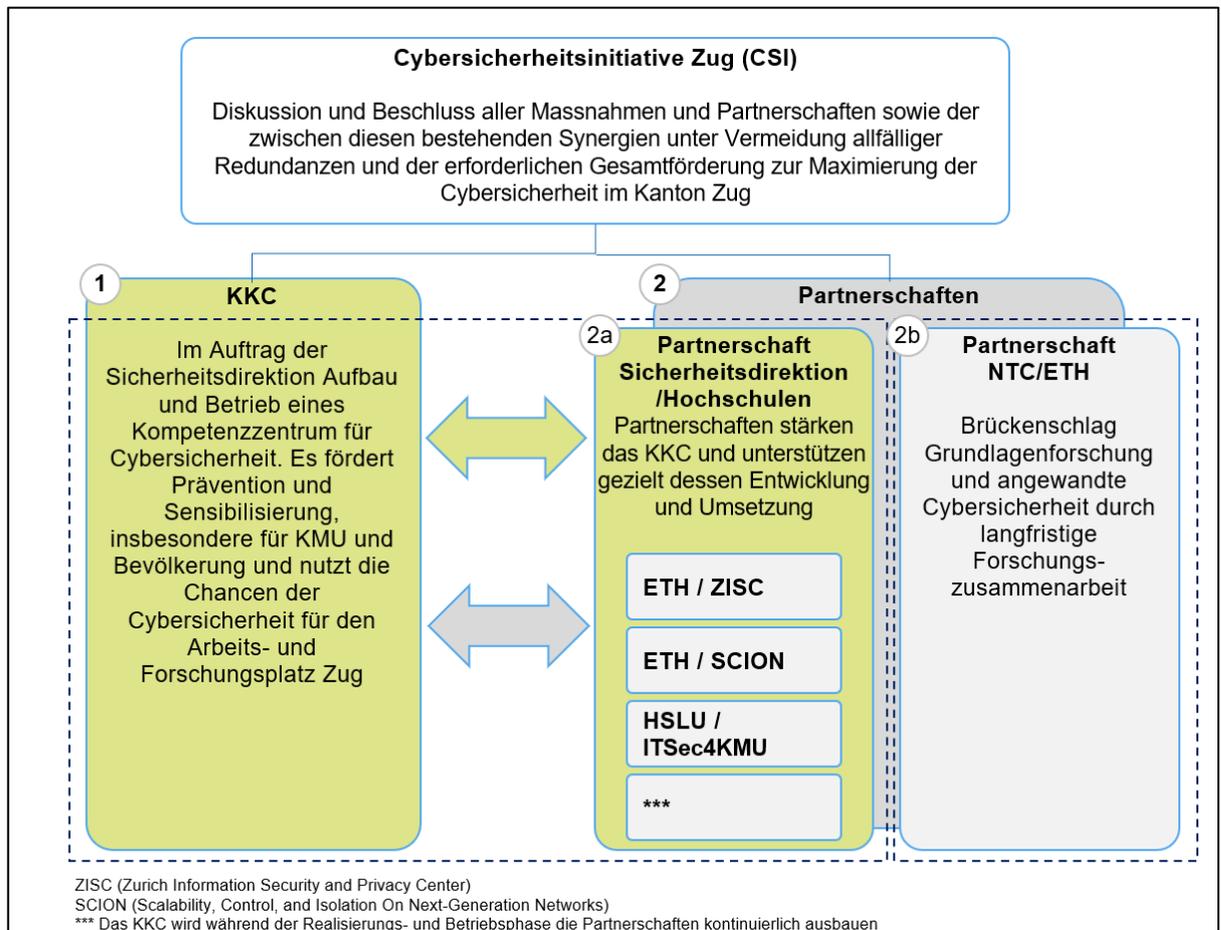


Abbildung 1: Das 3-Säulen Modell der Cybersicherheitsinitiative Zug (CSI)

Durch die enge Abstimmung zwischen der Sicherheits- und der Finanzdirektion sowie die koordinierte Zusammenarbeit von KKC, HSLU, ETH und NTC werden gezielt Synergien genutzt, Doppelspurigkeiten vermieden und eine nachhaltige Cybersicherheitsstrategie für den Kanton bereitgestellt, indem insbesondere die vulnerablen Anspruchsgruppen «Bevölkerung» und «kleine/mittelständische Unternehmen» regelmässig sensibilisiert und aufgeklärt werden. Dabei werden wissenschaftliche Forschung, strategische Steuerung sowie praxisorientierte Sicherheitslösungen gezielt miteinander verknüpft, um die digitale Sicherheit im Kanton nachhaltig und integral zu stärken.

- Der Regierungsrat entwickelt mit dem **KKC** die strategische Cybersicherheitsagenda des Kantons und verfolgt das Ziel, eine nachhaltige Sicherheitskultur in Gesellschaft und Wirtschaft im Kanton Zug zu fördern und zu verankern. Dabei stehen Prävention, Sensibilisierung und Aufklärung als essenzielle Massnahmen für die besonders vulnerablen Anspruchsgruppen «Bevölkerung» und «Zuger KMU» im Mittelpunkt der Bekämpfung digitaler Kriminalität. Die Zusammenarbeit zwischen der Sicherheitsdirektion und der **Hochschule Luzern (HSLU)** ist bereits durch zahlreiche erfolgreiche Projekte etabliert unter anderem durch die Initiative «**ITSec4KMU**», einem vom Kanton Zug initiierten Projekt zur Stärkung der Cybersicherheit in kleinen und mittleren Unternehmen. Ziel ist es, die bestehende Partnerschaft weiter zu stärken und das gemeinsame Potenzial im Interesse der öffentlichen Sicherheit insbesondere für die Anspruchsgruppen KMU und Bevölkerung noch gezielter zu nutzen.

- Durch die enge Zusammenarbeit zwischen der **Sicherheitsdirektion**, der **Hochschule Luzern**, der **ETH Zürich** sowie den Mitgliedschaften im Zurich Information Security and Privacy Center (ZISC) und bei SCION (Scalability, Control, and Isolation On Next-Generation Networks) entsteht eine einzigartige Brücke zwischen Forschung und Praxis. Diese Partnerschaften stärken den Wissens- und Technologiestandort des Kantons Zug, fördert wirtschaftliches Wachstum und schafft hochwertige Arbeitsplätze. Der Kanton Zug positioniert sich so als führender Standort für digitale Sicherheit in der Schweiz.
- Die Schnittstellen des KKC zu Wissenschaft und privatwirtschaftlichen Partnern werden gezielt institutionalisiert und gebündelt. Aufbauend darauf entstehen durch substantielle Innovationsförderungen erhebliche Wachstumspotentiale für den Wirtschafts- und Forschungsraum Zug. Ziel der projektbezogenen Förderung ist es Rahmenbedingungen für die Ansiedlung von ETH- und HSLU-Ausgründungen zu schaffen. Auf diese Weise wird hochrelevantes Wissen generiert, das auch gezielt den Bedürfnissen der «Zuger KMU» zugutekommt.
- Die **Sicherheitsdirektion** kann auf die Expertise des **Nationalen Testzentrum für Cybersicherheit NTC** im Bereich der Sicherheitsüberprüfungen und -analysen zurückgreifen und diese kontinuierlich in die strategische Cybersicherheitsagenda des Kantons integrieren. Die Zusammenarbeit zwischen dem KKC und dem NTC bietet schweizweit eine einzigartige Gelegenheit, Erkenntnisse aus den praxisnahen Sicherheitsprüfungen direkt für wirtschaftsnahe Anwendungen nutzbar zu machen. Die Sicherheitsdirektion nutzt dieses Potenzial, um sicherheitsrelevante Prüfungen und Analysen gezielt in die kantonale Cybersicherheitsstrategie einzubetten. Insbesondere Zuger KMU profitieren davon, indem das KKC beim NTC gezielt Prüfaufträge für vernetzte Infrastrukturen, Geräte und Anwendungen initiiert und die daraus gewonnenen Erkenntnisse breit, jedoch nicht ausschliesslich, der Zuger Wirtschaft zur Verfügung stellt.

3. Ziel und Auftrag des Kantonalen Kompetenzzentrums Cybersicherheit (Säule 1)

3.1. Ziel und Leistungsauftrag

Die fortschreitende Digitalisierung sämtlicher Lebens- und Arbeitsbereiche stellt den Kanton Zug vor neue sicherheitspolitische, technische und organisatorische Herausforderungen. Cybersicherheit ist dabei weit mehr als nur eine technische Frage, sie ist eine grundlegende Voraussetzung für das Vertrauen in digitale Prozesse, für die Funktionsfähigkeit staatlicher Institutionen und für den Schutz der Bevölkerung. Vor diesem Hintergrund kommt dem Aufbau und dem Betrieb eines kantonalen Kompetenzzentrums eine zentrale Rolle zu. Es soll als strategische Drehscheibe fungieren, die bundesweite Vorgaben mit lokalem Fachwissen und kantonalen Bedürfnissen vereint und so eine koordinierte, nachhaltige und zukunftsorientierte Sicherheitsarchitektur schafft.

Das KKC erfüllt einen vierfachen Leistungsauftrag:

1. Das KKC hilft gezielt besonders **vulnerablen Anspruchsgruppen innerhalb der Bevölkerung**.
2. **Kleine und mittlere Unternehmen** werden vom KKC unterstützt, ihre **Cyberresilienz zu erhöhen**.
3. Das KKC fördert die **Vernetzung und Koordination** von privaten und öffentlichen Partnern.
4. Die Potentiale der Cybersicherheit für die Erhöhung der **Attraktivität des Wirtschafts- und Forschungsplatzes Zug** werden vom KKC gezielt genutzt.

