MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

Cybersicherheit in Irland

Geschäftsanbahnung für deutsche Unternehmen aus dem Bereich der zivilen Sicherheitstechnologien und -dienstleistungen mit Schwerpunkt auf Cybersicherheit

Dublin, 13.05.2024 – 16.05.2024

Durchführer

AHK Deutsch-Irische Industrie- und Handelskammer
German-Irish Chamber of Industry and Commerce

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

AHK Deutsch-Irische Industrie- und Handelskammer
German-Irish Chamber of Industry and Commerce

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

Bundesministerium für Wirtschaft und Klimaschutz

MITTELSTAND GLOBAL
MARKTERSCHLIESSUNGS-PROGRAMM FÜR KMU

MITTELSTAND GLOBAL
EXPORTINITIATIVE ZIVILE SICHERHEITSTECHNOLOGIEN

IMPRESSUM

Herausgeber
Deutsch-Irische Industrie- und Handelskammer (AHK Irland)
5 Fitzwilliam Street Upper
Dublin 2, Irland

Text und Redaktion
David Parkmann, Emer Clissmann, Nicolas Bauer, Levi Berlinski, Leonie Kostic, Carina Hüttenmeister

Stand
18.04.2024

Druck
Deutsch-Irische Industrie- und Handelskammer (AHK Irland)

Gestaltung und Produktion
Deutsch-Irische Industrie- und Handelskammer (AHK Irland)

Bildnachweis
Microsoft 365 Stock-Images

Inhaltsverzeichnis

I. Abbildungsverzeichnis 1
II. Tabellenverzeichnis 1
III. Abkürzungsverzeichnis 1
1 Abstract 3
2 Zielmarkt Republik Irland 4
2.1 SWOT-Analyse 7
3 Brancheninformationen Cybersicherheit in Irland 8
3.1 Allgemeine Information 8
3.2 Irische und EU-Gesetze und Vorschriften in der Cybersicherheitsbranche 9
3.3 Die Cyberbedrohungslage in Irland 11
3.4 Künftige Entwicklungen in den relevanten Segmenten und Nachfragesektoren & Marktpotenziale und -chancen 13
3.4.1 Künftige Entwicklungen in den relevanten Segmenten und Nachfragesektoren 13
3.4.2 Marktpotenziale und -chancen 14
3.5 Irlands Strategie für Cybersicherheit/Aktuelle Vorhaben, Projekte und Ziele 17
3.6 Wettbewerbssituation und Key Players 18
3.7 Stärken und Schwächen des Marktes für die Branche Cybersicherheit 22
3.7.1 SWOT-Analyse der irischen Cybersicherheitsbranche 23
4 Kontaktadressen 24
5 Literaturverzeichnis 25

I. Abbildungsverzeichnis

Abbildung 1: Irlands SWOT-Analyse vom Jahr 2022 ..... **7**
Abbildung 2: Irlands geschätzte Bruttowertschöpfung und Einnahmen im Bereich Cybersicherheit im Jahr 2021 8
Abbildung 3: Die Cyberkriminalität in Irland 12
Abbildung 4: Die größten Cyberbedrohungen in Irland 13
Abbildung 5: Künstliche Intelligenz im Bereich Cybersicherheit 15
Abbildung 6: SWOT-Analyse der irischen Cybersicherheitsbranche vom Jahr 2022 23

II. Tabellenverzeichnis

Tabelle 1: Anbieter von Cybersicherheitskompetenzen 21

III. Abkürzungsverzeichnis

BIP:	Bruttoinlandsprodukt
BPFI:	Banking and Payment Federation Ireland
BWS:	Bruttowertschöpfung
CCI:	Cybercrime Investigation
CIS:	Center of Internet Security

