MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

Zivile Sicherheit – Cybersecurity mit dem Fokus auf Cloud und Data

Handout zum Zielmarktwebinar

Geschäftsanbahnung Kanada Cybersecurity

01. - 6. Juni 2025

Durchführer

AHK

Mit der Durchführung dieses Projekts im Rahmen des Bundesförderprogramms Mittelstand Global/ Markterschließungsprogramm beauftragt:

AHK

Das Markterschließungsprogramm für kleine und mittlere Unternehmen ist ein Förderprogramm des:

Bundesministerium für Wirtschaft und Klimaschutz

MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

IMPRESSUM

Herausgeber
Deutsch-Kanadische Industrie- und Handelskammer (AHK Kanada)
480 University Ave, Suite 1500
Toronto, ON M5G 1V2
Kanada
Tel.: +1 (416) 598-7081
Fax: +1 (416) 598-1840
Web: www.kanada.ahk.de

Text und Redaktion
Patricia Trinkaus, Project Manager
Lilly Schrank, Project Manager
Lunis Bormann, Project Coordinator

Stand
April 2025

Gestaltung und Produktion
Patricia Trinkaus, Project Manager

Bildnachweis
Shutterstock

Die Studie wurde im Rahmen des Markterschließungsprogramms für die Exportinitiative Zivile Sicherheitstechnologien und -dienstleistungen erstellt.

Inhalt

Abstract

Im Zuge der zunehmenden Digitalisierung und einer weltweit verschärften geopolitischen Lage steht Kanada vor wesentlichen Herausforderungen hinsichtlich der zivilen Sicherheit und insbesondere der Cybersicherheit. Aufgrund der stetig wachsenden Nutzung digitaler Infrastrukturen sieht sich Kanada zunehmender Cyberkriminalität und gezielter Angriffe auf kritische Infrastrukturen ausgesetzt. Die kanadische Regierung begegnet diesen Herausforderungen durch strategische Initiativen, umfangreiche Investitionen in Forschung und Entwicklung sowie gezielte Förderprogramme auf nationaler und provinzieller Ebene, um die Cyberresilienz öffentlicher und privater Akteure nachhaltig zu erhöhen.

Der kanadische Markt für zivile Sicherheitslösungen zeichnet sich durch eine hohe Nachfrage nach Produkten und Dienstleistungen im Bereich Cybersecurity, Datenschutz, Cloud- und Infrastruktur aus. Die hohe Nachfrage an Cybersicherheitslösungen führt gleichzeitig zu einem erheblichen Fachkräftebedarf. Der dadurch entstehende derzeitige Fachkräftemangel, begünstigt den Marktzugang insbesondere für Anbieter von Sicherheitstechnologien, Beratungsleistungen und Weiterbildungsangeboten. Durch diverse interdisziplinäre Kooperationsnetzwerke bestehend aus Universitäten, Forschungszentren sowie öffentliche und private Institutionen treibt Kanada die Forschung und Entwicklung innovativer Lösungen voran, stärkt das Sicherheitsbewusstsein zu und adressiert den Fachkräftemangel gezielt.

Kanada bietet deutschen Unternehmen ein attraktives und investitionsfreundliches Geschäftsumfeld mit starkem Innovationspotenzial, etablierten Forschungsstrukturen und einer stabilen, proaktiven wirtschaftlichen und rechtlichen Förderlandschaft. Vor diesem Hintergrund eröffnen sich für Anbieter von Sicherheitslösungen und -dienstleistungen umfangreiche Markteintrittsmöglichkeiten, insbesondere durch strategische Partnerschaften, technologische Zusammenarbeit sowie durch die Nutzung gezielter staatlicher Unterstützungsmaßnahmen. Das vorliegende Zielmarkthandout soll eine Grundlage für die gezielte Markterschließung der teilnehmenden Unternehmen der Delegationsreise nach Kanada darstellen.

Wirtschaftsdaten kompakt

WIRTSCHAFTSDATEN KOMPAKT

Kanada

Dezember 2024

GTAI GERMANY TRADE & INVEST

Bevölkerung und Ressourcen

Fläche (km^2)	9.984.670
Einwohner (Mio.)	2024: 39,7*; 2029: 41,4*; 2034: 42,7*
Bevölkerungswachstum (%)	2024: 1,0*; 2029: 0,7*; 2034: 0,6*
Fertilitätsrate (Geburten/Frau)	2024: 1,3*
Altersstruktur	2024: 0-14 Jahre: 15,1%; 15-24 Jahre: 11,6%; 25-64 Jahre: 53,5%; 65 Jahre und darüber: 19,8%*
Geschäftssprachen	*Englisch, Französisch*
Rohstoffe	Bauxit, Eisenerz, Nickel, Zink, Kupfer, Gold, Blei, Uran, seltene Erden, Molybdän, Pottasche, Diamanten, Silber, Kohle, Erdöl und Erdgas
Gas - Produktion (Mrd. cbm)	2021: 172,3; 2022: 184,8; 2023: 190,3
Gas - Reserven (Billionen cbm)	2020: 2,4
Erdöl - Produktion (Tsd. bpd)	2021: 5.414; 2022: 5.575; 2023: 5.653
Erdöl - Reserven (Mrd. Barrel)	2020: 168,1

Wirtschaftslage

Währung	Bezeichnung Kurs (August 2024) Jahresdurchschnitt	Kanadischer Dollar (kan$); 1 kan$ = 100 Cents 1 Euro = 1,492 kan$; 1 US$ = 1,349 kan$ 2023: 1 Euro = 1,460 kan$; 1 US$ = 1,350 kan$ 2022: 1 Euro = 1,370 kan$; 1 US$ = 1,301 kan$ 2021: 1 Euro = 1,480 kan$; 1 US$ = 1,254 kan$
Bruttoinlandsprodukt (BIP, nominal)		
- Mrd. US$		2023: 2.142; 2024: 2.215*; 2025: 2.330*
- Mrd. kan$		2023: 2.892; 2024: 3.019*; 2025: 3.165*
BIP/Kopf (nominal)		
- US$		2023: 53.607; 2024: 53.834*; 2025: 55.890*
- kan$		2023: 72.365; 2024: 73.370*; 2025: 75.898*
BIP-Entstehung (Anteil an nominaler Bruttowertschöpfung in %)		2022: Bergbau/Industrie 17,6; Handel/Gaststätten/Hotels 12,7; Transport/Logistik/Kommunikation 7,7; Bau 7,7; Land-/Forst-/Fischereiwirtschaft 2,0; Sonstige 52,2
BIP-Verwendung (Anteil an BIP in %)		2022: Privatverbrauch 54,3; Bruttoanlageinvestitionen 23,1; Staatsverbrauch 21,0; Bestandsveränderungen 1,4; Außenbeitrag 0,2

* vorläufige Angabe, Schätzung bzw. Prognose

Wirtschaftswachstum	**Bruttoinlandsprodukt** Veränderung in %, real

Inflationsrate (%)	2023: 3,9; 2024: 2,4*; 2025: 1,9*
Arbeitslosenquote (%)	2023: 5,4; 2024: 6,2*; 2025: 6,2*
Haushaltssaldo (% des BIP)	2023: -0,6; 2024: -2,0*; 2025: -1,0*
Leistungsbilanzsaldo (% des BIP)	2023: -0,7; 2024: -1,0*; 2025: -1,3*
Investitionen (% des BIP, brutto, öffentlich und privat)	2023: 24,0; 2024: 23,4*; 2025: 23,4*
Ausgaben für F&E (% des BIP)	2020: 1,9; 2021: 1,7; 2022: 1,6
Staatsverschuldung (% des BIP, brutto)	2023: 107,5; 2024: 106,1*; 2025: 103,2*
Ausländische Direktinvestitionen	
- Nettotransaktionen (Mrd. US$)	2021: 60,4; 2022: 46,2; 2023: 50,3
- Bestand (Mrd. US$)	2021: 1.548,8; 2022: 1.496,0; 2023: 1.665,8
- Hauptländer (Anteil in %, Bestand)	*2023: USA 45,4; Niederlande 12,7; Vereinigtes Königreich 7,8; Luxemburg 5,2; Japan 2,7; Schweiz 2,6; Hongkong, SVR 2,4; Australien 2,0; China 1,8; Deutschland 1,8*
- Hauptbranchen (Anteil in %, Bestand)	*2023: Beteiligungsgesellschaften 33,0; verarbeitende Industrie 17,4 (darunter Chemie 3,5; Lebensmittel 2,9; Transportindustrie 2,0); Finanz- und Versicherungswirtschaft 11,3; Bergbau/Öl/Gas 11,1; Großhandel 9,4; Unternehmensdienstleistungen 4,0; Einzelhandel 1,5*
Währungsreserven (Mrd. US$, zum 31.12.)	2021: 78,1; 2022: 79,7; 2023: 89,9
Auslandsverschuldung (Mrd. US$, zum 31.12.)	*2021: 2.875; 2022: 2.917; 2023: 3.078*

Außenwirtschaft

Warenhandel (Mrd. US$, Veränderung zum Vorjahr in %, Abweichungen durch Rundungen)

	2021	%	2022	%	2023	%
Ausfuhr	501,5	29,2	596,8	19,0	566,7	-5,0
Einfuhr	491,4	21,3	571,6	16,3	558,5	-2,3
Saldo	10,1		25,2		8,2	

* vorläufige Angabe, Schätzung bzw. Prognose

Außenhandel Deutschlands mit Kanada

Warenhandel (Mrd. Euro, Veränderung zum Vorjahr in %, Abweichungen durch Rundungen)

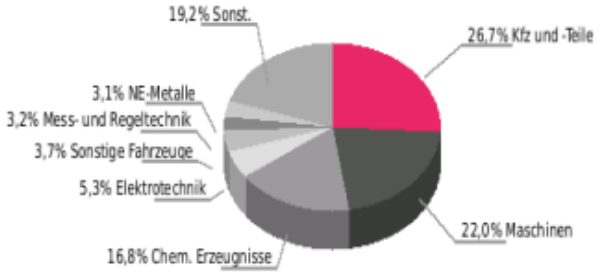
	2021	%	2022	%	2023	%
dt. Exporte	10,1	7,8	12,8	26,9	12,7	-0,3
dt. Importe	6,2	11,7	8,0	29,6	6,9	-13,5
Saldo	3,9		4,8		5,8	

Halbjahreswert (Mrd. Euro)

- deutsche Exporte: H1/2024: 6,6 (-0,1%)
- deutsche Importe: H1/2024: 3,6 (+1,0%)

Deutsche Exportgüter

Deutsche Exportgüter nach SITC
2023; % der Gesamtexporte



Deutsche Importgüter nach SITC (% der Gesamtimporte): 2023: Rohstoffe (ohne Brennstoffe) 27,0; Chem. Erzeugnisse 19,4; Maschinen 10,1; Erdöl 8,2; Gold 6,0; Mess- und Regeltechnik 4,0; Elektronik 3,0; Kohle 2,4; Sonstige Fahrzeuge 2,4; NE-Metalle 2,2; Sonstige 15,3

Rangstelle bei deutschen Exporten: 2023: 24 von 239 Handelspartnern

Rangstelle bei deutschen Importen: 2023: 35 von 239 Handelspartnern

Dienstleistungshandel (ohne Reiseverkehr) (Mrd. Euro, Veränderung zum Vorjahr in %, Abweichungen durch Rundungen)

	2021	%	2022	%	2023	%
Einnahmen	2,9	k.A.	4,3	48,6	4,1	-4,3
Ausgaben	2,9	k.A.	3,8	30,0	3,5	-7,7
Saldo	-0,1		0,5		0,6	

Deutsche Direktinvestitionen (Mio. Euro)

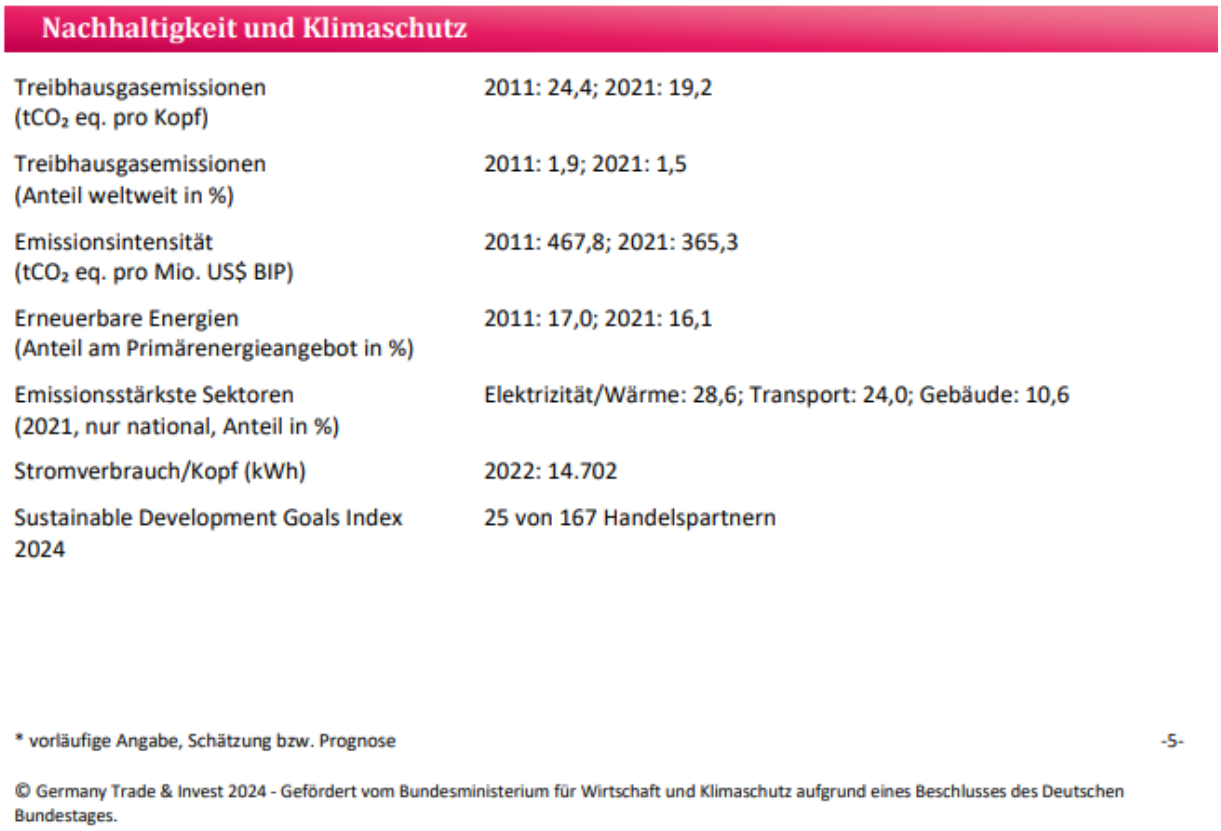
- Bestand: 2020: 19.518; 2021: 22.451; 2022: 23.166
- Nettotransaktionen: 2021: +498; 2022: +1.215; 2023: +38*

Direktinvestitionen Kanadas in Deutschland (Mio. Euro)

- Bestand: 2020: 483; 2021: 1.418; 2022: 243
- Nettotransaktionen: 2021: -2.592; 2022: +816; 2023: +572*

Doppelbesteuerungsabkommen: Abkommen vom 23.03.2002; in Kraft seit 28.03.2002

* vorläufige Angabe, Schätzung bzw. Prognose



Nachhaltigkeit und Klimaschutz

Treibhausgasemissionen (tCO_2 eq. pro Kopf)	2011: 24,4; 2021: 19,2
Treibhausgasemissionen (Anteil weltweit in %)	2011: 1,9; 2021: 1,5
Emissionsintensität (tCO_2 eq. pro Mio. US$ BIP)	2011: 467,8; 2021: 365,3
Erneuerbare Energien (Anteil am Primärenergieangebot in %)	2011: 17,0; 2021: 16,1
Emissionsstärkste Sektoren (2021, nur national, Anteil in %)	Elektrizität/Wärme: 28,6; Transport: 24,0; Gebäude: 10,6
Stromverbrauch/Kopf (kWh)	2022: 14.702
Sustainable Development Goals Index 2024	25 von 167 Handelspartnern

* vorläufige Angabe, Schätzung bzw. Prognose -5-

Abbildung 1: *Wirtschaftsdaten kompakt*

Weitere Informationen über Zivile Sicherheit – Cybersecurity mit Fokus auf Cloud und Data

Tabelle 1: GTAI Informationen zu Kanada

GTAI-Informationen zu Kanada	Link
Prognosen zu Investitionen, Konsum und Außenhandel	Wirtschaftsausblick von GTAI
Potentiale kennen, Risiken richtig einschätzen	Link zur SWOT-Analyse
Länderspezifische Basisinformationen zu relevanten Rechtsthemen in Kanada	Link zu Recht kompakt
Kompakter Überblick rund um die Wareneinfuhr in Kanada	Link zu Zoll und Einfuhr kompakt

Branchenspezifische Informationen

3.1 Zivile Sicherheit – Cybersecurity mit Fokus auf Cloud und Data in Kanada

Als flächenmäßig zweitgrößtes Land der Erde mit rund 40 Millionen Einwohnern, die hauptsächlich an den Küstenregionen des kanadischen Ostens und Westens angesiedelt sind, blickt Kanada auf eine weitläufig zu vernetzende Gesellschaft. Mit starken Migrationszahlen und dem Erschließen immer mehr digitaler Räume, wird der Schutz eben dieser digitalen Räume zu einer stetig wachesenden Herausforderung. Die kanadische Regierung hat hierzu im Rahmen des Action Plan for Critical Infrastructure im Jahr 2022 eine enge Zusammenarbeit zwischen Regierungsbehörden und Unternehmen im Bereich der digitalen kritischen Infrastruktur beschlossen. Ziele sind die Früherkennung von Gefahren im Datenverkehr und deren Prävention sowie ein engerer Austausch zwischen Regierungsbehörden und Privatwirtschaft. Ein verbessertes Risiko- und Notfallmanagement, wie z.B. im Fall von Cyberattacken, sollen Ausfälle von Einrichtungen der kritischen Infrastruktur vermindern.

