Stadt Luzern
Stadtrat
Hirschengraben 17
6002 Luzern
www.stadtrat.stadtluzern.ch

T 041 208 82 11
stadtrat@stadtluzern.ch

Bericht und Antrag 36
an den Grossen Stadtrat von Luzern

Aufbau Security-Operations-Team

– Zusätzliche Stellen und Dienstleistungen
– Sonder- und Nachtragskredit

Vom Stadtrat zuhanden des Grossen Stadtrates verabschiedet mit StB 658 vom 18. September 2024

Vom Grossen Stadtrat beschlossen am 28. November 2024

Politische und strategische Referenz

Legislaturprogramm 2022–2025

Legislaturziel Z2.2: Datenmanagement: Die Stadt Luzern bewirtschaftet und nutzt ihre Daten sicher, effizient und zielorientiert.

Massnahme M2.2c: Die Stadt Luzern stellt bis 2023 innerhalb der Stadtverwaltung die notwendigen Ressourcen und Kompetenzen für Cybersicherheit (Datensicherheit und Datenschutz) sicher.

In Kürze

Die städtische Dienstabteilung Zentrale Informatikdienste (ZID) ist gemäss politischem Leistungsauftrag die zentrale ICT-Dienstleisterin für die Verwaltung und die Volksschule der Stadt Luzern (Schulinformatik) sowie für die Tochtergesellschaften und nahestehenden Organisationen aus dem öffentlichen Bereich (Pensionskasse Stadt Luzern, Viva Luzern AG, ZSOpilatus). Damit ist sie auch für den sicheren Betrieb aller Informationssysteme zuständig, unabhängig davon, ob diese intern erbracht oder als Service extern bezogen werden (insbesondere Cloud Services).

In den letzten Jahren und Monaten haben Angriffsversuche gegen die städtische IT-Infrastruktur deutlich zugenommen. Das Risiko, dass die Stadt Luzern Opfer einer Cyberattacke wird, ist als hoch einzustufen. Die ZID unternimmt bereits heute im Rahmen ihrer Möglichkeiten grosse Anstrengungen, um die Wahrscheinlichkeit und die Tragweite eines Angriffs so tief wie möglich zu halten. Die ZID arbeitet in diesen Themengebieten eng mit der Fachstelle für digitale Sicherheit und Privatsphäre (FDSP) der Dienstabteilung Digital (DIG) zusammen.

Die FDSP und die ZID orientieren sich in der Ausgestaltung von Massnahmen im Bereich der Cybersicherheit am internationalen und branchenübergreifenden Standard NIST CSF. Die ZID verfügt neben dem auftragsgemässen Betrieb der Fachanwendungen und ICT-Systeme sowie der Mitwirkung in Digitalisierungsprojekten jedoch nur über sehr begrenzte Ressourcen und Fähigkeiten, um Cyberattacken zu vermeiden, zu erkennen und schnell darauf zu reagieren. Es fehlen fachliche Fähigkeiten und technische Systeme, um den sich ständig weiterentwickelnden Angriffen und sozialen Manipulationen wirksam entgegenzutreten.

Die ZID könnte nicht gewährleisten, dass auf erkannte Angriffe jederzeit und unmittelbar reagiert wird. Die dafür erforderlichen personellen und fachlichen Ressourcen fehlen und können mit den zur Verfügung stehenden Stellen nicht abgedeckt werden.

Gemäss vorliegendem Bericht und Antrag (B+A) sind bei der ZID zusätzliche 400 Stellenprozent notwendig, um die neuen Aufgabenbereiche zu verstärken, die bisher bei der Stadt Luzern nicht ausreichend adressiert sind. Für die Sicherstellung der Rund-um-die-Uhr-Überwachung, -Erkennung und -Reaktion auf Vorfälle wird die Zusammenarbeit mit einem Cyber Defence Center (CDC), einem Team von externen Cybersicherheitsfachleuten, gesucht.

Mit vorliegendem Bericht und Antrag beantragt der Stadtrat den dazu notwendigen Sonderkredit von 9,482 Mio. Franken für die Dauer von 10 Jahren sowie einen Nachtragskredit von 0,782 Mio. Franken für die Personal- und Betriebskosten für das Budgetjahr 2025.

Inhaltsverzeichnis

Seite

Der Stadtrat von Luzern an den Grossen Stadtrat von Luzern

Sehr geehrter Herr Präsident
Sehr geehrte Mitglieder des Grossen Stadtrates

1 Ausgangslage

1.1 Bedrohungsbild

Cyberkriminalität stellt in ihren verschiedenen Formen eine zunehmende Bedrohung dar. Cyberangriffe und Online-Betrug sind komplexe Straftaten und manifestieren sich in unterschiedlichen Formen. Die Anpassungsfähigkeit der Täterschaft an neue Technologien und gesellschaftliche Entwicklungen ist hoch, Zusammenarbeit und Spezialisierung nehmen kontinuierlich zu. Cyberkriminalität hat ein immer weiter reichendes Ausmass und fügt Einzelpersonen, öffentlichen und privaten Organisationen sowie der Wirtschaft schweren Schaden zu.[1]

Beim Bundesamt für Cybersicherheit (BACS) gehen wöchentlich 1'000 bis 2'500 Meldungen zu Cyberbedrohungen ein.[2] Täglich werden Angriffe auf verschiedene Organisationen und Behörden publik gemacht. Die Komplexität der Angriffe steigt stetig. Die Angreifenden analysieren die generelle Verteidigungslage der potenziellen Opfer und passen ihre Angriffsvektoren kontinuierlich an die aktuellen Gegebenheiten an. Durch erfolgreiche Angriffe mit entsprechenden Lösegeldzahlungen steigen zudem die finanziellen, personellen und technischen Ressourcen und Möglichkeiten der Angreifenden stark an.

Besonders die Fälle von Angriffen mit Ransomware nehmen stark zu. Dabei werden die Daten der Opfer zuerst abgezogen und danach verschlüsselt. Das Opfer wird mit Lösegeldforderungen erpresst. Falls die Geldforderungen nicht erfüllt werden, droht die Publikation der gestohlenen und ein Verlust der verschlüsselten Daten. Da die Angreifenden bei dieser Art von Angriffen meistens in der Lage sind, sich erhöhte Berechtigungen auf sämtliche Systeme zu verschaffen, sind danach enorm aufwendige und kostspielige Prozesse zur Wiederherstellung der IT-Systeme und der Daten notwendig.

Diskutiert wurden in der Stadt Luzern in jüngster Zeit die Cyberattacke gegen die Verkehrsbetriebe Luzern AG (vbl) oder die Attacke gegen einen deutschen IT-Dienstleister, in dessen Folge über 70 Gemeindeverwaltungen über Monate hinweg ohne funktionierende Informatiksysteme auskommen mussten.[3] Ebenso folgen immer wieder breit angelegte Angriffswellen, die weltweit zu grossen Schäden führen – auch in der Schweiz. Zu den bekanntesten Opfern zählen hierzulande die SBB, die Universität Zürich, die NZZ, die AMAG, die Emil Frey AG, aber auch diverse Gemeinden und einige Kantone.

[1] Internet organized crime threat assessment (IOCTA) 2023, European Union Agency for Law Enforcement Cooperation (Europol).
[2] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/aktuelle-zahlen.html.
[3] https://notfallseite.sit.nrw/aktuelle-meldungen.

Die Angriffsversuche gegen die städtische IT-Infrastruktur haben deutlich zugenommen. Sogenannte Phishing-E-Mails stellen nach wie vor den primären Angriffsvektor von Cyberattacken dar und sind deshalb so erfolgreich, weil sich der Angriff gegen die «Schwachstelle Mensch» richtet. Jährlich werden Hunderte bis Tausende von Phishing-E-Mails durch die Sicherheitsinfrastruktur der ZID abgewehrt oder von aufmerksamen Mitarbeitenden gemeldet, bevor es zu einem wesentlichen Schaden kommen kann. Die aktuellen Zahlen der Stadtverwaltung stellen sich folgendermassen dar:

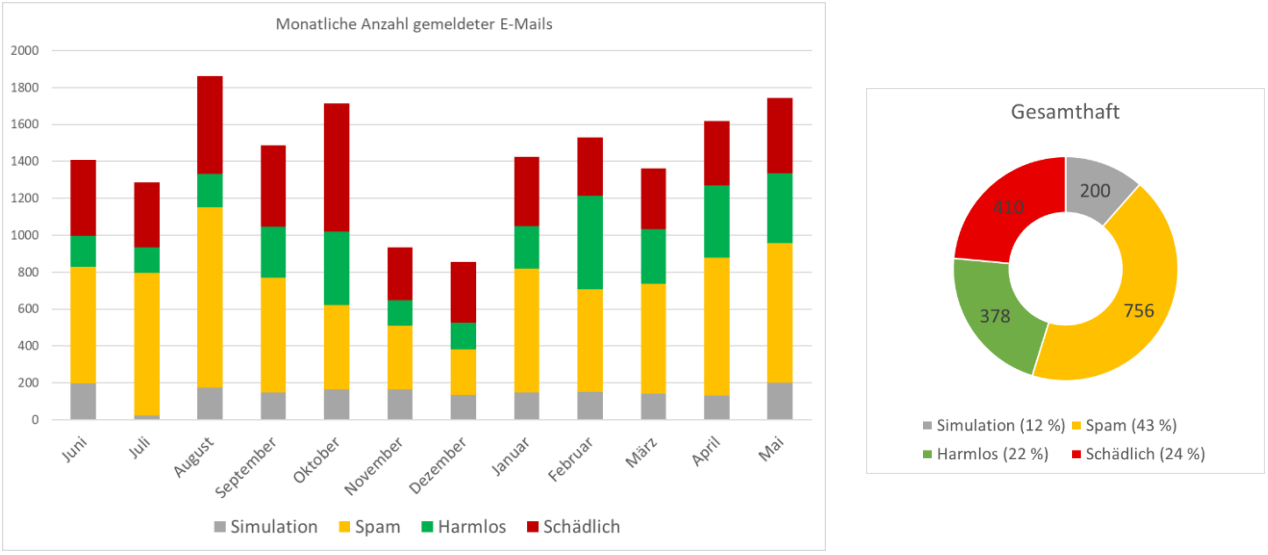

Abb. 1: Anzahl gemeldete E-Mails mit Phishing-Verdacht zwischen Juni 2023 und Mai 2024

Bemerkenswert ist diesbezüglich, dass monatlich zwischen 300 und 500 potenziell schädliche E-Mails gemeldet werden, die trotz der technischen Vorkehrungen im Posteingang der Mitarbeitenden landen. Anhand der Messungen aus den Phishing-Simulationen ist bei den oben dargestellten Werten davon auszugehen, dass nur etwa 50 Prozent der potenziell schädlichen E-Mails gemeldet werden. Das heisst, dass monatlich schätzungsweise 600 bis 1'000 potenziell schädliche E-Mails in den Postfächern der Stadtverwaltung eintreffen.

Des Weiteren zeigen die kontinuierlich stattfindenden Simulationen, dass sich durchschnittlich etwa 10 Prozent der Mitarbeitenden bei Phishing-E-Mails falsch verhalten, indem potenziell gefährliche Hyperlinks angeklickt werden, Passwörter bekannt gegeben oder Dateianhänge geöffnet werden, die Schadsoftware enthalten können. Hochgerechnet bedeutet das, dass praktisch jeden Tag mit einer Kompromittierung der Informatik-Infrastruktur gerechnet werden muss. Wenn diese Ereignisse nicht rechtzeitig erkannt werden, nicht schnell und wirksam darauf reagiert wird und die technischen Hilfsmittel dazu unzureichend sind, wird eine Cyberattacke früher oder später erfolgreich sein. Speziell in diesem Bereich hat sich die Situation zugespitzt, und es fehlen die notwendigen Ressourcen und Fähigkeiten (vgl. Kapitel 4 und 5).

Erfolgreiche Cyberangriffe führen in der Regel dazu, dass sensible Datenbestände gestohlen, unbemerkt manipuliert, gelöscht oder verschlüsselt werden. Insbesondere bei der Verschlüsselung durch sogenannte Ransomware werden von den Angreifenden hohe Geldbeträge erpresst, um die Verschlüsselung rückgängig zu machen. Bei den aktuellen Angriffsmustern werden zudem sensible Daten gestohlen, und es wird damit gedroht, diese zu veröffentlichen oder an andere kriminelle Akteure zu verkaufen, falls dem Erpressungsversuch nicht nachgekommen wird.

Neben den direkten finanziellen Auswirkungen einer Erpressung schlagen vor allem die Kosten der Wiederherstellung von kompromittierten Daten und Systemen zu Buche. Zudem führt eine solche Attacke zu einer massiven Beeinträchtigung der Verwaltungstätigkeiten, was einer Nichterfüllung des Leistungsauftrags gleichkommt. Dies wiederum führt zu einem Vertrauens- und Reputationsverlust bei der Bevölkerung.