CPS	Cyber-Physical Systems
CRA:	CRA Cyber Resilience Act
CSF:	Cyber Security Framework
DCCAE:	Department of the Environment, Climate and Communications
DLT:	Distributed ledger technology
DORA:	Digital Operational Resilience Act
DPC:	Data Protection Commission
DSVGO:	Datenschutz- Grundverordnung
EI:	Enterprise Ireland
ENISA:	Europäische Agentur für Netz- und Informationssicherheit
ESRI:	Economic and Social Research Institute
FIT	Fastrack into Information Technology
GPU:	Graphics processing unit
HMI:	Human Machine Interface
HPC:	High-performance computing
HSE:	Health Service Executive
EU:	Europäische Union
IBM:	International Business Machines
IBRD:	International Bank for Reconostruction and Development
IDA:	Industrial Development Agency
GDPR:	General Data Protection Regulation
NIST:	National Institute of Standards and Technology
IF:	International Finance Corporation
IKT:	Informations- und kommunikationstechnik
IMF:	International Monetary Fund
IoMT:	Internet of Medical Things
ISC2	International Information System Security Certification Consortium
ISMS:	Information Security Management System
ISO:	International Organization for Standardization
itag Skillnet:	Innovation Technology AtlanTec Gateway
IWF:	Internationaler Währungsfonds
KI:	Künstliche Intelligenz
KMU:	Kleines und/oder mittleres Unternehmen
Mio.:	Millionen
MNU:	Multinationales Unternehmen
Mrd.:	Milliarden
MSSP:	Managed Security Service Provision
MTU	Munster Technological University in Cork
NATO:	North Atlantic Treaty Organisation (Nordatlantische Vertragsorganisation)
NCC-IE:	National Cybersecurity Coordination and development centre Ireland
NCSC:	National Cyber security centre
NIS:	Netzwerk- und Informationssicherheit
OECD:	Organisation for Economic Co-operation and Development
OGCIO:	Office of the Government Chief Information Officer
OT:	Operational Technology
OTSec:	Operational Technology Cyber Security Solutions
PKW:	Personenkraftwagen
PSD	Payment Services Directive
RFID:	Radio Frequency Identification
SCADA:	Supervisory Control and Data Acquisition
SOC	Security Operations Center
TUD:	Technological University Dublin
UCD:	University College Dublin

1 Abstract

Vom 13.05.24 bis zum 16.05.24 führt die AHK Irland im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) eine Geschäftsanbahnung im Bereich Cybersicherheit nach Irland durch. Diese Zielmarktanalyse untersucht die Cybersicherheitsbranche in der Republik Irland und beleuchtet dabei die aktuelle Situation sowie zukünftige Entwicklungen. Die Analyse umfasst die Betrachtung aktueller nationaler und EU-Gesetze, Richtlinien und Vorschriften, die Cyberbedrohungslage, geplante Projekte und Strategien, die Wettbewerbssituation sowie die wichtigsten Akteure, und die Stärken und Schwächen der Branche, einschließlich einer SWOT-Analyse. Dabei stehen die Marktchancen für deutsche Unternehmen im Fokus.

Das Land beherbergt bedeutende IT-Unternehmen, die auf dem europäischen Markt tätig sind. Darüber hinaus verzeichnet die Cybersicherheitsbranche einen enormen jährlichen Umsatz. Diese Stellung macht das Land jedoch auch anfälliger für Cyberangriffe. Bestätigt wird dies durch Daten von Hiscox, die eine Zunahme von Cyberangriffen in den vergangenen Jahren dokumentierten. Die steigende Anzahl von Angriffen auf irische Unternehmen und die Verwundbarkeit der kritischen Infrastruktur des Landes verdeutlichen die Dringlichkeit von Cybersicherheitslösungen und präventiven Maßnahmen.

In der Cybersicherheitsbranche in Irland sind verschiedene Entwicklungen zu beobachten, die den Markt beeinflussen könnten. Bei steigenden Investitionen in Cybersicherheitstechnologie sowie der Implementierung von Verordnungen und Richtlinien müssen Führungskräfte im irischen Markt spezifische Aspekte berücksichtigen. Eine weitere Herausforderung ist der Mangel an Fachkräften im Cybersicherheitsarbeitsmarkt, welche gleichzeitig eine große Herausforderung und ein großes Potenzial darstellt.

Des Weiteren hat der Cyberangriff auf das nationale Gesundheitswesen 2021, die irische Herangehensweise bei der Cybersicherheit, sowie die Rolle der Regierung geändert und zu mehr Investitionen in der Branche beigetragen. Dabei wird nach Lösungen gesucht, um die Herausforderungen der fehlenden strategischen Infrastrukturen sowie der steigenden Bedrohungen durch Cyberangriffe zu bewältigen. Diese Entwicklungen und Potenziale bieten deutschen Unternehmen im Bereich Cybersicherheit die Chance, ihre Expertise und Produkte in den irischen Markt einzubringen und von den wachsenden Investitionen und Bedürfnissen zu profitieren.