Die folgende Abbildung veranschaulicht die Aufgaben des KKC, gegliedert nach seinen dedizierten Wirkungsfeldern und Anspruchsgruppen sowie den dazugehörigen Aktivitäten und Umsetzungen. Die einzelnen Wirkungsfelder und Anspruchsgruppen werden im Anschluss an die Abbildung noch im Detail erläutert.

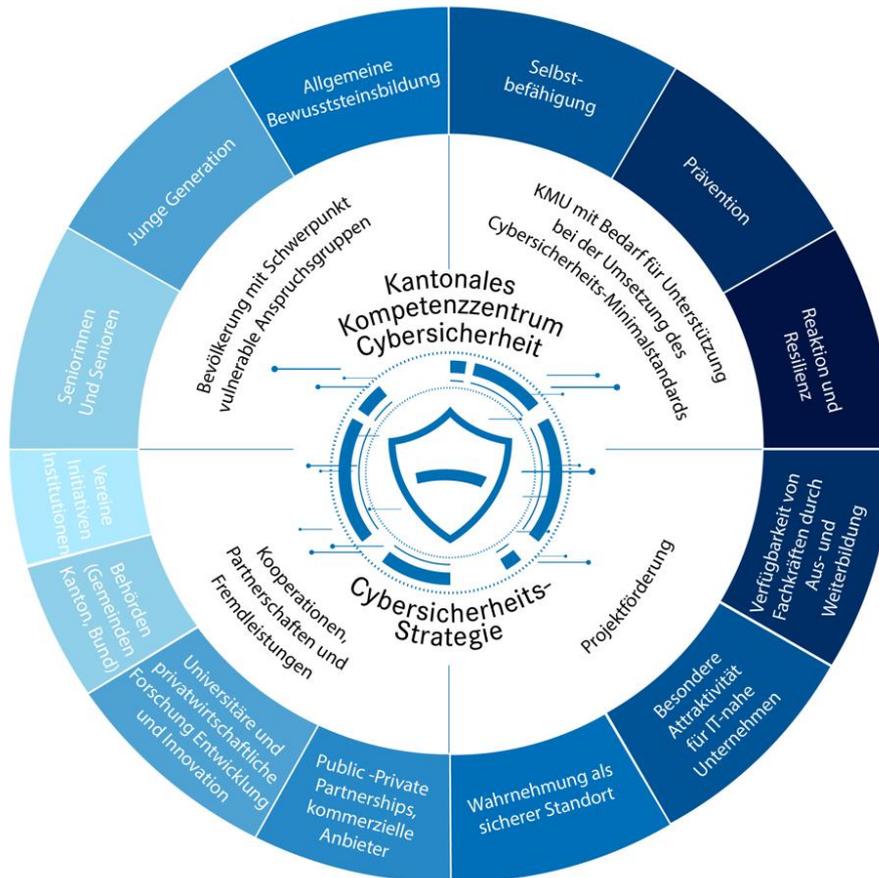


Abbildung 2: Kantonales Kompetenzzentrum Cybersicherheit

- 1. Bevölkerung mit Schwerpunkt vulnerable Anspruchsgruppen:** Das KKC richtet sich an alle Menschen. Ein besonderer Fokus liegt auf Gruppen, die im digitalen Raum besonders gefährdet sind, wie ältere Personen oder die junge Generation. Ziel ist es, das Bewusstsein für Risiken im Cyber-Raum zu schärfen und zu zeigen, wie man sich schützen kann. Das KKC unterstützt mit verständlichen Informationen und verschiedenen Angeboten zum Beispiel durch Kurse, E-Learnings, Vorträge, Flyer oder persönliche Beratungen. Beispiele aus dem Alltag:

 - Herr Sorglos (70) bekommt eine Phishing-E-Mail von seiner vermeintlichen Bank. Das KKC zeigt ihm, wie er solche Betrugsversuche erkennt und sich davor schützt.
 - Frau Risky (75) erhält einen Anruf oder eine WhatsApp-Nachricht von einer angeblichen Enkelin, die dringend Geld braucht. Das KKC erklärt ihr, wie der sogenannte «Enkeltrick» funktioniert und wie sie richtig reagiert.
 - Leon Phish (12) wird im Internet gemobbt und weiss nicht, was er tun soll. Beim KKC findet er Informationen, Anlaufstellen und Tipps, wie er sich beraten lassen und wehren kann.
- 2. Zuger KMU mit Bedarf für Unterstützung bei der Umsetzung des Cybersicherheits-Minimalstandards:** Viele kleine und mittlere Unternehmen (KMU) haben nicht die Mittel, sich umfassend vor digitalen Bedrohungen und deren Auswirkung auf Forschung, Entwicklung, Produktion, Vertrieb usw. zu schützen. Das KKC hilft diesen Unternehmen, grundlegende

Sicherheitsstandards umzusetzen. Es unterstützt bei der Vorbeugung, vermittelt Wissen zur Selbsthilfe und zeigt, wie man bei einem Cyber Notfall richtig reagiert und widerstandsfähig bleibt. Beispiele aus dem Unternehmensalltag mit fiktiven Firmennamen:

- Die «Cookie-Bäckerei» speichert Kundendaten für ihren Lieferdienst. Das KKC zeigt dem Geschäftsführer Herrn Backdoor, wie er seine Systeme absichern kann, damit keine Unbefugten darauf zugreifen, etwa durch sichere Passwörter, aktuelle Software und regelmässige Updates und externe Überprüfungen.
- Das Architekturbüro «Planlos und Partner» profitiert vom Know-how des KKC, um Baupläne und vertrauliche Kundendaten wirksam vor Cyberangriffen zu schützen, etwa unter anderem durch verschlüsselte Datenübertragung, regelmässige Backups, wirkungsvolle Detektionsmassnahmen zur Erkennung von Cyberangriffen und den Einsatz sicherer Netzwerke.
- Der Sanitär «Phish und Spül AG» erhält eine gefälschte Rechnung per E-Mail. Dank der vom KKC bereitgestellten Schulungsunterlagen erkennt die Buchhaltung den Betrugsversuch frühzeitig und verhindert so eine unberechtigte Zahlung.
- Eine kleine Werbeagentur «Ctrl+Alt+Design AG» arbeitet mit vielen externen Partnern zusammen. Das KKC unterstützt sie dabei, Zugriffsrechte sinnvoll zu regeln und gemeinsam genutzte Daten sicher zu verwalten und auszutauschen.
- Der Familienbetrieb «Riskante AG» wird Opfer eines Erpressungstrojaners (Ransomware). Durch die Vorbereitung mit dem KKC weiss die Geschäftsführung, wie sie reagieren muss und hat funktionierende Backups und Notfallpläne, um den Betrieb schnell wiederherzustellen.

3. **Vernetzung und Koordination von öffentlichen und privaten Partnern:** Um eine möglichst breite Wirkung zu erzielen, kooperiert das KKC eng mit einer Vielzahl von Partnern darunter Behörden, Gemeinden, Hochschulen, Universitäten, Public-Private Partnerships sowie weitere Institutionen und Anbieter. Zentral sind Partnerschaften mit Institutionen wie dem Bundesamt für Cybersicherheit (BACS), dem Cyberdefence Campus, dem Nationalen Testzentrum für Cybersicherheit (NTC), ETH Zürich, Hochschule Luzern (HSLU) sowie kantonalen und regionalen Akteuren wie bspw. TFZ, Startups und spezialisierten Unternehmen. Internationale Institutionen wie INTERPOL, EUROPOL oder auch NEDIK sichern die grenzüberschreitende Koordination. Durch diese Zusammenarbeit können Wissen und Ressourcen gebündelt und gemeinsame Lösungen entwickelt werden. Dazu gehört im Bereich Innovationen und Standards auch die engere Zusammenarbeit der HSLU mit dem Dienst Digitale Forensik der Zuger Polizei, welche das Interkantonale Kompetenzzentrum Digitale Forensik betreibt.

Es ist festzuhalten, dass es nicht zum Auftrag des KKC gehört, in Konkurrenz zur privaten IT- und Security-Privatwirtschaft zu treten. Vielmehr versteht sich das KKC als komplementärer Akteur, der bestehende Angebote gezielt ergänzt und im Sinne einer Win-Win-Situation partnerschaftlich mit privatwirtschaftlichen Organisationen zusammenarbeitet. Es gilt der Grundsatz der «Beschaffung vor Eigenentwicklung». In diesem Kontext wurde eine Marktstudie durchgeführt, die aufzeigt, in welchen Bereichen Synergien genutzt und tragfähige Partnerschaften aufgebaut werden können. Die Pflege und Weiterentwicklung dieser Kooperationen liegt in der Verantwortung des KKC. Die Umsetzung der entsprechenden Massnahmen erfolgt in Zusammenarbeit mit der Zuger Polizei, da Präventionsarbeit bereits Teil ihres Leistungsauftrags ist. Diese Präventionsarbeit wird insbesondere mit der Umsetzung des Projektes «bürgernehe Polizei» vorgenommen werden. Die folgenden Beispiele sind nicht abschliessend und dienen lediglich der Veranschaulichung möglicher Kooperationen:

- Eine Zuger Gemeinde arbeitet mit dem KKC zusammen, um Schulklassen praxisnahe Workshops zu Cybermobbing anzubieten. Mithilfe der vom KKC zur Verfügung

gestellten Schulungsunterlagen können die Workshops erfolgreich durchgeführt werden. Das KKC bietet keine Kurse an, die von Privaten Anbietern kommerzialisiert sind (z.B. Sicherheitsschulungsangebote von ICT-Firmen).