Das Risiko, dass die Stadt Luzern Opfer einer Cyberattacke wird, ist folglich als hoch einzustufen. Die Stadt unternimmt bereits heute im Rahmen ihrer Möglichkeiten grosse Anstrengungen, um die Wahrscheinlichkeit und die Tragweite eines Angriffs so tief wie möglich zu halten. Dabei kommen sowohl technische, organisatorische wie auch Sensibilisierungsmassnahmen zur Anwendung. Das Sicherheitsdispositiv der Stadt Luzern muss jedoch ständig an die aktuellen Bedrohungen angepasst werden.

1.2 Zunahme des Mengengerüstes und der technischen Komplexität

Im Zuge der Digitalisierung der Verwaltung wie auch des Unterrichts an den Volksschulen hat sich das Mengengerüst der betreuten Anwendungen und Systeme in den letzten Jahren vervielfacht. Die Systeme werden komplexer – auch im Zusammenhang mit Cloud-Anwendungen – und die Betreuung intensiver.

Folgende Tabelle zeigt das heutige Mengengerüst der durch die ZID betriebenen Systeme und Anwendungen:

Endgeräte	Stadt Luzern	Volksschulen	VIVA Luzern AG	**Gesamt**
Notebooks	1’108	4’928	358	**6’394**
Desktop-PCs	145	32	68	**245**
Tablets	28	310	275	**613**
Smartphones	55	16		**66**
Smartphones gemanaged (BYOD)[4]	520	–	108	**628**
Applikationen				
Fachanwendungen On-premises[5]	74	–	17	**91**
Fachanwendungen Cloud (SaaS)[6]	46	1	1	**48**
Basisapplikationen (z. B. MS Office, Browser, Telefonie)	25	1	10	**43**
Kleine Applikationen (individuelle Anwendungen wie CAD, Photoshop, Designer, Viewer usw.)	113	27	10	**160**
Unterstützungsprogramme (Software zur Betriebsunterstützung, z. B. Scanner-Software, Sicherstellungssoftware, Auswertungssoftware usw.)	65	2	2	**69**
Datacenter				
Serversysteme	301	14	29	**343**
Sicherheitssysteme	8	–	–	**8**
Netzwerkkomponenten	30	–	–	**30**

[4] BYOD steht für «Bring Your Own Device» und bedeutet «Bring dein eigenes Gerät (mit)». Mitarbeitende bringen ihre privaten mobilen Endgeräte (Smartphones, Tablets) zum Arbeiten mit. Diese werden bedarfsgerecht in die Systeme der Verwaltung integriert.
[5] On-premises: Die Anwendung wird in den Rechenzentren der Stadt Luzern installiert und betrieben.
[6] SaaS: Software-as-a-Service bezeichnet die Bereitstellung von Anwendungssoftware aus der Cloud. Die mit der Bereitstellung verbundenen Dienstleistungen werden durch spezialisierte Anbieter über das Internet offeriert und erbracht. Die Bereitstellung erfolgt aus privaten Datacentern der Anbieter oder aus öffentlichen Rechenzentren.

Netzwerk	Stadt Luzern	Volksschulen	VIVA Luzern AG	**Gesamt**
Vernetzte Standorte	51	40	10	**101**
Netzwerkkomponenten (Switches, Routers usw.)	138	276	90	**504**
Netzwerkkomponenten kabellos (WLAN-Access-Points)	525	993	611	**2'129**

Tab. 1: Mengengerüste nach Kundenstruktur

Der Aufbau des kabellosen Netzwerkes der Volksschulen (seit 2017) und der Verwaltung (seit 2018) parallel zum bereits bestehenden kabelgebundenen Netzwerk führt zu Mehraufwand im Betrieb und in der Aufrechterhaltung der Sicherheit. Exemplarisch zeigt sich der steigende Betriebsaufwand ebenfalls an der Anzahl der durch die ZID bereitgestellten und verwalteten Endgeräte in der Verwaltung und der Volksschule.

Betriebsjahr	PCs Verwaltung	Notebooks Verwaltung	Notebooks Volksschule
2018	1090	35	1150
2019	1010	160	1882
2020	1027	180	1900
2021	199	955	2995
2022	171	1066	4662
2023	145	1108	4928

Tab. 2: Anzahl Endgeräte seit 2018

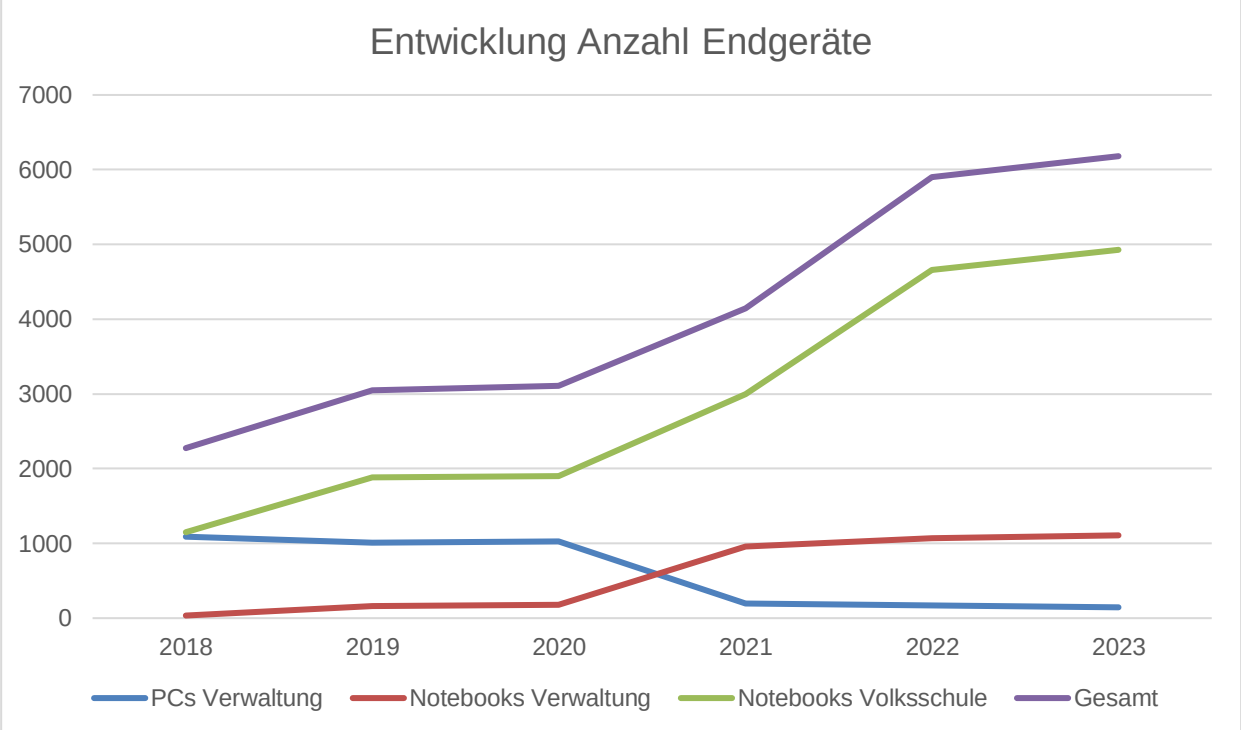

Abb. 2: Entwicklung der Anzahl Endgeräte seit 2018

Trotz hohem Automatisierungsgrad, dem Einsatz moderner Werkzeuge für das Gerätemanagement und Optimierung der Prozesse führt das Wachstum zu erhöhtem Ressourcenbedarf im Betrieb.

1.3 Erhöhtes Projektaufkommen

Die Digitalstrategie der Stadt Luzern (B+A 1/2019: «Stadt Luzern digital» und B+A 29/2021: «Digitalstrategie und Smart City Luzern») und die damit verbundenen Investitionen in personelle Ressourcen der Dienstabteilung Digital und der anderen Dienstabteilungen führen erfreulicherweise zu einer steigenden Anzahl von Mehrwertprojekten. Die Mitarbeitenden der ZID sind mit verschiedenen Aufgaben in die Projekte direkt eingebunden. Sie übernehmen die technische Projektleitung, konzeptionieren den zukünftigen Betrieb der Applikationen und Systeme, erstellen und verhandeln die Verträge und Lizenzvereinbarungen, bauen die notwendige Infrastruktur auf, führen die Systeme ein, erstellen die erforderlichen Services und nehmen diese in Betrieb.

Geschäftsjahr	Anzahl gestartete Mehrwertprojekte	Geleistete Projektstunden Mehrwertprojekte
2018	10	3’759
2019	18	4’118
2020	14	5’398
2021	13	5’491
2022	17	6’925
2023	29	6’355

Tab. 3: Anzahl gestarteter Mehrwertprojekte und Projektstunden pro Jahr

Die Zunahme der Anzahl Digitalisierungsprojekte ist bei der ZID spürbar. Immer häufiger werden Projekte der Verwaltung und von Drittkunden zeitlich verzögert oder können gar nicht gestartet werden, da die Ressourcen der ZID nicht zur Verfügung stehen. Die Mitarbeitenden der ZID können maximal 15 Prozent ihrer Arbeitszeit für Projektarbeit aufwenden. 85 Prozent ihrer täglichen Arbeit setzen sie für den operativen Betrieb der Anwendungen, der Systeme und der Kommunikationsnetzwerke ein. Diese Situation ist unbefriedigend und führt dazu, dass Innovationen immer häufiger gar nicht oder erst verspätet umgesetzt werden können. Für das Geschäftsjahr 2024 sind 8’000 Projektstunden für Mehrwertprojekte budgetiert.

1.4 Zunahme der Investitionen

Die Digitalisierung sowohl der Verwaltung wie auch der Volksschule führt zu erhöhtem Investitionsbedarf. Die zunehmende Anzahl neuer Fachanwendungen hat direkten Einfluss auf die notwendige Infrastruktur.

Geschäftsjahr	Infrastrukturprojekte Franken	Mehrwertprojekte Franken
2018	1’278’335.60	938’529.95
2019	2’475’537.60	939’711.65
2020	1’776’746.76	1’044’158.10
2021	2’323’208.29	1’622’763.33
2022	1’556’908.32	2’287’579.34
2023	2’164’581.50	2’064’119.09

Tab. 4: Summe der Investitionen seit 2018

Eine Zunahme der Investitionen für zusätzliche Anwendungen, Systeme und Endgeräte führt unweigerlich zu höherem Betriebsaufwand.

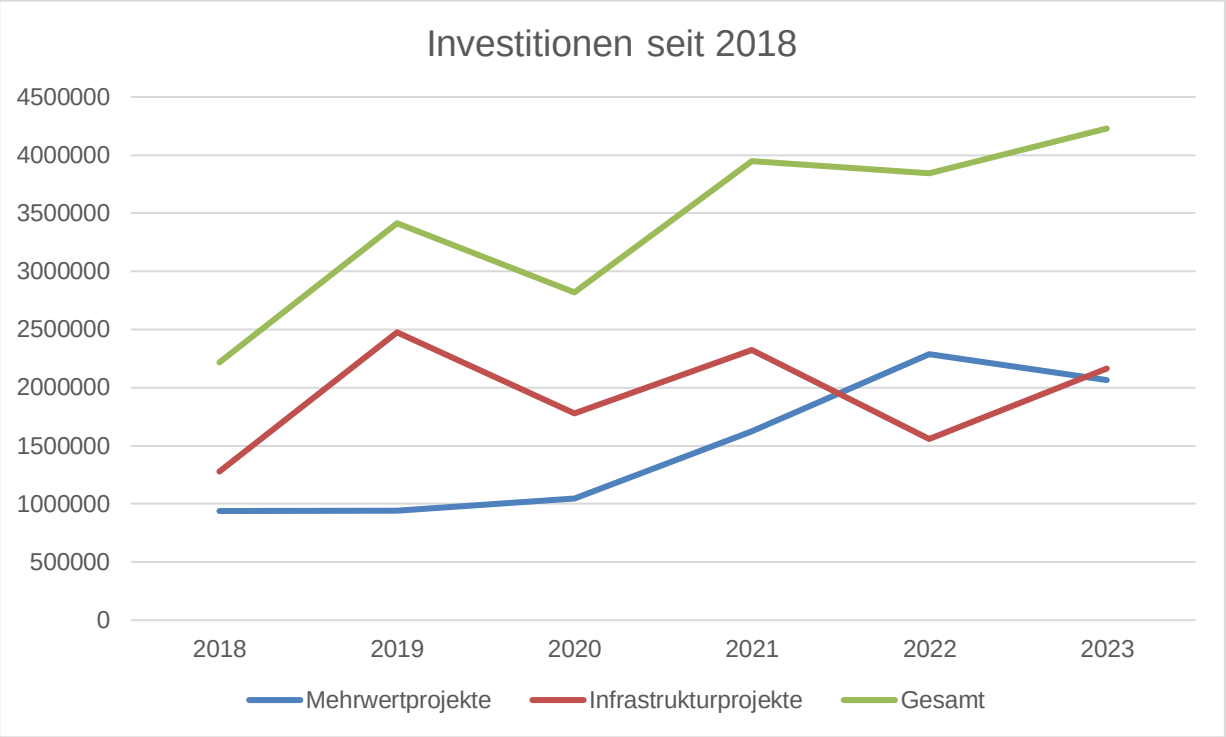

Abb. 3: Zunahme der Investitionen seit 2018

2 Zielsetzungen

Mit dem vorliegenden Bericht und Antrag werden die nachfolgend beschriebenen Ziele verfolgt:

Auf übergeordneter Ebene geht es darum,
– die Interessen der Bevölkerung bezüglich der Verfügbarkeit, Integrität und Vertraulichkeit der Daten vor Cyberattacken zu schützen und
– die Resilienz der Stadtverwaltung für den Umgang mit Cyberrisiken umfassend zu erhöhen.