Ebenso bietet die steigende Sensibilisierung für Cybersicherheit den Unternehmen Chancen für deutsche Beratungsdienste. Diese könnten das allgemeine Bewusstsein in der irischen Cybersicherheitsbranche erhöhen, zum Beispiel hinsichtlich der Einhaltung von Gesetzen und Richtlinien, die zum Schutz der Infrastruktur beitragen. Zudem besteht beim Mangel an qualifizierten Fachkräften, die Chance für deutsche Anbieter im Bereich Schulungen und Training, ihre Dienste anzubieten und die Sensibilisierung innerhalb des Arbeitsmarktes hinsichtlich zum Beispiel E-Mail Kompromittierung zu stärken.

Die Verwendung des generischen Maskulinums in dieser Zielmarktanalyse dient ausschließlich der Vereinfachung der Lesbarkeit und bezieht sich sowohl auf männliche, weibliche als auch diverse Personen. Es soll in keiner Weise eine geschlechtliche Diskriminierung oder Vernachlässigung anderer Geschlechter ausdrücken. Jegliche Verwendung des generischen Maskulinums soll nicht dazu führen, dass andere Geschlechter oder Identitäten abgewertet und ausgegrenzt werden. Es wird empfohlen, bei der Interpretation der verwendeten Sprache eine geschlechtsneutrale Lesart einzunehmen.

2 Zielmarkt Republik Irland

WIRTSCHAFTSDATEN KOMPAKT

Irland

Dezember 2023

	Irland	Deutschland	EU-27
Fläche (in km²)	70.273	357.590	4.236.351
Einwohner (2023, Mio.)*	5,2	84,4	448,4
Bevölkerungswachstum (2022, %)	2,6	1,3	0,4
Sustainable Development Goals (2023, Rang von 166 Ländern)	17	4	
Corruption Perceptions Index (2022, Rang von 180 Ländern)	10	9	

Klimaindikatoren

	2010	2020	Deutschland 2020
Treibhausgasemissionen (tCO_2 eq. pro Kopf; (Anteil weltweit in %))	16,0 (0,03)	13,3 (0,03)	8,2 (1,43)
Emissionsintensität (tCO_2 eq. pro Mio. US$ BIP)	327,9	156,1	177,1
Erneuerbare Energien (Anteil am Primärenergieangebot %)	4,6	12,9	16,4

Emissionsstärkste Sektoren (2020, nur national, Anteil in %) Landwirtschaft: 39,0; Transport: 17,0; Elektrizität/Wärme: 15,0

Wirtschaftslage

	2021	2022	2023*	2024*	Deutschland 2022
BIP (Mrd. US$)	514,7	533,6	589,6	629,6	4.082
Reales BIP-Wachstum (%)	15,1	9,4	-1,9	1,2	1,8
BIP je Einwohner (US$)	101.984	103.311	112.284	117.979	48.712
Inflationsrate (%)	2,4	8,1	5,2	2,2	8,7
Haushaltssaldo (% des BIP)	-1,5	1,7	0,9	0,6	-2,6
Arbeitslosenquote (%)	6,2	4,5	4,2	4,2	3,1

Staatsverschuldung (% des BIP, brutto)	54,4	44,4	42,7	41,4		66,3
Leistungsbilanzsaldo (% des BIP)	13,7	10,8	9,9	10,6		4,2

Quellen: Internationaler Währungsfonds (IWF), Eurostat

Außenhandel mit Waren	**Mrd. US$**	**2020**	**%**	**2021**	**%**	**2022**	**%**
	Einfuhr	99,4	-2,5	122,7	23,4	147,9	20,5
	Ausfuhr	185,2	8,4	196,0	5,8	219,3	11,9
	Saldo	85,8		74,3		71,4	
Hauptabnehmerländer (2022, % der Gesamtausfuhr)	USA 30,3; Deutschland 12,1; Vereinigtes Königreich 10,6; Belgien 8,4; Niederlande 6,8; China 6,3; Andere 25,5						
Hauptlieferländer (2022, % der Gesamteinfuhr)	Vereinigtes Königreich 21,0; USA 15,7; China 10,3; Frankreich 8,5; Deutschland 7,4; Andere 37,1						
Mitgliedschaft in Zollunion	EU, seit 01.01.1973						