Seit dem Aufkommen der Covid-19 Pandemie im Jahr 2020 erlebten 78 Prozent der kanadischen KMUs mindestens einen Cyberangriff jährlich. Dieser Wert stieg auf 85.7 Prozent im Jahr 2021 und auf knapp 90 Prozent im Jahr 2022. Die jährlich steigende Zahl von Cyberattacken verdeutlicht die Notwendigkeit von Schutzmaßnahmen und entsprechenden Produkten sowie Dienstleistungen. Laut dem National Cyber Threat Assessment 2023/2024 des Kanadischen Zentrums für Cybersecurity ist Ransomware eines der schädlichsten Formen von Cyberkriminalität in Kanada. Die kanadische Regierung plant im Rahmen ihrer *Cyber Security Strategy* über CAD 500 Mio. für die Sicherung von Regierungsnetzwerken und kritischer Infrastruktur sowie für Aufklärungsarbeit zu investieren. Laut dem Institut CyberEdge investierten kanadische Firmen 2021 lediglich 11.1 Prozent ihres jährlichen Budges für Cybersecurity, was in den Folgejahren einen positiven Trend verzeichnete. Die kanadische Regierung hat mit besonderem Augenmerk auf kritische Infrastruktur wie z.B. rund um Krankenhäuser, Transport-Infrastruktur sowie Flughäfen das *Canadian Cyber Incident Response Centre* eingerichtet und Firmen zur Forschung und Entwicklung an Schutzmaßnahmen aufgerufen. Innovative IT-Dienstleister und Produkthersteller aus den Bereichen Cybersecurity Cloudsicherheit, Überwachung und Sicherung von Log-In und Zahlungsdaten sowie vielen weiteren Geschäftsbereichen können dementsprechend in Kanada einen Absatzmarkt finden.

Die Nachfrage nach innovativen Lösungen im Bereich Cybersicherheit wird besonders durch neue Praktiken von Cyberkriminellen und fortlaufenden technologischen Fortschritten beeinflusst. Aufgrund des kontinuierlichen Anstiegs in Cyberattacken sieht sich Kanada, ebenso wie Deutschland, einem zunehmenden Sicherheitsrisiko und einer steigenden Zahl von Angriffen ausgesetzt. Durchschnittlich belief sich der Schaden, ausgelöst durch eine Cyberattacke, für eine kanadische Firma auf rund CAD 7 Mio. Neben den reinen Ausgaben für Cybersicherheit ist der Mangel an geschultem Personal im Umgang mit IT-Lösungen und Cybersicherheit ein weiterer Ansatzpunkt für Geschäftschancen. Viele Firmen sehen sich der Herausforderung gegenüber, ihre IT-Infrastruktur stetig anzupassen. Die europäische DSGVO bietet aufgrund ihrer Diversifizierung und Tiefe, viele Anhaltspunkte für die Ausarbeitung und Entwicklung eines Cybersicherheitsprogramms auf kanadischer Seite. Technische Lösungen und Dienstleistungen deutscher Firmen sind deswegen besonders gefragt. Die kanadische Bundesregierung sowie die Provinzregierungen nehmen sich dem Thema Cybersecurity, insb. Daten und Cloudsicherheit, wie zuvor erwähnt durch die Steigerung der geplanten Ausgaben für Cybersecurtiy im Haushalt, als auch durch eine Anpassung von vorhanden Leitlinien, wie dem *NIST Cybersecurity Framework (CSF)* an. Beides bietet beste Voraussetzungen für Geschäfts- und Kooperationspartnerschaften zwischen kanadischen und deutschen Akteuren.

In Kanada arbeiten alle Ministerien und Behörden, die im Bereich der Cybersecurity tätig sind, mit ***Public Safety Canada (PSC)*** zusammen, um die nationale Sicherheit und den Schutz der kanadischen Bürger zu gewährleisten. PSC ist für die Koordination aller Ministerien und Behörden, als auch die Veröffentlichung von Leitlinien zu den Grundlagen der Cybersicherheit für Kanadas kritische Infrastruktur zuständig. Das ***Communications Security Establishment (CSE)*** ist die Fachbehörde für Cybersicherheit und Informationssicherung und agiert auf Grundlage des *Communications Security Establishment Act* (S.C. 2019, c. 13). Im Rahmen seines Mandats betreibt das CSE auch das Kanadische Zentrum für Cybersicherheit und gibt Warnungen und Hinweise zu potenziellen, drohenden oder tatsächlichen Cyber-Bedrohungen, Schwachstellen oder Vorfällen heraus, die Kanadas kritische Infrastrukturen betreffen. Der am 14. Juni 2022 vorgelegte Gesetzentwurf *C-26* und die damit einhergehende Verabschiedung des *Critical Cyber Systems Protection Act* (CCSPA) beabsichtigt Kanadas Regierung rechtliche Anforderungen an Cyber-Security verstärken. Das Gesetz zielt darauf ab, in vier vom Bund regulierten Sektoren – Telekommunikation, Finanzwesen, interprovinzielle Pipeline- und

Stromleitungsanbieter, sowie Transportwesen – die Einrichtung von Cybersicherheitsprogrammen vorzugeben und Meldepflichten für Sicherheitsvorfälle zu schaffen. Es würde somit zu strengeren Compliance- und Meldepflichten für jene Betreiber kommen, die bislang nur rund ein Drittel der kanadischen Unternehmen erfüllt.

Der kanadische Markt für Cyber-Security wächst besonders durch die Nachfrage in den Bereichen Cloud-Sicherheit, IoT-Sicherheit, Cyber-Security Beratung, Managed Security Services, Datenschutz und Compliance durch expandierenden Onlinehandel. Der erhöhte Verkehr sensibler Daten und Zuwachs an digitalen Arbeitsplätzen steigert gemeinsam mit Technologien wie 5G die Anfälligkeit für Cyberattacken von privaten und Firmen-Netzwerken. Dies lässt die Risiken aber auch zugleich die Marktchancen im Bereich Cybersecurity merklich ansteigen. Der kanadische E-Commerce wuchs im Jahr 2023 auf über 74,5 Mrd. CAD an, relativ hierzu stiegen auch die Verluste durch Cyberattacken von acht Prozent auf 23 Prozent an. Zugleich erhöhten kanadische Unternehmen branchenabhängig seit 2019 ihre Ausgaben für Cybersecurity um 25 bis 50 Prozent.

Kanadas Sektor für Cybersecurity beschäftigte im Jahr 2022 rund 124.000 Fachkräfte. Zugleich werden mehr als 25.000 Experten und Fachkräfte in der Branche gesucht. Aufgrund der zunehmenden Frequenz an Cyberattacken durch die zunehmende Digitalisierung der Unternehmen wird der jährliche Wachstumsbedarf an Fachkräften auf 2.9 Prozent prognostiziert. Als Gegenmaßnahme investierte die kanadische Regierung im Jahr 2022 CAD 80 Mio. in das ***Nationale Cybersecurity Consortium (NCC)*** für die Leitung des ***Cyber Security Innovations Netzwerke (CSIN)*** und damit der Förderung der Wirtschaft, Forschung und Entwicklung zur Entwicklung von Fachkräften im Bereich der Cybersecurity. Marktchancen bestehen besonders für deutsche, DSGVO-konform operierende Cyber-Security Firmen, als auch für Bildungseinrichtungen und Institutionen mit Fokus auf Cybersecurity, insb. Daten und Cloudsicherheit.

<u>Toronto, Ontario</u>
Die Provinz Ontario bildet eines der größten Technologiezentren Nordamerikas für IT- und Cloud-Lösungen. Im September des Jahres 2021 eröffnete Google Cloud eine neue Cloud-Region in Toronto. Durch Unternehmenskooperationen und der damit beeinflussten Weiterentwicklung eines sicheren Cloud-Ecosystems, wie beispielsweise zwischen Think On Inc. und Lorica Cybersecurity, erhöht sich der Datenschutz für Kunden in der Cloud. Das 2023 von Ontarios Regierung eingerichtete Kompetenzzentrum für Cybersecurity unterstützt Regierungsministerien und öffentliche Organisationen durch Aufklärung, Anleitung und Bereitung in Cybersicherheit. Dazu gehört auch die online Lernportal „*Cyber Security Ontario*“. Im Gesundheitssektor Ontarios wurde in Zusammenarbeit mit dem Gesundheitsministerium das ***Ontario Health Cyber Security Center*** eingerichtet. Jene Initiativen sollen dazu dienen den vorliegenden Problemen Datenverlust und -missbrauch entgegenzuwirken sowie die Sicherheit im Umgang mit sensitiven Daten im Zeitalter der Industrie 4.0 zu erhöhen. Trotz ihrer technisch-wirtschaftlich starken Ausrichtung, ist Ontario im nationalen Vergleich die am stärksten von Cyberattacken betroffene Region. Zur Stärkung der digitalen Sicherheit und des Vertrauens der Bevölkerung wurde *Bill 194: the Strengthening Cyber Security and Building Trust in the Public Sector Act*, 2024 im Mai 2024 initiiert. Es umfasst Cybersecurity Standards, ein AI-Regierungsleitfaden, sowie Restriktionen im Umgang und der Verarbeitung von Personenbezogenen Daten. Mit einem Gesamtbudget von CAD 10 Mio, davon CAD 5 Mio. Förderung von der Provinzregierung Ontario, ist die ***Ontario Cybersecurity Excellence Initiative (OCEI)*** eine wichtige Initiative zur Förderung der Wettbewerbsfähigkeit und Widerstandsfähigkeit gegen Cyberattacken in den Bereichen Smart Infrastructure, Life Science, Mining, Manufacturing, Strafverfolgung und Automobilindustrie. Ziele sind, neue Sicherheitslösungen zu entwickeln, KMU in der Übernahme und Integration von Cybersicherheitstechnologien zu schulen und ihnen somit einen verbesserten Zugang zu internationalen Lieferketten zu eröffnen.

<u>Montreal, Quebec</u>
Die Provinz Quebec verfügt über ein fortschrittliches technologisches Ökosystem und eine wachsende Gemeinschaft von Fachkräften im Bereich der Cybersecurity. Von den etwa 10.000 IT-Unternehmen beherbergt die Stadt Montreal über 7.000, mit mehr als 170.000 Beschäftigten IT-Fachkräften, davon 26.000 im Bereich der Cybersecurity. Die strategische Lage mit geografischer Nähe zum kanadischen Regierungssitz in Ottawa, und die franco-englische, Bevölkerung mit Europäischem Kern erleichtern Geschäftsbeziehungen mit deutschen Firmen. Quebec ist Sitz von renommierten Forschungszentren, Firmen sowie Institutionen und Bildungseinrichtungen, wie der Université du Québec en Outaouais und das Artificial Intelligence for Cybersecurity Lab der Université de Montréal. Das Verteidigungsministerium förderte zuletzt die Concordia University in Höhe von mehr als 123 Millionen CAD zur Entwicklung u.a. von Technologien und Richtlinien im Bereich KI, IoT und Cybersicherheit. Zudem investieren Unternehmen wie Google, Facebook, Microsoft, SAP, Deutsche Telekom AG, Lufthansa Group und Software AG in lokale F&E. Mit dem diversen Talentpool, drei der besten Forschungsuniversitäten in ganz Kanada, den staatlichen

Unterstützungen und der Regierungsnähe ergeben sich gute Bedingungen für Firmen in der Provinz zu expandieren.

Die Nationale Cybersecurity Strategie in Kanada

Pillar 1: Partnerschaftliche Zusammenarbeit zum Schutz von Kanadiern und kanadischen Unternehmen vor Cyberkriminalität

1.1 Zivilgesellschaftliche Zusammenarbeit

Die kanadische Bundesregierung intensiviert die Zusammenarbeit zwischen föderalen, provinziellen und territorialen Behörden sowie mit indigenen Gemeinschaften und der Zivilgesellschaft. Ziel ist ein koordinierter Schutz der gesamten Bevölkerung und die Integration der meist privaten kritischen Infrastruktur in die nationale Sicherheitsstrategie. Im Rahmen dieses Transformationsprozesses etablierten ***Public Safety Canada*** und das ***Canadian Centre for Cyber Security das Canadian-Cyber Defence-Collective (CCDC)***. Das CCDC soll als nationales Multi-Stakeholder-Engagement-Gremium zur Förderung der Cyber-Resilienz Kanadas durch direkte öffentlich-private Partnerschaften die Cyber-Resilienz Kanadas stärken und nationale Sicherheitsherausforderungen adressieren.

1.2 Internationale Vertretung kanadischer Interessen

Die Regierung hat eine Erklärung zum internationalen Völkerrecht im Cyberspace veröffentlicht, um einen Beitrag zum laufenden internationalen Dialog über die Anwendung des Völkerrechts im Cyberspace zu leisten. Kanada treibt die Implementierung der UN-Normen für verantwortliches staatliches Verhalten voran, indem es ein besseres Verständnis und die Einhaltung seiner Normen für verantwortungsvolles staatliches Verhalten fördert. Gleichzeitig unterstützt die Regierung internationale Initiativen zum Aufbau von Kapazitäten zur Erkennung und Abwehr von Cyberbedrohungen, insbesondere durch eine verstärkte Zusammenarbeit im indopazifischen Raum.

1.3 Ausbau des nationalen Medienbewusstseins

Das Programm „***Get Cyber Safe***“ bietet den Kanadiern kostenlosen Zugang zu grundlegenden Tipps und Informationen zur Cyberhygiene. Das Kanadische Zentrum für Betrugsbekämpfung (*CAFC*), das Wettbewerbsamt und die kanadische Steuerbehörde koordinieren die Bemühungen zur Aufklärung über Betrug. Die Verbesserung der kollektiven Cyber-Hygiene und des Cyber-Bewusstseins gewährleistet die Sicherheit von mehr Kanadiern und verringert das Risiko, dass Kanadier Opfer von Cyber-Kriminalität werden. Überlegungen zur Cybersicherheit sollen in die täglichen Abläufe der kanadischen Unternehmen und in die kanadische Innovation einfließen, insbesondere in Sektoren von nationaler Bedeutung wie Gesundheit, Energie und grüne Technologie.

Pillar 2: Führende Rolle Kanadas in der Cybersecurity-Industrie

2.1 Priorisierung von Cybersecurity

Die kanadische Regierung beabsichtigt, gezielte Anreizsysteme zu etablieren, um Organisationen verstärkt dazu zu motivieren, den Schutz und die Sicherheit der Verbraucher als zentrale Komponente ihrer strategischen Geschäftsausrichtung zu betrachten. Zu diesem Zweck werden insbesondere Cybersicherheitszertifizierungen sowie die Auszeichnung vertrauenswürdiger Unternehmen durch Vergabe eines bevorzugten Auftragnehmerstatus evaluiert. Weiterhin plant die Regierung, spezifische Kennzeichnungssysteme für IoT-Geräte einzuführen, um Cybersicherheitsstandards transparenter darzustellen und deren Vergleichbarkeit zu erleichtern. Um die internationale Anerkennung und Kompatibilität dieser Maßnahmen sicherzustellen, strebt die kanadische Regierung eine verstärkte Zusammenarbeit und Koordination mit internationalen Partnern an. In diesem Zusammenhang kündigte die Regierung außerdem die Einführung des *Canadian Cyber Security Certification Program* an, welches derzeit noch vorrangig darauf abzielt, die Cybersicherheitsstandards im Verteidigungssektor signifikant zu erhöhen. Mittelfristig erwägt die kanadische Regierung jedoch, das Zertifizierungsprogramm über den Verteidigungssektor hinaus auf andere Branchen auszuweiten. Parallel hierzu sollen Maßnahmen zum Schutz der Privatsphäre im kanadischen Privatsektor verstärkt und klare Leitlinien für die verantwortungsvolle Entwicklung sowie den Einsatz von KI etabliert werden.

2.2 Ausbildung von Fachkräften

Die Initiative ***„Weiterbildung für die Industrie“*** ermöglicht Arbeitgebern, gezielt Qualifikationsbedarfe in schnell wachsenden Sektoren zu identifizieren und diese durch maßgeschneiderte Weiterbildungsangebote in Zusammenarbeit mit Bildungseinrichtungen zu adressieren. Hierdurch sollen über 15.000 Kanadier, darunter Personen mit unterrepräsentiertem Hintergrund, einen verbesserten Zugang zu Beschäftigungsmöglichkeiten erhalten. Zur Gewinnung von Fachkräften in der Cybersecurity Branche setzt die Regierung außerdem auf das Express-Entry-

Programm, das qualifizierten ausländischen Fachkräften die Einwanderung nach Kanada ermöglicht.

2.3 Unterstützung von Forschung

Als integraler Bestandteil des globalen Marktes bezieht Kanada einen Großteil seiner Cybersicherheitsprodukte derzeit von internationalen Anbietern. Um jedoch die eigene Cybersicherheitsbranche gezielt zu fördern und zugleich die globale Wettbewerbsfähigkeit sowie die nationale Cyber- und Wirtschaftssicherheit Kanadas nachhaltig zu stärken, beabsichtigt die kanadische Regierung, strategische Kooperationen mit Hochschulen sowie weiteren staatlichen Institutionen einzugehen. Ziel dieser Partnerschaften ist es, gezielt Forschung und Innovation innerhalb der kanadischen Cybersicherheitsindustrie voranzutreiben. Darüber hinaus wird die kanadische Regierung auch künftig mit Organisationen wie CANARIE zusammenarbeiten, um insbesondere die Sicherheitsinfrastrukturen innerhalb der kanadischen Forschungs- und Bildungslandschaft effektiv zu schützen und auszubauen.

Pillar 3: Bekämpfung von Cyberkriminalität

Die kanadische Regierung plant, die bisherigen Erfolge der Initiativen *„Get Cyber Safe“* und des ***Canadian Anti-Fraud Centre (CAFC)*** gezielt weiterzuentwickeln und dabei noch stärker auf die Expertise des Cyber Centre zurückzugreifen. Schwerpunkte bilden dabei aktuelle Themenbereiche wie künstliche Intelligenz, Risiken im Umgang mit großen Sprachmodellen (LLMs) sowie die frühzeitige Erkennung von Fehlinformationen, Desinformation und Malinformation (MDM). Durch gezielte Veröffentlichung von Informationsmaterialien und verstärkte Kommunikationsmaßnahmen soll die Zusammenarbeit und der Dialog mit der kanadischen Öffentlichkeit intensiviert werden, um ein erhöhtes Bewusstsein für neuartige und zunehmend komplexe Cyberbedrohungen zu schaffen. Im Zuge der fortschreitenden Digitalisierung, durch die sich neue Bedrohungsszenarien eröffnen, wird die kanadische Regierung ihre Kampagnen zur Sensibilisierung und Prävention kontinuierlich weiterführen und ausbauen, um auf nationaler Ebene die Cybersicherheit Kanadas nachhaltig zu stärken und zukünftigen Herausforderungen wirksam entgegenzutreten.