Bezogen auf den konkreten Antrag bedeutet das,
– innerhalb der ZID die Voraussetzungen für eine schnelle und wirksame Erkennung von und Reaktion auf Cyberattacken, gemäss dem gesetzlichen Auftrag[7], zu schaffen,
– die hierzu erforderlichen finanziellen und personellen Ressourcen bereitzustellen und
– die dringend notwendigen Fähigkeiten im Bereich der Cybersicherheit aufzubauen und dauerhaft sicherzustellen.

[7] Art. 23 lit. f Informatik- und Digitalverordnung vom 11. März 2020 (sRSL 0.6.1.1.2).

3 Rahmenbedingungen

3.1 Rechtliche und politische Rahmenbedingungen

Die Informationssicherheit (IS) der Stadt Luzern hat der Stadtrat in der Weisung «Digitale Sicherheit und Privatsphäre» (Informationssicherheitspolitik) geregelt. Neben den Grundsätzen und Zielen definiert die Weisung auch die Verantwortlichkeiten für die digitale Sicherheit und die Privatsphäre der Stadt Luzern. Die Informatik- und Digitalverordnung vom 11. März 2020 (sRSL 0.6.1.1.2) regelt die operative Umsetzung.

Der Stadtrat trägt die oberste Verantwortung für die digitale Sicherheit und die Privatsphäre und die zur Kenntnis gebrachten Restrisiken. Er stellt sicher, dass die Ziele, Grundsätze und Verantwortlichkeiten bezüglich digitaler Sicherheit und Privatsphäre festgelegt und mit der strategischen Ausrichtung der Stadtverwaltung vereinbar sind.

Das Thema Cybersicherheit ist auch Teil der politischen Diskussion der Stadt Luzern geworden. Am 4. August 2023 hat Benjamin Gross im Namen der SP-Fraktion die Interpellation 284: «Gewährleistung der Cybersicherheit» eingereicht. Der Stadtrat führte in der Antwort aus, dass die Stadt Luzern kurzfristig die technischen und organisatorischen Fähigkeiten zur systematischen und umfassenden Identifikation von Schwachstellen und Bedrohungen aufbauen muss. Er erachtet es aufgrund der Grösse und Heterogenität der Stadtverwaltung, der Volksschule sowie Viva Luzern AG als unumgänglich, diese Fähigkeiten im Sinne eines Security-Operations-Teams[8] zeitnah aufzubauen.

3.2 Fachstelle digitale Sicherheit und Privatsphäre (FDSP)

Die FDSP ist in Zusammenarbeit mit den Leistungserbringerinnen (Dienstabteilung Zentrale Informatikdienste [ZID], Geoinformationszentrum [GIS]) für die strategische und taktische Informationssicherheit und den Datenschutz der Stadt Luzern verantwortlich. Eine wesentliche Grundlage für ihre Tätigkeiten ist neben der kantonalen Datenschutzgesetzgebung die Norm ISO/IEC 27001[9]. Die FDSP definiert technische und organisatorische Sicherheitsstandards, die in städtischen Projekten und im Informatikbetrieb einzuhalten sind. Sie kontrolliert deren Umsetzung und Wirksamkeit und entscheidet über Ausnahmen und Abweichungen. Ausserdem informiert, sensibilisiert und schult sie die Mitarbeitenden und weitere Anspruchsgruppen punkto bestehender Risiken sowie einzuhaltender Datenschutz- und Sicherheitsmassnahmen, insbesondere auch bezüglich des Umgangs mit Phishing-E-Mails.

Die FDSP ist der Bildungsdirektion, Dienstabteilung Digital, zugeordnet und besteht heute aus dem Leiter (CISO), der Beauftragten für Digitale Privatsphäre (Datenschutz) sowie dem Beauftragten für Digitale Sicherheit. Sie ist mit 230 Stellenprozent dotiert.

3.3 Zentrale Informatikdienste (ZID)

Die Dienstabteilung ZID ist gemäss politischem Leistungsauftrag die zentrale ICT-Dienstleisterin für die Verwaltung und die Volksschule der Stadt Luzern (Schulinformatik) sowie für die Tochtergesellschaften und nahestehenden Organisationen aus dem öffentlichen Bereich (Pensionskasse der Stadt Luzern PKSL; Viva Luzern AG; Zivilschutzorganisation Horw, Kriens und Luzern ZSOpilatus). Sie ist verantwortlich für den sicheren Betrieb aller Informationssysteme, unabhängig davon, ob diese intern betrieben oder

[8] Ein Security-Operations-Team ist ein unternehmensinternes, externes oder gemischtes (hybrides) Team von IT-Sicherheitsexpertinnen und -experten. Die Hauptaufgabe des Teams besteht darin, den Betrieb der gesamten IT-Infrastruktur eines Unternehmens oder einer Verwaltung rund um die Uhr zu überwachen, Angriffe in Echtzeit zu erkennen und zu bekämpfen.
[9] Die ISO/IEC 27001 ist eine internationale Norm für Informationssicherheits-Managementsysteme (ISMS). Sie bietet Unternehmen jeder Grösse Orientierung für die Planung, Umsetzung, Überwachung und Optimierung der Informationssicherheit.

als Service extern bezogen werden (insbesondere Cloud Services). Sie definiert die IT-Sicherheitsarchitektur, gewährleistet die operative digitale Sicherheit im Betrieb und in IT-Projekten und koordiniert sich diesbezüglich mit der FDSP. Zudem ist sie dafür verantwortlich, dass technische Schwachstellen identifiziert werden und deren Behebung überwacht wird.
Die ZID ist nach Funktionen organisiert und in fünf Bereiche aufgeteilt:

Applikations-Services (AS)
Die Applikations-Managerinnen und -Manager betreuen und koordinieren die Beschaffung, die Installation und den Betrieb der in den Rechenzentren der Stadt Luzern oder extern (Cloud Services) betriebenen Fachapplikationen. Als Bindeglied zwischen den Anwendenden und den Lieferanten der Lösungen kümmern sie sich um einwandfreie Dienstleistungsvereinbarungen, das Lizenzmanagement sowie Support- und Wartungsverträge.

Infrastruktur-Services (IS)
Der Betrieb der gesamten Infrastruktur der beiden städtischen Rechenzentren sowie des Daten- und Kommunikationsnetzwerks obliegt den Mitarbeitenden des Bereichs Infrastruktur-Services. Sie sind zuständig für den reibungslosen Bau, den Betrieb und die Weiterentwicklung der Basisdienste. Dazu gehören unter anderem die Virtualisierungsplattformen, das Endgerätemanagement, alle Speichersysteme, die E-Mail-Dienste, die Druckerdienste und das Kommunikationsnetzwerk (kabelgebunden und kabellos). Sie sind ebenfalls verantwortlich für den Betrieb der Sicherheitssysteme wie beispielsweise Firewalls, Systeme für den sicheren Zugriff aus dem Internet oder Antivirus-Software.

Kundenbetreuung (KB)
Die Kundenbetreuung ist die zentrale Anlaufstelle für sämtliche Anfragen der Anwendenden. Die Mitarbeitenden betreiben den Service Desk (erste Anlaufstelle für Unterstützung bei allen ICT-Problemen) und leisten falls notwendig Vor-Ort-Support. Gleichzeitig unterstützen sie die Kundschaft in allen Prozessen der ICT-Logistik.

Projekt-Services (PS)
Die IT-Projektleitenden begleiten sämtliche IT- und Digitalisierungsprojekte der Kundschaft und unterstützen dabei die Projektleitenden aus den Fachabteilungen. Zudem führen sie IT-Infrastruktur-Projekte zur Einführung stadtweiter Lösungen oder zur Erneuerung bestehender Services und Systeme durch.

Zentrale Services (ZS)
Der Bereich Zentrale Services ist für die administrativen Prozesse der Abteilung und die Leistungsverrechnung an die Kundschaft zuständig. Das IT-Verarbeitungszentrum erledigt zudem alle Druck- und Kopieraufträge, während der Postdienst den internen und externen Postverkehr der Stadtverwaltung sicherstellt.

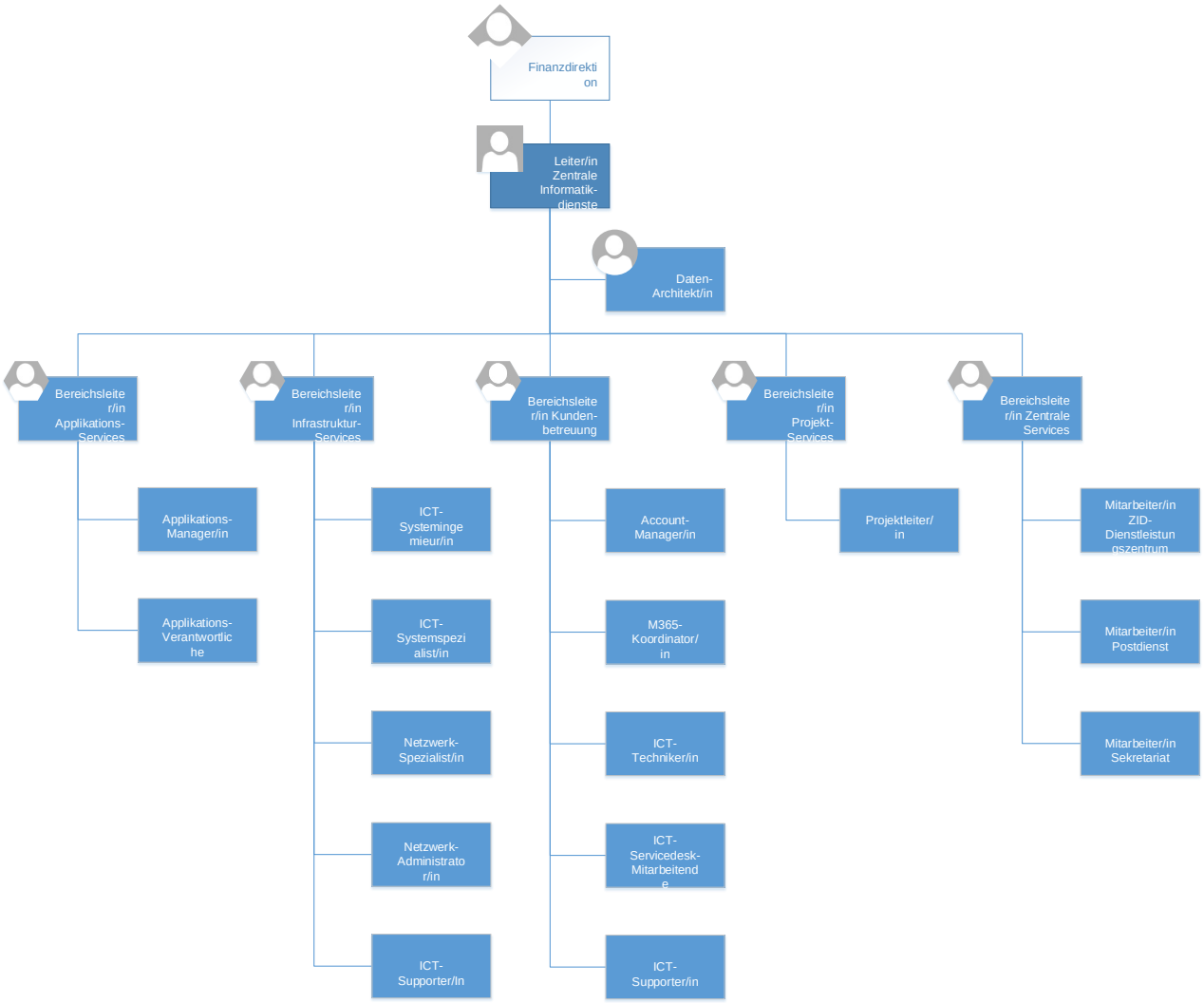

Abb. 4: Organigramm Dienstabteilung Zentrale Informatikdienste

3.4 Fachteam «Security Operations»

Seit Anfang 2023 besteht innerhalb der ZID und der DIG ein interdisziplinäres Fachteam «Security Operations». Dieses nimmt in Zusammenarbeit mit der Fachstelle FDSP operative Aufgaben im Bereich Cybersicherheit wahr.