Wirtschaftsbeziehungen mit Deutschland

Warenhandel mit Deutschland	**Mrd. Euro**	**2021**	**%**	**2022***	**%**	**1.Hj. 2023***	**%**
	Deutsche Einfuhr	21,2	0,2	28,3	33,7	13,0	-11,0
	Deutsche Ausfuhr	7,8	1,2	10,7	37,4	4,9	-6,7
	Saldo	-13,4		-17,6		-8,1	

Rangstelle bei dt. Einfuhren (2023~~2~~) 16 von 239 Handelspartnern

Rangstelle bei dt. Ausfuhren (2023~~2~~) 28~~31~~ von 239 Handelspartnern

Direktinvestitionen (Mio. Euro, Bestand)
Deutschland in Irland: 2019: 23.505; 2020: 22.924; 2021: 20.030
Irland in Deutschland: 2019: 15.955; 2020: 25.803; 2021: 15.652

Doppelbesteuerungsabkommen Es gilt das mit Irland abgeschlossene Abkommen vom 30.03.11, in Kraft seit dem 28.11.12 (letzte Änderung vom 19.01.21.*) vorläufige Angabe, Schätzung bzw. Prognose

2023 Germany Trade and Invest - Gefördert vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages.

Weitere Informationen zu Wirtschaftslage, Branchen, Geschäftspraxis, Recht, Zoll, Ausschreibungen und Entwicklungsprojekten können Sie unter www.gtai.de/irland abrufen.

Für die Reihe Wirtschaftsdaten kompakt werden die folgenden Standardquellen verwendet: ADB, BMF, BMWK, CIA, Climatewatch, Destatis, Europäische Kommission, Eurostat, IEA, IWF, Sustainable Development Report, United Nations, UN Comtrade, Transparency International, WTO. Zum Teil wird zudem auf nationale und weitere internationale Quellen zurückgegriffen.

Quellen: *Germany Trade & Invest* bemüht sich, in allen Datenblättern einheitliche Quellen zu nutzen, so, dass die Daten für unterschiedliche Länder möglichst vergleichbar sind. Die ***kursiv gedruckten Daten*** stammen aus nationalen Quellen oder sind für das jeweilige Land in unserer Standardquelle nicht verfügbar. Dies ist bei einem Vergleich dieser Daten mit den Angaben in Datenblättern zu anderen Ländern zu berücksichtigen.

Germany Trade & Invest ist die Wirtschaftsförderungsgesellschaft der Bundesrepublik Deutschland. Die Gesellschaft sichert und schafft Arbeitsplätze und stärkt damit den Wirtschaftsstandort Deutschland. Mit über 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.

Ihre Ansprechpartnerin bei Germany Trade & Invest:
Charlotte Hoffmann

T +49 (0)228 249 93-259
charlotte.hoffmann@gtai.eu

Germany Trade & Invest

Standort Bonn

Villemombler Straße 76

53123 Bonn

Deutschland

T +49 (0)228 249 93-0 F +49 (0)228 249 93-212 www.gtai.de

Germany Trade & Invest

Hauptsitz

Friedrichstraße 60

10117 Berlin

Deutschland

T +49 (0)30 200 099-0 F +49 (0)30 200 099-111 www.gtai.com

2023 Germany Trade and Invest - Gefördert vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages.

Weitere Informationen über verschiedene Branchen im Land

GTAI-Informationen zum Land	Link
Prognosen zu Investitionen, Konsum und Außenhandel	Wirtschaftsausblick von GTAI
Potenziale kennen, Risiken richtig einschätzen	Link zur SWOT-Analyse

Länderspezifische Basisinformationen zu relevanten Rechtsthemen in Irland	Link zu Recht kompakt

Quelle: Germany Trade & Invest. (2023) „Wirtschaftsdaten kompakt- Irland“.