3.1 Identifizierung und Bekämpfung

Das *Communications Security Establishment Canada* führt im Rahmen seines Mandats Cyberoperationen gegen ausländische Eingriffe und staatlich gesteuerte feindliche Aktivitäten durch, häufig in Kooperation mit den *kanadischen Streitkräften (CAF)* und internationalen Verbündeten. Der *Canadian Security Intelligence Service (CSIS)* unterstützt die nationale Sicherheit durch gezielte Untersuchung cyberbezogener Bedrohungen, basierend auf seinen Mandaten zur Informationsbeschaffung und Gefahrenabwehr. Zusätzlich untersucht das *Federal Policing Cybercrime Program* der ***Royal Canadian Mounted Police (RCMP)*** cyberkriminelle Aktivitäten, insbesondere solche gegen Regierungseinrichtungen, kritische Infrastrukturen sowie bedeutende kanadische Unternehmen und Institutionen.

3.2 Verbesserung von Bekämpfungskapazitäten

Die kanadische Regierung setzt aktuell strategische Cybermaßnahmen ein, um die Effizienz und Profitabilität von Cyberkriminellen gezielt zu reduzieren, insbesondere hinsichtlich Ransomware-Angriffe und dem Handel mit gestohlenen Daten. Zusätzlich werden neue Instrumente zur Verhinderung von Lösegeldzahlungen geprüft, um Cyberkriminalität finanziell weniger attraktiv zu gestalten. Zu diesen Instrumenten gehört die Etablierung von Cyberversicherungspolicen, um gezielt Anreize für kriminelle Geschäftsmodelle zu verringern. Im Einklang mit der *Counter Ransomware Initiative (CRI)* wird die Regierung die Zusammenarbeit mit der Industrie intensivieren, um Unternehmen aktiv von Lösegeldzahlungen abzuhalten. Abschließend verfolgt die Regierung einen umfassenden Ansatz zur Verstärkung der nationalen Sicherheits- und Strafverfolgungskapazitäten.

3.3 Resilienz von kritischer Infrastruktur

Eigentümer und Betreiber kritischer Infrastrukturen sehen sich zunehmend gezielten, finanziell gut ausgestatteten und technologisch fortschrittlichen Cyber-Angriffen gegenüber. Solche Vorfälle können das Vertrauen in Netzwerke, Betriebssysteme sowie öffentliche und private Institutionen, die den Schutz sensibler und personenbezogener Daten verantworten, beeinträchtigen. Aufgrund der vielfältigen Organisationsstrukturen, die Kanadas kritische Infrastrukturen betreiben, ist eine enge Zusammenarbeit zwischen Regierung und Privatwirtschaft entscheidend, um Informationssysteme, Betriebstechnologien, industrielle Kontrollsysteme und Software-Lieferketten umfassend abzusichern. Zu diesem Zweck arbeitet die kanadische Regierung kontinuierlich mit Industriepartnern und Interessenvertretern, insbesondere im Rahmen der *Global Coalition on Telecommunications*, zusammen, um widerstandsfähige Lieferketten sowie sichere und interoperable Telekommunikationsstandards zu gewährleisten. Darüber hinaus unterstützt sie aktiv die Initiativen wichtiger Cybersicherheitsorganisationen wie der ***Canadian Internet Registration Authority (CIRA)***, ***Rogers Cybersecure Catalyst, Canadian Cyber Threat Exchange (CCTX)*** und

CANARIE. Zukünftig wird zudem das *Canadian Cyber Defence Collective (CCDC)* eine zentrale Rolle als Plattform für sektorübergreifende Abstimmungen hinsichtlich kritischer Infrastrukturen einnehmen. Um die Widerstandsfähigkeit gegenüber Cyberangriffen weiter zu stärken, baut die kanadische Regierung ihre Kapazitäten zur Prävention und Reaktion auf Cybervorfälle kontinuierlich aus. Insbesondere das ***Canadian Centre for Cyber Security*** stellt eine zunehmende Zahl fortschrittlicher Cybersicherheitsmaßnahmen für Betreiber kritischer Infrastrukturen bereit, um essenzielle nichtstaatliche Dienste wie das Banken- und Telekommunikationswesen noch besser zu schützen und zu unterstützen.

Stabinstitutionen in der Kanadischen zivilen Sicherheitsbranche

Die folgenden Einrichtungen übernehmen zentrale Cyber-Rollen und -Funktionen und fungieren als primäre Schnittstellen zur kanadischen Regierung, die der Öffentlichkeit uneingeschränkt zugänglich sind. Die Strategie der kanadischen Regierung die Zugänglichkeit für alle kanadischen Bürger und Organisationen jeder Größenordnung zu gewähren, folgt dem Aufruf zur gemeinsamen Zusammenarbeit im Kampf gegen Cyber-Vorfälle und Cyberkriminalität. Es soll die digitale Kompetenz aller gestärkt und das öffentliche Bewusstsein geschärft werden, um künftig alle Vorfälle, unabhängig von deren Art, erfassen zu können. Die gezielte Ressourcenzuweisung verfolgt das Ziel Cyber-Innovationen zu fördern und Öffentliche Institutionen, Gemeinden sowie Unternehmen bei der Verbesserung ihrer Cyber-Resilienz zu unterstützen.

Canadian Centre for Cyber Security (Communications Security Establishment Canada)

Das Canadian Centre for Cyber Security ist zuständig für die fachkundige Beratung, Anleitung, Dienstleistungen und Unterstützung zur Förderung der Cybersicherheit.

Public Safety Canada

Public Safety Canada war federführend in der Entwicklung der Nationalen Cybersecurity Strategie und ist als Regierungsdepartment für die öffentliche Sicherheit und den Katastrophenschutz zuständig.

Royal Canadian Mounted Police (RCMP)

Das RCMP National Cybercrime Coordination Centre (NC3) arbeitet mit kanadischen Strafverfolgungsbehörden sowie nationalen und internationalen Partnern zusammen, um die Bedrohung, Auswirkungen und die Zahl der Opfer von Internetkriminalität in Kanada zu verringern.

Canadian Security Intelligence Service

Der nationale Nachrichtendienst der kanadischen Regierung, insbesondere für die Abwehr von Terrorismus und den Schutz der kritischen Infrastruktur verantwortlich.

In Kapitel 3.4 wird auf weitere wichtige öffentliche und nicht öffentliche Institutionen eingegangen.

3.2 Marktpotenziale und -chancen

3.2.1 Marktchancen in der kanadischen zivilen Sicherheit – Cybersecurity

Es besteht eine Vielzahl an Marktchancen für deutsche Unternehmen im Bereich zivile Sicherheitstechnologien und -dienstleistungen mit dem Fokus auf Cybersecurity, insb. Daten und Cloudsicherheit. In den Provinzen Ontario und Quebec sind mit rund 700.000 KMUs von insgesamt 1.3 Millionen kanadischen Unternehmen die größten regionalen Marktchancen für Anbieter von IT-Lösungen für KMU vorhanden. Markchancen mit Fokus auf Cybersecurity und Cloudsicherheit ergeben sich für Produkte und Dienstleistungen aus den Bereichen Datenschutz- und Compliance Lösungen, Cloud Sicherheit, Cybersecurity und Lösungen zur Sicherheit der IoT-Umgebung. In Kanada ansässig sind bereits Unternehmen wie Siemens AG, Infineon Technologies AG, Atos Canada, Nagarro SE, Rohde & Schwarz Canada Inc. und Bechtle AG mit ihrer Global IT-Alliance. Dem kanadischen Fachkräftemangel im Cybersecurity-Sektor können deutsche Unternehmen mit Inhouse-Schulungsformaten sowie Beratungsdienstleistungen gewinnbringend entgegenwirken. Da viele kanadische Firmen ihre Unternehmens- und Kundendaten nach eigenen Angaben nicht ausreichend sichern, bieten sich besonders im Angebot von sicheren Cloudlösungen Marktchancen für deutsche Anbieter. Kanadas hohe politische Bereitschaft für Förderung von Innovationen im IT-Bereich stärkt die langfristigen Geschäftschancen für deutsche Unternehmen, die sich auf Cybersecurity insbesondere Daten und Cloudsicherheit spezialisiert haben. Im Zuge des vorliegenden Antrags wurde eine Einschätzung der Marktchancen mit diversen Partnern

(siehe unten) in persönlichen Gesprächen abgefragt und von diesen kritisch eingeschätzt. Die kollektiv positiven Rückmeldungen der befragten relevanten Vertreter bestärken die bestehende Einschätzung der AHK Kanada.

3.2.2. Cloud und Daten als Schlüsselthema

Der rasante technologische Wandel im Kontext von Industrie 4.0, begleitet von zunehmender Digitalisierung und Integration cloudbasierter Dienste, stellt kanadische Unternehmen und Organisationen vor komplexe Herausforderungen im Bereich Cybersecurity. Während die digitale Transformation enorme Chancen für Effizienzsteigerungen und Innovation bietet, geht sie gleichzeitig mit einer Zunahme von Cyberbedrohungen einher, die erhebliche Auswirkungen auf Unternehmen, kritische Infrastrukturen und die nationale Sicherheit Kanadas haben. Allein in der ersten Jahreshälfte 2024 registrierte Statistics Canada 41.162 Fälle von Cyberkriminalität, wobei Betrug und Identitätsdiebstahl mit einem Anteil von 56 % dominierten. Trotz eines leichten Rückgangs der insgesamt betroffenen Unternehmen (16 % im Jahr 2023 gegenüber 21 % im Jahr 2019) nahmen spezifische Angriffsmethoden, insbesondere Identitätsdiebstahl (31 %, +11 Prozentpunkte) und Betrug (50 %, +6 Prozentpunkte), deutlich zu. Der verstärkte Einsatz cloudbasierter Technologien erhöht zudem Risiken wie Fehlkonfigurationen, reduzierte Transparenz und unvollständige Datenlöschung, was die Einführung moderner Sicherheitslösungen wie Cloud Native Application Protection Platforms (CNAPPs), Zero-Trust-Modellen und KI-gestützter Systeme zur Bedrohungserkennung notwendig macht. Trotz dieser Entwicklungen sehen 61 % der Unternehmen Sicherheits- und Compliance-Bedenken weiterhin als größte Hürde bei der Cloud-Adoption und 76 % beklagen einen erheblichen Mangel an Cloud-Sicherheitsexpertise. Darüber hinaus verschärfen sich Datenschutzanforderungen, wodurch quantensichere Verschlüsselung sowie Continuous Threat Exposure Management (CTEM) zunehmend relevant werden. Die zunehmende Rolle des Datenschutzes wird besonders in Anbetracht der fast 62,919 von der Polizei im Jahr 2024 gemeldeten Verstößen im Zusammenhang mit Betrug (Betrug, Identitätsbetrug und Identitätsdiebstahl) im Bereich der Cyberkriminalität deutlich. Eine Steigerung um 200% gegenüber 2019. Laut der Canadian Internet Use Survey stieg der Anteil der Kanadier, die Cybersicherheitsvorfälle erlebt haben, von 58 % im Jahr 2020 auf 70 % im Jahr 2022. Der Erhalt von unerwünschtem Spam (60 %) und der Erhalt betrügerischer Inhalte (40 %) waren die häufigsten Vorfälle. Der National Cyber Threat Assessment 2023–2024 hebt besonders die Bedrohungen kritischer Infrastruktur durch Cyberkriminelle und staatlich unterstützte Akteure hervor, während der 2023 CIRA Cybersecurity Survey zeigt, dass generative KI als potenzielles Sicherheitsrisiko betrachtet wird, wobei nur 32 % der Unternehmen über entsprechende KI-Richtlinien verfügen. Insgesamt verdeutlichen diese Entwicklungen die Notwendigkeit, dass kanadische Unternehmen und Einzelpersonen in robuste Cybersicherheitsmaßnahmen investieren, ihre Teams gezielt schulen und eine enge Kooperation mit spezialisierten Anbietern anstreben müssen, um den wachsenden digitalen Bedrohungen wirksam entgegenzuwirken.

3.2.3 Industrieinteresse in zivile Sicherheitslösungen - Cybersecurity

Die weltweite Wirtschaft hat bedingt durch die beschleunigte digitale Transformation im Kontext von Industrie 4.0 ein zunehmendes Interesse an umfassenden Cybersicherheitslösungen. Die Einführung von Automatisierung, IoT-Technologien, cloudbasierten Diensten und fortschrittlicher Datenanalyse steigert die Angriffsfläche für Cyberbedrohungen erheblich und führt zu einem erhöhten Risikoprofil der Unternehmen. Cybersicherheitsvorfälle, die kritische Infrastruktursektoren wie die Energieversorgung, das Finanz-, Gesundheits- und Verkehrswesen betreffen, bergen erhebliche Gefahren für die operative Kontinuität, wirtschaftliche Stabilität sowie nationale Sicherheit. In Kanada haben sich die finanziellen Folgen solcher Vorfälle zwischen 2021 und 2023 drastisch verschärft, wobei die Ausgaben zur Wiederherstellung nach Cyberangriffen von etwa 860 Millionen CAD im Jahr 2021 auf rund 1,7 Milliarden CAD im Jahr 2023 anstiegen. Im Jahr 2023 berichteten 13 % der betroffenen Organisationen, Opfer eines Ransomware-Angriffs geworden zu sein, gegenüber 11 % im Jahr 2021. 88% dieser Unternehmen entschied sich gegen eine Lösegeldzahlung. Von den zahlungsbereiten Unternehmen beglichen 84 % Beträge unter 14.300 CAD, während 4 % Zahlungen über 716.000 CAD tätigten. Die Entwicklung deutet darauf hin, dass, obwohl der prozentuale Anteil betroffener Unternehmen leicht rückläufig ist, der wirtschaftliche Schaden pro Vorfall signifikant zunimmt.

Parallel dazu erzwingen strenge regulatorische Vorgaben, darunter das kanadische Datenschutzgesetz PIPEDA, von Organisationen ein höheres Maß an Cybersicherheitsmaßnahmen zur Einhaltung gesetzlicher Vorschriften sowie zur Sicherstellung des Verbrauchervertrauens. Zudem erhöht die zunehmende Komplexität und Professionalität der Cyberbedrohungen, sichtbar durch die steigende Zahl von Ransomware-Angriffen und wachsende Sicherheitsbedenken bezüglich generativer KI, den Bedarf an proaktiven und technologisch fortgeschrittenen Sicherheitslösungen. Hinzu kommt ein erheblicher Mangel an qualifizierten Cybersicherheitsfachkräften in Kanada. Derzeit sind etwa 25.000 Stellen unbesetzt, was die Unternehmen dazu zwingt, vermehrt auf automatisierte und ganzheitliche Cybersicherheitsstrategien zu setzen, um diese Kompetenzlücken effektiv zu schließen. Investitionen in präventive und detektive Cybersicherheitsmaßnahmen nahmen vergleichsweise moderat zu. Von rund 14 Milliarden CAD im Jahr 2021 auf rund

15,7 Milliarden CAD im Jahr 2023. Knapp die Hälfte dieser Ausgaben entfiel auf große Unternehmen (6,8 Milliarden CAD), gefolgt von mittleren (5,4 Milliarden CAD) und kleinen Unternehmen (3,7 Milliarden CAD). Zugleich ging der Anteil der Unternehmen, die in Prävention und Detektion investieren, von 61 % (2021) auf 56 % (2023) zurück. Obgleich der Fachkräftemangel ein brisantes Thema ist, stellen die Personalkosten mit 5,4 Milliarden CAD die größten Ausgaben dar. Der Anteil der Unternehmen mit eigenem Cybersicherheitspersonal sank im Jahr 2023 auf 50 %. Zum Entgegenwirken gegen den eignen Fachkräftemangel nehmen Unternehmen vermehrt externe Beratungs- und Dienstleistungsleistungen in Anspruch und investierten gezielt in Cybersicherheitsschulungen für nicht-technisches Personal sowie Lieferanten und Geschäftspartner, mit 2,7 Milliarden CAD die drittgrößte Position hinter Cybersicherheitssoftware (4,2 Milliarden CAD). Darüber hinaus investierte etwas mehr als jedes fünfte Unternehmen (22 %) gezielt in Cybersicherheitsschulungen für nicht-technisches Personal sowie Lieferanten und Geschäftspartner, was Kosten von insgesamt über 430 Millionen CAD verursachte.

Insgesamt haben sich robuste Cybersicherheitskonzepte somit nicht nur zur notwendigen Risikominderung, sondern auch zur essenziellen Voraussetzung für den Schutz der Unternehmensreputation, Wettbewerbsfähigkeit und langfristigen Geschäftskontinuität entwickelt.

3.2.4 Vorreiterprojekte

Das ***Cyber Security Innovation Network (CSIN)***, eine Initiative der Bundesregierung zur Stärkung des nationalen Cybersicherheitsökosystem Kanadas, hat das Ziel die Forschung und Entwicklung zu verbessern, die Kommerzialisierung von IT-Sicherheit zu steigern und den Talentpool des Landes zu erweitern. Diese pan-kanadische Initiative wird vom ***National Cybersecurity Consortium (NCC)*** geleitet, einer föderal gegründeten gemeinnützigen Organisation, der die Concordia University, die Ryerson University, die University of Calgary, die University of New Brunswick und die University of Waterloo angehören. Ihre Projekte konzentrieren sich auf den Schutz kritischer Infrastrukturen, der Privatsphäre, datenschutzfördernde Technologien, menschenzentrierte Cybersicherheit, Softwaresicherheit und Netzsicherheit.

3.3 Aktuelle Gesetze, Initiativen und Finanzierung

3.3.1 Gesetze

Am 6. Februar 2025 kündigte die kanadische Regierung ihre neue *National Cyber Security Strategy (NCSS)* an. Das neue NCSS umfasst zwei übergreifende Prinzipien, die Kanadas Ansatz zur Cybersicherheit leiten werden. Durch Gesellschaftliches Engagement sollen Partnerschaften mit wichtigen Interessengruppen, etwa mit anderen Regierungsebenen, Strafverfolgungsbehörden, indigenen Gemeinschaften, dem Privatsektor, der Wissenschaft und der Zivilgesellschaft vertieft werden, um entscheidende Fragen in der Cybersicherheitslandschaft anzugehen. können. Durch agile Führung sollen Cybersicherheitslösungen in enger Zusammenarbeit mit Partnern und Interessengruppen entwickelt und in den kommenden Jahren in einer Reihe von themenspezifischen Aktionsplänen dargelegt werden, die der kanadischen Regierung die Möglichkeit bieten, kontinuierlich in die kanadische Cybersicherheit zu investieren.