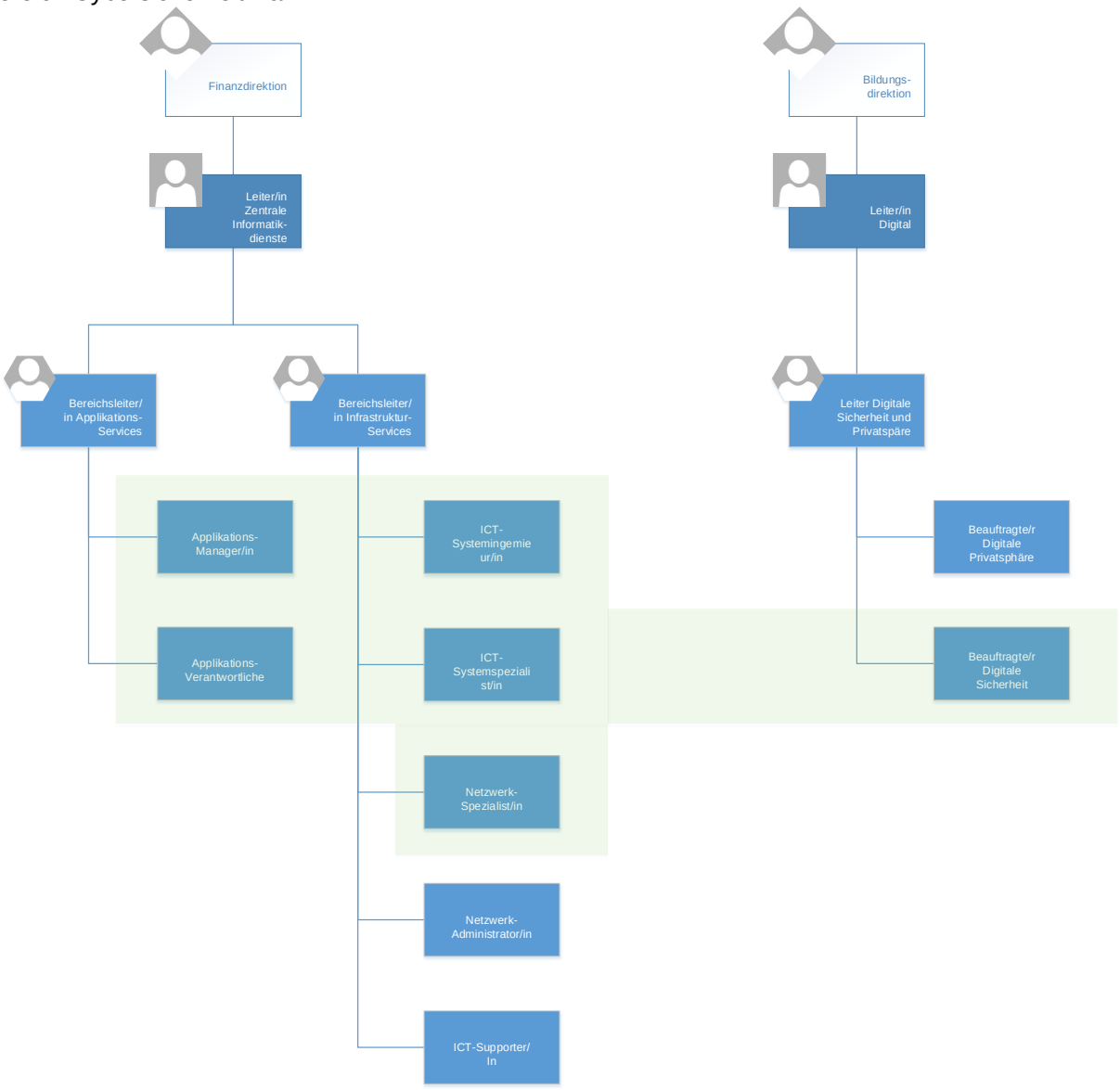

Abb. 5: Organigramm Fachteam «Security Operations»

Das Team besteht aus dem Beauftragten für Digitale Sicherheit der FDSP, zwei ICT-Systemspezialisten oder ICT-Systemingenieuren und einem Netzwerkspezialisten aus dem Bereich IS sowie einem Applikations-Manager oder Applikations-Verantwortlichen aus dem Bereich AS. Die Mitglieder des Teams sind ihren Linienvorgesetzten unterstellt, arbeiten aber im Fachteam «Security Operations» unter der fachlichen Leitung des Beauftragten für Digitale Sicherheit an Aufgaben der Cybersicherheit. Zusätzlich zu ihren operativen Betriebsaufgaben sind sie zudem in Infrastruktur- und Digitalisierungsprojekte eingebunden.

Weitere Tätigkeiten der Mitarbeitenden des Fachteams sind insbesondere:

– Überwachen von Blogs, Newslettern und E-Mail-Sicherheitsmeldungen der diversen Hersteller und Lieferanten;
– Überwachen der Meldungen von offiziellen Stellen wie dem Bundesamt für Cybersicherheit (BACS);
– Teilnahme am Sicherheitsbriefing des BACS (wöchentliches Cyber-Lage-Briefing);
– Schwachstellenuntersuchungen von neu eingeführten Applikationen und Systemen;
– Unterstützen von Projektteams bei technischen Sicherheitsaspekten und deren operativer Umsetzung.

3.5 Ziele der Informationssicherheitspolitik

Gestützt auf Art. 12 der Informatik- und Digitalverordnung hat der Stadtrat die Informationssicherheitspolitik in Form der Weisung «Digitale Sicherheit und Privatsphäre» per 1. November 2023 erlassen. Darin hat er in Bezug auf die Cybersicherheit die folgenden Ziele festgelegt:
- Gewährleisten des sicheren und zuverlässigen Betriebs der digitalisierten Verwaltungsprozesse;
- Aufrechterhaltung eines den Risiken angemessenen Sicherheitsdispositivs, welches auch die Wirtschaftlichkeit und die betriebliche Effizienz mitberücksichtigt;
- eine wirkungsvolle Resilienz gegenüber Cyberattacken.

Diese Ziele werden in den Grundsätzen der Informationssicherheitspolitik in der Weisung «Digitale Sicherheit und Privatsphäre» weiter konkretisiert:

Grundsatz 4.8: Cybersecurity
Die Stadtverwaltung verfügt über ein wirksames Sicherheitsdispositiv gegen Cyberattacken. Dieses Dispositiv umfasst die Identifikation von Bedrohungen, Massnahmen zur Prävention und Detektion von Attacken, zur Reaktion auf Vorfälle und zur Wiederherstellung nach Vorfällen. Die Wirksamkeit des Sicherheitsdispositivs wird regelmässig geprüft und mittels Übungen trainiert.

Grundsatz 4.10: Umgang mit Vorfällen und Schwachstellen
Es besteht eine konsistente und wirksame Herangehensweise für den Umgang mit Vorfällen und Schwachstellen bezüglich der digitalen Sicherheit und Privatsphäre. Dabei ist sichergestellt, dass
- Cyberattacken schnellstmöglich erkannt und eingedämmt werden können,
- technische Schwachstellen systematisch identifiziert und behoben werden,
- Vorfälle erfasst, beurteilt und angemessen behandelt werden,
- geeignete Eskalationswege bestehen,
- angemessen und gezielt über Vorfälle kommuniziert wird,
- Ursachen analysiert und Erkenntnisse zur Optimierung der digitalen Sicherheit und Privatsphäre genutzt werden, und
- unbefugte Bearbeitung und Offenlegung von Personendaten gemäss den gesetzlichen Vorgaben gemeldet und betroffene Personen bei Bedarf informiert werden.

4 Vorgehen: Ist-Analyse Stadt Luzern

4.1 Das NIST Cybersecurity Framework (NIST CSF)

Das NIST CSF[10] ist ein international und branchenübergreifend bewährter und weit verbreiteter Standard zur Ausgestaltung der Cybersicherheit in Unternehmen und anderen Organisationen. Es beinhaltet sechs sogenannte Funktionen. Diese Funktionen beschreiben die Fähigkeiten einer Organisation bzw. eines Unternehmens, die zur Gewährleistung der Cybersicherheit erforderlich sind. In diesem Abschnitt werden die Funktionen des NIST CSF zusammenfassend dargestellt.

Das Grundverständnis für diese Funktionen ist wesentlich, da sich die Situationsanalyse (s. Kapitel 4.3 und 4.4), die Erläuterung des Handlungsbedarfs (s. Kapitel 5) sowie die Beschreibung des Zielbildes (s. Kapitel 6.1) jeweils auf diese Funktionen beziehen.

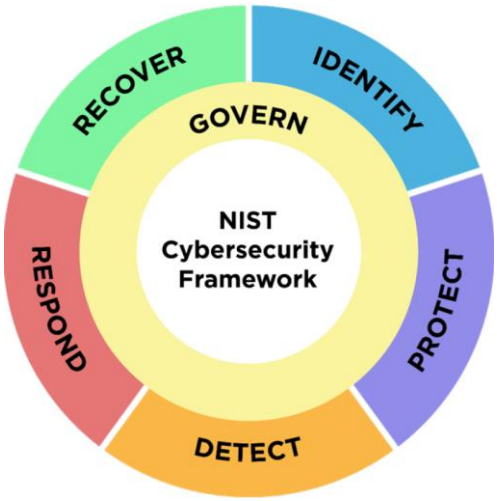

Abb. 6: Die sechs Funktionen des NIST CSF

Identify (Identifizieren)
Dies beinhaltet einerseits die Identifikation der zu schützenden Geschäftsprozesse, Datenbestände, Informationssysteme, Infrastrukturen und Services und andererseits die Identifikation von Bedrohungen und Risiken, insbesondere auch hinsichtlich der Lieferkette bei extern bezogenen Leistungen wie Cloud Services.

Protect (Schützen)
Dabei geht es um die Entwicklung und Implementierung von Schutzmassnahmen sowie um die Reduktion der Eintretenswahrscheinlichkeit und der Auswirkungen von Cyberangriffen auf die Informationssysteme. Dazu gehören die Sicherheit digitaler Identitäten, das Management von Zugangs- und Zugriffsberechtigungen, die Sensibilisierung des Personals, die Datensicherung und -wiederherstellung, das Aktualisieren und Absichern von Systemen und Software sowie der Einsatz von Schutztechnologien wie bspw. Antivirensoftware.

Detect (Erkennen)
Die Funktion «Detect» beinhaltet das Auffinden und Analysieren möglicher Cyberattacken und Kompromittierungen. Sie ermöglicht die rechtzeitige Entdeckung und Analyse von Anomalien, Indikatoren einer Kompromittierung und von anderen potenziell nachteiligen Ereignissen, die auf Cyberangriffe und -vorfälle hindeuten können.

[10] https://www.nist.gov/cyberframework.

Respond (Reagieren)
Dies betrifft das Ergreifen von Massnahmen bei einem festgestellten Cybersicherheitsvorfall. Die Funktion «Respond» unterstützt die Fähigkeit, die Auswirkungen von Cybersicherheitsvorfällen einzudämmen. Dazu gehören das Incident Management[11], die Analyse, die Schadensbegrenzung, die Berichterstattung sowie die interne und externe Kommunikation bei einem Vorfall.

Recover (Wiederherstellen)
Adressiert wird damit die Wiederherstellung von Vermögenswerten und Abläufen, die durch einen Cybersicherheitsvorfall beeinträchtigt wurden. Die Funktion «Recover» unterstützt die rechtzeitige Wiederherstellung des normalen Betriebs, um die Auswirkungen von Cybersicherheitsvorfällen zu verringern und eine angemessene Kommunikation während der Wiederherstellungsmassnahmen zu ermöglichen.

Govern (Steuern)
Damit wird die Festlegung und Überwachung der Strategie, der Erwartungen und der Politik der Organisation im Bereich des Cybersicherheits-Risikomanagements adressiert. Die Funktion «Govern» ist bereichsübergreifend, steuert und definiert Vorgaben und liefert Ergebnisse, die Aufschluss über die Risikolage und die Behandlungsstrategie geben. Dazu gehören das Risikomanagement für die Lieferkette, Rollen, Verantwortlichkeiten und Befugnisse, Richtlinien, Prozesse und Verfahren sowie die Überwachung der Cybersicherheitsstrategie.

4.2 Ausrichtung an NIST CSF

Die FDSP und die ZID orientieren sich in der Ausgestaltung von Massnahmen im Bereich der Cybersicherheit bereits heute am NIST CSF. Die ZID verfügen jedoch nur über sehr begrenzte Ressourcen und Fähigkeiten, um Cyberattacken zu vermeiden, rechtzeitig zu erkennen und schnell und wirksam darauf zu reagieren.