- Ein Zuger Verein bspw. ein Seniorenverein, der vom KKC befähigt und begleitet wurde, organisiert eigenständig regelmässige Infoabende zu aktuellen Betrugsmaschen und Möglichkeiten der Prävention. Das KKC bietet hierbei keine von Privaten Anbietern kommerzialisierten Leistungen an (z.B. PC-Anwenderschulung).
 - Studierende der HSLU erarbeiten im Rahmen von Bachelor- oder Masterarbeiten konkrete Sensibilisierungsmassnahmen für die verschiedene Zielgruppen resp. Anspruchsgruppen. Der Sensibilisierungseffekt bietet neue Potentiale für private Dienstleistungsangebote (z.B. sichere Backupleistungen).
 - Ein lokales spezialisiertes Sicherheitsunternehmen unterstützt die Arbeit des KKC, etwa durch die Bereitstellung von Ressourcen und Technologien.
 - Das KKC macht seine Services und Angebote auch über die Kantonsgrenzen hinaus bekannt und stellt diese bei Bedarf auch ausserkantonalen Partnern zur Verfügung. Dies führt zu einem Leuchtturmeffekt mit positiver Ausstrahlung auf nationaler Ebene.
4. **Attraktivität des Wirtschafts- und Forschungsstandortes Zug:** Durch die Förderung von Cybersicherheit trägt das KKC dazu bei, den Kanton als sicheren, zukunftsfähigen und attraktiven Standort für Unternehmen zu positionieren. Gleichzeitig stärkt es in Zusammenarbeit mit Hochschulen, Universitäten und privaten Anbietern die Aus- und Weiterbildung im Bereich Cybersicherheit. So wird dazu beigetragen, genügend Fachkräfte für die sichere digitale Zukunft bereitzustellen. Beispiele zur Standort- und Fachkräfteförderung:
- Ein internationales IT-Unternehmen entscheidet sich für eine Niederlassung in der Region auch wegen der guten Zusammenarbeit mit dem KKC und den bestehenden Sicherheitsstandards.
 - Ein innovatives KMU kann dank der Zusammenarbeit seines ICT-Anbieters mit dem KKC und dem BACS einen Cyberangriff frühzeitig abwehren und nutzt das als Vertrauensvorteil in der Kommunikation mit seinen Kunden.
 - Zuger Unternehmen und Unternehmen aus der Region profitieren von gemeinsamen Sicherheitsstandards und werben gezielt damit, besonders gut gegen Cyberrisiken gerüstet zu sein.
 - In enger Kooperation mit Berufsfachschulen und Hochschulen entwickelt das KKC praxisnahe Lehrinhalte und Zertifikatslehrgänge, die direkt auf die Bedürfnisse von Wirtschaft und Verwaltung abgestimmt sind. So werden neue Fachkräfte für IT- und Cybersicherheit ausgebildet und stärken damit den kantonalen Arbeitsmarkt.

3.2. Strategische Grundsätze mit ihren Wirkungsfeldern und Messung des Erfolges

Die nachgelagerten Grundsätze bilden gemeinsam mit dem zentralen und verbindenden Element eines kantonalen Kompetenzzentrums für Cybersicherheit die Grundlage der Cybersicherheitsstrategie des Kantons. Die folgenden acht Grundsätze sollen das Wirken, den Mitteleinsatz und die Messung des Erfolges des KKC bestimmen:

Grundsatz 1: Die kantonale Cybersicherheitsstrategie und ihre nachgeordneten Strukturen und Aktivitäten haben eine langfristige Ausrichtung und sind in die kantonalen Aktivitäten zur Umsetzung einer integralen Sicherheit integriert.

Wirkungsfeld:

- Der virtuelle Raum ist Teil der Lebensrealität vieler Menschen und fast aller Unternehmen. Beide profitieren von einem integralen Sicherheitsverständnis der öffentlichen Hand.

- Ein integraler Ansatz mit Bezug aller betroffenen Instanzen hat die Chance auf gute Akzeptanz bei Vermeidung von Doppelspurigkeiten.
- Die Strategie legt den Grundstein für sichere digitale Dienste und fördert innovative Entwicklungen.
- Ein langfristiger Ansatz stärkt die Resilienz gegen wachsende Cyberbedrohungen und gewährleistet anpassungsfähige Sicherheitsstrukturen.
- Die Einbettung in die integrale Sicherheit fördert die Zusammenarbeit und spart Ressourcen.

Messung des Erfolges:

- Input-orientierte Grössen (FTE, CHF) und deren Entwicklung und Auslastung über die Zeit

Grundsatz 2: Es muss eine messbare Reduktion der Auswirkung von Cyber-Risiken auf ein für die jeweiligen Anspruchsgruppen (Bevölkerung, KMU) akzeptables Mass erreicht und regelmässig aufgezeigt werden.

Wirkungsfeld:

- Messbarkeit ergibt Kreditibilität für die Zukunft und Verständnis für die nötigen Investitionen, schafft Vertrauen der Bevölkerung und KMU in die öffentliche Hand im Kanton und steigert die Standortattraktivität.
- Es kann idealerweise gezeigt werden, dass mit angemessenen Investitionen ein ausreichender Schutz vor Schäden durch Cyber-Risiken geschaffen und aufrechterhalten werden kann.

Messung des Erfolges:

- Input-orientierte Grössen (Kampagnen, Öffentlichkeitsarbeit pro Anspruchsgruppe usw.)
- Output-orientierte Grössen, sofern erhebbar: Schadensvolumen, Anzahl Fälle usw.
- Messung durch Befragungen und Zufriedenheitsstudien.

Grundsatz 3: Der Cyber-Schutz und die Attraktivität des Wohn- und Wirtschaftsstandortes müssen sowohl durch Schutzmassnahmen als auch durch Innovation sowie Aus- und Weiterbildung aktiv gefördert werden.

Wirkungsfeld:

- Sicherstellung von Kontinuität (Innovation und Ausbildung sind der Schutz von morgen).
- Synergien zu Innovationsförderung des Kantons, z.B. durch Ansiedlung von IT-lastigen Unternehmen, Start-ups und Spin-offs aus dem Hochschulumfeld.
- Erhöhung der Standortattraktivität für KMU und Fachkräfte fördert Innovation im Bereich Cybersicherheit und kann so neue Geschäftsmodelle sowie Arbeitsplätze schaffen.

Messung des Erfolges:

- Anzahl relevanter Firmenzuzüge, Startups und Spin-offs
- Anzahl Ausbildungsplätze / Lehrstellen mit Schwerpunkt Cybersicherheit
- Anzahl neu geschaffener Arbeitsplätze im Bereich Cybersicherheit
- Relevante Forschung und Entwicklung, Bachelor- und Masterarbeiten, Weiterbildungsangebote usw.
- Umfragen zur Zufriedenheit von KMU und der Bevölkerung mit der Cybersicherheit im Kanton

Grundsatz 4: Alle präventiven und reaktiven Massnahmen zur Risikoreduktion und zur Erhöhung der Resilienz gegen Cyber-Angriffe und Ausfälle müssen auf die jeweiligen Anspruchsgruppen (Bevölkerung, KMU usw.) zugeschnitten sein und deren Bedürfnisse möglichst zielgenau abdecken.

Wirkungsfeld:

- Schaffung von Mehrwert und «Gefühl der Sicherheit». Bevölkerung und KMU fühlen sich durch die gezielten Massnahmen besser geschützt.
- Bereitschaft zur aktiven Mitwirkung, Übernahme von Eigenverantwortung.
- Gezielte Massnahmen erhöhen die Sicherheit für unterschiedliche Zielgruppen wie KMU und Bevölkerung.
- Mittel werden bedarfsgerecht eingesetzt, was Aufwand und Kosten senkt.

Messung des Erfolges:

- Kundenbefragungen, Kursfeedbacks, Anzahl spezifischer Veranstaltungen
- Interesse an aktiver Beteiligung der Anspruchsgruppen (runder Tisch, Selbsthilfegruppen)
- Anzahl resp. Trend der Sicherheitsvorfälle pro Anspruchsgruppe (Messung der Wirksamkeit der Massnahmen)
- Beteiligungsrate an Schulungen und Awareness-Initiativen
- Zufriedenheit der jeweiligen Anspruchsgruppen mit der wahrgenommenen Relevanz und Angemessenheit der Massnahmen.

Grundsatz 5: Aufbau, Betrieb und stetige Weiterentwicklung des kantonalen Kompetenzzentrums Cybersicherheit und dessen langfristige Ausstattung mit ausreichenden Ressourcen und Kompetenzen ist eine unabdingbare Voraussetzung für die Umsetzung der Cybersicherheitsstrategie.

Wirkungsfeld:

- Bündelung der Kräfte, Koordination, Priorisierung / Planung, Massnahmen und Berichterstattung «aus einer Hand».
- Enge Koordination mit politischer Willensbildung, Legislaturzielen und Budgets.
- Zentrale Anlaufstelle gegenüber kantonalen Anspruchsgruppen sowie gegenüber übergeordneten Instanzen auf Bundesebene.
- Die Förderung der Zusammenarbeit mit Kanton und KMU bietet eine Plattform für den Austausch von Informationen zu neuesten Technologien und «Best Practices».

Messung des Erfolges:

- Meilensteine bei Aufbau und Ausbau des Cyber-Kompetenzzentrums
- Auslastungsgrad der Ressourcen (FTE, CHF) und Ausbauplanung
- Bewertung der Effektivität und Effizienz der eigenen Aktivitäten gegenüber dem SLA
- «Backlog» wünschenswerter weiterer Aktivitäten
- Fortschrittsberichte zur transparenten Bewertung der Zielerreichung.

Grundsatz 6: Der Schutz vor Cyber-Risiken muss einerseits durch die Bereitstellung entsprechender Auskunfts- und Hilfsmittel, andererseits aber auch durch eine Stärkung der Eigenverantwortung und Selbstbefähigung der betroffenen Personen, Firmen und Institutionen gefördert werden.