In diesem Zuge wurde eine Änderung des Telekommunikationsgesetzes durch den Gesetzentwurf *C-26* beschlossen. Dieser gibt der Bundesregierung die rechtliche Befugnis, kanadischen Telekommunikationsdienstanbietern zu verbieten, bestimmte Anbieter zu nutzen, die als "risikoreich" gelten. Die Änderungen würden es der Bundesregierung ermöglichen, ihre erklärte Absicht umzusetzen, Huawei und ZTE die Teilnahme an 5G-Netzen zu verbieten und Telekommunikationsunternehmen zu verpflichten, alle von den Unternehmen bereitgestellten 4G-Geräte bis Ende 2027 zu entfernen oder zu beenden. Diese Änderungen würden sich in erster Linie auf TSPs und andere Unternehmen in der Telekommunikationslieferkette auswirken.

<u>Schutz personenbezogener Daten</u>

Der Schutz personenbezogener Daten in Kanada beruht auf strikten gesetzlichen Vorgaben, die Organisationen zur Implementierung robuster Cybersicherheitsmaßnahmen verpflichten, um Datenverlust, Diebstahl und unbefugten Zugriff zu verhindern. Gemäß dem *Personal Information Protection and Electronic Documents Act (PIPEDA)* sind Unternehmen dazu verpflichtet Datenschutzverletzungen umgehend zu melden, betroffene Personen zu benachrichtigen und Vorfälle detailliert zu dokumentieren. Ergänzend dazu erweitert der im Jahr 2023 verabschiedete *Bill C-26 (An Act Respecting Cyber Security)* und der *Bill C-27 (Digital Charter Implementation Act, 2022)* gezielt die Datenschutz- und Cybersicherheitsstandards, indem sie staatliche Kompetenzen im Schutz kritischer Infrastrukturen stärken und die Regelungen für den privaten Sektor modernisieren. Zudem schreibt das Datenschutzgesetzen auf Bundes- und Provinzebene (z. B. *PIPEDA, Alberta's PIPA, BC's PIPA*) vor, dass Organisationen für die Einhaltung der

Sicherheitsvorkehrungen verantwortliche Personen benennen müssen. Nationale Aufsichtsbehörden haben darüber hinaus Leitfäden und Best Practices veröffentlicht, die als Empfehlungen für die Erstellung von Vorfallreaktionsplänen, Cyber-Risikobewertungen sowie Penetrationstests dienen. Diese sind zwar nicht rechtsbindend, jedoch kann die Nichtbefolgung zu Compliance-Verstößen führen. Organisationen wird daher dringend empfohlen, standardisierte Maßnahmen zur Cyber-Risikoanalyse, Vorfallreaktion, Schwachstellenbewertung und Penetrationstests in ihre unternehmensweiten Sicherheitsrichtlinien zu integrieren.

Unternehmensregelungen

Im Juli 2022 veröffentlichte das ***Office of the Superintendent of Financial Institutions (OSFI)*** die endgültige Fassung der Richtlinie *B-13*, in der die Erwartungen des OSFI in Bezug auf den Einsatz von Technologie durch ***„Federally Regulated Financial Institutions“ (FRFI)***, also föderal regulierter Finanzinstitutionen, und bewährte Praktiken des Cyber-Risikomanagements dargelegt sind. Im April 2023 veröffentlichte das OSFI den ***„Intelligence Led Cyber Resilience Test“ („I-CRT“)***, ein Rahmenwerk zur Ermittlung von besonders gefährdeten Bereichen fur Cyberangriffe. Seit 2023 erwartet das OSFI, dass systemrelevante Banken und international tätige Versicherungsgruppen mindestens alle drei Jahre eine I-CRT-Bewertung durchführen. In Übereinstimmung mit Leitlinie *B-13* werden die FRFI die Tests insgesamt verwalten, während das OSFI von den FRFI erwartet, dass sie Maßnahmen ergreifen, um auf Schwachstellen zu reagieren, indem sie die Widerstandsfähigkeit gegen Cyber-Angriffe und -Störungen verbessern.

3.3.2 Zertifizierung

Global

Der **ISO/IEC 15408** ist der international anerkannte Standard für IT-Sicherheitszertifizierungen, welcher insbesondere für öffentliche Einrichtungen und Betreiber kritischer Infrastruktur herangezogen wird und für die meisten Firewalls und Verschlüsselungssysteme unerlässlich ist.

Des Weiteren werden folgende allgemeine Sicherheitsstandards in Kanada vorausgesetzt:

ISO/I7EC 27001	Der globale Standard für Information Security Management Systems (ISMS)
ISO/IEC 27017	Für Cloud Services
ISO/IEC 27018	Für den Schutz von persönlichen Daten in Cloudumgebungen
ISO/IEC 22301	Für die Betreiber von kritischer Infrastruktur zum kontinuierlichen Erhalt ihres Geschäftes
ISO/IEC 27701	Für das Management von persönlichen Daten. Für kanadische Gesetze zum persönlichen Datenschutz relevant.

Kanada

Für den Umgang mit persönlichen Daten ist in Kanada die Einhaltung von *PIPEDA*, dem Gesetz zum Schutz persönlicher Daten, obligatorisch. Darüber hinaus wird von kanadischen Kunden und Regierungsbehörden häufig die Einhaltung des *SOC 2 Standards*, insbesondere der *Typen I und II*, vorausgesetzt. Als Kunde von Regierungsinstitutionen oder Betreiber von kritischer Infrastruktur wird allgemein die Zertifizierung durch das *Canadian Centre for Cyber Security* empfohlen, welches 13 allgemeine Sicherheitskontrollen speziell für KMUs bereitstellt. Ebenso sollten die ***IT Security Requirments (ITSR)*** und das ***Contract Security Program (CSP)*** erfüllt sein.

Wenn auf öffentliche Gesundheits- oder Bildungseinrichtungen abgezielt wird ist das *CSP* des Public Services and Procurement Department zu beachten, welches die Daten von kanadischen Institutionen und Bürgern sichern soll. Dabei werden die privaten Angebote von den Behörden auf Datenlücken geprüft. Bei Geschäftstätigkeiten in diesen Bereichen wird angeraten, sich unter anderem bei ***ProServices, Task-Based Informatics Professional Services (TBIPS)*** und ***Cloud***

Framework Agreements zu registrieren. Im Gesundheitssektor müssen ***HiPAA***-kompatible Praktiken entwickelt werden, falls ein Austausch mit US-amerikanischen Kunden vorgesehen ist. In Ontario muss ebenso eine Kompatibilität mit ***PHIPA*****,** welches persönliche Gesundheitsdaten verwaltet gewährleistet sein. Allgemein müssen Daten bei Übermittelung immer verschlüsselt sein und spezielle Anforderungen lokaler Gesundheitsnetzwerke überprüft werden. Im Bildungssektor müssen Cloud-Dienstleistungen allgemein mit den Datenvorschriften der jeweiligen Bildungsanstalten übereinstimmen. Dabei werden insbesondere die Systeme ***ISO 27001, SOC 2*** und ***Canadian data residency*** genutzt.

Im Finanzsektor müssen die Guidelines des **OSFI** zur Finanzstabilität befolgt werden.

Optional sind die Nutzung des ***NIST Cybersecurity Framework***, einer Guideline des U.S. National Institute of Standards and Technology (NIST), welches ein Vertrauensvorteil bei nordamerikanischen Kunden bringen kann. Daneben kann das Zurückgreifen auf das ***TAA Compliance*** für öffentliche Vereinbarungen hilfreich sein, welches im Rahmen des Trade Agreement Acts Importprodukte in die USA zertifiziert. Des Weiteren wird die ***Accessibility Certification (WCAG 2.1 Level AA)*** oft für Weiterbildungs-Software genutzt.

Bereich	**Verbindlichkeit**	**Zertifizierung/Standard**
Cloud- und Datensicherheit (Bundesebene)	Ja	PIPEDA
Cloud- und Datensicherheit (Provinzebene)	Ja	PHIPA, HIA, Law 25
Cloud- und Datensicherheit	Stark empfohlen	ISO 27001, ISO 27018, SOC 2
Public Procurement	Falls relevant	CSP, Supply Arrangements
Gesundheitssektor	Ja	PHIPA, HIPAA-equivalent
Bildungssektor	Je nach Institution vorgeschrieben	SOC 2, WCAG, ISO 27001
Data Hosting in Kanada	Oft vorausgesetzt	Canadian-hosted cloud
Cloud- und Datensicherheit	Optional	CyberSecure Kanada NIST/CIS Frameworks

3.3.3 Initiativen

Cyber security innovation network

Im Februar 2022 kündigte François-Philippe Champagne, der damalige Minister für Innovation, Wissenschaft und Industrie, an, dass das *National Cybersecurity Consortium* für den Zeitraum von vier Jahren mit bis zu 80 Millionen kanadischen Dollar zur Leitung des *Cyber Security Innovation Network* gefördert werde. Das NCC wurde 2020 durch Cybersicherheits-Kompetenzzentren an fünf kanadischen Universitäten gegründet: der University of Calgary, der Concordia University, der University of New Brunswick, der Ryerson University sowie der University of Waterloo. Ziel des Cyber Security Innovation Network-Programms war es, ein nationales Cybersicherheitsnetzwerk zu etablieren, welches durch an Hochschulen angegliederte Fachzentren für Cybersicherheit koordiniert wurde. Das Netzwerk umfasste mindestens drei solcher Zentren und wurde in enger Kooperation mit der Privatwirtschaft sowie weiteren relevanten Stakeholdern aufgebaut. Zentrale Ziele der Initiative waren die nachhaltige Stärkung der Forschung und Entwicklung (F&E) im Bereich Cybersicherheit auf nationaler Ebene, die gezielte Beschleunigung der Kommerzialisierung innovativer Cybersicherheitslösungen sowie der Aufbau einer robusten und diversifizierten Talentpipeline im Bereich Cybersicherheit in Kanada. Im Vordergrund des Netzwerks standen insbesondere die Förderung der interdisziplinären Zusammenarbeit zwischen Hochschulen, Privatwirtschaft und weiteren Partnern sowie die Reduzierung bestehender Hürden bei der Kommerzialisierung von Cybersicherheitsprodukten und -dienstleistungen. Zusätzlich widmete sich das Netzwerk intensiv der Vertiefung und Diversifizierung des kanadischen Talentpools im Bereich Cybersicherheit. Dazu gehörten insbesondere Maßnahmen zur Rekrutierung und langfristigen Bindung

hochqualifizierter Lehrkräfte und Trainer, die Weiterentwicklung zielgerichteter Ausbildungsprogramme sowie Investitionen in innovative Lehrpläne und gezielte Fortbildungs- und Umschulungsangebote für Fachkräfte.

Center for Cyber Security (Cyber Centre)

Das Cyber Centre unterstützt die Regierung bei der Weiterentwicklung der internen Cyber-Expertise, etwa durch seinen Learning Hub, der die Kompetenzen im Bereich Cybersicherheit innerhalb der Verwaltung stärkt und gleichzeitig kanadische Hochschulen darin unterstützt, ihre Lehrpläne an die Anforderungen des Arbeitsmarktes anzupassen. In enger Zusammenarbeit mit dem *Communications Security Establishment* engagiert sich das Cyber Centre gezielt dafür, unterrepräsentierte Bevölkerungsgruppen zu motivieren, eine Ausbildung und Karriere in den MINT Bereichen zu verfolgen. Zudem arbeitet die kanadische Regierung mit Partnern aus anderen Regierungsstellen, dem Bildungssektor und der Privatwirtschaft zusammen, um eine qualifizierte und vielfältigen Talentpool im Bereich Cybersicherheit aufzubauen. Im Rahmen des *Cyber Security Cooperation Program (CSCP)* stellt *Public Safety* Canada Fördermittel für Initiativen bereit, die darauf abzielen, Cyberkriminalität zu reduzieren, den Schutz kritischer Infrastrukturen zu verbessern, das Cybersicherheitsbewusstsein der Bevölkerung zu erhöhen sowie die Cyber-Kompetenzen und internationale Wettbewerbsfähigkeit Kanadas langfristig zu stärken.

Programm für Cybersicherheit und kritische Energieinfrastrukturen (CCEIP)

Die kanadische Regierung unterstützte im Rahmen ihrer nationalen Cybersicherheitsstrategie von 2019 bis Ende 2024 das *CCEIP* mit einer Gesamtförderung von 2,42 Millionen kanadischen Dollar. Ziel dieser Initiative war es, die Cybersicherheit sowie die Resilienz nationaler und grenzüberschreitender Energieinfrastrukturen substanziell zu erhöhen. Die im Rahmen des CCEIP finanzierten Projekte konzentrierten sich darauf, die Fähigkeit des Energiesektors zur Prävention, Vorbereitung, Reaktion und schnellen Erholung von Cyberbedrohungen gezielt zu stärken. Besonderer Fokus lag dabei auf der Behebung von Schwachstellen industrieller Kontrollsysteme (ICS). Zu den Kernzielen zählten ein verbessertes Risikomanagement entlang der Lieferkette – einschließlich Integritätsprüfung, Identifikation gefälschter Komponenten und Konformitätskontrolle industrieller IoT-Geräte –, sowie die systematische Identifikation, Bewertung und gezielte Reduktion von Cyberrisiken. Zusätzlich wurden Maßnahmen umgesetzt, um den Zugang zu zeitnahen Informationen über Cyberbedrohungen zu verbessern sowie die Kapazitäten zur Überwachung, Erkennung und Reaktion auf Cybervorfälle auszubauen.

Programme zur Anwerbung von Fachkräften

Das *Cyber Centre* hat mit seiner Lerneinrichtung zur Weiterentwicklung der Cyber Workforce und der Lehrpläne kanadischer postsekundärer Einrichtungen beigetragen, um so den Anforderungen des Arbeitsmarktes besser gerecht zu werden. Das *Communications Security Establishment Canada* und das *Cyber Centre* arbeiten daran, unterrepräsentierte Gruppen zu ermutigen, eine Ausbildung und Karriere in den MINT Bereichen zu verfolgen. Dazu gehören auch verbesserte Bildungsmöglichkeiten, einschließlich erweiterter Ausbildungs- und Ausbildungsprogramme für den privaten Sektor. Darüber hinaus stellt *Public Safety Canada* über das *Cyber Security Cooperation Program (CSCP)* Zuschüsse und Beiträge zu diversen Initiativen bereit, die darauf abzielen, die Cyberkriminalität zu reduzieren, Kanadas Fähigkeit zum Schutz seiner kritischen Infrastrukturen zu stärken, das Bewusstsein der Kanadier für Cybersicherheit zu erhöhen, die Cybersicherheitsfähigkeiten der Kanadier zu erweitern und die Wettbewerbsfähigkeit Kanadas auf globaler Ebene zu verbessern.

3.3.4 Finanzierung

Kanada trägt durch steuerliche Anreize, strategisch ausgerichtete Förderungsprogramme und umfassenden Unterstützungsangeboten maßgeblich zur Entwicklung innovativer Sicherheitstechnologien, Qualifizierungsmaßnahmen für die Ausbildung und Umschulung von Fachkräften und die aktive Förderung der Zusammenarbeit mit privatwirtschaftlichen Akteuren u.a. im Bereich der Bedrohungserkennung und -abwehr bei. Zentrale Programme wie der Accelerated Investment Incentive und die steuerliche Förderung durch das Scientific Research and Experimental Development (SR&ED) -Programm senken insbesondere für KMU die Investitions- und F&E-Kosten erheblich. Hinzunehmend wird der Zugang zu öffentlichen Aufträgen u.a. durch Procurement Assistance Canada erleichtert. Insbesondere bietet das *Cyber Security Innovation Network* Unterstützung für Forschungs-, Entwicklungs- und Kommerzialisierungsprojekte. Weitere finanzielle Unterstützung zur Verbesserung der Cyberresilienz kommunaler Infrastrukturen sowie zur Modernisierung sicherheitskritischer Notfallkommunikationssysteme bietet u.a. das Asset Management Planning Program und das Next Generation. Jene Förderungsprogramme können sowohl von inländischen, als auch von internationalen Unternehmen beansprucht werden, solange ihr Fokus auf der Innovationsförderung und dem Ausbau von nationalen Sicherheitskapazitäten zur

Stärkung der Cybersecurity und zivilen Sicherheit von Kanada liegen.

3.4 Weitere wichtige öffentlichkeitswirksame Institutionen und Wettbewerbssituation

3.4.1 Staatliche Institutionen und ihre Aufgaben im Bereich der zivilen Sicherheit

Innovation, Science and Economic Development Canada (ISED)

Im Jahr 2022 stellte ISED CAD 80 Mio für das *Cyber Security Innovation Network* bereit, um ein breit angelegtes kanadisches Kommunikationssystem für Cybersecurity zu etablieren. Hervorgegangen ist das Department 2015 aus dem zu vorigen Department Industry Canada. Mit den von ihnen bereitgestellten Fördergeldern sollen Investitionsbedingungen kontinuierlich verbessert, Innovationsleistungen gesteigert, und somit Kanadas Anteil am Welthandel erhöht und ein fairer, effizienter und wettbewerbsfähiger Markt ermöglicht werden.

Natural Resources Canada

Natural Resources Canada ist die federführende Bundesbehörde für Cybersicherheit im Energiesektor und unterstützt die Umsetzung von Initiativen im Rahmen des *Emergency Management Act, der National Strategy for Critical Infrastructure* und *der National Cyber Security Strategy.* Gegründet im Jahr 1994 ist es zuständig für die Bundesgesetzgebung im Bereich der natürlichen Ressourcen, Energie, Wälder, Mineralien und Metalle.

Transport Canada

Transport Canada war 2020 federführend in der Erstellung der *Canada Vehicle Cyber Security Guidance*, Leitlinien zur Verbesserung der Cybersicherheit von Fahrzeugen. Gegründet im Jahr 1935 ist es zuständig für die Verkehrspolitik und -programme und fördert einen sicheren, effizienten und umweltfreundlichen Transport.

National Research Council (NRC)

Das *CIC-NRC Cybersecurity Collaboration Consortium* setzt sich zusammen aus dem NRC und dem Canadian Institute for Cybersecurity (UNB-CIC) der University of New Brunswick. Der Schwerpunkt der Forschung liegt auf der Sicherheit des Internet of things (IoT), dem Schutz kritischer Infrastrukturen und der Sicherheit von Zugängen in die kanadischen Cybernetze, insbesondere von staatlichen Behörden.

Public Services and Procurement Canada

Ein Department unter Leitung von Ali Ehsassi, welches 1996 gegründet wurde. Public Services and Procurement Canada unterstützt Bundesministerien und -behörden bei ihren täglichen Aufgaben als zentraler Einkäufer, Immobilienverwalter, Schatzmeister, Buchhalter, Gehalts- und Rentenverwalter, Integritätsberater, gemeinsamer Dienstleister und Sprachbehörde.