2.1 SWOT-Analyse

Abbildung 1: Irlands SWOT-Analyse vom Jahr 2022

Strengths (Stärken) • Globale Technologiekonzerne stärken die irische Wirtschaft als moderner Industrie- und Dienstleistungsstandort • Überdurchschnittlich starkes Wirtschaftswachstum und hohe Exportüberschüsse • Starke akademische und außeruniversitäre Forschungslandschaft • Hohes Preisniveau bietet Exporteuren attraktive Margen • Niedrige Unternehmensbesteuerung	**Weaknesses (Schwächen)** • Hohe Abhängigkeit von ausländischen Investoren • Kleiner Binnenmarkt in dezentraler Insellage • Hohes Kostenniveau bei Immobilien, Löhnen und Waren • Großes Ungleichgewicht in der Wirtschaftskraft zwischen Regionen und Branchen • Fachkräftemangel
Opportunities (Chancen) • Nordirland über grüne Grenze mit Irland weiterhin zu EU-Binnenmarktregeln erschließbar • Neuordnung des irischen Außenhandels nach dem Brexit ermöglicht Stärkung deutsch-irischer Handelsbeziehungen • Neue Fährverbindungen stärken irischen Direkthandel innerhalb der Europäischen Union • Bevölkerungswachstum dank Zuzug von qualifizierten Arbeitskräften und hoher Geburtenrate • Ausbau der Verkehrs-, Energie- und IKT-Infrastruktur, Bau von Wohn- und Gewerbeimmobilien	**Threats (Risiken)** • Globale Mindeststeuer könnte Irlands Markenkern gefährden • Neue Zollgrenze erschwert Zugang zum wichtigen Absatzmarkt Großbritannien • Steigende Inflation gefährdet Privatkonsum als Wachstumstreiber im Binnenmarkt • Anhaltende Coronakrise fordert teure staatliche Hilfsmaßnahmen • Stadtentwicklung hält vor allem in Dublin nicht mit Einwohneranstieg Schritt

Quelle: Eigene Darstellung, basierend auf Informationen von Germany Trade & Invest (GTAI)[1]

[1] Lehnfeld, M. (2022). „Irisches Geschäftsmodell zeigt sich krisenfest“.

3 Brancheninformationen Cybersicherheit in Irland

3.1 Allgemeine Information

Irlands nationales Cluster im Bereich Cybersicherheit ist „Cyber Ireland“, eine Organisation, die die Interessen und Bedürfnisse der Cybersicherheitsbranche in Irland repräsentiert. Ihr Ziel ist es, Innovation, Wachstum und Wettbewerbsfähigkeit ihrer Mitglieder zu fördern.[2] Laut der National Cyber Security Strategy wird Cyber Security wie folgt definiert: „The means of ensuring the confidentiality, integrity, authenticity, and availability of networks, devices, and data.“, übersetzt: „Die Mittel zur Sicherstellung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Netzen, Geräten und Daten.“.[3]

Die Cybersicherheitsbranche in Irland wächst und wird immer bedeutender. Laut dem Bericht „State of the Cyber Security Sector in Ireland“ (2022) trug die Branche im Jahr 2021 mit etwa 1,1 Mrd. Euro zur irischen Bruttowertschöpfung (BWS) bei. Die irische Cybersicherheitsbranche könnte nach den aktuellen Schätzungen jährlich bis zu 2,5 Mrd. Euro an Bruttowertschöpfung generieren.[4] Zudem belief sich der geschätzte jährliche Umsatz im Jahr 2021 auf ca. 2,1 Mrd. Euro (siehe Abbildung 2).[5]

Abbildung 2: Irlands geschätzte Bruttowertschöpfung und Einnahmen im Bereich Cybersicherheit im Jahr 2021

TYPE OF FIRM	AVERAGE SALARY	ESTIMATED GVA PER EMPLOYEE	ESTIMATED NUMBER OF EMPLOYEES	TOTAL GVA
Dedicated	€75k	€136k	3,372	€459m
Diversified	€77k	€155k	3,983	€617m
Total estimate GVA:				**€1.1bn**
Total revenue estimate:				**€2.1bn**

Quelle: Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.38[5]

Darüber hinaus erwähnt der Bericht von Cyber Ireland, dass die Cybersicherheitsbranche mehr als 7.300 Beschäftigte umfasst. In dieser Branche haben Großunternehmen den größten Anteil an Arbeitsplätzen mit 5.304, was 72% entspricht. 65% der Cybersicherheitsteams sind klein und bestehen aus einem bis neun Cybersicherheitsexperten. Des Weiteren, haben 27% der Unternehmen zwischen zehn und 49 Experten und 8% mehr als 50. Trotzdem besteht ein Mangel an fachqualifiziertem Personal im Arbeitsmarkt. Aus dem Bericht von Cyber Ireland über den Arbeitsmarkt in Irland geht hervor, dass 61% der befragten Unternehmen einen Mangel an Wettbewerb mit anderen Cybersicherheitsunternehmen, nichttechnische Qualifikationen und Gehälter in der Branche beklagen. Der Arbeitsmarkt weist ein Potenzial von über 17.000 Stellen bis 2030 auf, was bedeutet, dass zusätzliche 1.000 Personen pro Jahr entweder ausgebildet, weitergebildet oder eingestellt werden müssen, um die Nachfrage zu decken. Cyber Ireland zitierte im Bericht die Lightcast Spotlight Plattform, und weist darauf hin, dass eine wachsende Nachfrage für Cybersicherheitsexperten in Irland besteht.[6]