Im Kontext des NIST CSF stellt sich die Situation derzeit folgendermassen dar:

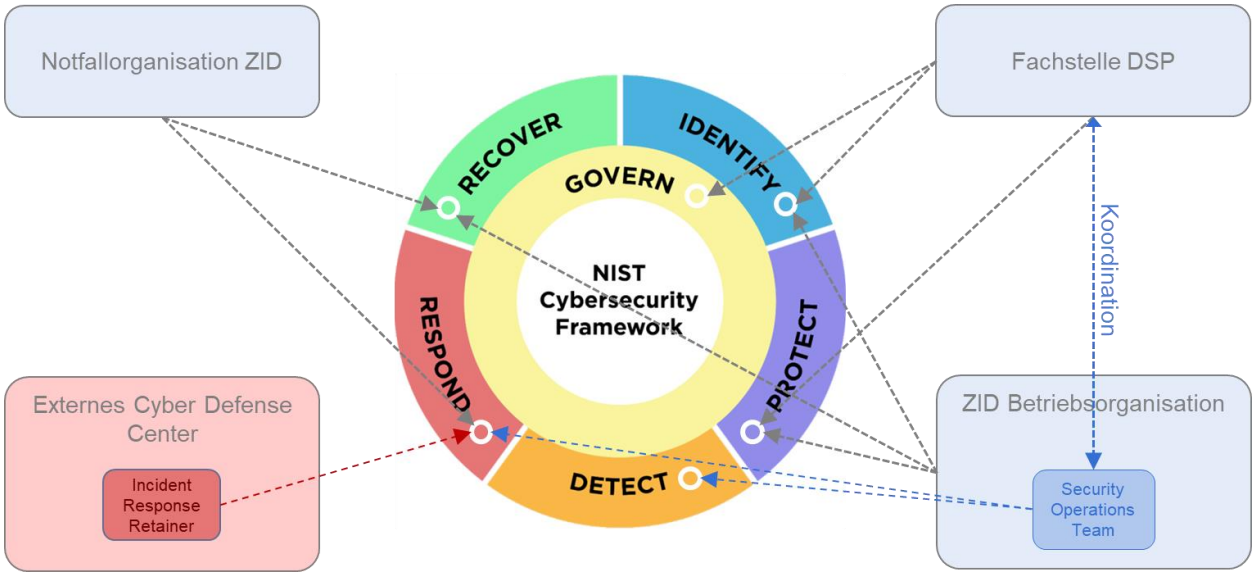

Abb. 7: Ist-Situation Stadt Luzern

[11] Beim Incident Management geht es um die Identifizierung, Priorisierung und Lösung von kritischen Störungen.

4.3 Situation bezüglich Zuständigkeiten

Die FDSP ist zuständig für das Management und die Koordination der Cybersicherheit («Govern»), für die Identifikation der zu schützenden Informationswerte und der Risiken («Identify») sowie für die Definition und die Kontrolle von Schutzmassnahmen («Protect»).

Das Fachteam «Security Operations» unterstützt die Umsetzung von Schutzmassnahmen («Protect»), überwacht nach Möglichkeit einzelne technische Sicherheitssysteme («Detect»), bewältigt nicht kritische Ereignisse und hat Zugang zum externen Dienstleister bei wesentlichen Vorfällen («Respond»).

Um bei einer Cyberattacke einen schnellen und unkomplizierten Zugang zu erfahrenen Fachleuten zu erhalten, wurde eine Vereinbarung mit einem spezialisierten Unternehmen getroffen (Incident Response Retainer). Dies anstelle einer zuvor vorhandenen Cyberversicherung, die bei geringerem Nutzen wesentlich höhere Kosten verursachte («Respond»).

Die Notfallorganisation ZID (NOZ) ist die ZID-interne Organisation, die bei einem Ernstfall weitere Notfall-, Überbrückungs- und Wiederherstellungsmassnahmen in die Wege leitet und bei Bedarf an den Stab für Betriebliche Notlagen BENO[12] eskaliert.

Daraus folgt, dass heute die Zuständigkeiten in der Organisation in den Funktionen
– «Govern» und «Identify» angemessen adressiert sind,
– «Protect» und «Recover» nur teilweise adressiert sind und
– «Detect» und «Respond» aufgrund fehlender personeller Ressourcen ungenügend adressiert sind. Die ungenügende Besetzung ist insbesondere bei einem tatsächlichen Cyberangriff kritisch.

4.4 Situation bezüglich Fähigkeiten

Identify (Identifizieren)
Zur Identifikation der zu schützenden Informationswerte sind die Fähigkeiten und die erforderlichen Ressourcen vorhanden. Für die Identifikation, Beurteilung und Steuerung der Informationssicherheitsrisiken sind Fähigkeiten und Methoden vorhanden. Die zugehörigen Prozesse sind implementiert oder befinden sich im Aufbau.

Protect (Schützen)
Die Beschaffung und der Betrieb der technischen Infrastruktur der Stadt sowie die Integration von externen Cloud Services erfolgen immer unter Berücksichtigung der aktuellen Bedrohungen und unter Einbezug der FDSP. In Projekten werden die Sicherheitsanforderungen bereits in der Konzeptphase mitberücksichtigt.

Notebooks, mobile Geräte, Serversysteme, Netzwerkgeräte usw. sowie die in der Infrastruktur eingesetzten Betriebs- und Virtualisierungsprogramme werden bei der Einführung in Zusammenarbeit mit spezialisierten Firmen nach den neuesten Sicherheitsstandards aufgebaut. Im Betrieb erkannte Schwachstellen werden zeitnah mit den notwendigen Aktualisierungen der Hersteller versehen.

Sowohl Endgeräte als auch Serversysteme sind ausnahmslos mit den notwendigen Systemen zur Erkennung und Bekämpfung von Schadsoftware ausgerüstet. Auch der E-Mail-Verkehr (Anti-Phishing, Anti-Spam und Malware-Schutz), der Zugriff aufs Internet (Malware-Schutz) und Zugriffe von extern auf die Infrastruktur (Verschlüsselungen) der Stadt Luzern sind mit modernen technischen Sicherheitsmassnahmen geschützt.

[12] Vgl. Art. 43 Verordnung zum Reglement über die Organisation der Stadtverwaltung Luzern (sRSL 0.5.1.1.2; Organisationsverordnung).

Im Betrieb fehlt aufgrund der heterogenen System- und Applikationsvielfalt der Überblick über bestehende Schwachstellen. Darum ist es notwendig, sämtliche Systeme regelmässig und möglichst automatisiert auf bestehende Schwachstellen zu untersuchen und diese zu beheben. Dazu fehlen die technischen und personellen Möglichkeiten. Ein vollständiges und akkurates Bild über die Schwachstellen der technischen Infrastruktur, der Cloud Services und der städtischen Websites zu erhalten und diese Schwachstellen gezielt und schnellstmöglich zu beheben, ist nicht möglich. Die tatsächliche Verletzlichkeit bzw. Angriffsfläche gegenüber Cyberattacken ist deshalb schwer abschätzbar.

Für eine ganzheitliche Planung der technischen Sicherheitsarchitektur, die das effektive Zusammenwirken der technischen Schutzsysteme zum Ziel hat und so den zielgerichteten Einsatz der Ressourcen verbessert, sind die notwendigen fachlichen Fähigkeiten nicht vorhanden.

Detect (Erkennen)
Die Anzahl und die Komplexität der Cyberangriffe haben massiv zugenommen. Die frühzeitige Erkennung von Anomalien im Netzwerkverkehr und ungewöhnlichen Aktivitäten, die auf Sicherheitsverletzungen hinweisen könnten, erfordern die umfassende Aufzeichnung und Auswertung von Systemprotokolldaten.

Protokolldaten von sicherheitsrelevanten Systemen und Komponenten werden aufgezeichnet. Aufgrund der grossen Datenmenge werden diese jedoch nicht regelmässig, strukturiert und automatisiert ausgewertet. Dies birgt die Gefahr, dass Angriffsmuster oder Anzeichen von Kompromittierungen nicht zeitnah festgestellt werden können. Zukünftig müssen Protokolldaten von sämtlichen Geräten (auch Endgeräte wie Notebooks oder Smartphones) gespeichert und analysiert werden, um Anomalien zu erkennen, zu verstehen und akkurat auf Vorfälle zu reagieren. Hierzu fehlen geeignete Werkzeuge (Software und Systeme), das erforderliche Fachwissen und die personellen Ressourcen.

Die vorhandenen Sicherheitsvorrichtungen genügen damit nicht mehr für die rasche und systematische Erkennung von Angriffen aus dem Internet. Die laufende Überwachung der Sicherheitssysteme sowie das Analysieren und Bearbeiten von Sicherheitsvorfällen sind aufwendig und benötigen viel Zeit. Insbesondere die Analyse ist technisch anspruchsvoll und verlangt spezifisches Fachwissen, das in der Stadt Luzern nur teilweise vorhanden ist. Mit der unvermeidlichen Zunahme der Komplexität der Vorfälle und der sich laufend ändernden Bedrohungsszenarien werden auch die Anforderungen an das Fachwissen laufend steigen.

Abgesehen davon, dass die notwendigen Systeme zur Erkennung und Eindämmung von Kompromittierungen fehlen, kann die ZID auch nicht gewährleisten, dass auf erkannte Angriffe rund um die Uhr reagiert wird. Die dafür erforderlichen personellen und fachlichen Ressourcen fehlen und können mit den zur Verfügung stehenden Stellen nicht abgedeckt werden. Demzufolge ist eine Rund-um-die-Uhr-Überwachung von Angriffen nicht gewährleistet.

Respond (Reagieren)
Aufgrund der Schwächen in der Funktion «Detect» ist die Reaktion bei einem Vorfall zeitlich verzögert und nur eingeschränkt möglich. Dies führt dazu, dass eine laufende Cyberattacke höchstwahrscheinlich zu spät erkannt wird und nicht wirksam oder nur begrenzt reagiert wird. Die Folge kann eine unnötige und massive Ausweitung der Schäden bei einer Cyberattacke sein, beispielsweise durch Ransomware (Verschlüsselungstrojaner und Erpressung).

Die Mitarbeitenden der ZID und der FDSP haben weder ausreichendes Wissen noch genügend Erfahrung noch technische Hilfsmittel zur Eindämmung einer laufenden Cyberattacke bzw. im Umgang mit Erpressung durch Cyberkriminelle. Zur teilweisen Abdeckung dieser Lücke besteht eine Vereinbarung mit einem externen spezialisierten Cyber Defence Center. Dadurch wird im Ereignisfall der Zugang zu externen Fachleuten vereinfacht und die Reaktionsfähigkeit verbessert.

Recover (Wiederherstellen)
Die ZID verfügt über eine eigene Notfallorganisation (NOZ), die bei ausserordentlichen Lagen und Ausfällen der ICT-Infrastruktur zum Einsatz kommt, unter anderem auch bei Cyberattacken. Nicht Bestandteil der NOZ ist die operative Bewältigung der Folgen einer Cyberattacke, beispielsweise die Wiederherstellung von verschlüsselten Daten, der Neuaufbau von kompromittierten Systemen bzw. der gesamten ICT-Infrastruktur, die Reaktion auf erpresserische Offenlegung sensibler Daten und dergleichen. Insbesondere diese Fähigkeiten und personellen Ressourcen werden typischerweise von externen Fachleuten bezogen.

Govern (Steuern)
Dies umfasst einen wesentlichen Teil der Aufgaben der FDSP. Die fachlichen Kompetenzen zur zielgerichteten Steuerung der Cybersicherheit sind vorhanden, und die zugehörigen, primär organisatorischen Massnahmen sind etabliert oder befinden sich in Umsetzung.

Im Sinne der Steuerung wird jedoch die künftige organisatorische und prozessuale Einbettung des Security-Operations-Teams von zentraler Bedeutung sein.

4.5 Auswirkungen auf das Klima

Laut Relevanzcheck im Tool Klimafolgenabschätzung der Stadt Luzern ist das Geschäft nicht klimarelevant. Das heisst, dass durch das Projekt keine erkennbaren Auswirkungen auf das Klima zu erwarten sind. Auf eine weiter gehende Prüfung wurde daher verzichtet.

5 Ergebnisse: Handlungsbedarf

Der Handlungsbedarf im Bereich der Cybersicherheit lässt sich wie folgt zusammenfassen:

- Es fehlen massgebliche personelle Ressourcen für ein wirksames Sicherheitsdispositiv gegen Cyberattacken. Diese Ressourcen sind zu ergänzen.
- Es fehlen fachliche Fähigkeiten, insbesondere in den Funktionen «Detect» und «Respond» sowie teilweise in den Funktionen «Protect» und «Recover». Diese Fähigkeiten sind aufzubauen.
- Es fehlen geeignete technische Systeme und Software-Werkzeuge, um überhaupt eine schnelle Erkennung und Reaktion auf Cyberattacken zu ermöglichen. Diese sind zu beschaffen bzw. mit externer Unterstützung zu integrieren, und die Mitarbeitenden sind zu befähigen.
- Es fehlt eine Rund-um-die-Uhr-Überwachung von Angriffsmustern zur Erkennung von Vorfällen sowie die Fähigkeit zur Reaktion auf Vorfälle. Diese sind sicherzustellen.

Abb. 8: Handlungsbedarf der Stadt Luzern

Aufgrund der sich stets verschärfenden Gefährdungslage, der steigenden Komplexität der Informationssysteme, der hohen Abhängigkeit der Stadtverwaltung von ihren Informations- und Kommunikationssystemen sowie der entsprechend hohen potenziellen Schäden bei einer erfolgreichen Attacke gehören die Risiken einer Cyberattacke zu den Top-Risiken der Stadtverwaltung. Diese wurden identifiziert, im Risikoinventar ausgewiesen und vom Stadtrat zur Kenntnis genommen.

6 Zielbild und Massnahmen

6.1 Zielbild

Um die Voraussetzungen für eine schnelle und wirksame Erkennung von und Reaktion auf Cyberattacken zu schaffen und die erforderlichen Funktionen und Fähigkeiten im Bereich der Cybersicherheit aufzubauen und nachhaltig sicherzustellen, soll das Cybersicherheitsdispositiv massgeblich verstärkt werden.