In Bezug auf Cybersecurity formuliert die Behörde Anforderungen an Lieferanten von Verteidigungsaufträgen oder anderen sicherheitskritischen Geschäftsfeldern in Bezug auf Kompatibilität und Qualitätssicherung der Produkte mit der kanadisches Cybersicherheitsorganisation.

Standards Council of Canada

Der Standards Council of Canada ist Kanadas nationales Normungsgremium und führende Akkreditierungsorganisation. Gegründet im Jahr 1970 als staatliches Unternehmen, arbeitet dieser mit einem ausgedehnten Netzwerk von Partnern im Inland und in der ganzen Welt zusammen. Dieser soll Vertrauen auf dem Markt sicherstellen, indem die Konformitätsbewertungsstellen die höchsten Erwartungen erfüllen.

Der Council ist ebenfalls in das CPCSC-Programm als Zertifizierungsanstalt eingebunden (siehe „Public Services and Procurement Canada“). Im März 2025 werden diese einen Cybersicherheitsstandard für Unternehmen einführen, welche im Rahmen von Verteidigungsaufträgen mit sensiblen, nicht als Verschlusssache eingestuften Regierungsinformationen umgehen.

3.4.2 Größte kanadische Unternehmen für Cybersecurity

Open Text

Die OpenText Corporation, gegründet im Jahr 1991 aus einer akademischen Kooperation zwischen der University of Waterloo und der Oxford University, hat sich zu einem der bedeutendsten Softwareunternehmen Kanadas entwickelt. Mit rund 14.400 Mitarbeitenden (Stand: 2022) gilt OpenText als das viertgrößte Softwareunternehmen des Landes. Das Unternehmen ist ein zentraler Akteur im Bereich Enterprise Information Management (EIM) und bietet umfassende Lösungen in den Bereichen Enterprise Content Management, Cloud-basierte Dienste, Digital Asset Management, LegalTech und Business Process Management. Im Kontext der Cybersicherheit ist OpenText insbesondere durch seine Cybersecurity-Suite unter dem Namen OpenText Security Solutions relevant, die Funktionen wie Threat Detection, E-Mail-Sicherheit, Endpunktabsicherung sowie Data Loss Prevention umfasst. Durch strategische Übernahmen – u.a. von Guidance Software und Carbonite – hat sich OpenText als ein Schlüsselakteur im Bereich datenbasierter Sicherheit und forensischer Analyse etabliert und trägt damit wesentlich zur Absicherung digitaler Infrastrukturen in Kanada bei.

Softchoice

Softchoice, ist ein in Toronto ansässiger IT-Lösungsanbieter, der auf Cloud-Infrastruktur, Software-Services und moderne Arbeitsplatzlösungen spezialisiert ist. Als Teil des globalen Technologieunternehmens World Wide Technology (WWT) profitiert Softchoice vom Zugriff auf das Advanced Technology Center, ein weltweit führendes Innovationslabor für Hardware- und Softwareintegration. In der kanadischen Cybersicherheitslandschaft spielt Softchoice eine bedeutende Rolle als Integrator KI-gestützter Cloud-Sicherheitslösungen, insbesondere für hybride IT-Umgebungen in kleinen und mittleren Unternehmen (KMU) sowie im öffentlichen Sektor. Das Unternehmen fördert zudem Zero-Trust-Modelle und Managed Security Services, was seinen Beitrag zur professionellen IT-Sicherheitsinfrastruktur in Kanada unterstreicht.

Absolute Software

Im Jahr 1993 in Vancouver gegründet, hat sich das Unternehmen als führender Anbieter von Cybersicherheitslösungen für Endgeräte etabliert. Das Unternehmen ist insbesondere durch seinen in Firmware verankerten „Persistence"-Agenten bekannt, der die Widerstandsfähigkeit gegen Angriffe auf Laptops, Tablets und andere Endgeräte auch bei Deinstallation oder Manipulation aufrechterhält. Die Lösung ist für behördliche Einrichtungen, Bildungseinrichtungen sowie den privaten Sektor konzipiert und ermöglicht umfassende Kontrolle über Geräteflotten, inklusive Remote-Löschung, Policy Enforcement und Echtzeit-Überwachung.

Cybeats Technology

Cybeats wurde 2016 in Toronto gegründet und ist spezialisiert auf Sicherheitslösungen für die Software Supply Chain und IoT-Infrastrukturen. Durch die Integration von Sicherheitsmechanismen bereits in der Entwicklungsphase von Software und vernetzten Geräten ermöglicht Cybeats einen „Security-by-Design"-Ansatz, der für die Einhaltung regulatorischer Anforderungen (z. B. NIST, IEC 62443) zunehmend an Bedeutung gewinnt.

3.5 Zivile Sicherheit – Cybersecurity in Ontario

Cybersecurity-Strategie von Ontario

Im Jahr 2020 initiierte das Ministerium für Regierungs- und Verbraucherdienste von Ontario das Expertengremium für Cybersicherheit im breiteren öffentlichen Sektor *(„Broader Public Sector Cyber Security Expert Panel", BPS)*, um Kommunen, Organisationen und Unternehmen in Ontario bei der Erhöhung ihrer Widerstandsfähigkeit gegen Cyberbedrohungen gezielt zu unterstützen. Das Mandat dieses Expertengremiums umfasste insbesondere die systematische Identifizierung und Analyse sowohl allgemeiner als auch sektorspezifischer Cybersicherheitsrisiken sowie die Erarbeitung entsprechender Handlungsempfehlungen zur Unterstützung der Regierung bei der Implementierung wirksamer Risikominderungsmaßnahmen innerhalb des BPS-Sektors.

Zur nachhaltigen Umsetzung und Sicherstellung der langfristigen Wirksamkeit seiner strategischen Empfehlungen formulierte das Gremium fünf zentrale Leitprinzipien: Orientierung am öffentlichen Interesse, verantwortliche Führung, Förderung kontinuierlicher Weiterbildung und Kompetenzentwicklung, Sicherstellung der Rechenschaftspflicht der beteiligten Akteure sowie die Ermöglichung fortlaufender Verbesserungen der Cybersicherheitsstandards innerhalb der vielfältigen Organisationen des BPS.

Im Zeitraum zwischen 2019 und 2022 fokussierten sich die Aktivitäten der Cybersicherheitsstrategie insbesondere auf

den Ausbau und die Diversifizierung der eingesetzten Cybertechnologieplattformen innerhalb des ***Ontario Public Service (OPS)***. Ziel war es, die Überwachungskapazitäten sowie die Qualität der Bedrohungsanalysen signifikant zu verbessern. Durch diese erweiterten technischen Plattformen gelang es dem OPS, Cyberrisiken proaktiv zu steuern und gleichzeitig die Nutzererfahrung für OPS- und BPS-Kunden sicherer und effizienter zu gestalten. Das Ministerium für öffentliche und geschäftliche Dienstleistungen und Beschaffung führte regelmäßig standardisierte Reifegradbewertungen der Cybersicherheit innerhalb des OPS durch, basierend auf etablierten Branchenstandards und Leitlinien. Diese Bewertungen erfolgten dabei ganzheitlich und umfassten neben technologischen Aspekten auch menschliche Faktoren und Prozessabläufe, einschließlich operativer Prozesse sowie bestehender Sicherheitsmaßnahmen. Die Cybersicherheitsprozesse wurden kontinuierlich an veränderte gesetzliche, regulatorische und geschäftliche Anforderungen angepasst, um sicherzustellen, dass sowohl technologische als auch organisatorische Maßnahmen im gesamten Lebenszyklus von Produkten und Betriebsabläufen aktuell bleiben und den sich wandelnden Bedürfnissen der Bevölkerung Ontarios gerecht werden.

Aktuelle Gesetze

Im Jahr 2024 verabschiedete die Provinz Ontario das Gesetz *„Bill 194 – Strengthening Cyber Security and Building Trust in the Public Sector Act“,* mit dem der *„Enhancing Digital Security and Trust Act“ (EDSTA)* eingeführt wurde. Ziel dieser Gesetzesinitiative ist es, einen regulatorischen Rahmen zur Stärkung der Cybersicherheit, zum verbesserten Schutz personenbezogener Daten – einschließlich sensibler Daten von Kindern – sowie zur Etablierung eines verantwortungsvollen Umgangs mit Künstlicher Intelligenz (KI) im öffentlichen Sektor Ontarios zu schaffen. Mit dieser Gesetzgebung positioniert sich Ontario als eine der ersten Jurisdiktionen Kanadas, die eine ganzheitliche rechtliche Grundlage für die drei zentralen Pfeiler digitaler Sicherheit im öffentlichen Sektor – Cybersicherheit, Datenschutz und KI-Governance – implementiert. Die Verabschiedung des EDSTA unterstreicht das strategische Ziel der Provinz, digitales Vertrauen zu stärken, regulatorische Transparenz zu gewährleisten und eine innovationsfördernde Governance-Struktur zu etablieren. Im Dezember 2024 veröffentlichte Ontario zudem das *„Trustworthy Artificial Intelligence Framework“*, das erstmals in Kanada verbindliche Leitlinien für den verantwortungsvollen Einsatz von KI im öffentlichen Sektor formuliert. Die Rahmenvorgaben verpflichten Ministerien und nachgeordnete Behörden zur Durchführung eines systematischen KI-Risikomanagements, wenn KI-Systeme in die Entwicklung oder Bereitstellung öffentlicher Programme und Dienstleistungen eingebunden werden. Darüber hinaus adressiert das Framework Anforderungen in Bezug auf Transparenz, Nachvollziehbarkeit sowie Rechenschaftspflicht und setzt damit Maßstäbe für eine verantwortungsvolle und ethisch fundierte Nutzung algorithmischer Systeme im Verwaltungskontext. Das Gesetz EDSTA ermächtigt die Provinzregierung zur Festlegung detaillierter Verordnungen und Richtlinien zur Cybersicherheit für Organisationen des öffentlichen Sektors. Dies schließt die verpflichtende Einführung von Cybersicherheitsprogrammen sowie die Implementierung technischer Standards ein. Die Ausarbeitung solcher Verordnungen erfolgt in enger Abstimmung mit den betroffenen Akteuren und unter Berücksichtigung sektoraler Besonderheiten. Alle geplanten regulatorischen Maßnahmen unterliegen einem öffentlichen Konsultationsprozess über das Ontario Regulatory Registry, wodurch ein partizipativer und transparenter Gesetzgebungsprozess gewährleistet wird. Zur Sicherstellung einer umfassenden Interessensvertretung führt die Provinz kontinuierliche Konsultationen mit Schlüsselakteuren des öffentlichen Sektors durch, darunter indigene Gemeinschaften, postsekundäre Bildungseinrichtungen, zivilgesellschaftliche Organisationen, Technologie- und Rechtsexpertinnen und -experten, die Ontario Human Rights Commission sowie den Information and Privacy Commissioner of Ontario. Ziel dieser kooperativen Vorgehensweise ist es, zukünftige Verordnungen im Rahmen des EDSTA evidenzbasiert, inklusiv und wirksam zu gestalten.

Aus- und Weiterbildungsmöglichkeiten im Bereich Cybersecurity

Verschiedene Institutionen bieten cyberbezogene Programme auf Bachelor-, Master-, College- und Berufsebene an (z. B. die Bachelor- und Master-Abschlüsse der University of Toronto mit Schwerpunkt auf Identität, Datenschutz und Sicherheit, die Cybersicherheits-Diplomprogramme des Seneca College und Rogers Cybersecure Catalyst). Das ***Ministry of Public and Business Service Delivery and Procurement (MPBSD)*** und andere entwickeln Partnerschaften mit *Rogers Cybersecure Catalyst*, um das BPS-Bewusstsein und Schulungen zu unterstützen. MPBSD hat mehrere Module auf dem Cyber Security Ontario Learning Portal veröffentlicht, die eine Vielzahl von Cybersicherheitsthemen abdecken, welche darauf abzielen, Organisationen auf die Herausforderungen einer zunehmend digitalen Zukunft vorzubereiten. MPBSD organisiert zudem jährlich eine Cybersicherheitskonferenz für die BPS (gegründet 2020), die vom *Cyber Security Centre of Excellence* in Ontario veranstaltet wird.

Das *Cyber Security Centre of Excellence* hilft bei der Aufklärung von Ministerien, BPS-Organisationen und kommunale Partner über Cybersicherheit und bewährte Praktiken aufklären, damit die Informationen für die Bürger von Ontario

sicher und geschützt sind. Es bietet Beratung, Anleitung, Informationen, Kurse und Dienstleistungen, um die digitale Widerstandsfähigkeit zu stärken und gleichzeitig die Erwartungen an die Bereitstellung digitaler Dienste zu erfüllen. Das Cyber Security Centre of Excellence bietet in Zusammenarbeit mit *Emergency Management Ontario* Schulungen zur Cybersicherheit für Gruppen an, die wichtige Grundlagenkenntnisse vermitteln. Darüber hinaus entwickelt und fördert das Cyber Security Centre of Excellence vielfältige und integrative Initiativen zur Sensibilisierung für Cybersicherheit und OPS-Schulungen für alle Lernstufen, unterstützt durch eine Vielzahl gemeinsamer und maßgeschneiderter Inhalte und praktischer Aktivitäten, die unter ***cybersecurityontario.ca***. verfügbar sind. Abschließend bildet die in 2023 eingeführte *K-12-Zone* eine Online-Ressource für Schüler, Lehrer und Eltern, um sie über die Bedeutung der Online-Sicherheit zu informieren.

Wirtschaftliches Akteurfeld Ontario

Ontario stellt mit rund 40% des gesamten nationalen Bruttoinlandsprodukts das wirtschaftliche Zentrums Kanada dar und verfügt über ein hochdiversifiziertes, technologieorientiertes Wirtschaftsökosystem. Die Provinz profitiert von seinem divers ausgeprägtem Wirtschaftsfeld besonders in den Sektoren der Informations- und Kommunikationstechnologie (IKT), Künstliche Intelligenz, Quantenforschung, Cloud-Computing und Cyber Security. Mit mehr als 400.000 Beschäftigten in der Informations- und Kommunikationstechnologie (IKT) ist die Provinz einer der größten Informationstechnologie-Cluster in Nordamerika. Herausragende Forschungseinrichtungen wie das ***Quantum Valley in Waterloo***, bestehend u.a. aus ***Perimeter Institute***, das ***Institute of Quantum Computing***, die ***Quantum NanoFab Facility***, die ***Quantum Valley Ideas Laboratories***, und dem ***Quantum Valley Investment***, und die Präsenz global agierender Unternehmen wie IBM, OpenText, SAP und Oracle verschaffen der Provinz einen signifikanten Standortvorteil. Ein wesentliches Element der Innovationsinfrastruktur Ontarios ist das ***Vector Institute for Artificial Intelligence*** in Toronto, das eine Schlüsselrolle bei der Erforschung und Kommerzialisierung von KI-Anwendungen übernimmt und enge Verbindungen zur Industrie pflegt. Weitere bedeutende Akteure sind das ***Rogers Cybersecure Catalyst*** in Brampton sowie das ***Ontario Cybersecurity Centre of Excellence***, die beide Cybersicherheitskapazitäten im öffentlichen und privaten Sektor gezielt stärken. Das kanadische Forschungsförderprogramm ***Mitacs*** fördert zudem gezielt praxisnahe Forschungskooperationen im Bereich Cybersecurity zwischen Hochschulen und Industriepartnern. Ergänzt wird dieses Innovationsökosystem durch non-for-profit Organisationen wie der Cyber Security Global Alliance (CSGA) und durch strategische Investitionen in Forschung und Entwicklung, insbesondere im Bereich der industriellen Telekommunikation. Rund 90 % der industriellen Telekommunikationsforschung findet in Ottawa statt, sowie durch gezielte Fördermaßnahmen für Schlüsseltechnologien wie KI und 5G. Allein im Zeitraum 2022–2023 wurden in Ontario mehr als 20.500 neue Arbeitsplätze im KI-Sektor geschaffen, 27 KI-Unternehmen gegründet und 1,1 Mrd. CAD an Risikokapital generiert. Zugleich steht die Region vor demografischen und strukturellen Herausforderungen, zum einen durch die alternde Bevölkerung, dem steigenden Fachkräftemangel, einem leicht unter dem nationalen Durchschnitt steigenden Produktivitätswachstum von 1,1%, zum anderen durch den zeitgleich stark zunehmenden globalen Wettbewerb. Zugleich bietet Ontario strategische Chancen durch die aktive Förderung zukunftsweisender Technologien wie generativer Künstlicher Intelligenz, und der zivilen Sicherheitstechnologien, fortgeschrittenen Netzwerken, Quanten- und Halbleitertechnologien und deren wirtschaftliches Potenzial langfristig signifikante Produktivitätsgewinne verspricht, sowie in einer robusten Zuwanderungspolitik, die zur Stabilisierung des Erwerbspersonenpotenzials beiträgt. Zuletzt ist die demografische Lage mit der Nähe zu den United States of Amerika ein Standortvorteil. Dies verschafft der Provinz eine vorteilhafte Position zur Bewältigung struktureller Herausforderungen und zur Sicherung nachhaltigen Wirtschaftswachstum.

3.6 Zivile Sicherheit – Cybersecurity in Quebec

Cybersecurity-Strategie von Quebec

Das ***Centre québécois d'excellence numérique (CQEN)***, eine Einrichtung, die sich ausschließlich mit der digitalen Transformation der Regierung befasst, wurde im Juni 2019 mit einer klaren Mission gegründet: die digitale Transformation durch die Förderung von Austausch und Zusammenarbeit zu beschleunigen und zu erleichtern. Ziel ist es, den Einsatz von Automatisierung oder künstlicher Intelligenz in öffentlichen Dienstleistungen mit Regierungsbezug zu verbessern.

Das im Jahr 2020 gegründete Regierungszentrum für Cyberverteidigung (***„Centre gouvernemental de cyberdéfense“***, CGCD) trägt die Verantwortung für den Schutz der digitalen Infrastrukturen in der Provinz Québec. Zu den Kernaufgaben des CGCD zählen insbesondere die kontinuierliche Überwachung und proaktive Bekämpfung von Cyberrisiken und Bedrohungen, die auf öffentliche Einrichtungen und Ministerien abzielen. Darüber hinaus gehört es zum Mandat des CGCD, bekannte Sicherheitslücken auf Regierungsebene frühzeitig zu identifizieren und wirksam zu

schließen sowie umfassende Schutzmaßnahmen zur Sicherung staatlicher Datenbestände umzusetzen. Diese Aufgabe erfüllt das CGCD in enger Abstimmung mit dem Regierungsnetzwerk für Cyberverteidigung, das nahezu 30 operative Zentren für Cyberabwehr (***„Centres opérationnels de cyberdéfense", COCDs***) umfasst und somit sämtliche staatliche Institutionen der Provinz Québec im Bereich Cybersicherheit abdeckt.