Darüber hinaus haben 20 in Irland ansässige Cybersicherheitsunternehmen externe Investitionen durchgeführt. Insgesamt haben diese Unternehmen etwa über 110 Mio. Euro an externen Investitionen erbracht.[7] Des Weiteren wird die Investitionslandschaft für die Branche durch die heimische Agentur für KMUs sowie die Risikokapitalgesellschaft der Regierung Enterprise Ireland (EI) unterstützt.[8]

[2] Cyber Ireland. „About Cyber Ireland”.
[3] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.19.
[4] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.53.
[5] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.38.
[6] Cyber Ireland (2023). „State of the Cyber Security Labour Market in Ireland“. Vgl. S.14 ff.
[7] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.49.
[8] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland”. Vgl. S.51.

3.2 Irische und EU-Gesetze und Vorschriften in der Cybersicherheitsbranche

Es existieren Gesetze in der irischen Cybersicherheitsbranche die es zu betrachten gilt. Die Studie von Adam Finlay und Ruth Hughes (2023) erwähnt die folgenden relevanten Gesetze den Bereich Cybersicherheit in Irland:

e-Privacy:

- Die Verordnung, welche in Irland umgesetzt wurde, verlangt von Anbietern öffentlich zugänglicher Telekommunikationsnetze oder -dienste, dass sie geeignete technische und organisatorische Maßnahmen zum Schutz der Sicherheit ergreifen.[9]

Netz- und Informationssysteme:

- Die Sicherheit dieser Systeme gemäß der Richtlinie 2016/1148/EU (NIS-Richtlinie) wurde in Irland umgesetzt. Das Ziel besteht darin, sicherzustellen, dass Betreiber wesentlicher Dienste Maßnahmen ergreifen, um ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in EU-Ländern zu gewährleisten. Dies wird derzeit durch die neue Richtlinie 2022/2555 (NIS2-Richtlinie) ersetzt und soll bis zum 17. Oktober 2024 in Irland umgesetzt werden.[10]

Zahlungsdienste:

- Die Richtlinie Zahlungsdienste II (2015/2366/EU oder auch „PSD2“) wurde durch die EU umgesetzt. Hierbei müssen Zahlungsdienstleister die nationale Behörde über größere Betriebs- oder Sicherheitsvorfälle informieren.[11]

Das Beschaffungswesen in Irland umfasst die Prozesse und Richtlinien, die von den Regierungsbehörden und Unternehmen befolgt werden, um Güter und Dienstleistungen zu erwerben. Die öffentliche Beschaffung in Irland unterliegt EU-Vorschriften und nationalen Regeln, die eine offene, transparente, wettbewerbsfähige und nicht-diskriminierende Umgebung gewährleisten. Das ‚Office of Government Procurement' (Amt für öffentliche Beschaffung) ist dafür verantwortlich, einen einheitlichen Rahmen für öffentliche Beschaffung zu entwickeln und umzusetzen.[12]

Die Leitlinien zu Cybersicherheitsspezifikationen (2023) vom ‚Department of the Environment, Climate and Communications' erwähnen verschiedene nationale/EU-Gesetzgebungen, die im irischen Recht für öffentliche Beschaffung, Datenschutz und Cybersicherheit umgesetzt wurden. Die folgenden Richtlinien und Gesetze sind:

EU Directive 2014/24: EU Procurement Directive/EU-Vergaberichtlinie

- Diese Reglungen sind für alle öffentlichen Einrichtungen verbindlich und betreffen insbesondere die Beschaffung von IKT-Produkten und -Dienstleistungen. Darüber hinaus schreiben die Vorschriften vor, dass nationale Behörden verpflichtet sind, alle Bewerber gerecht und gleichberechtigt zu behandeln und keine Diskriminierung bei der Vergabe öffentlicher Ausschreibungen für Arbeiten, Lieferungen oder Dienstleistungen zuzulassen.[13]

EU Directives 2014/23: Zugeständnisse

- Diese EU-Richtlinie zielt darauf ab, einen angemessenen, ausgewogenen und flexiblen Rechtsrahmen für die Vergabe von Konzessionen zu schaffen, die zwei Hauptziele verfolgt:
  - Sicherstellung, dass alle Wirtschaftsbeteiligten der Union einen effektiven und diskriminierungsfreien Zugang zum Markt erhalten.