Gestützt auf die in den vorangehenden Kapiteln erläuterte Situation und um die in Kapitel 2 genannten Ziele im Sinne des gesetzlichen Auftrags zu erreichen, wird das nachfolgend dargestellte Zielbild angestrebt.

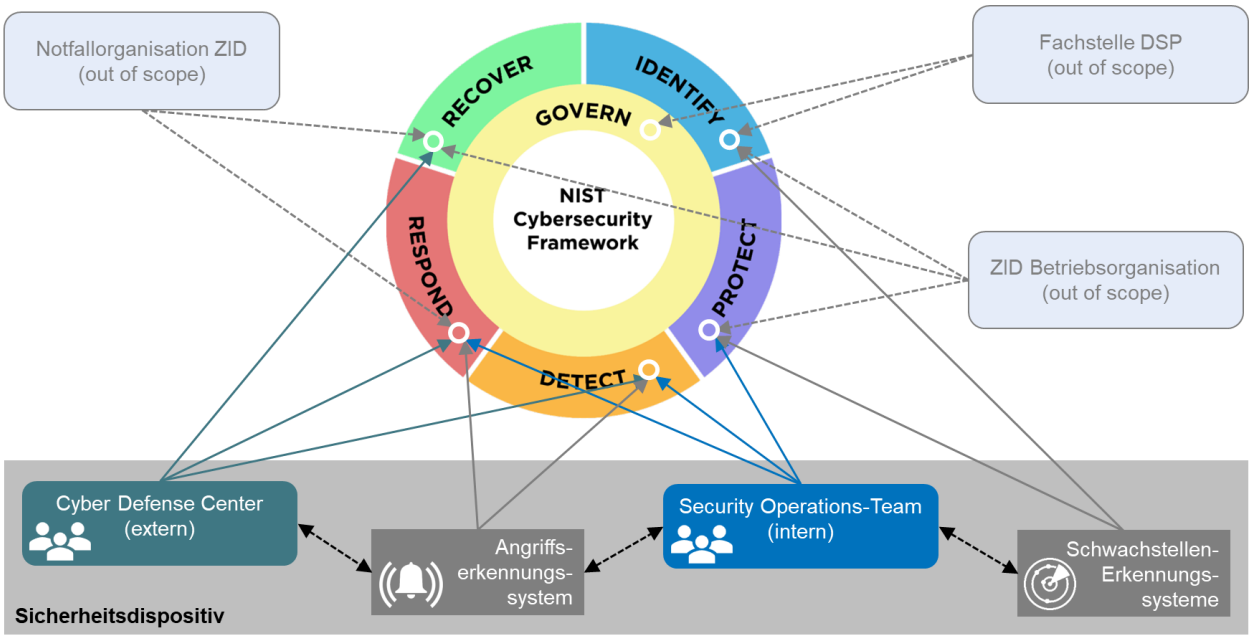

Abb. 9: Zielbild Cybersicherheitsdispositiv

Security-Operations-Team (intern) Erweiterung des internen Security-Operations-Teams, damit dieses mit den notwendigen personellen Ressourcen ausgestattet ist und über die fachlichen Kompetenzen verfügt (s. Kapitel 6.2).
Cyber Defence Center (extern) Technische und organisatorische Anbindung an ein externes, professionelles und rund um die Uhr verfügbares Cyber Defence Center zur kontinuierlichen Überwachung technischer Ereignisse hinsichtlich Anzeichen einer Kompromittierung, zur schnellen Reaktion auf Vorfälle und laufenden Analyse der Bedrohungslage (s. Kapitel 6.3).
Angriffserkennungssystem Beschaffung, Integration und Betrieb von Systemen und Services zur automatisierten Erkennung, Aufzeichnung und Auswertung von technischen Ereignissen und Angriffsmustern (s. Kapitel 6.4.1).
Schwachstellen-Erkennungssystem Systeme und Werkzeuge zur kontinuierlichen, automatisierten Kontrolle der städtischen ICT-Infrastruktur und Webservices hinsichtlich Softwareschwachstellen und Fehlkonfigurationen zur Minimierung der Angriffsfläche gegenüber Cyberattacken (s. Kapitel 6.4.2).

Tab. 5: Massnahmen zum Zielbild Sicherheitsdispositiv

6.2 Internes Security-Operations-Team

Das bereits bestehende Fachteam «Security Operations», das sich aus Vertretungen der ZID sowie der FDSP zusammensetzt, wird neu strukturiert und mit zusätzlichen personellen Ressourcen verstärkt.

6.2.1 Funktionen, Aufgaben und Zuständigkeiten

Im Security-Operations-Team werden prinzipiell zwei Funktionen benötigt, deren Aufgaben und Zuständigkeiten sich folgendermassen darstellen:

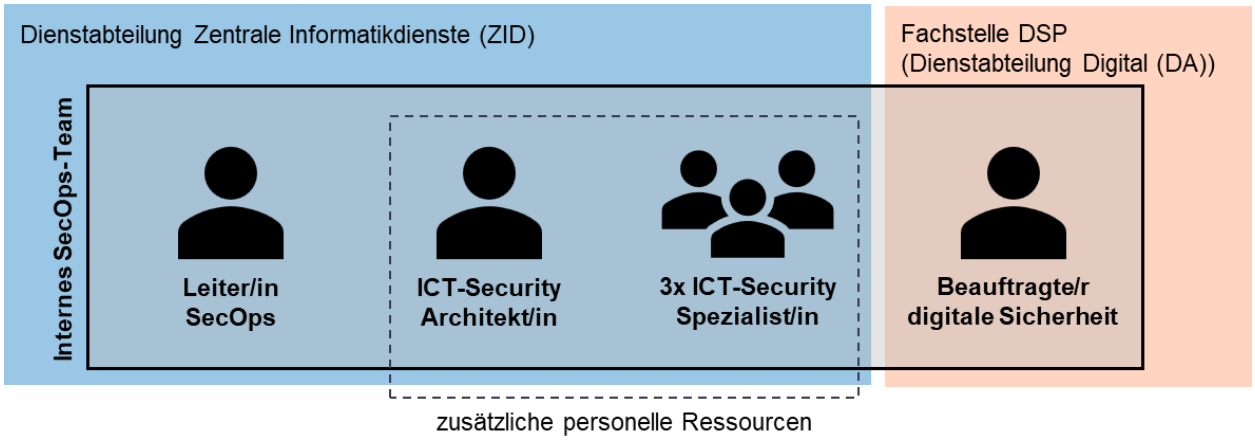

Abb. 10: Zusammensetzung internes Security-Operations-Team

Die zusätzlichen personellen Ressourcen sind für den technischen Betrieb der neuen Mittel und Systeme (s. Kapitel 6.4), für die fachliche Weiterbildung sowie für den erweiterten Aufgabenbereich des Security-Operations-Teams erforderlich. Die neuen Aufgabenbereiche verstärken die Funktionen nach dem NIST Cybersecurity Framework, die bisher bei der Stadt Luzern nicht ausreichend adressiert sind:

Funktion	Aufgaben und Zuständigkeiten	Bemerkungen
ICT-Security-Architekt/in ZID	– Design der technischen Sicherheitsarchitektur auf Netzwerk-, System- und Applikationsebene inklusive Cloud Services – Definieren und Durchsetzen von technischen Grundanforderungen zur sicheren Konfiguration von Netzwerken, Systemen, Applikationen und Cloud Services – Analysieren der Bedrohungslage, Beurteilen der Risiken und Ableiten von gezielten Schutzmassnahmen – Minimieren von Verletzlichkeiten, Erkennen von Schwachstellen, Überwachen von deren Behebung – Identifizieren der in Projekten anwendbaren Sicherheitsstandards in Abstimmung mit der FDSP – Festlegen der konkreten Umsetzung der Sicherheitsanforderungen (Requirements Engineering) in Projekten und im Betrieb – Koordinieren von Audits und Penetrationstests in Abstimmung mit der FDSP	Die Zuständigkeiten dieser Rolle beziehen sich primär auf die Funktion «Protect» (schützen).

Funktion	Aufgaben und Zuständigkeiten	Bemerkungen
ICT-Security-Spezialist/in ZID	– Primäre Ansprechperson für das externe Cyber Defence Center – Ansprechperson für den ZID-Pikettdienst – Betreiben und Aktualisieren der Angriffserkennungssysteme, der Schwachstellen-Erkennungssysteme und allfälliger weiterer technischer Hilfsmittel – Durchführen periodischer Schwachstellenanalysen – Beauftragen und Kontrollieren der Behebung von Schwachstellen – Überwachen der operativen Netzwerke, Systeme, Applikationen und Cloud Services – Erkennen von Anomalien und kritischen Ereignissen, Analyse, Abschätzen von Auswirkungen – Threat Hunting: Erkennen von bisher unbekannten oder noch nicht behobenen Bedrohungen – Entwickeln von Detektionslogiken zur Erkennung neuer Angriffsszenarien – interne technische Audits, Überprüfen der Sicherheit von Netzwerken, Systemen, Applikationen und Cloud Services – Eskalation / Koordination von Vorfällen mit CDC und NOZ – Unterstützen bei der Wiederherstellung nach allfälligen Cyberattacken – Mitarbeit in der Umsetzung von Sicherheitsanforderungen – Analyse sicherheitsrelevanter Meldungen von Mitarbeitenden – Austausch mit seinesgleichen in anderen Organisationen	Die Zuständigkeiten fokussieren sich auf die Funktionen «Detect» (Erkennen), «Respond» (Reagieren) und teilweise auf «Recover» (Wiederherstellen). ICT-Security-Spezialistinnen und -Spezialisten sind von anderweitigen betrieblichen Aufgaben entbunden.

6.2.2 Personalbedarf

Zur Abdeckung des in Kapitel 5 dargestellten Handlungsbedarfs und zur Erfüllung obiger Aufgaben sind zusätzliche 400 Stellenprozent erforderlich. Die bestehende Betriebsorganisation der ZID ist, wie in der Ausgangslage beschrieben, durch die stetig steigende Anzahl der Endgeräte sowie die Zunahme des Projektvolumens bereits heute sehr stark ausgelastet. Sie vermag den Handlungsbedarf im Sinne der nachfolgend beschriebenen Aufgaben und Zuständigkeiten weder in fachlicher noch in personeller Sicht ausreichend abzudecken. Die Betriebsorganisation soll durch zusätzliche personelle Ressourcen im Security-Operations-Team von Aufgaben der Cybersicherheit entlastet werden und sich auf ihre Kernaufgaben in den verschiedenen Bereichen fokussieren.

– Für die Erfüllung der Aufgaben der ICT-Security-Spezialist/innen sowie der ICT-Security-Architekt/in ist umfassendes Spezialwissen im Bereich der Cybersicherheit erforderlich. Netzwerktechnologien, Betriebssysteme verschiedenster Hersteller, Applikationen, Webapplikationen, Endgeräte aller Art sowie die stetige Neuentwicklung im Bereich dieser Technologien veranschaulichen die Komplexität, welche diese Aufgaben mit sich bringen.
– Die hohe Dynamik sowohl im Bereich der technologischen Neuentwicklungen als auch in der Cybersicherheits-Bedrohungslage erfordern, dass sich die ICT-Security-Spezialist/innen sowie die ICT-

Security-Architekt/in im Detail mit den aktuellen Entwicklungen auseinandersetzen. Das wiederum ist eine zeitintensive Aufgabe, die Selbststudium, Weiterbildungen und die Teilnahme an Fachgremien erfordert.
- Die Analyse und Konzeption der technischen Sicherheitsarchitektur bedingt ein sehr gutes Verständnis technischer und organisatorischer Zusammenhänge und bringt einen hohen Dokumentationsaufwand mit sich.
- Die interdisziplinäre Zusammenarbeit mit dem externen Cyber Defence Center, mit den verschiedenen internen sowie auch externen Fachstellen und Projektteams führt zu einem wesentlichen Koordinationsaufwand. Dies trägt aber im gleichen Zuge massgeblich zu einer Verbesserung der Cybersicherheit der Stadt Luzern bei.
- Der Aufbau, der Betrieb und die stetige Anpassung und Optimierung der Schwachstellen- und Angriffserkennungssysteme erfordert Zeit. Mithilfe dieser Systeme entsteht eine wesentlich bessere Transparenz hinsichtlich Verletzlichkeiten, und es werden deutlich mehr Anomalien erkannt. Deren Behandlung muss effizient und zeitnah erfolgen, was selbstredend zu einem höheren Aufwand als mit der bisherigen Situation führt.
- Die personellen Ressourcen sind zudem zur Abdeckung von Ferienabwesenheiten sowie für die Stellvertretungen notwendig, damit die ZID jederzeit über die Fähigkeiten und die personellen Ressourcen verfügt, um den sicheren Betrieb der IT-Infrastruktur zu gewährleisten.

All dies kann nicht von Einzelpersonen, sondern nur mit einem sich ergänzenden Team mit einer minimalen Grösse von vier Personen abgedeckt werden.