Wirkungsfeld:

- Verständnis des Themas als geteilte Aufgabe und Verantwortung ohne einseitige Abwälzung auf den Kanton.
- Chance zur geführten «Hilfe zur Selbsthilfe» innerhalb und zwischen den Anspruchsgruppen.
- Die Förderung der Eigenverantwortung führt mittelfristig zu einer geringeren Belastung der kantonalen Ressourcen, da weniger Vorfälle eine direkte Intervention erfordern.
- Durch gezielte Informations- und Beratungsangebote sowie durch Schulungen werden Bevölkerung und KMUs auf Cyber-Risiken vorbereitet.

Messung des Erfolges:

- Anzahl und Abdeckungsgrad der bereitgestellten Hilfsmittel
- Anzahl und Art der erhaltenen / bearbeiteten Auskunfts- und Hilfebegehren
- Reduktion der Vorfälle: Die Anzahl gemeldeter Cybervorfälle pro Jahr im Kanton kann als zentraler KPI dienen. Eine Verringerung dieser Zahl wäre ein Indikator für die Wirksamkeit der Strategie
- Anzahl geschulter Personen und Firmen, ggf. unterteilt nach Branchen / Kritikalität
- Feedback und Umfragen zur Zufriedenheit betreffend die bereitgestellten Informations- und Hilfsmittel.

Grundsatz 7: Um Doppelspurigkeiten zu vermeiden, die vorhandenen Ressourcen optimal zu nutzen und die Ziele der Strategie mit angemessenem Mitteleinsatz zu erreichen, werden Kooperationen und Synergien mit umgebenden Strukturen (Hochschulen, nationale, kantonale und ausserkantonale Kompetenzzentren, Dienstleister usw.) aktiv gesucht und bewirtschaftet. Hierbei wird im Grundsatz ermöglicht, eigene Dienstleistungen fallweise auch anderen Kantonen zur Nutzung anzubieten.

Wirkungsfeld:

- Ein Grundsatz der «Beschaffung vor Eigenentwicklung» und der Beizug aller relevanten Instanzen ergibt Vertrauen, ist ressourceneffizient und schafft keine Konkurrenz zu Privatanbietern, sondern Mehrwert für alle Beteiligten.
- Die Möglichkeit zur fallweisen Mitnutzung durch andere Kantone kann in einer breiteren Verteilung der Kosten und der Nutzung weiterer Synergien resultieren.
- Durch das Angebot eigener Dienstleistungen an andere Kantone können der eigene Aufwand reduziert und gleichzeitig Einnahmen generiert werden, was die Strategie langfristig tragfähiger macht.
- Die Kooperation mit Hochschulen und Kompetenzzentren ermöglicht eine gezielte Nutzung von Fachwissen und technologischen Ressourcen, wodurch die eigene Leistungsfähigkeit gestärkt wird, ohne zusätzliche personelle Ressourcen aufbauen zu müssen.

Messung des Erfolges:

- Anzahl, Volumen, Zeitdauer und Art von Kooperationsvereinbarungen
- Controlling der Umsetzung von Kooperationen und umgesetztes versus noch nicht ausgeschöpftes Verbesserungspotential
- Anzahl, Umfang und Zielerreichung der gemeinsam durchgeführten Projekte
- Regelmässige Befragungen der Partnerorganisationen, um die Zufriedenheit und die wahrgenommene Effektivität und Effizienz der Zusammenarbeit zu messen.

Grundsatz 8: In einer sich technologisch rasch wandelnden Welt muss die Fähigkeit zur Antizipation und Beurteilung neuer Trends und Technologien (künstliche Intelligenz, Einbindung des «Internet der Dinge» usw.) bezüglich Chancen, Risiken, Einsatzoptionen und Schutzmassnahmen im Bereich Cybersicherheit stark ausgeprägt sein und in Kooperation mit geeigneten Forschungs- und Entwicklungspartnern jederzeit aufrechterhalten werden.

Wirkungsfeld:

- Vorausschauende Identifikation und Beurteilung relevanter Trends, Technologien usw. erlaubt eine rechtzeitige Einordnung in die geplanten Aktivitäten inklusive Priorisierung, Budgetierung, Know-how-Aufbau usw.
- Schäden können ggf. präventiv und nicht erst nach einem ersten Auftreten verhindert werden.
- Durch die Antizipation von Trends kann der Kanton schneller auf neue Gefährdungen und Chancen reagieren und entsprechende Massnahmen planen und umsetzen.
- Die proaktive Zusammenarbeit mit Forschungs- und Entwicklungspartnern stärkt die kantonale Innovationskraft und macht den Standort attraktiver für Unternehmen im Technologiesektor.

Messung des Erfolges:

- Technologische «Heat Map» oder «Hype Curve»
- Kontinuierlich aktualisierte Lage- und Risikobeurteilung mit Identifikation der eigenen Reaktionsfähigkeit / Umsetzung
- Stundenaufwand pro Jahr für Technologie-«Scouting» mit Relevanz für Zielgruppen
- Messung der Anzahl und Tiefe der Kooperationen mit Forschungs- und Entwicklungseinrichtungen (Anzahl gemeinsamer Projekte, Anzahl der durch die Partner bereitgestellten Resultate, Forschungsberichte, etc.).

4. Leistungsspektrum und Betriebsmodell des KKC (Säule 1)

Aus den zuvor beschriebenen Grundsätzen leiten sich konkrete Massnahmen zur Umsetzung ab, die im Folgenden dargestellt werden. Sie bilden die Grundlage für die notwendige Priorisierung und Finanzierung entsprechender Arbeitspakete im Rahmen der Legislatur- und Budgetplanung. Eine tragfähige Governance-Struktur ist dabei von zentraler Bedeutung für den erfolgreichen Aufbau und Betrieb des KKC. Dieser erfordert eine ausgewogene Balance zwischen zentraler Steuerung und lokaler Verankerung. Während gesetzliche Grundlagen und nationale Strategien eine koordinierte und kohärente Governance sicherstellen, sind kantonsspezifisches Fachwissen und dezentrale Ressourcen entscheidend für eine wirksame Umsetzung auf regionaler Ebene. Wo gesetzliche Anpassungen erforderlich sind, initiiert und begleitet das KKC die Prüfung und Ausarbeitung entsprechender rechtlicher Grundlagen. So wird gewährleistet, dass die strukturellen und juristischen Rahmenbedingungen den Anforderungen einer modernen, kooperativen und effektiv gesteuerten Institution entsprechen. Für die Akzeptanz und Wirksamkeit der Cybersicherheitsmassnahmen ist zudem eine offene und transparente Kommunikation mit allen relevanten Anspruchsgruppen zentral. Das KKC wird diesen Dialog koordinieren und kontinuierlich pflegen, orientiert an den jeweiligen Informationsbedürfnissen von Verwaltung, Wirtschaft, Bevölkerung und Partnern.

4.1. Organisation

Der geplante Ressourcenaufbau des KKC erfolgt schrittweise und orientiert sich an den wachsenden Anforderungen und der Etablierung des KKC. Im Startjahr 2025 ist noch keine feste personelle Besetzung vorgesehen. Die Initialisierungsphase wird durch interne Mitarbeitende der Sicherheitsdirektion sichergestellt. Ab 2026 beginnt der Aufbau mit zwei Vollzeitstellen (FTE) für Cyber-Expertinnen und -Experten. Es folgt eine sukzessive Erweiterung des Teams:

2027 auf sieben FTE, 2028 auf neun FTE und ab 2029 mit einer stabilen Besetzung von zehn FTE, die auch für das Jahr 2030 beibehalten wird. Diese Zahlen stellen aktuelle Schätzungen dar und können je nach Entwicklung der Aufgaben und Prioritäten angepasst werden. Bei Projektbeginn wird das KKC eine verwaltungsinterne Fachstelle der Sicherheitsdirektion sein aber nicht ein Amt. In der Aufbauphase ist eine Symbiose/Zusammenarbeit mit dem Nationalen Testzentrum für Cybersicherheit erstrebenswert, um von Synergien zu profitieren.

Mittelfristig werden gezielt die Rahmenbedingungen des Forschungsplatzes gefördert. Ziel ist ein produktives Umfeld interdisziplinärer Zusammenarbeit, Forschung und Innovation, perspektivisch auch in Kooperation mit Hochschulen im Rahmen von Professuren. Eine konkrete Umsetzung der Professuren ist derzeit nicht terminiert.

Mit dem erwarteten Wachstum der Organisation wird zudem geprüft, geeignete Räumlichkeiten für das KKC bereitzustellen, um auch dem wachsenden interdisziplinären Zusammenarbeitsraum eine physische Heimat zu geben. Zeitpunkt und Umfang dieser räumlichen Entwicklung sind aktuell noch offen und Teil des laufenden Planungsprozesses. Sowohl die räumlichen als auch die personellen Entwicklungen wurden in der Kostenplanung berücksichtigt und ermöglichen eine flexible Anpassung an die dynamischen Anforderungen im Bereich der Cybersicherheit.

4.2. Einbindung in den politischen Willensbildungs- und Entscheidungsprozess

Die erfolgreiche Umsetzung des Vorhabens setzt eine frühzeitige und kontinuierliche Einbindung in die politischen Willensbildungs- und Entscheidungsprozesse voraus. Für das KKC umfasst dies insbesondere:

- **Transparente Kommunikation und Meinungsbildung:**
Das KKC stellt den regelmässigen Informationsaustausch mit politischen Gremien und relevanten Stakeholdern sicher. Es informiert sachlich über Projektfortschritte, holt aktiv Rückmeldungen ein und prüft deren Integration. Fragen werden zeitnah und nachvollziehbar beantwortet, um Vertrauen und Akzeptanz zu fördern.
- **Verankerung in politische Planungsprozesse:**
Das KKC koordiniert die inhaltliche und finanzielle Einbettung der Massnahme in Legislaturziele und Budgetprozesse. Es sorgt für die rechtzeitige Berücksichtigung der wiederkehrenden Personal- und Sachkosten in der mittelfristigen Finanzplanung.