Im Juni 2021 wurde die *„Strategie zur Integration künstlicher Intelligenz in die öffentliche Verwaltung 2021–2026"* verabschiedet, die zum Ziel hat, Québec als Vorbild im Einsatz von KI-Technologien im öffentlichen Sektor zu positionieren. Diese Strategie dient sowohl als wichtiger Katalysator für die digitale Transformation öffentlicher Prozesse als auch als Instrument zur Bewältigung bestehender Fachkräfteengpässe.

Aktuelle Gesetze

Das seit 2021 geltende Gesetz zur Steuerung der Informationsressourcen öffentlicher Einrichtungen in Québec *G-1.03 „Loi sur la gouvernance et la gestion des ressources informationnelles"*, verpflichtet öffentliche Institutionen, jährliche Pläne zur digitalen Transformation aufzustellen und kontinuierlich an die Digitalisierungsstrategie 2024–2028 anzupassen. Hierdurch muss aufgezeigt werden, wie die Maßnahmen jener Einrichtungen zu den strategischen Regierungszielen beitragen, und als Grundlage für koordinierte Aktivitäten im Bereich Cybersicherheit und Digitalisierung dienen.

Am 22. September 2021 verabschiedete Québec mit dem *Gesetz 25„QC Privacy Law"* eine umfassende Modernisierung des Datenschutzgesetzes für den privaten Sektor. Die Änderungen umfassen verpflichtende Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen, Anforderungen an Datenschutz-Folgenabschätzungen (z.B. bei Datentransfers außerhalb Québecs oder Einführung neuer Informationssysteme) sowie eine ausdrückliche Zustimmungspflicht bei der Verarbeitung sensibler personenbezogener Daten.

Aus- und Weiterbildungsmöglichkeiten in Quebec

Das *Programm für Cybersicherheitsinitiativen (CIP)*, welches seit Herbst 2020 für Hochschulen und bestimmte Forschungszentren angeboten wird, besteht aus fünf Initiativen. Diese werden von *CANARIE*, einer non-profit-Organisation des nationalen Forschungs- und Bildungsnetzwerks Kanadas entwickelt und in Partnerschaft mit *RISQ* für förderfähige Einrichtungen in Quebec bereitgestellt. Dieses nationale Kooperationsprogramm zielt darauf ab, relevante Initiativen zu finanzieren, welche der kanadische Bildungs- und Forschungssektor als vorrangig im Hinblick auf die Cybersicherheit betrachtet. Somit wird die Konsolidierung von Aktivitäten und die Entwicklung von Fachwissen im Bereich der Cybersicherheit ermöglicht.

Wirtschaftliches Akteurfeld Quebec

Das wirtschaftliche Profil der Provinz Québec ist gekennzeichnet durch ein zunehmend diversifiziertes Exportportfolio sowie ein hochentwickeltes, staatlich unterstütztes Innovationsökosystem im Bereich der KI und Cybersicherheit. Seit 2016 hat sich Québec zu einem der weltweit führenden KI-Zentren entwickelt und belegt aktuell Rang sieben unter den globalen KI-Ökosystemen. Diese Position wurde durch gezielte Investitionen von etwa 975 Mio. CAD sowie strategische Maßnahmen zur Integration von KI in die öffentliche Verwaltung, steuerliche Anreize, günstige Standortkosten und den Aufbau international wettbewerbsfähiger akademischer Institutionen wie ***MILA – Montreal Artificial Intelligence Institute*** – erreicht. MILA gilt als eine der weltweit führenden Forschungseinrichtungen im Bereich des Deep Learning und spielt eine zentrale Rolle in der Entwicklung und Umsetzung angewandter KI-Lösungen in Wirtschaft und öffentlicher Verwaltung. Das starke Innovationsumfeld wird zudem durch Programme wie Mitacs unterstützt, die Hochschulen und Industriepartner miteinander vernetzen, um gezielt hochqualifizierte Fachkräfte in technologieintensiven Bereichen wie KI und Cybersicherheit auszubilden und in Québec zu halten. Der wirtschaftliche Akteursraum in Québec ist dabei eng mit zentralen Cybersicherheitsinstitutionen verknüpft. Das ***Centre gouvernemental de cyberdéfense (CGCD)*** koordiniert die Cyberabwehraktivitäten auf Ebene der Provinzverwaltung und arbeitet mit fast 30 operativen Cyberabwehrzentren (*COCDs*) zusammen, um die digitale Infrastruktur öffentlicher Einrichtungen effektiv zu schützen. Ergänzt wird dieses Ökosystem durch universitäre Forschungszentren, technologieorientierte Start-ups sowie etablierte Unternehmen mit Schwerpunkten in kritischen Infrastrukturen, Softwareentwicklung und digitaler Sicherheit. Private Investitionen in KI und Cybersicherheit beliefen sich zwischen 2017 und 2021 auf knapp 2 Mrd. CAD während KI-bezogene Aktivitäten allein in diesem Zeitraum mehr als 2 Mrd. CAD zum BIP beitrugen. Trotz dieser Stärken steht Québec vor strukturellen Herausforderungen, insbesondere aufgrund der alternden Bevölkerung und dem steigenden Fachkräftemangel. Gleichzeitig bietet die technologische Spezialisierung, das robuste Forschungsumfeld und die institutionalisierte Zusammenarbeit zwischen Staat, Wissenschaft und Wirtschaft Québec substanzielle strategische Chancen, sich dauerhaft als international wettbewerbsfähiger Standort für KI und Cybersicherheit zu positionieren.

3.7 Künftige Entwicklungen in den relevanten Segmenten und Nachfragesektoren

Schätzungen zur Marktentwicklung

Vor dem Hintergrund zunehmender digitaler Vernetzung und wachsender Bedrohungslagen zeigt die zivile Sicherheitsbranche in Kanada ein deutliches Wachstumspotenzial. Prognosen zufolge wird der kanadische Cybersicherheitsmarkt im Jahr 2025 ein Volumen von rund CAD 20,58 Mrd. erreichen und bis 2030 auf etwa CAD 34,68 Mrd. anwachsen. Die Einführung neuer Technologien wie 5G beschleunigt nicht nur die Digitalisierung von Wirtschafts- und Verwaltungsstrukturen, sondern erhöht auch die Komplexität und Verwundbarkeit digitaler Infrastrukturen – insbesondere in Bereichen wie kritische Infrastruktur, Telekommunikation und Cloud-Systeme. Damit einhergehend entstehen neue Geschäftschancen für etablierte Anbieter wie auch für neue Marktteilnehmer, die mit innovativen Lösungen zur Absicherung vernetzter Systeme auftreten. Gleichzeitig bleibt der Markt durch strukturelle Herausforderungen geprägt. So verzeichnet Kanada trotz hoher Nachfrage einen signifikanten Mangel an qualifizierten Fachkräften im Bereich der Cybersicherheit: 2021 lag die Zahl entsprechender Arbeitskräfte bei lediglich 123.969 – im Vergleich zu über 1,14 Mio. in den USA und rund 300.000 im Vereinigten Königreich. Die zunehmende Frequenz und Raffinesse von Cyberangriffen verstärken diesen Druck zusätzlich: Bereits 2021 berichteten rund 39 % der kanadischen Unternehmen von Ransomware-Vorfällen, während 65 % der befragten nicht-betroffenen Firmen mit künftigen Angriffen rechnen. Diese Rahmenbedingungen verdeutlichen nicht nur die wachsende Bedeutung robuster Sicherheitslösungen, sondern machen auch den Aufbau strategischer Fachkräftekapazitäten und Investitionen in nationale Innovationsökosysteme zu einem zentralen Handlungsfeld für Politik und Wirtschaft.

Zivile Sicherheitslösungen

Im Jahr 2023 verfügte etwas mehr als jedes vierte kanadische Unternehmen (26 %) über schriftlich festgelegte Cybersicherheitsrichtlinien, was dem gleichen Anteil wie im Jahr 2021 entspricht. Im gleichen Zeitraum erhöhte sich der Anteil der Unternehmen mit einer Cyberrisikoversicherung auf 22 %, ein Anstieg um sechs Prozentpunkte gegenüber 2021 (16 %). Die abgeschlossenen Versicherungspolicen deckten typischerweise direkte Schäden durch Cybervorfälle (53 %), Kosten für die Wiederherstellung von Software, Hardware und elektronischen Daten (44 %), Betriebsunterbrechungen (39 %) sowie finanzielle Folgeschäden (38 %) ab. Der Anteil der Unternehmen, die aktive Maßnahmen zur Identifikation von Cybersicherheitsrisiken ergriffen, blieb mit 59 % im Jahr 2023 gegenüber 60 % im Jahr 2019 stabil. Die häufigsten Sicherheitsmaßnahmen waren dabei die kontinuierliche Überwachung von Netzwerk- und Geschäftssystemen (46 %) sowie die gezielte Beobachtung des Risikoverhaltens von internen Mitarbeitenden („Insider Threat Monitoring“) mit 22 %.

Internationale Sicherheitsrisiken

Kanada erlebt aktuell eine zunehmende Anfälligkeit im Bereich der Cybersicherheit, geprägt durch eine Vielzahl an Bedrohungen, deren Auswirkungen auf Unternehmen, öffentliche Institutionen und Bürger zunehmend spürbar werden. Das *Communications Security Establishment Canada* sowie dessen nationale und internationale Partner, insbesondere innerhalb der Five-Eyes-Allianz, beobachten und analysieren kontinuierlich die Aktivitäten staatlicher und nichtstaatlicher Akteure im Cyberraum. Im Rahmen des jüngsten Berichts *„National Cyber Threat Assessment 2025–2026“*, veröffentlicht durch das *Canadian Centre for Cyber Security* (Teil des CSE), werden detaillierte Analysen zu gegenwärtigen und potenziellen zukünftigen Cyberbedrohungen präsentiert. Der Bericht dokumentiert insbesondere die Methoden und Strategien relevanter Akteure und bietet eine sachliche Prognose zur Entwicklung der Bedrohungslage in den kommenden zwei Jahren. Diese Einschätzungen dienen öffentlichen und privaten Entscheidungsträgern als Grundlage für eine fundierte Risikoeinschätzung und effektive strategische Planung im Bereich Cybersicherheit.

3.8 Die Zukunftstrends für 2025

Clouds

Fortinet zufolge nutzen 82 % der befragten Unternehmen heute Cloud-Umgebungen, um eine größere Skalierbarkeit, Flexibilität und Ausfallsicherheit zu erreichen. Zu diesem Zweck ist der Anteil der hybriden Clouds auf 54 % gestiegen, was es den Unternehmen ermöglicht, ihre lokalen Systeme mit öffentlichen Cloud-Plattformen zu integrieren. Mit diesem Ansatz können Unternehmen die Bereitstellung ihrer Anwendungen je nach Bedarf optimieren und dabei ein Gleichgewicht zwischen Kontrolle und Compliance herstellen. So können IT-Teams beispielsweise öffentliche Clouds für kundenorientierte Anwendungen nutzen, während sensible Daten in ihren privaten Umgebungen sicher aufbewahrt werden.

61 % der Befragten gaben jedoch an, dass Sicherheits- und Compliance-Bedenken die größten Hindernisse für die Einführung der Cloud darstellen. So müssen beispielsweise Gesundheitsdienstleister, die Patientendaten in die Cloud migrieren, die HIPAA-Vorschriften einhalten und gleichzeitig sensible Daten schützen.

Diese Herausforderungen werden durch die Lücke bei den Cybersecurity-Fähigkeiten noch verschärft. 76 % der Unternehmen geben an, dass es ihnen an Fachwissen und Personal für die Cloud-Sicherheit mangelt, was ihre Möglichkeiten zur Bereitstellung und Verwaltung umfassender Sicherheitslösungen einschränkt. Dieser Mangel unterstreicht die Notwendigkeit gezielter Schulungen und Weiterbildungen, um die Lücke zu schließen und die Strategien für die Cloud-Bereitstellung zu überdenken, um die Komplexität zu verringern und die Sicherheitseffektivität zu erhöhen. Der 2025 State of Cloud Security Report betont die Implementierung einer einheitlichen Cloud-Sicherheitsplattformstrategie, um diese Herausforderungen zu bewältigen. Überwältigende 97 % der Befragten bevorzugen zentralisierte Lösungen, die die Richtlinienverwaltung vereinfachen, die Transparenz verbessern und eine einheitliche Durchsetzung in verschiedenen Umgebungen gewährleisten. Folglich wird Unternehmen dringend empfohlen, in den Erwerb und die Bereitstellung einer einheitlichen Cloud-Plattform zu investieren. Im Durchschnitt entfallen derzeit 35 % der gesamten IT-Sicherheitsausgaben auf die Cloud-Sicherheit, was die wachsende Bedeutung des Schutzes von Hybrid- und Multi-Cloud-Umgebungen widerspiegelt. Da die Cloud-Sicherheit für die Unternehmen inzwischen oberste Priorität hat, planen 63 %, ihre Budgets in den nächsten 12 Monaten zu erhöhen.

Künstliche Intelligenz

KI und maschinelles Lernen analysieren Datenmuster, identifizieren verdächtige Verhaltensweisen, erkennen Malware und können Eindringversuche verhindern. Unternehmen, die diese Technologien einsetzen, verbessern ihre Cybersicherheitslage und können das Vertrauen ihrer Kunden stärken. KI-gesteuerte Bedrohungserkennung und -reaktion verändern die Cyber- und Cloud-Sicherheit im Jahr 2025, indem sie die Echtzeitanalyse großer Datenmengen ermöglichen, um abnormales Verhalten und potenzielle Bedrohungen zu identifizieren. Dieser proaktive Ansatz ermöglicht es Unternehmen, Angriffe schneller zu erkennen und zu entschärfen, den Schaden zu minimieren und die Abhängigkeit von menschlichen Eingriffen zu verringern. Mit zunehmender Akzeptanz verbessert KI die Sicherheit, indem sie Reaktionen automatisiert, Fehlkonfigurationen erkennt und das Cloud Security Posture Management (CSPM) verbessert. Da die Cloud-Bedrohungen weiter zunehmen, nutzen immer mehr Unternehmen KI-gestützte Lösungen, um ihre Verteidigungsstrategien zu stärken und eine robuste Cyber-Resilienz aufrechtzuerhalten.

The internet of things

Im Zuge der fortschreitenden digitalen Transformation wird dem Internet der Dinge (Internet of Things, IoT) eine zentrale Rolle als zukünftiger Wachstumstreiber in zahlreichen Industriezweigen zugeschrieben. Der Begriff beschreibt ein Netzwerk internetfähiger physischer Objekte – von intelligenten Haushaltsgeräten über vernetzte Fahrzeuge bis hin zu industriellen Sensoren –, die Daten erfassen, austauschen und in Echtzeit verarbeiten können. Prognosen von IoT Analytics zufolge wird die Zahl globaler IoT-Verbindungen bis 2025 auf über 30 Milliarden anwachsen, was durchschnittlich vier IoT-Geräte pro Person entspricht. Auch in Kanada entwickelt sich der IoT-Markt dynamisch: Der Umsatz im Bereich Consumer-IoT wird bis 2025 voraussichtlich 2,67 Mrd. USD (3,82 Mrd. CAD) erreichen, mit einer geschätzten jährlichen Wachstumsrate von 8,58 % bis 2029 – was einem Marktvolumen von rund 5,33 Mrd. CAD entspricht. Gleichzeitig wirft die zunehmende Verbreitung von IoT-Technologien erhebliche sicherheitsrelevante Fragestellungen auf. Viele aktuell verfügbare IoT-Geräte verfügen über unzureichende Sicherheitsstandards, insbesondere im Bereich der Zugriffskontrolle, Authentifizierung und Datenverschlüsselung. Dies macht sie anfällig für Cyberangriffe, bei denen Bedrohungsakteure etwa auf Umweltkontrollsysteme, Gebäudesicherheitsinfrastruktur oder personenbezogene Daten zugreifen können. Der Schutz von IoT-Ökosystemen erfordert daher die Implementierung robuster Sicherheitsarchitekturen sowie sektorübergreifende regulatorische Maßnahmen zur Sicherstellung der Interoperabilität, Datenintegrität und Netzwerksicherheit. Vor diesem Hintergrund gelten Investitionen in IoT-spezifische Cybersecurity-Lösungen – insbesondere im industriellen und städtischen Kontext – als strategisch bedeutsam, um das langfristige Vertrauen in IoT-Anwendungen zu stärken und deren wirtschaftliches Potenzial voll auszuschöpfen.

Autonomes Fahren

Im Kontext zukünftiger Mobilitätstrends stellen autonome Fahrzeuge eine Schlüsseltechnologie dar, deren Entwicklung und Integration in Kanada intensiv vorangetrieben wird. Mit der Veröffentlichung der Leitlinien *"Testing Highly Automated Vehicles in Canada: Guidelines for Trial Organizations"* haben Transport Canada und der Canadian Council of Motor Transport Administrators (CCMTA) bereits frühzeitig regulatorische Rahmenbedingungen geschaffen, um das Potenzial fahrerloser Systeme sicher zu erschließen. Prognosen gehen davon aus, dass vollständig autonome Fahrzeuge

künftig einen signifikanten Beitrag zur Verkehrssicherheit leisten könnten, indem sie Unfälle reduzieren, die derzeit noch häufig auf menschliches Fehlverhalten – wie Alkohol- oder Drogenkonsum, Ablenkung oder mangelnde Erfahrung – zurückzuführen sind. Gleichzeitig zeichnen sich jedoch zentrale Herausforderungen ab, die das zukünftige Entwicklungstempo autonomer Mobilität maßgeblich beeinflussen werden. Dazu zählen insbesondere die Interoperabilität und Kommunikation zwischen Fahrzeugen (V2V), sowie zwischen Fahrzeugen und Infrastruktur (V2I), die für eine flächendeckende Vernetzung notwendig sind – auch in ländlichen Gebieten mit geringer Konnektivität. Darüber hinaus gewinnen Themen wie Datensouveränität und Cybersecurity zunehmend an Bedeutung, da autonome Fahrzeuge kontinuierlich große Mengen personenbezogener Daten generieren, austauschen und analysieren. Die Absicherung dieser Daten gegen Manipulation und externe Angriffe wird damit zu einem kritischen Erfolgsfaktor für die Akzeptanz autonomer Systeme. Langfristig bedarf es einer umfassenden Modernisierung des kanadischen Verkehrsrechts, um klare rechtliche Rahmenbedingungen für die Zulassung, Nutzung und Haftungsverteilung bei autonomen Fahrzeugen zu schaffen. Die zukünftige Haftungsarchitektur wird nicht nur Einfluss auf die Hersteller- und Betreiberverantwortung haben, sondern auch auf die Struktur des kanadischen Versicherungswesens. Vor diesem Hintergrund stellt die rechtssichere Integration autonomer Fahrzeuge nicht nur ein technologisches, sondern auch ein regulatorisches Innovationsfeld dar – mit weitreichenden wirtschaftlichen, gesellschaftlichen und sicherheitspolitischen Implikationen.