Weitere beteiligte Stellen innerhalb der ZID und der DIG (nicht Teil des Antrages):

Funktion	Aufgaben und Zuständigkeiten	Bemerkungen
Leiter/in Security-Operations-Team ZID	– Koordinieren der Aufgaben und Tätigkeiten innerhalb des Teams – Unterstützen bei Vorfällen – Kommunikation mit internen Stellen bei Vorfällen – Entscheiden über Massnahmen bei Vorfällen – Review von Ergebnissen aus Audits und Penetrationstests, Koordinieren und Planen von Massnahmen – Mitwirken bei Risikoanalysen – Planen und Koordinieren von Cyber-Notfallübungen zusammen mit der FDSP und NOZ – Kontakt zu Behörden (BACS) – Stellvertretung des ICT-Security-Architekten / der ICT-Security-Architektin – Mitsprache bei der Sicherheitsarchitektur – Primäre Ansprechperson der FDSP	Wird zukünftig durch den Bereichsleiter Infrastruktur-Services wahrgenommen.

Funktion	Aufgaben und Zuständigkeiten	Bemerkungen
Beauftragte/r digitale Sicherheit FDSP	– Koordinieren der Tätigkeiten zwischen der FDSP und dem Security-Operations-Team – Definieren und Vermitteln der Sicherheitsstandards für den ICT-Betrieb und in Projekten – Kontrolle von Massnahmen und Überwachung von deren Wirksamkeit – Planen und Koordinieren von Audits und Penetrationstests – Planen und Koordinieren von Cyber-Notfallübungen zusammen mit der NOZ – Primärer Kontakt zu Behörden (BACS) – Behandeln von datenschutzrelevanten Vorfällen	Diese Aufgaben werden von der FDSP bereits heute wahrgenommen.

6.3 Externes Cyber Defence Center

Das Cyber Defence Center (CDC) ist ein Team von externen Cybersicherheitsfachleuten, das die gesamte ICT-Infrastruktur der Stadt Luzern rund um die Uhr überwacht. Seine Hauptaufgabe besteht darin, Cybersicherheitsereignisse in Echtzeit zu erkennen und diesen so schnell und effektiv wie möglich entgegenzutreten. Es ergänzt damit die internen Fähigkeiten, Ressourcen und zeitlichen Verfügbarkeiten des Security-Operations-Teams. Insbesondere verfügt ein CDC über hochgradig spezialisierte Mitarbeitende für die Aufgaben des Incident Handlers, Incident Responders, Analysten sowie des Threat Hunters.

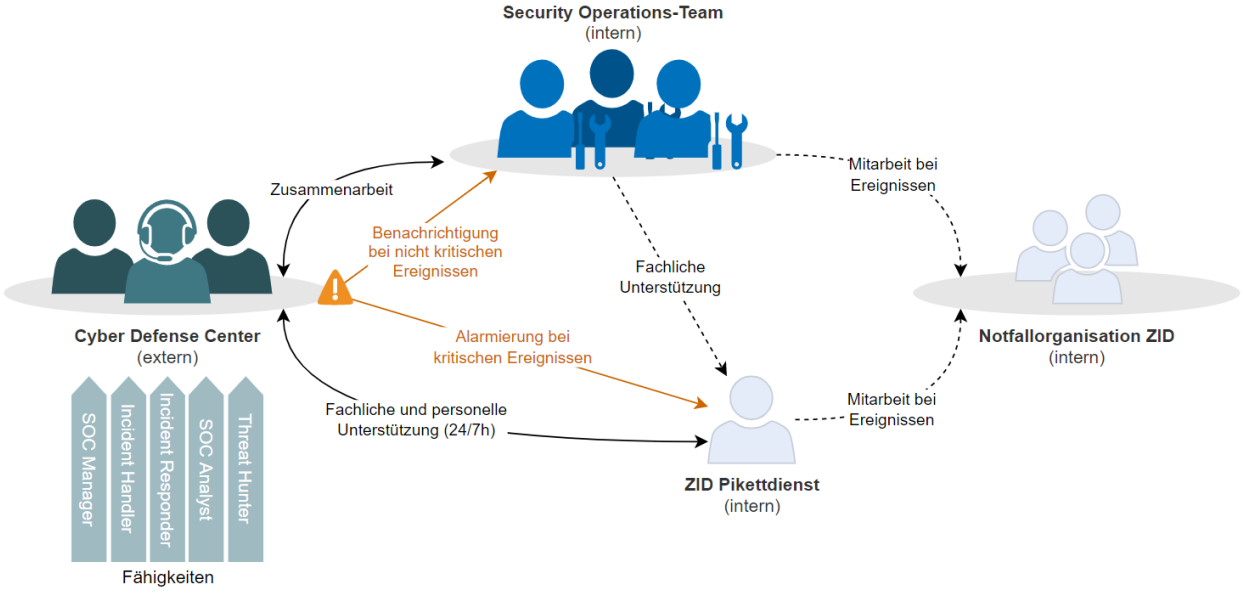

Abb. 11: Zusammenarbeit des CDC mit der Stadt Luzern

Durch die Zusammenarbeit mit einem externen CDC verstärkt die Stadt Luzern folgende, bisher nicht ausreichend adressierte Funktionen gemäss dem NIST Cybersecurity Framework:

Detect (Erkennen)
Das CDC stellt eine kontinuierliche Überwachung der technischen Infrastruktur und Cloud Services hinsichtlich Cybersicherheitsvorfällen bereit. Rund um die Uhr, 365 Tage im Jahr überwacht das CDC verdächtige Aktivitäten, prüft Anzeichen der Ausnutzung bekannter Schwachstellen (Exploits) und reagiert umgehend auf diese.

Das Angriffserkennungssystem (s. Kapitel 6.4.1) bildet dabei die Grundlage für die Arbeit der Security Incident Handlers. Sie bearbeiten eingehende Meldungen über Cybersicherheitsvorfälle, beurteilen die Auswirkungen sowie das potenzielle Risiko und beginnen umgehend mit der Reaktion auf den Vorfall. Bei kritischen Ereignissen werden die Incident Handlers zudem durch Security-Analystinnen und -Analysten bei der Bewältigung des Ereignisses unterstützt.

Wenn die Lage eine tiefgehende Analyse der betroffenen technischen Infrastruktur erfordert, kommen zudem hochgradig spezialisierte forensische Analystinnen und Analysten hinzu, um betroffene Systeme im Detail zu analysieren.

Durch gemeinsame Threat Huntings mit dem internen Security-Operations-Team vermittelt das CDC sein Fachwissen an die interne Organisation, und bisher unbekannte oder noch nicht behobene Bedrohungen werden aufgedeckt.

Respond (Reagieren)
Bei einem erkannten Cybersicherheitsvorfall ist die unverzügliche Reaktion absolut entscheidend, um den Schaden auf ein Minimum zu begrenzen. Ein CDC verfügt mit Incident Responders über Fachpersonen, die bei einem Cybersicherheitsvorfall jederzeit und zielgerichtet mit der Schadensbegrenzung beginnen. Je nach Art und Ausprägung werden die Incident Responders durch weitere Fachleute des CDC unterstützt, die softwarebasierte Tools zur Eindämmung oder Analyse der Attacken in der Systemumgebung installieren und auswerten.

Die Stadt Luzern wird mit dem CDC vertraglich vereinbaren, welche Reaktionen ein Incident Responder ohne Rücksprache mit der Betriebsorganisation der ZID durchführen darf.

Das CDC unterstützt die Stadt auch in Verhandlungen mit Cyberkriminellen, wenn es darum geht, auf Erpressung mit Lösegeldforderungen zu reagieren.

Recover (Wiederherstellen)
Das CDC unterstützt die Betriebsorganisation der ZID auch in der operativen Bewältigung der Folgen einer Cyberattacke. Beispielsweise beim Umgang mit verschlüsselten Daten, bei der Entfernung von Malware oder bei der Planung eines allfälligen Neuaufbaus von Systemen.

6.4 Technische Mittel und Systeme

6.4.1 Angriffserkennungssysteme

Diese Systeme und Softwarewerkzeuge sind Voraussetzung, um technische Ereignisse und Protokolldaten aller relevanten Systeme aufzuzeichnen, systematisch und automatisiert auszuwerten, um laufende Angriffe zu erkennen und kompromittierte Systeme zu identifizieren und zu isolieren.

Extended Detection and Response System (XDR)
Fähigkeiten: Protect, Detect, Respond
Extended Detection and Response ist eine umfassende Sicherheitslösung für Unternehmen, die sowohl vor als auch nach einem Sicherheitsvorfall Schutz bietet. Die Plattform koordiniert die Erkennung, Prävention, Untersuchung und Reaktion auf Bedrohungen über verschiedene Bereiche wie Endgeräte, Benutzeridentitäten, E-Mails und Applikationen hinweg. Ihr Ziel ist es, einen integrierten Schutz gegen komplexe Angriffe zu gewährleisten.

Als zentraler Datenkollektor sammelt ein XDR relevante Ereignisse und Protokolldaten auf den Endpunkten wie Computern, Notebooks oder Servern. Mit der Threat Intelligence der Plattform werden die Daten KI-gestützt verarbeitet. Bei erkannten Gefahren generiert ein XDR Alarme in einem Security Information and Event Management (SIEM) oder gleichwertigen System.

Security Information and Event Management (SIEM)
Fähigkeiten: Protect, Detect
Eine Security-Information-and-Event-Management-Plattform unterstützt die Organisation bei der konsolidierten Erkennung und Analyse von Cybergefahren und ermöglicht eine sofortige Reaktion auf diese. Die Technik Extended Detection and Response (XDR) liefert dazu Logs sowie Ereignisse, die durch eine SIEM-Plattform verarbeitet werden.

Je nach Schweregrad der Cybergefahr wird das externe Cyber Defence Center oder das interne Security-Operations-Team über den Vorfall benachrichtigt. Ebenfalls abhängig vom Schweregrad werden automatisierte Reaktionen, wie bspw. die Isolation eines Endpunkts, ausgelöst, oder die Reaktion erfolgt manuell durch die Spezialistin oder den Spezialisten, die oder der das Ereignis bearbeitet. Dadurch wird eine schnelle Reaktion und wirksame Intervention gewährleistet.

Ein SIEM-System ist somit die zentrale Plattform zur Vorbeugung und Bewältigung von Cyberattacken zwischen dem externen Cyber Defence Center, dem internen Security-Operations-Team sowie der restlichen Betriebsorganisation der ZID.

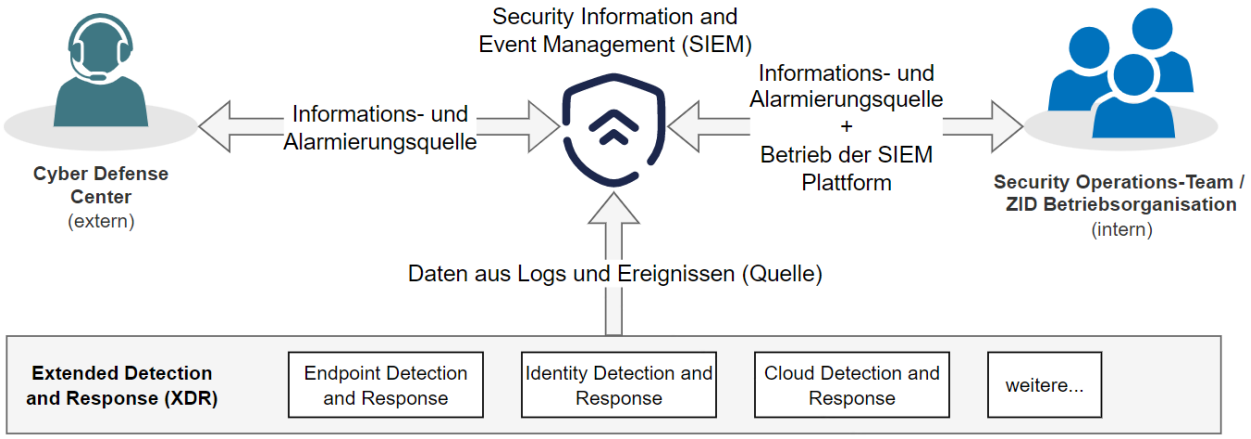

Abb. 12: Funktionsweise des SIEM bei der Stadt Luzern

6.4.2 Schwachstellen-Erkennungssysteme

Die nachfolgenden Plattformen sind notwendig, um Sicherheitsschwachstellen in der IT-Infrastruktur frühzeitig zu erkennen. Zusätzlich wird die Konformität der IT-Infrastruktur gegenüber Standards und Richtlinien regelmässig überprüft.

Vulnerability-Managementsystem
Fähigkeiten: Protect
Ein Vulnerability-Managementsystem dient der Identifikation und Behebung von Schwachstellen in der IT-Infrastruktur. Gesammelte Informationen über Endpunkte werden dazu mit Schwachstellen-Datenbanken abgeglichen, um so Verwundbarkeiten im Betriebssystem oder darauf installierten Applikationen zu erkennen.