4.3. Lagebild Cybersicherheit und strategische Handlungsfelder

Zur fortlaufenden Bewertung der kantonalen Cybersicherheitslage etabliert das KKC einen strukturierten Analyseprozess. Dieser dient der Erkennung von Handlungsfeldern und der strategischen Weiterentwicklung bestehender Massnahmen. Die Analyse erfolgt unter Einbezug relevanter Anspruchsgruppen und orientiert sich an nationalen und kantonalen Zielsetzungen. Auf dieser Grundlage werden Massnahmen identifiziert, priorisiert und in den strategischen Entwicklungsprozess integriert. Der Analyseprozess wird regelmässig wiederholt, um neue Herausforderungen frühzeitig zu erkennen und eine kontinuierliche Optimierung sicherzustellen.

4.4. Leistungsspektrum zur Stärkung der Cybersicherheit

Die folgende Liste soll das breite Leistungsspektrum möglicher Ansätze zur Stärkung der Cybersicherheit auf kantonaler Ebene sichtbar machen. Ziel ist es, insbesondere vulnerable Anspruchsgruppen wie die Bevölkerung sowie kleine und mittlere Unternehmen, aber auch weitere relevante Zielgruppen für Cyberrisiken zu sensibilisieren, ihre Schutzkompetenz zu stärken und so einen nachhaltigen Sicherheitsstandard im digitalen Raum des Kantons zu etablieren. Die konkreten Massnahmen werden vom KKC auf Basis des aktuellen Lagebildes sowie der strategischen Handlungsfelder entwickelt. Ihre Priorisierung, Budgetierung und Umsetzung erfolgen durch das KKC und unterliegen einer regelmässigen Überprüfung und

Weiterentwicklung. Dies ist notwendig sowohl im Hinblick auf technologische, politische und gesellschaftliche Veränderungen als auch unter Berücksichtigung gewonnener Erkenntnisse aus bestehenden Initiativen. Das KKC wird gemeinsam mit externen Partnern Massnahmen erarbeiten und umsetzen. Bestehende Synergien sollen dabei genutzt werden, sodass nicht zwingend alle Inhalte von Grund auf neu entwickelt werden müssen.

1. Kantonales Kompetenzzentrum Cybersicherheit
 - Etablierung einer kantonalen Anlaufstelle und Cyber-Hotline zur Ergänzung bestehender Angebote (bspw. BACS)
 - Funktion als Einsatzzentrale Cyberraum (z. B. bei Cyber Vorfällen)
 - Einsatz eines KI-basierten Chatbots für Erstberatung
2. Präventions- und Aufklärungskampagnen für die Bevölkerung
 - Plakate, Radiospots, Social Media und Veranstaltungen
 - Jährliche Themenschwerpunkte (z. B. Passwortsicherheit, Phishing, etc.)
3. Schulische und berufliche Bildung
 - Integration von Cyber-Hygiene und Medienkompetenz in den Lehrplan
 - Pflichtkurse und Weiterbildungen für Verwaltung und Wirtschaft
4. Online-Kurse und Simulationen
 - Interaktive Lernformate, E-Learnings, Phishing-Simulationen
 - Zielgruppenspezifisch: Senioren, Jugendliche, Eltern, KMUs
5. Technische Unterstützung und Empfehlungen
 - Beratende Rolle hinsichtlich geeigneter Tools wie Passwortmanager, Zwei-Faktor-Authentifizierung und Schutzprogrammen (z. B. Virenschutz).
 - Schritt-für-Schritt-Anleitungen für sichere Nutzung digitaler Geräte
6. Nationale und regionale Initiativen unterstützen
 - Durchführung eines «Zuger Security Day»
 - Förderung und Positionierung der Initiative «ITSec4KMU» der HSLU
 - Teilnahme am «nationalen SwissSecurityDay»
 - Zusammenarbeit mit dem Bundesamt für Cybersicherheit (BACS)
7. Zielgerichtete Awareness-Förderung und Communitybasiertes Lernen
 - Schulungen durch Cyberbotschafter und Cyberbotschafterinnen bspw. in Gemeinden, Vereinen, etc.
 - Laufende Sensibilisierungsinitiativen für verschiedene Anspruchsgruppen
 - Koordination und Durchführung von Workshops in Zusammenarbeit mit Schulen, Berufsverbänden, der Öffentlichkeit, KMU, Vereinen, Bibliotheken, etc.
 - Koordination mit Schulen, Berufsverbänden, Öffentlichkeit, KMU, etc.
 - Durchführen von Workshops in Vereinen, Bibliotheken, Schulen, etc.
8. Gamification und Storytelling
 - Entwicklung von Security Games, Comics oder Kurzfilmen zum Thema Cyber-Sicherheit
 - Praxisnahe Fallbeispiele zur Vermittlung digitaler Risiken
9. Sicherheits-Mindeststandards
 - Definition auf Basis von IKT-Minimalstandard für KMU
 - Anwendung für kritische Infrastrukturen und sensible Gruppen
10. Bereitstellung praxisnaher Ressourcen
 - Checklisten, Wegleitungen, Risiko-Assessments
 - Sicherheitstools für KMUs und Gemeinden
11. Cyber Incubator
 - Koordination / Vernetzung von Startups und Sicherheitsanbietern mit der ETH und weiteren Organisationen

5. Partnerschaften mit Hochschulen (Säule 2a)

5.1. Partnerschaft mit der ETH Zürich

Die ETH Zürich zählt weltweit zu den führenden Hochschulen im Bereich Cybersicherheit, Informatik und Künstlicher Intelligenz. Ihre international vernetzte und marktnahe Forschung greift aktuelle sicherheitsrelevante Fragestellungen auf und liefert praxisnahe Lösungen. Mit Strukturen wie dem Zurich Information and Privacy Security Center (ZISC) und weiteren gezielten Kooperationen wird die Exzellenz der ETH kontinuierlich ausgebaut. In Zusammenarbeit mit dem Kanton Zug sollen diese Kompetenzen gezielt genutzt werden, um den Aufbau eines national sichtbaren Kantonalen Kompetenzzentrums für Cybersicherheit (KKC) zu unterstützen. Die Sicherheitsdirektion mit dem KKC und die Finanzdirektion mit dem NTC planen mit dieser gemeinsamen Partnerschaft mit der ETH ein zukunftsorientiertes Fundament zu legen. Die geplanten Massnahmen fördern Forschung, Innovation und Wissenstransfer und leisten einen strategischen Beitrag zur Umsetzung der kantonalen Cybersicherheitsstrategie. Nachfolgend werden zwei konkrete Partnerschaften vorgeschlagen, die in enger Zusammenarbeit mit der ETH Zürich realisiert werden.

5.1.1. Partnerschaft mit dem Zurich Information Security and Privacy Center (ZISC)

Das Zurich Information Security and Privacy Center (ZISC) wurde 2003 an der ETH Zürich gegründet mit dem Ziel, Forschung und Industrie im Bereich der Informationssicherheit enger zu vernetzen. Das Zentrum vereint acht Professuren der ETH Zürich, deren Forschungsgruppen gemeinsam über 100 Doktorierende und Postdocs umfassen. Gemeinsam decken sie ein breites Spektrum ab – von Kryptographie, sicherem Computing und Datenschutz bis hin zur Sicherheit von KI-Systemen und Internetarchitekturen der Zukunft.

Das ZISC verfolgt drei zentrale Ziele:

- **Forschung:** Durchführung innovativer Projekte mit starkem wissenschaftlichem Fundament und Relevanz für reale Sicherheitsfragen.
- **Ausbildung:** Förderung der nächsten Generation von Experten durch akademische Lehre sowie Outreach-Programme an Schulen.
- **Innovation:** Unterstützung junger Talente bei der Gründung von Start-ups und beim Technologietransfer in die Praxis.

Das ZISC arbeitet eng mit weiteren ETH-Fakultätsmitgliedern sowie Partnern aus Wirtschaft und öffentlicher Hand zusammen. Aus dieser Kooperation sind zahlreiche erfolgreiche Spin-offs und anwendungsorientierte Forschungsprojekte hervorgegangen.

Mit seiner einzigartigen Kombination aus wissenschaftlicher Exzellenz, Praxisnähe und Innovationskraft leistet das ZISC einen wichtigen Beitrag zur Gestaltung einer sicheren digitalen Zukunft.

5.1.1.1. Nutzen für den Kanton Zug

Durch die Partnerschaft mit dem ZISC erhält der Kanton Zug Zugang zu führender Expertise, fundiertem Wissen, langjähriger Erfahrung und modernsten Ressourcen im Bereich der Cybersicherheit. Dies befähigt ihn, seiner Verantwortung in diesem Schlüsselbereich noch gezielter nachzukommen und seine Vorreiterrolle weiter auszubauen.

Die Zusammenarbeit stärkt zugleich die regionale Präsenz und Wirkung der ETH Zürich im Raum Zürich–Zug. Daraus entsteht eine multiplizierende Wirkung auf Innovationskraft und Fachkompetenz, die über die Region hinausstrahlt. Im engen Schulterschluss werden sowohl grundlegende als auch anwendungsnahe Fortschritte in der Cybersicherheit erzielt – mit Wirkung auf regionaler, nationaler und internationaler Ebene. Damit leisten Zug, Zürich und die

Schweiz einen nachhaltigen Beitrag zur Stärkung ihrer Position als führende Technologie- und Forschungsstandorte.

Damit wird zugleich der Entstehung eines Kompetenzzentrums für Cybersicherheit Vorschub geleistet, dessen katalytische Wirkung für den Innovations- und Technologiestandort Zug und darüber hinaus reichen wird. Wissen und Humanpotenzial werden gestärkt und strategisch ausgebaut. Die daraus resultierenden Produkte und Dienstleistungen, sei es in etablierten Zuger Unternehmen oder neuen Gründungen, führen zu wirtschaftlichem Wachstum sowie zur Schaffung hochqualifizierter Arbeitsplätze in der Region und darüber hinaus.