Cybersecurity-Versicherungen

In den letzten fünf Jahren hat sich der Markt für Cyberversicherungen angesichts wachsender Cyberbedrohungen, insbesondere der Zunahme von Ransomware-Angriffen seit 2018 und der verstärkten Umstellung auf Telearbeit infolge der COVID-19-Pandemie, substanziell verändert. Diese Entwicklungen führten zu einem sogenannten „harten Markt“, gekennzeichnet durch eingeschränkte Versicherungskapazitäten, deutlich erhöhte Prämien und strengere Policen Anforderungen – insbesondere für größere Unternehmen. Obwohl sich der Zugang zu Cyberversicherungen für viele Unternehmen als kostenintensiv und administrativ aufwendig erwiesen hat, bleibt ihre strategische Bedeutung im Rahmen eines umfassenden Cyber-Risikomanagements unbestritten. Cyberversicherungen bieten eine Absicherung gegen finanzielle Restrisiken, die trotz vorhandener Informationssicherheits-Governance und technischer Schutzmaßnahmen bestehen bleiben. Der Markt zeigt aktuell Anzeichen einer allmählichen Stabilisierung: Versicherungsbedingungen werden transparenter, Deckungsumfänge ausgeweitet und Prämien flachen ab. Dennoch liegt die Verbreitung von Cyberversicherungen weiterhin bei lediglich 40 % aller Unternehmen. Zugleich entwickelt sich die Rolle der Versicherungsmakler weiter – hin zu spezialisierten Dienstleistern, die neben der Vermittlung zunehmend auch Beratungsleistungen im Bereich Risikoprävention und Cyberresilienz anbieten. Für das Jahr 2025 ist mit einer Zunahme neuer Marktteilnehmer, einer konsolidierten Tarifstruktur und der stärkeren Integration von Cyberversicherungen in unternehmerische Sicherheitsstrategien zu rechnen. Externer Druck durch Aufsichtsräte, Geschäftspartner und Regulatoren dürfte den Trend zur breiteren Adoption weiter verstärken.

3.9 Trends im Bereich der zivilen Sicherheit - Cybersecurity

Identity Threat Detection and Response

Im Zuge der zunehmenden Verlagerung unternehmenskritischer Prozesse in Cloud-Umgebungen und der wachsenden Komplexität verteilter IT-Infrastrukturen gewinnt der Bereich Identity Threat Detection and Response (ITDR) als eigenständige sicherheitsrelevante Disziplin strategisch an Bedeutung. Während etablierte Konzepte wie Cloud Security Posture Management (CSPM) und Security Information and Event Management (SIEM) bereits wesentliche Schutzfunktionen für Cloud-Infrastrukturen abdecken, reagiert ITDR gezielt auf das rapide Ansteigen identitätsbezogener Angriffe, die sich insbesondere jenseits traditioneller Netzwerkgrenzen manifestieren. ITDR umfasst eine integrierte Kombination aus sicherheitstechnologischen Tools, Bedrohungsanalysen, Wissensdatenbanken und organisatorischen Prozessen zur proaktiven Erkennung, Untersuchung und Abwehr identitätsbasierter Cyberangriffe. Zentraler Bestandteil ist die kontinuierliche Überwachung und Analyse von Authentifizierungs- und Autorisierungsprozessen sowie von Verhaltensanomalien in Zugriffssystemen. Ziel ist es, kompromittierte Identitäten frühzeitig zu identifizieren, potenzielle Schäden zu begrenzen und die Integrität der Identitätsinfrastruktur wiederherzustellen. Angesichts des steigenden Missbrauchs von Zugriffsrechten und der zunehmenden Verknüpfung identitätsbasierter Angriffe mit Ransomware- und APT-Kampagnen wird ITDR künftig eine Schlüsselrolle im Rahmen ganzheitlicher Cybersecurity-Architekturen einnehmen.

Schutz vor zivilem Datenraub

Datengetriebene Cyberangriffe zählen zunehmend zu den kostspieligsten und gravierendsten Bedrohungen für Unternehmen aller Branchen. Die gezielte Kompromittierung sensibler Informationen – darunter personenbezogene

Daten, Finanzinformationen, Gesundheitsdaten oder geistiges Eigentum – hat sich zu einem zentralen Angriffsziel entwickelt, das tiefgreifende operative und strategische Konsequenzen nach sich zieht. Trotz der Implementierung etablierter Sicherheitsmaßnahmen und Kontrollmechanismen geraten schützenswerte Datenströme regelmäßig in die Hände unbefugter Dritter, was deren missbräuchliche Nutzung zur potenziellen Unternehmensgefährdung macht. Der IBM-Bericht *Cost of a Data Breach 2024* verdeutlicht die ökonomische Dimension solcher Sicherheitsvorfälle: Kanadische Unternehmen verzeichneten im Durchschnitt Schadenssummen in Höhe von 6,32 Millionen CAD pro Datenverletzung. Sektorspezifisch lagen die Schäden im Finanzwesen bei 9,28 Millionen CAD, im Technologiesektor bei 7,81 Millionen CAD und in der Industrie bei durchschnittlich 7,84 Millionen CAD. Diese Zahlen unterstreichen die wachsende Relevanz datenzentrischer Sicherheitsstrategien. Die Tatsache, dass selbst Organisationen mit bestehenden Governance-Strukturen und Sicherheitsrichtlinien betroffen sind, verdeutlicht die Notwendigkeit einer strategischen Neuausrichtung – weg von reaktiven Modellen hin zu dynamischen, risikobasierten Sicherheitsarchitekturen mit stärkerer Betonung auf Echtzeitüberwachung, Zero-Trust-Prinzipien und datenorientierter Resilienz.

3.10 Stärken und Schwächen des Marktes für die Branche der zivilen Sicherheit - Cybersecurity

Der kanadische Markt für Cybersicherheit ist stark fragmentiert und von intensivem Wettbewerb zwischen den führenden Akteuren geprägt. Die zunehmenden Cyberangriffe veranlassen Unternehmen dazu, ihre Strategien zu überdenken und ihre Serviceangebote zu erweitern. Um dem Mangel an qualifizierten Fachkräften im Bereich Cybersicherheit entgegenzuwirken, arbeiten Unternehmen und Organisationen zusammen, um spezialisierte Weiterbildungskurse für Talente und Mitarbeiter anzubieten. Der Markt sieht auch Partnerschaften als strategische Maßnahmen, um verbesserte Cybersicherheitslösungen bereitzustellen.

Stärken	Schwächen
Standortvorteile für Investitionen und Marktzugang durch **- hohe Innovationsdichte** **- akademische Exzellenz und Forschungskooperationen** **- klare politische Rahmensetzung** **- staatliche Förderstruktur** Kanada ist ein wirtschaftlich- und rechtlich stabiler Standort und verfügt über ein dichtes Netz an Universitäten und Hochschulen mit spezialisierten Programmen in den Bereichen Cybersicherheit, IT-Sicherheit und digitaler Forensik, die sich als zentrale Wissensplattformen positionieren.	**Fachkräftemangel** Trotz der vorhandenen akademischen Infrastruktur besteht derzeit ein Fachkräftemangel von rund 25.000 Cybersecurity-Fachkräfte. **Regionale Disparitäten im Zugang zu Aus- und Weiterbildung** Insbesondere in dünn besiedelten oder abgelegenen Regionen bestehen infrastrukturelle Hürden beim Zugang zu Schulungen oder Industriekooperationen.
Chancen	**Risiken**
Ausgeprägte technologische Expertise und globale Sichtbarkeit Kanada hat eine führende Rolle in den Bereichen der KI, Quanten- und Netzwerktechnologien. Die starke Forschungslandschaft in Ontario und Québec verstärkt die internationale Wettbewerbsfähigkeit im sicherheitsrelevanten Technologiesektor und bietet zahlreiche Chancen. **Wachsende Marktnachfrage nach Cybersicherheitslösungen** Die Zunahme von datengestützten Geschäftsmodellen, steigende Cloud-Adoptionen, kontinuierlich steigende Ransomware-Angriffe führend zu einer erhöhten Risikowahrnehmung und damit zu einer erhöhten Nachfrage nach Cybersicherheitslösungen, Managed Services und präventiven Schutzlösungen in der Privatwirtschaft und im öffentlichen Sektor.	**Anpassungsdruck durch technologische Dynamik** Die Geschwindigkeit, mit der sich Bedrohungslagen und technologische Anforderungen verändern kann Risiken bei nicht-Anpassung bergen. **Fragmentierung von Zuständigkeiten und fehlende Standardisierung** Eine unzureichende Koordination zwischen Bund, Provinzen, akademischen Einrichtungen und Industrie kann ein Risiko darstellen.

Kontaktadressen

Verbände und Behörden

Tabelle 2: Verbände und Behörden

Institution	Kurzbeschreibung
Germany Trade & Invest	Germany Trade & Invest (GTAI) ist die Außenwirtschaftsagentur der Bundesrepublik Deutschland. Mit 60 Standorten weltweit und dem Partnernetzwerk unterstützt Germany Trade & Invest deutsche Unternehmen bei ihrem Weg ins Ausland, wirbt für den Standort Deutschland und begleitet ausländische Unternehmen bei der Ansiedlung in Deutschland.
Bundesamt für Sicherheit und Informationstechnik (BSI)	Das Bundesamt für Sicherheit in der Informationstechnik ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene und damit für den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge verantwortlich. Für Wirtschaft, Wissenschaft und Gesellschaft fungiert es als Berater zur Informationssicherheit.
SBS systems for business solutions (SBS)	SBS unterstützt die AHK Kanada bei der Akquise deutscher Teilnehmer und greift dabei auf ein langjährig aufgebautes Kontaktnetzwerk im relevanten Bereich zurück.
Bundesministerium für Wirtschaft und Klimaschutz	Die AHK Kanada arbeitet eng mit dem Länderreferat und verschiedenen Fachreferaten des BMWKs zusammen. Etwa kann sich diese auf geförderte Ausschreibungen für Projekte bewerben.
Gesellschaft für Informatik e.V. (GI)	Große Interessenvertretung der Informatik im deutschsprachigen Raum. Ziel ist die Förderung der Informatik in Forschung und Lehre, Anwendung und in der Weiterbildung.
Verband für Sicherheitstechnik e. V.	Der Verband entwickelt maßgeschneiderte sicherheitstechnische Lösungen für Banken, Flughäfen, die Industrie, Justizvollzugsanstalten und Krankenhäuser.
Bitkom e.V.	Bitkom ist der Branchen-, bzw. Interessenverband der deutschen Informations- und Telekommunikationsbranche. Dieser vertritt neben Mittelständlern und Start-Ups nahezu alle Global Player aus dem Bereich Telekommunikation und Internetdienste.
Bundesverband IT-Mittelstand e.V. (BITMi)	Der Verband vertritt ausschließlich mittelständische IT-Unternehmen und Start-Ups zur Verbesserung des deutschen Wirtschaftsstandorts und zur Kommunikation mit dem Bundeswirtschaftsministerium. Zudem stellt er aktuelle Informationen und Lösungen zur Informationstechnologie bereit.
Kanadische Botschaft Berlin / Canadian Trade Commissioner Service	Die kanadische Botschaft ist die diplomatische Vertretung Kanadas in Deutschland. Die Abteilung für Trade Commissioner Service agiert als Vernetzungs- und Verteilungsinstrument von Förderungen und Events im Auftrag der kanadischen Botschaft und ist ein langjähriger Partner der AHK Kanada
Institut Cyber Security & Privacy (ICSP) Hochschule Bonn-Rhein-Sieg	Das Institut für Cyber Security & Privacy (ICSP) bündelt Forschung, Lehre und Transfer an der Hochschule zu Themen der digitalen Sicherheit und Privatheit im Cyberraum. Der Verband hat sein Interesse an einer Zusammenarbeit bekundet und unterstützt die Bewerbung des Projekts.
National Cybersecurity Consortium (NCC)	Das NCC unterstützt ein Netzwerk aus Cybersecurityunternehmen und anderen Stakeholdern aus dem Bereich der Cybersicherheit durch Recherche, Vernetzung und Förderungen.
Information and Communications Technology Council (ICTIC)	Von der kanadischen Regierung gegründet in Zuge des Sectoral Council Program. Der Council vermittelt zwischen Unternehmen, Entscheidungsträgern und akademischen Institutionen und stellt des weiteren Wirtschaftsanalysen, politische Beratung und Ausbildung für Fachkräfte zur Verfügung.
Canadian Institute for Cybersecurity (CIC) / University of New Brunswick	Das Institut ist Teil der University of New Brunswick in Fredericton, wo es das Cybersecurity Collaboration Consortium (CNCCC) betreut, eine Kollaboration zur Bildung eines Innovations-Hubs für Cybersecurity. Dieser vernetzte Forscher und Unternehmen, um einen innovativen Austausch zum Thema Cybersecurity zu gestalten.

CyberQuébec (CCTT)	CyberQuebec erstellt für Unternehmen jeder Größe individualisierte Sicherheitsstrategien und betreut diese langfristig. Dazu bietet das Unternehmen Trainingsaktivitäten zur Verbesserung der allgemeinen Cybersecuritykenntnisse, Rechtsberatung (siehe Bill 25) und sicherheitskritische Netzwerkanalysen an.
Cybersecurity and Privacy Institute at the University of Waterloo	Das Institut ist Teil der Universität von Waterloo und gestaltet interdisziplinäre Forschungszusammenarbeit zur Cybersicherheit. Es forscht insbesondere zum Datenschutz, Kryptografie und zur quantensicheren Kommunikation. In Partnerschaft mit vier weiteren Instituten anderer Universitäten gründete dieses das National Cybersecurity Consortium (NCC), welches die genannten 80 Mio. CAD zur Bildung eines Cybersecurity-Netzwerks erhielt.
Faculty of Liberal Arts & Professional Studies, York University	Im Zuge der hohen Nachfrage nach Fachkräften bietet die Universität spezifische Bachelorstudiengänge im Bereich der Computer Security an.
Waterloo Region Economic Development Corporation	Waterloo EDC unterstützt Unternehmen beim Investieren und Expandieren in Waterloo mit Informationen zur Marktstruktur und dem Vernetzen mit lokalen Partnern. Zudem vermittelt es Unternehmen zu den genannten Förderungen von Regierungsinstitutionen. Insbesondere liegt ein Schwerpunkt auf KI, wobei Waterloo bereits das dynamischste Tech-Ökosystem in Kanada bildet.
Toronto Global	Toronto Global ist eine zentrale Anlaufstelle für internationale Unternehmen, die ihre Expansion beschleunigen, Kontakte knüpfen und Zugang zu Talenten in der Region Toronto erhalten möchten.
Canadian Chamber of Commerce	Die kanadische Handelskammer repräsentiert die kanadische Wirtschaft im In- und Ausland und trägt zu deren Vernetzung in den entsprechenden Märkten bei. Ihre Mitglieder profitieren vom in Kontakt kommen mit Geschäftspartnern und einem Sprachrohr in die politischen Entscheidungsgremien.
Quebec International	Quebec International unterstützt bei Investitionsvorhaben in Quebec durch spezifische Trainings, Veranstaltungen und Bereitstellung von Informationsmaterial zum Markt.
Deutsche Botschaft und Generalkonsulat in Kanada	Die deutsche Botschaft ist die diplomatische Vertretung Deutschlands in Kanada und ein langjähriger Partner der AHK Kanada. Diese unterstützt konkret bei der Bewerbung des Projektes und bei der Kontaktvermittlung.
Ontario International Trade & Invest	Invest Ontario ist ein Vermittlungspartner für Unternehmen, die strategisches Wachstum in Ontario anstreben. Ein langjähriger Partner der AHK Kanada, und Unterstützung wurde zugesagt.