Wurden Schwachstellen entdeckt, werden diese mithilfe der Informationen aus der Schwachstellen-Datenbank auf deren Schweregrad und Auswirkung klassifiziert. Das interne Security-Operations-Team sowie die gesamte Betriebsorganisation der ZID erhalten dadurch eine Übersicht über aktuell vorhandene Schwachstellen in der IT-Infrastruktur, um diese zeitnah und risikoorientiert beheben zu können.

Technisches Compliance-Management
Fähigkeiten: Protect
Mit einer Compliance-Management-Plattform wird die IT-Infrastruktur auf deren gesamte Konformität bewertet. Dazu werden Endpunkte gegenüber bewährten Sicherheitsstandards aus der Industrie (bspw. CIS-Benchmarks) sowie intern definierten Sicherheitsrichtlinien geprüft. Dies hilft dem internen Security-

Operations-Team bei der Identifikation und Bewertung von Abweichungen und bei der Priorisierung entsprechender Korrekturmassnahmen.

6.5 Zeitplan

Die neue Organisation mit dem Cyber Defence Center soll per Mai 2025 operativ in Betrieb sein, sodass die erhöhten Schutzmassnahmen vor Cyberattacken der Stadt Luzern zeitnah zur Verfügung stehen. Die volle Leistungsfähigkeit der gesamten Organisation kann erst erreicht werden, wenn die zusätzlich notwendigen Stellen besetzt sind. Die Suche nach qualifizierten Mitarbeitenden wird aufgrund des Fachkräftemangels herausfordernd sein, und die Stellenbesetzung könnte sich verzögern.
Die Evaluation des externen Cyber Defence Center wird vor dem definitiven Entscheid durch den Grossen Stadtrat gestartet. Verbindliche Verpflichtungen durch die Stadt Luzern werden aber erst nach dem Beschluss des Grossen Stadtrates eingegangen. Dieses Vorgehen unterstützt die schnelle Einführung des externen Cyber Defence Centers.

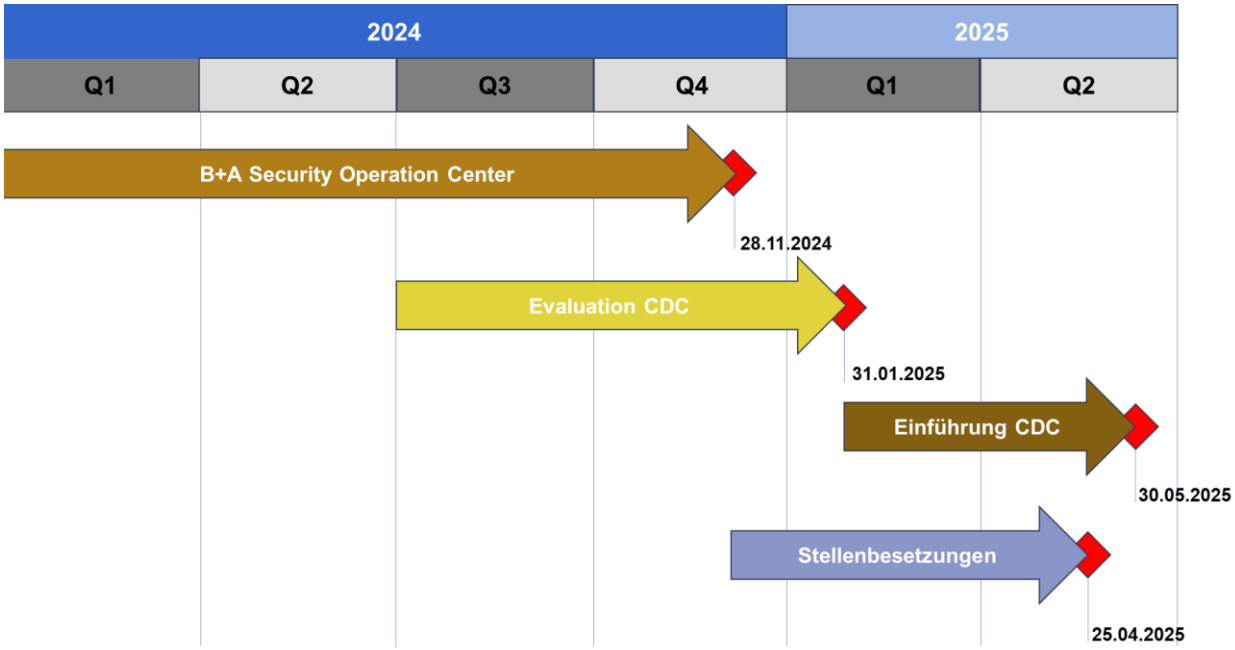

Abb. 13: Terminplan

7 Ressourcenbedarf

7.1 Gesamtausgabe

Der zusätzliche Ressourcenbedarf (Personalaufwand und Sachaufwand) ergibt sich aus den im Kapitel 6 beschriebenen Massnahmen. Zur Bestimmung der Vollkosten werden jeweils 25 Prozent für die Sozialleistungen und Flächenbereitstellungskosten zu den Lohnkosten addiert. Die jährlichen Personalgesamtkosten berechnen sich wie folgt:

a. Personalaufwand

Stelle	Pensum	Richtfunktion	Ausgaben pro Jahr in Fr.	Höhe der Ausgabe in Fr. für die Ausgabenbewilligung
ICT-Security-Architekt/in	100 %	Spezialisierte/r Fachbearbeiter/in 3	200’000.–	2’000’000.–
ICT-Security-Spezialist/in	300 %	Spezialisierte/r Fachbearbeiter/in 1	510’000.–	5’100’000.–
Total	**400 %**		**710’000.–**	**7’100’000.–**

Damit belaufen sich die Personalkosten insgesamt auf 7,1 Mio. Franken oder jährlich Fr. 710’000.– inkl. Sozialleistungen. Der Finanzierungsbedarf fällt bereits ab Mai 2025 an, falls geeignetes Personal rekrutiert werden kann.

b. Sach- und übriger Betriebsaufwand

Der Sach- und Betriebsaufwand wurde durch eine Richtofferte gemäss den Anforderungen aus Kapitel 6.2 erhoben.

Massnahmen	Nr. und Name der Aufgabe	Ausgaben pro Jahr in Fr.	Höhe der Ausgabe in Fr. für die Ausgabenbewilligung
Externes Cyber Defence Center (Dienstleistungen inkl. Lizenzen für die technischen Mittel und Systeme gemäss Kapitel 6.3 und 6.4)	614.1 Dienstleistungen Informatik	212’000.–	2’120’000.–
Einführungskonzepte, Installation der neuen technischen Mittel, Integration der bestehenden Systeme der Stadt Luzern in die Überwachung	614.1 Dienstleistungen Informatik		76’000.–
Bearbeiten von auftretenden Incidents (Vorfällen)	614.1 Dienstleistungen Informatik	12’600.–	126’000.–
Integration von neuen Systemen zur Überwachung in den Betriebsjahren nach Einführung	614.1 Dienstleistungen Informatik	6’000.–	60’000.–
Total			**2’382’000.–**

c. Gesamtübersicht

Position	Ausgaben pro Jahr in Fr.	Höhe der Ausgabe in Fr. für die Ausgabenbewilligung
Personalaufwand	710’000.–	7’100’000.–
Sachaufwand	230’600.–	2’306’000.–
Sachaufwand einmalig		76’000.–
Total		**9’428’000.–**

7.2 Ausgabenrechtliche Zuständigkeit

Mit dem vorliegenden Bericht und Antrag sollen für das Vorhaben «Aufbau eines Security-Operations-Teams» Gesamtausgaben in der Höhe von insgesamt 9,482 Mio. Franken bewilligt werden. Freibestimmbare Ausgaben von mehr als 1 Mio. Franken hat der Grosse Stadtrat durch einen Sonderkredit zu bewilligen (§ 34 Abs. 2 lit. a des Gesetzes über den Finanzhaushalt der Gemeinden vom 20. Juni 2016, FHGG; SRL Nr. 160, in Verbindung mit Art. 69 lit. b Ziff. 3 der Gemeindeordnung der Stadt Luzern vom 7. Februar 1999, GO; sRSL 0.1.1.1.1). Sein Beschluss unterliegt nach Art. 68 lit. b Ziff. 2 GO dem fakultativen Referendum.

8 Finanzierung und zu belastendes Konto

Das Vorhaben im Umfang von insgesamt 9,482 Mio. Franken ist nicht im Aufgaben- und Finanzplan 2025–2028 mit Budget 2025 enthalten.

Die mit dem beantragten Sonderkredit zu tätigenden Aufwendungen (Erfolgsrechnung) sind verschiedenen Konten im Personalaufwand in der Kostenstelle 6141100 und der Kostenstelle 6142601 für den Sachaufwand zu belasten. Gemäss Terminplan sollte das Security-Operations-Team ab 1. April 2025 operativ sein. Weil die Kosten für die geplanten Massnahmen nicht im Globalbudget der Zentralen Informatikdienste enthalten sind, ist die Finanzierung für das Jahr 2025 (Einführung und Installation Fr. 76’000.–, Personalkosten Fr. 532’500.–, Betriebskosten externes Cyber Defence Center Fr. 172’950.–) mit einem Nachtragskredit in der Höhe von 0,782 Mio. Franken zu beantragen.

9 Politische Würdigung

Das Risiko, dass die Stadt Luzern Opfer einer Cyberattacke wird, ist als hoch einzustufen. Mit den an ISO/IEC 27001 angelehnten Sicherheitsstandards verfügt die Stadt über die notwendigen Regeln, Methoden und Prozesse, um die Informationssicherheit dauerhaft zu gewährleisten. Die Orientierung am NIST CSF bei der Ausgestaltung von Massnahmen zeigt dennoch Defizite, speziell im Bereich der Funktionen zur Analyse von technischen Schwachstellen und zur Erkennung und Behandlung von Sicherheitsvorfällen. Die ZID und die FDSP fokussieren sich momentan darauf, die Cyberabwehr mit technischen Mitteln und Sensibilisierungsmassnahmen sicherzustellen. Eine schnelle und systematische Erkennung und Behebung von Angriffen aus dem Internet auf die ICT-Infrastrukturen sind jedoch mit den heutigen Sicherheitsvorkehrungen und den vorhandenen personellen Ressourcen nicht möglich. Die zunehmende Anzahl aktueller Projekte und die hohe Arbeitslast erhöhen das Risiko eines kritischen Sicherheitsvorfalls deutlich.

Wie bereits in der Antwort auf die Interpellation 284 angekündigt, ist der Stadtrat der Meinung, dass ein Ausbau der personellen Ressourcen, der fachlichen Fähigkeiten und der technischen Systeme dringend erforderlich ist, um den sich ständig weiterentwickelnden Angriffen und sozialen Manipulationen wirksam entgegenzutreten. Mit dem vorgeschlagenen Aufbau eines internen Security-Operations-Teams, das sich ausschliesslich der operativen Cybersicherheit widmen kann, und dem Beizug eines externen Cyber Defence Centers können die Risiken eines Cybervorfalls deutlich reduziert und die Mankos in den Funktionen Detect, Respond, Protect und Recover nachhaltig behoben werden. Der Stadtrat ist überzeugt, dass damit Attacken erschwert, schneller erkannt und wirksam eingedämmt werden können.

10 Antrag

Der Stadtrat beantragt Ihnen,
- für zusätzliche unbefristete 400 Stellenprozent und für die Beschaffung eines externen Cyber Defence Centers einen Sonderkredit von 9,482 Mio. Franken zu bewilligen und
- für den Start des Security-Operations-Teams im Jahr 2025 für das Budget 2025 einen Nachtragskredit von 0,782 Mio. Franken zu bewilligen.

Er unterbreitet Ihnen einen entsprechenden Beschlussvorschlag.

Luzern, 18. September 2024

Beat Züsli
Stadtpräsident

Michèle Bucher
Stadtschreiberin

Der Grosse Stadtrat von Luzern,

nach Kenntnisnahme des Berichtes und Antrages 36 vom 18. September 2024 betreffend

Aufbau Security-Operations-Team

- **Zusätzliche Stellen und Dienstleistungen**
- **Sonder- und Nachtragskredit,**

gestützt auf den Bericht der Geschäftsprüfungskommission,

in Anwendung von § 14 Abs. 1 und § 34 Abs. 2 lit. a des Gesetzes über den Finanzhaushalt der Gemeinden vom 20. Juni 2016 sowie Art. 13 Abs. 1 Ziff. 2, Art. 29 Abs. 1 lit. b, Art. 68 lit. b Ziff. 1 und Art. 69 lit. a Ziff. 2 und lit. b Ziff. 1 der Gemeindeordnung der Stadt Luzern vom 7. Februar 1999,

beschliesst:

I. Für zusätzliche unbefristete 400 Stellenprozent und für die Beschaffung eines externen Cyber Defence Centers wird ein Sonderkredit von 9,482 Mio. Franken bewilligt.

II. Für den Start des Security-Operations-Teams im Jahr 2025 wird für das Budget 2025 ein Nachtragskredit von 0,782 Mio. Franken bewilligt.

III. Der Beschluss gemäss Ziffer I unterliegt dem fakultativen Referendum.

Luzern, 28. November 2024

Namens des Grossen Stadtrates von Luzern

Simon Roth
Ratspräsident

Michèle Bucher
Stadtschreiberin