5.1.1.2. Themenfelder der Zusammenarbeit

Die typische Art der Zusammenarbeit mit dem ZISC-Zentrum und seinen Forschern ist eine langfristige Partnerschaft von mindestens fünf, im Idealfall bis zu zehn Jahren. Während dieser Zeit bietet eine ZISC-Partnerschaft durch die Mitgliedschaft folgende Vorteile:

- **Massgeschneiderte Forschungsprojekte:** Das ZISC passt ihre Forschungsprojekte auf Promotionsebene an die Bedürfnisse und Interessen seiner Partner an.
- **Fachkundige Beratung:** Das ZISC bringt seine Partner mit führenden Forschungsexperten (in der Regel Professoren und Postdoktoranden) zusammen, um Fachgespräche zu führen und praktische Ratschläge zu erhalten. Dabei sind sowohl individuelle Gespräche als auch ein Workshop Setting unter Beteiligung verschiedener Stakeholder möglich.
- **Networking:** Das ZISC-Zentrum organisiert verschiedene Veranstaltungen, darunter ein zweiwöchentliches Lunch-Seminar mit Fachvorträgen. Diese bieten Mitgliedern Gelegenheit, sich untereinander auszutauschen und dabei voneinander zu lernen bzw. gegebenenfalls Möglichkeiten der Zusammenarbeit zu identifizieren und von bereits erfolgreich etablierten, praktischen Lösungen anderer zu profitieren.
- **Weiterbildung.** Das ZISC bietet ihren Partnern Zugang zu Weiterbildungsprogrammen im Bereich Cybersicherheit. Es stehen zwei Programme zur Verfügung: Certificate of Advanced Studies (<https://inf.ethz.ch/continuing-education/cas-cybersecurity.html>) und Diploma of Advanced Studies (<https://inf.ethz.ch/continuing-education/das-cyber-security.html>).
- **OpenLab:** Die kollaborative Arbeitsumgebung, das ZISC OpenLab, kann gemeinsame Projekte und längere Besuche an der ETH Zürich ermöglichen

Insgesamt ermöglicht das ZISC seinen Mitgliedern den Zugang zu einem weltweiten Experten-Netzwerk sowie den direkten Austausch mit führenden Fachleuten der ETH Zürich. So bleiben sie stets über die neuesten Entwicklungen im Bereich der Cybersicherheit informiert, sowohl über bereits etablierte als auch über bald verfügbare, konkrete Lösungen in Hard- und Software. Dieser Mehrwert liegt auf der Hand.

5.1.2. Partnerschaft mit der SCION-Association

Die digitale Vernetzung ist aus dem Alltag von Bevölkerung, Wirtschaft und Verwaltung nicht mehr wegzudenken. Gleichzeitig steigen die Anforderungen an die Sicherheit, Stabilität und Souveränität unserer digitalen Infrastruktur kontinuierlich. Die jüngsten Entwicklungen im Bereich der Cybersicherheit, von internationalen Angriffen auf kritische Infrastrukturen bis hin zu gezielten Manipulationsversuchen im Datenverkehr, zeigen die dringende Notwendigkeit robuster, zukunftsfähiger Netztechnologien.

Das aktuell genutzte Internetprotokoll wurde in einer Zeit entwickelt, in der Themen wie Datensicherheit, Pfadkontrolle oder digitale Vertrauenswürdigkeit kaum berücksichtigt wurden. Entsprechend weist das heutige Internet grundlegende Schwächen auf, die im Kontext moderner Sicherheitsanforderungen nur unzureichend adressiert werden können.

Ein innovativer Lösungsansatz wurde an der ETH Zürich entwickelt: SCION (Scalability, Control, and Isolation On Next-generation networks). Dieses neuartige Internetsystem wurde von Grund auf mit dem Ziel konzipiert, die Kontrolle über Datenflüsse zu verbessern, Ausfallsicherheit zu gewährleisten und die Integrität digitaler Kommunikation zu erhöhen. SCION erlaubt es, die Wege, über die Daten transportiert werden, explizit festzulegen. Dadurch wird verhindert, dass sensible Informationen über unsichere oder unerwünschte Netzwerke geleitet werden. Zudem ermöglicht SCION eine automatische Umleitung bei Ausfällen oder Angriffen, ohne dass Verbindungen unterbrochen werden.

Zur gezielten Weiterentwicklung und Koordination dieses Ansatzes wurde die SCION Association gegründet. Zu den Trägern gehören unter anderem die Schweizerische Nationalbank, die SIX Group (zuständig für zentrale Finanzmarktinfrasturktur) sowie die ETH Zürich. Die SCION Association fördert die Anwendung der Technologie in verschiedenen Sektoren, insbesondere dort, wo besondere Anforderungen an Sicherheit und Verfügbarkeit bestehen – etwa im Finanzwesen, im Gesundheitsbereich, in der öffentlichen Verwaltung und bei kritischen Infrastrukturen. Der Einsatz von SCION ist bereits Realität: Schweizer Banken, Spitäler und Behörden nutzen das System produktiv.

5.1.2.1. Nutzen für den Kanton Zug

Durch eine Mitgliedschaft bei der SCION Association erhält der Kanton Zug exklusiven Zugang zu Wissen, Erfahrung und Expertennetzwerken rund um sichere digitale Kommunikation. Dies unterstützt den Aufbau einer sicheren kantonalen Infrastruktur, stärkt den Innovationsstandort und verbessert die Cybersicherheit im öffentlichen und privaten Sektor. Die Partnerschaft fördert gleichzeitig die Positionierung des Kantons als digitaler Vorreiter und erhöht die Attraktivität für technologiegetriebene Unternehmen.

5.1.2.2. Themenfelder der Zusammenarbeit

Die typische Art der Zusammenarbeit mit der SCION Association und ihren Mitarbeitern und Mitgliedern ist eine langfristige Partnerschaft. Die Mitgliedschaft bietet folgende Vorteile:

- **Zugang zu Wissen, Netzwerken und Ausschüssen**

Die Mitgliedschaft ermöglicht dem Kanton Zug den direkten Zugang zu technischem Wissen, praxisrelevanten Erfahrungen und strategischem Know-how im Bereich sicherer digitaler Kommunikation. Der Kanton kann sich aktiv in die Ausschüsse der SCION Association einbringen, in denen führende Expertinnen und Experten die Weiterentwicklung der SCION-Standards und deren Open-Source-Implementierung steuern. Dadurch lassen sich Interessen und Anforderungen des öffentlichen Sektors frühzeitig einbringen und Innovationen gezielt mitgestalten.

- **Entwicklung eines digitalen Sicherheitskonzepts für den Kanton Zug**

Gemeinsam mit der SCION Association kann ein umfassendes Konzept zur digitalen Sicherheit erarbeitet werden, das sowohl die Verwaltung als auch private Akteure im Kanton adressiert. Potenzielle Anwendungsfelder umfassen:

- Sichere Kommunikation im Homeoffice
- Schutz kritischer Infrastrukturen (z. B. Energie, Wasser, Verkehr)
- Vertrauenswürdige Kommunikation zwischen Behörden und Bevölkerung
- Absicherung von Blaulicht- und Notfallnetzen
- Sichere Einbettung von Blockchain-Infrastrukturen

Ziel ist es, digitale Resilienz zu fördern und konkrete Massnahmen zur Erhöhung der Cyberresistenz umzusetzen.

- **Entwicklung von Richtlinien und Zertifizierungsmodellen**
In Zusammenarbeit mit der SCION Association können Richtlinien für eine sichere digitale Kommunikation im öffentlichen und privaten Sektor im Kanton Zug entstehen. Die Association kann zudem als neutraler Partner bei der Entwicklung und Durchführung eines möglichen kantonalen Zertifizierungsprogramms für digitale Sicherheit mitwirken.
- **Veranstaltungen, Schulungen und Wissenstransfer im Kanton**
Die Partnerschaft ermöglicht dem Kanton Zug die Durchführung gezielter Veranstaltungen, Workshops und Schulungsformate. Diese richten sich sowohl an Verwaltungsmitarbeitende als auch an Unternehmen und IT-Fachleute im Kanton. Ziel ist es, praktisches Wissen zur SCION-Technologie zu vermitteln und konkrete Anwendungsszenarien greifbar zu machen. Der jährliche SCION Day bietet darüber hinaus eine Plattform zum Austausch auf nationaler Ebene.
- **Profilierung als digital kompetenter Standort**
Die sichtbare Einführung von SCION und die damit verbundene Kommunikation stärken das Profil des Kantons Zug als innovativer, zukunftsorientierter Wirtschafts- und Technologiestandort. Der Kanton wird so als Vorreiter im Bereich digitaler Sicherheit wahrgenommen, was die Standortattraktivität erhöht und neue Impulse für Forschung, Entwicklung und Ansiedlung technologischer Unternehmen schafft.

5.2. Partnerschaft mit der Hochschule Luzern (HSLU)

Das Departement Informatik der Hochschule Luzern (HSLU) ist seit 2016 im modernen Campus Zug-Rotkreuz im Suurstoffi-Areal beheimatet. Es zählt heute zu den führenden Bildungs- und Forschungsinstitutionen der Schweiz im Bereich Information & Cyber Security. Besonders in diesem Themenfeld hat sich die HSLU als nationaler Kompetenzträger etabliert. Der Standort bietet eine moderne Infrastruktur, fördert den Austausch zwischen Forschung und Praxis und schafft ein innovatives Umfeld für Studierende, Dozierende und Partnerunternehmen.