Messen und Konferenzen

Tabelle 3: Messen und Konferenzen

Organisation	Beschreibung
ManuSec Canada: Cyber Security for Critical Manufacturing Summit Toronto, ON 08.-09.04.2025	Die **ManuSec** bietet insbesondere vor dem Hintergrund der geopolitischen Risiken einen Austausch über die Bedrohung von kanadischen Herstellern durch stark erhöhte Ransomwareattacken und dem Offenlegen von Schwachstellen von Fertigungsstätten. Deshalb wird sich insbesondere der kommende Gipfel auf den Schutz von privaten Unternehmen konzentrieren.
International Conference on Cybersecurity Studies Mississauga, ON 21.04.2025	Die Konferenz ist stark international orientiert und bringt Experten, Forscher, Pädagogen und Studenten aus der ganzen Welt zusammen, um ihre Erfahrungen und ihr Wissen auszutauschen. Sie wird eine Reihe von Sitzungen umfassen, darunter Hauptvorträge, Podiumsdiskussionen und Workshops.
Cybersecurity Identity Summit 2025 Ottawa, ON 22.-23.04.2025	Der **Cybersecurity & Identity Summit (CIS)** 2025 ist eine zweitägige Veranstaltung, die der Prävention von Cyberrisiken und dem digitalen Identitätsmanagement gewidmet ist. Die CIS 2025 verspricht gute Einblicke, praktisches Wissen und Networking-Möglichkeiten, um Unternehmen und Technologieexperten zu helfen, in der sich ständig weiterentwickelnden digitalen Landschaft erfolgreich zu sein.
FutureCon CyberSecurity Conference	Die **FutureCon CyberSecurity Conference** zielt auf das Zusammenführen von Führungskräften und neuen Vorreitern im Bereich der Cybersecurity ab. Über eine hybride Plattform wird eine Kommunikation auch vor und nach der

Toronto, ON 24.04.2025	Veranstaltung gewährleistet
21st Global Conference on Information Technology and Computer Science (GCITCS) Ottawa, ON 09.-11.05.2025	Diese internationale Konferenz mit Einladungsschreiben soll Akademikern, Branchenführern und Studenten als aktive Plattform dienen, um ihre neuesten Forschungsergebnisse und Durchbrüche zu präsentieren. Die Konferenz bietet umfangreiche Möglichkeiten zur Vernetzung und Vorschläge zur Bewältigung der neuesten Herausforderungen in der IT und Informatik. Auf dieser Konferenz wird es auch einen Hauptvortrag und eine Podiumsdiskussion über aktuelle und aufkommende Trends in der Branche geben.
IAPP Canada Privacy Symposium 2025 Toronto, ON 12-13.05.2025	Die Konferenz umfasst die Themen Privatsphäre, AI Governance und digitale Verantwortung im Zuge des sich ändernden Cyberraums. Sie bietet den Raum zum Vernetzen mit den Experten aus Politik, Privatwirtschaft und Forschung.
NorthSec Training 2025 Montreal, Quebec 10.-18.05.2025	Die Konferenzthemen werden unterschiedliche Themen wie Pentesting, Netzwerksicherheit, Ausnutzung von Software und/oder Hardware, Anwendungssicherheit, Reverse Engineering, Malware und Kryptographie behandeln. Zudem werden Trainingseinheiten zu allen Themen angeboten.
Toronto Cybersecurity Summit Toronto, ON 15.05.2025	Der 2. jährliche Toronto Cybersecurity Summit bringt Cybersecurity-Führungskräfte und Praktiker, die für den Schutz der kritischen Infrastrukturen ihrer Unternehmen verantwortlich sind, mit Lösungsanbietern und renommierten Experten für Informationssicherheit zusammen.
Information Security Forum Toronto, ON 20.05.2025	Das **Toronto Forum** ist für Informationssicherheitspraktiker aus allen Branchen gedacht, um sich mit spezifischen Themen (Sicherheitsarchitektur, Risikomanagement, Management) zu befassen, Erkenntnisse auszutauschen und sich mit Gleichgesinnten zu vernetzen. Diese eintägige Veranstaltung umfasst Breakouts mit der IANS-Fakultät und Spotlight-Sitzungen zu neuen Technologien.
International Conference on Security and Safety Integration ICSSI Wales Drive Regina, SK 02.-06.06.2025	Durch die sehr diverse Teilnehmerschaft zielt das Event auf einen allgemeinen Austausch zwischen Akademikern, Industrie und internationalen Organisationen ab. In diesem Diskurs sollen allgemeine Aspekte der IT-Security, Schutz kritischer Infrastruktur und Risiken durch KIs diskutiert werden.
Cyber Security for Critical Assets Summit (CS4CA) Calgary, Alberta 11.-12.06.2025	Im Zusammenhang mit den geopolitischen Risiken in der Cybersicherheit und den unbekannten Veränderungen durch KI konzentriert sich dieser Gipfel auf den Austausch zwischen den Verantwortlichen für die kritische Infrastruktur aus allen Bereichen.
International Conference on Computing and Information Technology ICCIT Montreal, Quebec 12.-13.06.2025	Die **ICCIT** zielt darauf ab, führende akademische Wissenschaftler und Forscher zusammenzubringen, um ihre Erfahrungen und Forschungsergebnisse zu allen Aspekten der Informatik, Cybersicherheit und Informationstechnologie auszutauschen. Sie bietet außerdem eine interdisziplinäre Plattform für Forscher, Praktiker und Pädagogen, um die neuesten Innovationen, Trends und Probleme sowie praktische Herausforderungen und Lösungen zu diskutieren.
Montreal Cybersecurity Conference Montreal, Quebec 18.06.2025	Die Konferenz befasst sich mit den aktuellsten Entwicklungen, insbesondere bezüglich Risikomanagement und strategischen Abwehrpraktiken.
International Conference on Computer Science, Programming and Security ICCSPS Toronto, ON 19.-20.06.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**“)

International Conference on Computing and Information Technology ICCIT Ottawa, ON 03.-04.07.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
29th Global Conference on Information Technology and Computer Science (GCITCS) Toronto, ON 12.07.2025	Die Konferenz bietet eine Plattform für Researcher, Industrieexperten und Studenten zur akademischen Kooperation und Vernetzung. Es sollen die aktuellen Trends in der Cybersicherheit beleuchtet und diskutiert werden,
International Conference on Computing and Information Technology ICCIT Quebec City, Quebec 17.-18.07.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computer Science, Cybersecurity and Information Technology ICCIT Toronto, ON 24.-25.07.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computing and Information Technology ICCIT Montreal, Quebec 07.-08.08.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computer Science, Programming and Security ICCSPS Vancouver, BC 07.-08.08.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computer Science, Cybersecurity and Information Technology ICCIT Totonto, ON 14.-15.08.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
22nd Annual International Conference on Privacy, Security, and Trust (PST2025) Fredericton, NB 26.-28.08.2025	Die jährliche internationale Konferenz über Datenschutz, Sicherheit und Vertrauen bietet ein Forum für den Austausch von Fortschritten in der Cybersicherheitsforschung und Sicherheitsanwendungen. Die PST2025 bietet drei Tage lang Vorträge, technische Präsentationen, Sondersitzungen und einen Industrietag mit einer Anbieterausstellung.
GoSec25 Montreal, Quebec 10.-11.09.2025	Bei der **GoSec25** werden in zahlreichen Sessions die Themen Datenschutz, Risikomanagement, Cloudsecurity und Risiken durch Hacker behandelt.
BSides Edmonton Edmonton 22.-23.09.2025	Die von Mitgliedern der Cybersecurity-Community organisiert Konferenz ist eine offene Plattform, um den Dialog zwischen Experten und Interessierten zu gestalten.
Operation: Defend the North 2025	Das Event simuliert einen fiktiven Cyberangriff auf die kritischen Sektoren

Ottawa, ON 24.09.2025	Kanadas - Energie, Finanz- und Bankwesen, Gesundheitswesen, öffentliche Dienste und Telekommunikation. Gemeinsam wird eine simulierte Cyber-Krise über ein interaktives Online-Tabletop-Event gelöst, das virtuell von überall aus zugänglich ist und Branchenführer, Cybersicherheitsexperten, politische Entscheidungsträger und Interessenvertreter einen Einblick in die Abwehr von Cyberangriffen gibt.
International Conference on Cyber Security and Artificial Intelligence ICCSIS Toronto, On 25.-26.09.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computing and Information Technology ICCIT Vancouver, BC 29.-30.09.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
Polar Conference – Canada Cybersecurity Symposium 2025 Quebec, Quebec 16.10.2025	Die Polar Confernece bietet Repräsentanten aus der Cybersecurity-Industrie die Gelegenheit zum Vorstellen von kürzlichen Errungenschaften und begegneten Hindernissen. Bei Panels und in Workshops bietet sich zudem die Gelegenheit zum Austausch mit den Vortragenden.
International Conference on Computer Science, Programming and Security ICCSPS Quebec City, Quebec 16.-17.10.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
Security Canada Central Toronto, ON 22.-23.10.2025	**Security Canada Central** verschafft Zugang zu den neuesten Produkten und Dienstleistungen und hilft sich über neue Entwicklungen und Trends zu informieren. Es werden zudem zahlreiche Netzwerkmöglichkeiten angeboten.
International Conference on Computer Science, Cybersecurity and Information Technology ICCIT Montreal, Quebec 30.-31.10.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
BSides Ottawa 2025 Ottawa, ON 20.-21.11.2025	Die BSides Ottawa wird von Hackers 4 Karma (H4K), einer eingetragenen kanadischen Non-Profit-Organisation, veranstaltet. Sie bietet eine Austauschplattform für Experten, Industrielle und Interessierte zur Bildung einer Cybersecurity-Gemeinschaft am Standort Ottawa.
International Conference on Computer Science, Cybersecurity and Informational Technology ICCIT Vancouver, BC 24.-25.11.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computer Science, Cybersecurity and Information Technology ICCIT Vancouver, BC 24.-25.11.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**")
International Conference on Computer	(siehe „International Conference on Computing and Information Technology

Science, Cybersecurity and Information Technology ICCSCIT Totonto, ON 27.-28.11.2025	**ICCIT**“)
International Conference on Computer Science, Programming and Security ICCSPS Vancouver, BC 18.-19.12.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Computing and Information Technology ICCIT Toronto, ON 18.-19.12.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Computer Science, Programming and Security ICCSPS Montreal, Quebec 25.-26.12.2025	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Computer, Information Systems and Technology Management ICISTM Montreal, Quebec 24.-25.05.2026	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Computing and Information Technology ICCIT Ottawa, ON 12.-13.07.2026	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Computer and Information Systems ICCSIS Toronto, ON 20.-21.09.2026	(siehe „International Conference on Computing and Information Technology **ICCIT**“)
International Conference on Information Systems and Operations Management ICISOM Vancouver, BC 23.-24.09.2026	(siehe „International Conference on Computing and Information Technology **ICCIT**“)

Quellenverzeichnis

Statistics Canada (2023): Impact of cybercrime on Canadian businesses, The Daily — Impact of cybercrime on Canadian businesses, 2023 (zugegriffen am 18.03.2025)

Statistics Canada (2024): Eh Sayers Episode 22 - Can Your Business Outsmart a Hacker?, Eh Sayers Episode 22 - Can Your Business Outsmart a Hacker?, (zugegriffen am 18.03.2025)

Statistics Canada (2025): Government of Canada introduces new National Cyber Security Strategy, Government of Canada introduces new National Cyber Security Strategy - Canada.ca, (zugegriffen am 18.03.2025)

Statistics Canada (2025): How much is fraud affecting Canadians and Canadian businesses, How much is fraud affecting Canadians and Canadian businesses? - Statistics Canada (zugegriffen am 18.03.2025)

Office of the Privacy Commissioner of Canada. (2021, December 8). *The Personal Information Protection and Electronic Documents Act (PIPEDA)*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (zugegriffen am 20.03.2025)

The Conference Board of Canada. (2023). Securing the future. In *Issue Briefing*. https://www.conferenceboard.ca/wp-content/uploads/2022/10/securing-the-future_2023_preview.pdf (zugegriffen am 20.03.2025)

Natural Resources Canada (2024, December 23). Cyber Security and Critical Energy Infrastructure Program (CCEIP). Cyber Security and Critical Energy Infrastructure Program (CCEIP) - Natural Resources Canada (zugegriffen am 20.03.2025)

Statistics Canada (2023): The changing landscape of cyber security following the COVID-19 pandemic, The changing landscape of cyber security following the COVID-19 pandemic, (zugegriffen am 19.03.2025)

McMillan (2024): Bill C-26: A New Chapter in Canadian Cybersecurity Regulation, Bill C-26: A New Chapter in Canadian Cybersecurity Regulation - McMillan LLP, (zugegriffen am 19.03.2025)

Ontario (2022), Ontario Broader Public Sector Cyber Security Strategy Report, Cyber Security Expert Panel - Report to the Minister of Public and Business Service Delivery of Ontario, (zugegriffen am 19.03.2025)

Statistics Canada (2022): Government of Canada announces next phase to strengthen Cyber Security Innovation Network, Government of Canada announces next phase to strengthen Cyber Security Innovation Network - Canada.ca, (zugegriffen am 19.03.2025)

Statistics Canada (2024): Cyber Security Innovation Network, Cyber Security Innovation Network - Cyber Security Innovation Network, (zugegriffen am 19.03.2025)

Public Safety Canada (2025), Public Safety Canada - Home (zugegriffen am 20.03.2025)

Canadian Centre for Cyber Security (2025), Canadian Centre for Cyber Security (zugegriffen am 20.03.2025)

National Cyber Crime Coordination Center (2025), National Cybercrime Coordination Centre | Royal Canadian Mounted Police (zugegriffen am 20.03.2025)

National Security (2025), National security - Canada.ca, (zugegriffen am 20.03.2025)

Natural Ressources Canada (2025), Transport Canada, (zugegriffen am 20.03.2025)

Transport Canada (2025), Transport Canada, (zugegriffen am 20.03.2025)

National Research Council (2025), Home - National Research Council Canada (zugegriffen am 20.03.2025)

Public Services and Procurement Canada (2025), Public Services and Procurement Canada - Canada.ca (zugegriffen am 20.03.2025)

Standards Council of Canada (2025), About us | Standards Council of Canada (zugegriffen am 20.03.2025)

Government of Canada (2025), Government of Canada announces first phase of Canadian Program for Cyber Security Certification, Government of Canada announces first phase of Canadian Program for Cyber Security Certification -

Canada.ca (zugegriffen am 21.03.2025)

The Standards Council of Canada (2025), About us, About us | Standards Council of Canada, (zugegriffen am 21.03.2025)

Iclg (2025), Cybersecurity Laws and Regulations Canada 2025, Cybersecurity Laws and Regulations Report 2025 Canada, (zugegriffen am 21.03.2025)

Quebec (2025), About the Government Strategy on Cyber Security and Digital Technology 2024-2028 About the Government Cyber Security and Digital Strategy 2024-2028 | Government of Quebec, (zugegriffen am 21.03.2025)

Government of Canada (2025), Cyber Security and Critical Energy Infrastructure Program (CCEIP) Cyber Security and Critical Energy Infrastructure Program (CCEIP) - Natural Resources Canada(zugegriffen am 21.03.2025)

Government of Canada (2025), Cyber security certification for defence suppliers in Canada, Cyber security certification for defence suppliers in Canada - Canada.ca , (zugegriffen am 24.03.2025)

Publications Quebec (2024), Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, G-1.03 - Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (zugegriffen am 24.03.2025)

Fortinet (2025), Navigating Todays Cloud Security Challenges, Navigating Today's Cloud Security Challenges | Fortinet Blog, (zugegriffen am 24.03.2025)

Security 101 (2022), The most important cloud security trends in 2025, The most important cloud security trends in 2025 (zugegriffen am 24.03.2025)

Cymulate (2025), The Future of Cloud Security: 7 Key Trends in 2025, 7 Cloud Security Trends to Watch for in 2025 (zugegriffen am 24.03.2025)

Opentxt (2025), Our story, About us | OpenText (zugegriffen am 24.03.2025)

Forbes (2025), Open Text, Open Text | Company Overview & News, (zugegriffen am 24.03.2025)

Absolute (2025), About us, About Us | Absolute Security, (zugegriffen am 24.03.2025)

Softchoice (2025), About Softchoice, About Softchoice | Softchoice, (zugegriffen am 26.03.2025)

Ontario (2025), Ontarios Trustworthy Artificial Intelligence (AI) Framework, Ontario's Trustworthy Artificial Intelligence (AI) Framework | ontario.ca (zugegriffen am 26.03.2025)Ontario (2025), Chapter 5: Harnessing Sector Strengths to Support Growth 2024,https://www.ontario.ca/document/ontarios-long-term-report-economy-2024/chapter-5-harnessing-sector-strengths-support2024#:~:text=This%20chapter%20highlights%20key%20sectors%20in%20Ontario%20that,economic%20growth%20and%20help%20improve%20Ontario%E2%80%99s%20productivity%20performance. (zugegriffen am 26.03.2025)

Quebec (2025), How has Québec's economy changed over the past 25 years?, https://statistique.quebec.ca/en/communique/how-quebec-economy-changed-over-past-25-years, (zugegriffen am 26.03.2025)

CEDEC (2024), OVERVIEW OF QUEBEC'S ECONOMIC LANDSCAPE, https://cedec.ca/wp-content/uploads/2024/11/CEDEC-OQEL-ENG.pdf#:~:text=This%20report%20offers%20strategic%20insights%20and%20illustrations%20of,leveraging%20demographic%20shifts%2C%20and%20capitalizing%20on%20green%20investments. (zugegriffen am 26.03.2025)

Quebec (2025), Principaux accomplissements du gouvernement en matière de cybersécurité et de numérique, https://www.quebec.ca/gouvernement/ministeres-organismes/cybersecurite-numerique/publications/strategie-gouvernementale-cybersecurite-numerique-2024-2028/principaux-accomplissements (zugegriffen am 27.03.2025)

Mordor Intelligence (2024), Cyber Security Market In Canada Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030), https://www.mordorintelligence.com/industry-reports/canada-cybersecurity-market, (zugegriffen am 27.03.2025)

Sophos News (2021), The State of Ransomware 2021, https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/, (zugegriffen am 27.03.2025)

ISC2 (2021), ISC2 Cybersecurity Workforce Study Sheds New Light on Global Talent Demand, https://www.isc2.org/Insights/2021/10/ISC2-Cybersecurity-Workforce-Study-Sheds-New-Light-on-Global-Talent-Demand (zugegriffen am 27.03.2025)

Canadian Cybersecurity Network (2025), The State of Cybersecurity in Canada 2025, https://canadiancybersecuritynetwork.com/hubfs/CS-Report-CCN-2025-All-v10.pdf, (zugegriffen am 27.03.2025)

Risq (2023), Point sur le programme d'initiatives en cybersécurité de CANARIE, https://www.risq.quebec/point-sur-le-programme-dinitiatives-en-cybersecurite-de-canarie/ (zugegriffen am 28.03.2025)

Canadadrives (2025), The Future of Self Driving Cars in Canada, https://www.canadadrives.ca/blog/news/self-driving-cars-in-canada (zugegriffen am 28.03.2025)

Government of Canada (2025), Internet of Things (IoT) Security TSAP.00.012, https://www.cyber.gc.ca/en/guidance/internet-things-iot-security-itsap00012 (zugegriffen am 28.03.2025)

Statista (2024), Consumer IoT – Canada, https://www.statista.com/outlook/tmo/internet-of-things/consumer-iot/canada?currency=USD, (zugegriffen am 28.03.2025)

University Affairs, Five universities support Canadas cybersecurity strategy, https://universityaffairs.ca/news/five-universities-supporting-canadas-cybersecurity-strategy/, (zugegriffen am 28.03.2025)

Bundesamt fuer Sicherheitspolitik in der Informationstechnik (2025), Beschleunigte Sicherheitszertifizierung, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Beschleunigte-Sicherheitszertifizierung/beschleunigte-sicherheitszertifizierung_node.html, (zugegriffen am 03.04.2025)

Bundesamt fuer Sicherheitspolitik in der Informationstechnik (2025), Kriterienkatalog C5, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html (zugegriffen am 03.04.2025)

Bundesamt fuer Sicherheitspolitik in der Informationstechnik (2025), IT-Grundschutz, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html (zugegriffen am 03.04.2025)

Government of Canada, Evaluation of Contract Security Program, https://www.publications.gc.ca/collections/collection_2022/spac-pspc/P4-102-2019-eng.pdf (zugegriffen am 03.04.2025)