Im Mittelpunkt stehen praxisorientierte Bachelor- und Masterstudiengänge mit klarem Fokus auf Sicherheit digitaler Systeme und Infrastrukturen. Ergänzt wird das Angebot durch hoch spezialisierte Weiterbildungsprogramme wie den MAS, DAS oder CAS Cyber Security. Diese befähigen Fach- und Führungskräfte, aktuelle Sicherheits Herausforderungen in Unternehmen, Behörden und kritischen Infrastrukturen fundiert zu bewältigen.

Die Forschung wird durch das Applied Cyber Security Research Lab gebündelt, das sich mit Themen wie Netzwerksicherheit, Sicherheitsarchitektur, digitale Forensik oder Security Governance befasst. Durch die enge Zusammenarbeit mit Wirtschaft und Verwaltung leistet die HSLU einen aktiven Beitrag zur digitalen Resilienz der Schweiz.

Darüber hinaus organisiert das Departement Informatik regelmässig Fachtagungen, Seminare und Konferenzen zu aktuellen Themen der IT- und Cybersicherheit. Diese Veranstaltungen fördern den Wissenstransfer, stärken den fachlichen Austausch und vernetzen Akteure aus Bildung, Forschung, Industrie und öffentlicher Hand.

5.2.1. Nutzen für den Kanton Zug

Die Zusammenarbeit zwischen der **Sicherheitsdirektion** und der **Hochschule Luzern (HSLU)** ist bereits durch zahlreiche erfolgreiche Projekte etabliert. Das KKC will die bestehende Partnerschaft weiter stärken und das gemeinsame Potenzial im Interesse der öffentlichen Sicherheit noch gezielter nutzen. Die Sicherheitsdirektion hat konkrete Kooperationsmöglichkeiten mit der HSLU identifiziert, die ohne Anspruch auf Vollständigkeit im nachfolgenden Abschnitt aufgeführt sind.

5.2.2. Themenfelder der Zusammenarbeit

- **Studentische Projekte (Bachelor und Master)**

Im Rahmen von Bachelor- und Masterarbeiten bearbeiten Studierende praxisnahe sicherheitsrelevante Fragestellungen regionaler Unternehmen oder öffentlicher Einrichtungen. Die Projekte fördern anwendungsorientiertes Lernen und liefern innovative Lösungen, die direkt in die Arbeit des KKC oder den regionalen Kontext einfließen. Besonders hervorzuheben ist das CAS Cyber Investigation & Digital Forensics, das technische und rechtliche Kompetenzen zur Aufklärung von Cyberkriminalität vermittelt. Das CAS Programm wird in enger Zusammenarbeit mit der Zuger Polizei gestaltet.
- **Angewandte bzw. anwendungsorientierte Forschungsprojekte**

Die HSLU bringt ihre umfassende Erfahrung in anwendungsorientierter Forschung ein – insbesondere in den Bereichen Cybersicherheit, Datenschutz, digitale Resilienz und Künstliche Intelligenz. Ihre Forschungsprojekte sind gezielt auf die praktischen Bedürfnisse regionaler KMU ausgerichtet und stärken den Wirkungskreis des KKC.
- **Transfer von Grundlagenkenntnissen in die Praxis**

Mit dem KKC übernimmt die HSLU eine zentrale Vermittlerrolle zwischen akademischer Grundlagenforschung (z. B. ETH) und konkreter Anwendung. So werden neue wissenschaftliche Erkenntnisse, etwa aus der KI-Sicherheitsforschung, gezielt in praxistaugliche Formate für KMU und öffentliche Einrichtungen überführt.
- **Technologie- und Wissenstransfer zur Wirtschaft/Industrie**

Die HSLU organisiert Tagungen, Kongresse sowie Referate, Workshops und Ausstellungen für interessierte Einzelpersonen und KMUs. Im Fokus stehen dabei essenzielle Innovationen, aktuelle Studien und zukünftige Herausforderungen – insbesondere in Themenfeldern, die für das KKC von Bedeutung sind, wie etwa Cybersicherheit, Datenschutz, Künstliche Intelligenz, Digitale Resilienz, Sensibilisierung, Forensik, etc.
- **Zugang zu bestehendem Netzwerk**

Das bestehende Netzwerk der HSLU mit Partnern aus Forschung, Verwaltung, Industrie und Verbänden steht dem KKC offen. Dies erleichtert die Anbahnung neuer Kooperationen, die Gewinnung von Expertinnen und Experten oder die Einbindung in überregionale Initiativen.
- **Ausbau für spezifische kantonale Bedürfnisse**

Die Partnerschaft mit der HSLU schafft gezielt neue Kontakte in der Region, um auf lokale Herausforderungen einzugehen. So kann ein kantonales Sicherheitsökosystem aufgebaut werden, das lokal verankert und national anschlussfähig ist. Die HSLU leistet dabei einen zentralen Beitrag zur inhaltlichen und strukturellen Entwicklung des entstehenden «Cyber Campus» im Kanton Zug.
- **Community-Building**

Das KKC wird durch die HSLU zu einer Plattform für den Austausch und die Vernetzung von sicherheitsinteressierten Personen und KMU's. Durch verschiedene Formate wie Tagungen, Konferenzen, Veranstaltungen, Workshops, etc. entsteht eine dynamische Community, die Wissen teilt, voneinander lernt und gemeinsam an Lösungen arbeitet.
- **Entwicklung zielgruppenspezifischer Angebote**

In enger Kooperation mit dem KKC werden Weiterbildungsformate für unterschiedliche Zielgruppen entwickelt.

 - Awareness, Sensibilisierung: Formate zur Bewusstseinsbildung richten sich sowohl an KMU als auch an die breite Bevölkerung. Die Inhalte reichen von sicheren Passwörtern über Phishing-Prävention bis zur sicheren Nutzung sozialer Medien, welche je nach Zielgruppe angepasst werden.

- Grundlagen-Workshops: Kompakte Formate vermitteln Basiswissen für den digitalen Alltag: etwa zu Backup-Strategien, Software-Updates oder Passwortmanagern. Die didaktische Aufbereitung erfolgt zielgruppen- und praxisgerecht.
- **Wissenschaftliche Begleitung und Unterstützung mit Know-how und Ressourcen**
Expertinnen und Experten der HSLU unterstützen das KKC mit fundiertem Fachwissen im Bereich Cybersecurity. Sie bringen ihre Kenntnisse und Erfahrungen sowohl in die vertiefte Analyse des Handlungsbedarfs als auch in die Konzeption des geplanten KKC ein und leisten zusätzlich Unterstützung mit spezifischem Know-how und personellen sowie infrastrukturellen Ressourcen.
- **Innovationspotenzial durch Künstliche Intelligenz**
Die HSLU verfügt über langjährige Erfahrung in der Entwicklung und Anwendung KI-gestützter Lösungen. Dieses Potenzial wird gezielt genutzt, um das Angebot des KKC innovativ und skalierbar zu gestalten:
 - Intelligente Dialogsysteme (Chatbots) für Bürgerinnen und Bürgern und KMU
 - Gamifizierte Trainingsmodule, die individuelles Lernverhalten fördern
 - Zielgruppenadaptive Inhalte, etwa durch automatisierte Textvereinfachung oder Sprachausgabe
 - etc.

Die Partnerschaft zwischen dem KKC und der HSLU wird sich zu einem zentralen Impulsgeber für zukünftige Innovationen, praxisrelevante Entwicklungen und wirksame Lösungen im Bereich der kantonalen Sicherheitskompetenz entfalten.

6. Finanzielle Auswirkungen und Anpassungen von Leistungsaufträgen

6.1. Umsetzungskonzept

Das Umsetzungskonzept sieht vor, bis zum ersten Halbjahr 2026 den politischen Willensbildungsprozess abzuschliessen. Hiernach soll ohne Verzug mit dem Aufbau des kantonalen Kompetenzzentrums Cybersicherheit begonnen werden. Im Sinne von spürbaren «Quick Wins» für die vulnerablen Zielgruppen sollen in Zusammenarbeit mit Hochschulen und IT-Branchenvertretern schnell Mindeststandards für KMU und zielgruppenspezifische e-Learnings entwickelt werden. Im operativen Betrieb erbringt das Kompetenzzentrum bereits losgelöst von den nachfolgenden Schritten einen erheblichen Mehrwert für die Zielgruppen. Dieser umfasst den Betrieb einer Hotline sowie die täglichen Unterstützungsdienstleistungen, darunter beispielsweise Präventionskampagnen für die Bevölkerung und die Unterstützung von KMU.

Bei Projektbeginn wird das KKC eine verwaltungsinterne Fachstelle der Sicherheitsdirektion sein aber nicht ein Amt. In der Aufbauphase ist eine Symbiose/Zusammenarbeit mit dem Nationalen Testzentrum für Cybersicherheit erstrebenswert, um von Synergien zu profitieren. In der weiteren Entwicklung gilt es, die Schnittstellen des Kompetenzzentrums zur Wissenschaft (insb. ETH und HSLU) und privaten Partnern so zu institutionalisieren und zu bündeln, dass Schritt für Schritt ein interdisziplinärer Zusammenarbeitsraum entsteht. Die dann eingespielte und Mitgliedschaft des Kantons Zug bei ZISC und beim SCION sind zwei wichtige Enabler dieser Entwicklung.

Aufbauend auf dem voll operativen Kompetenzzentrum, welches auch den lebendigen Dreh- und Angelpunkt des Cyber-Forschungsraumes Zug bildet, wird in der letzten Initiativphase mittels gezielter Innovationsförderungen angestrebt, maximale Wachstumsimpulse für den Wirtschaftsraum Zug zu generieren.

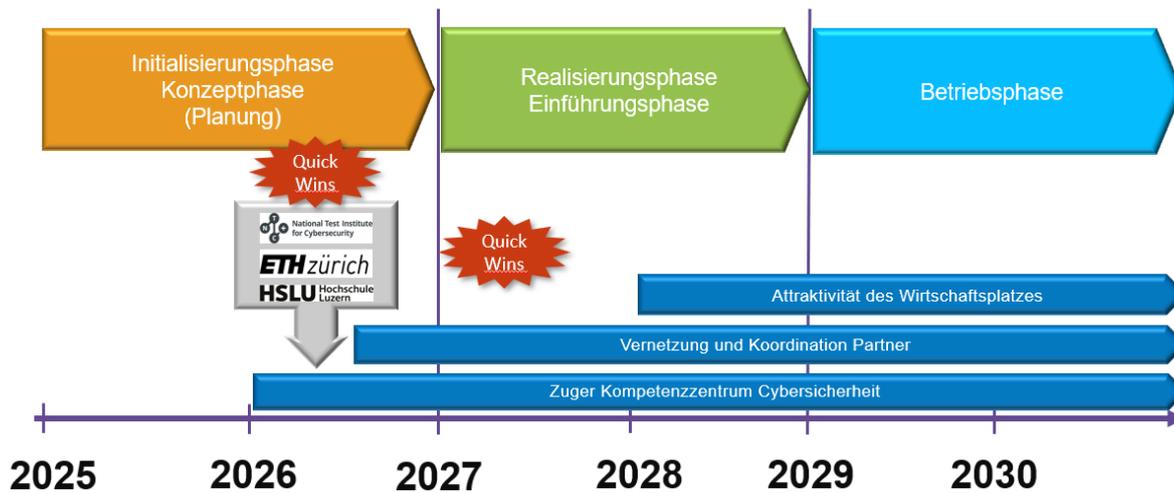


Abbildung 3: Umsetzungskonzept von 2025 - 2030

6.2. Finanzielle Auswirkungen auf den Kanton

Entlang des Umsetzungskonzeptes sollen zwei erfahrene Persönlichkeiten ab dem Jahr 2026 mit dem systematischen Aufbau des kantonalen Kompetenzzentrums beginnen. Bereits ab diesem Jahr und danach in jedem Jahr werden eigene Projekte mit Fokus auf Mehrwert für die vulnerablen Zielgruppen realisiert. Im Regelbetrieb ab 2029 sollen Festangestellte und unterstützende Kräfte im Umfang von zehn Vollzeitstellen das volle Spektrum an Unterstützungsleistungen anbieten.

Ab dem Jahr 2026 setzen erste gezielte Massnahmen zur Förderung eines interdisziplinären Cyber-Forschungsraumes ein. Die Mitgliedschaften des Kantons Zug, vertreten durch das Kantonale Kompetenzzentrum, bei ZISC und bei SCION stellen einen institutionellen und lebhaften Austausch mit der Wissenschaft sicher.

6.2.1. Aufbau- und Betriebskosten Kantonales Kompetenzzentrum Cybersicherheit (Säule 1)

Franken	2025	2026	2027	2028	2029	2030
Personal		2.0 PE / 380 000	7.0 PE / 1 190 000	9.0 PE / 1 520 000	10.0 PE / 1 720 000	10.0 PE / 1 720 000
Betrieb		100 000	200 000	250 000	250 000	250 000
Projekte inkl. KI Unterstützung	100 000	600 000	600 000	600 000	600 000	600 000
Summe	100 000	1 080 000	1'990 000	2 370 000	2 570 000	2 570 000

Tabelle 1: Betriebskosten KKC

6.2.2. Projektförderung (Säule 1)

Franken	2025	2026	2027	2028	2029	2030
Förderung Projekte im Forschungs- und Wirtschaftsraum Zug		2 000 000	2 000 000	4 000 000	4 000 000	2 000 000

Tabelle 2: Förderung Cybersicherheits-Projekte

Nach dem Jahr 2030 sind keine weiteren projektbezogene Förderungen vorgesehen.

6.2.3. Partnerschaften (Säule 2a)

Franken	2025	2026	2027	2028	2029	2030
ETH ZISC-Mitgliedschaft		750 000	750 000	750 000	750 000	750 000
ETH SCION Netzwerk Mitgliedschaft		100 000	100 000	100 000	100 000	100 000
HSLU		500 000	750 000	750 000	750 000	750 000
ITSec4KMU (Verein)		150 000	250 000	250 000	250 000	250 000
Vereine und Organisationen		150 000	150 000	150 000	150 000	150 000
Summe Partnerschaften	0	1 650 000	2 000 000	2 000 000	2 000 000	2 000 000

Tabelle 3: Kosten Partnerschaften

6.2.4. Gesamtkosten (Säule 1 und 2a)

A	Investitionsrechnung	2025	2026	2027	2028
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	100 000			
	bereits geplanter Ertrag				
6.	Gemäss vorliegendem Antrag: effektiver Aufwand	100 000	4 730 000	5 990 000	8 370 000
	effektiver Ertrag				

Tabelle 4: Finanztabelle KRB

Über den Fünfjahreszeitraum von 2026 bis 2030 setzt der Kanton Zug mit rund 34.2 Mio. eine einzigartige Initiative um.

Säulen	Franken
Summe Säule 1: Aufbau und Betrieb	10 580 000
Summe Säule 1: Projektbezogene Förderungen Wirtschafts- und Forschungsraum	14 000 000
Summe Säule 2 (Partnerschaften)	9 650 000
TOTAL 2026 – 2030	34 230 000

Tabelle 5: Summen pro Säule

6.3. Finanzierung aus Mehrerträgen der OECD-Mindeststeuer

Der Kanton Zug ist ein attraktiver Wirtschaftsstandort, der sich durch Stabilität, niedrige Steuern, qualifizierte Fachkräfte, gute Erreichbarkeit, Internationalität und hohe Lebensqualität auszeichnet. Er verfügt über eine effiziente Verwaltung, hochwertige Dienstleistungen und eine ausgezeichnete Infrastruktur, was ihn sowohl national als auch international wettbewerbsfähig macht. Die Einführung der OECD-Mindeststeuer, die eine globale Mindestbesteuerung für Unternehmen vorsieht, bedroht diese Attraktivität. Um diesen potenziellen Verlust an Attraktivität zu kompensieren, ist vorgesehen, die zusätzlichen Einnahmen aus der Mindeststeuer vollständig an Bevölkerung und Wirtschaft zurückzugeben und in Massnahmen zur Standortförderung zu investieren. Das Massnahmenmodell umfasst drei Themenfelder: Soziales (1),

Infrastruktur/Innovation (2) sowie Förderbeiträge an Unternehmen (3). Diese Strategie soll sicherstellen, dass Zug auch weiterhin wettbewerbsfähig bleibt und seine Rolle als attraktiver Wirtschafts- und Wohnstandort beibehält.

Die Beiträge für Massnahmen im ersten und zweiten Themenfeld sind als sogenannte Fixbeiträge ausgestaltet. Genügen die Mehrerträge nicht, um die Fixbeiträge zu decken, wird der Restbetrag aus der Erfolgsrechnung bezahlt.

Die Finanzierung der Konzeption, Umsetzung und des Betriebs eines kantonalen Kompetenzzentrums für Cybersicherheit (KKC) sowie einer strategischen Partnerschaft mit der Eidgenössischen Technischen Hochschule Zürich (ETH) und der Hochschule Luzern (HSLU) im Bereich Cybersicherheit soll mit einem Fixbetrag dem zweiten Themenfeld zugeordnet werden.

6.4. Finanzielle Auswirkungen auf die Gemeinden

Diese Vorlage hat keine finanziellen Auswirkungen auf die Gemeinden.

6.5. Anpassungen von Leistungsaufträgen

Diese Vorlage hat keine unmittelbaren Anpassungen von Leistungsaufträgen zur Folge. Mit Aufnahme des Betriebes des Kompetenzzentrums für Cybersicherheit sind jedoch zukünftige Anpassungen möglich.

6.6. Mehrwert für den Kanton Zug

Mit dieser Cybersicherheitsinitiative schafft der Kanton Zug ein schweizweit einzigartiges Kompetenzzentrum, das nicht nur die Bevölkerung und KMU aktiv vor Cyberbedrohungen schützt, sondern zugleich den Wirtschaftsstandort stärkt, Innovation fördert, hochwertige Arbeitsplätze schafft und Zug als führenden Standort für digitale Sicherheit national positioniert. Dabei entstehen Ansiedelungsimpulse für hoch innovative Unternehmen, mit entsprechendem Steuersubstrat als zusätzlichem volkswirtschaftlichem Nutzen. Dies führt sowohl zu einem qualitativen Return on Investment in Form von Sicherheit, Resilienz und Standortattraktivität als auch zu einem quantitativen Return on Investment durch zusätzliche Steuereinnahmen.

7. Zeitplan

28. August 2025	Kantonsrat, Kommissionsbestellung
Sept. – Okt. 2025	Kommissionssitzung(en)
November 2025	Kommissionsbericht
10. Dezember 2025	Beratung Staatswirtschaftskommission
Dezember 2025	Bericht Staatswirtschaftskommission
26. Februar 2026	Kantonsrat, 1. Lesung
26. März 2026	Kantonsrat, 2. Lesung
2. April 2026	Publikation Amtsblatt
1. Juni 2026	Ablauf Referendumsfrist
4. Juni	Publikation Amtsblatt (ohne Volksabstimmung)
5. Juni 2026	Inkrafttreten (ohne Volksabstimmung)
27. September 2026	Allfällige Volksabstimmung
1. Oktober 2026	Publikation Amtsblatt
2. Oktober 2026	Inkrafttreten (bei Volksabstimmung)

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

8. Antrag

Gestützt auf die vorstehenden Ausführungen beantragen wir Ihnen, auf die Vorlage Nr. 3957.2 - 18265 einzutreten und ihr zuzustimmen.

Zug, 8. Juli 2025

Mit vorzüglicher Hochachtung
Regierungsrat des Kantons Zug

Der Landammann: Andreas Hostettler

Der Landschreiber: Tobias Moser