[9] Finlay, A., Hughes, R., (2023). „Cybersecurity Laws and Regulations Ireland 2024".
[10] Finlay, A., Hughes, R., (2023). „Cybersecurity Laws and Regulations Ireland 2024".
[11] Finlay, A., Hughes, R., (2023). „Cybersecurity Laws and Regulations Ireland 2024".
[12] Department of Public Expenditure NDP Delivery and Reform/Office of Government Procurement (2023). „Public Procurement Guidelines for Goods and Services". Vgl. S.1.
[13] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)". Vgl. S.35.

- Gewährleistungen von Rechtssicherheit, um öffentliche Investitionen in Infrastrukturen und strategische Dienstleistungen für die Bürger zu erleichtern.[14]

Darüber hinaus wurde das EU-Resilienz Gesetz CRA (Cyber Resilience Act) entwickelt, um Verbraucher und Unternehmen zu schützen, die Produkte oder Software mit digitalen Komponenten kaufen oder verwenden. Durch die Einführung verbindlicher Anforderungen für Hersteller und Händler solcher Produkte zielt das Gesetz darauf ab, bestehende Sicherheitslücken zu beheben. Dieser Schutz soll den gesamten Produktlebenszyklus abdecken.[15]

GDPR: General Data Protection Regulation/Allgemeine Datenschutzverordnung:

- Diese Grundverordnung legt die Regeln für die Verarbeitung und den freien Verkehr von personenbezogenen Daten fest. Sie gilt für alle Bereiche des öffentlichen und privaten Sektors. Sowohl öffentliche Einrichtungen als auch ihre Lieferanten und Dienstleister sind verpflichtet diese einzuhalten:
  - angemessene technische und organisatorische Maßnahmen zu ergreifen,
  - Datenschutz-Folgenabschätzungen durchzuführen und
  - Datenschutzverletzungen innerhalb von 72 Stunden zu melden.[16]
- EU Cybersecurity Act: EU- Cybersicherheitsrechtsakt
  - Dieser Rechtsakt stärkt die Rolle der ENISA (Europäische Agentur für Netz- und Informationssicherheit) als zentrale Anlaufstelle für Cybersicherheitsfragen in der EU und etabliert einen europäischen Zertifizierungsrahmen für Cybersicherheit. Dieser Rahmen ersetzt nationale Zertifizierungsregelungen und umfasst verschiedene Kategorien von IKT-Produkten und -Dienstleistungen sowie Sicherheitsstandards und Bewertungsmethoden.[17]

Ferner geben die 2023 Leitlinien zu Cybersicherheitsspezifikationen vom Department of the Environment, Climate and Communications, auch relevante Industrienormen und Richtlinien:

- Cyber Security Baseline Standards: Basis für Cybersicherheitnormen
  - Diese Richtlinien wurde vom NCSC zusammen mit dem, Office of the Government Chief Information Officer (OGCIO)‘ erstellt, um eine akzeptable Sicherheitsgrundlinie zu schaffen. Das Rahmenwerk richtet sich an öffentliche Dienststellen und soll das Risikomanagement bewerten, verbessern und schließlich bewältigen.[18]
- ENISA Security Guide for ICT Procurement: ENISA Sicherheitsleitfaden für die IKT-Beschaffung
  - Das Ziel besteht darin, elektronische Kommunikationsdienstleister und IKT-Anbieter mit praxisorientierten Leitlinien zu unterstützen, um potenzielle Sicherheitsrisiken bei beschafften Gütern oder ausgelagerten Dienstleistungen zu bewältigen. Dabei werden Sicherheitsrisiken identifiziert und bestimmte Sicherheitsanforderung zugeordnet.[19]
- NIST Cyber Security Framework (CSF): NIST-Rahmenwerk für Cybersicherheit (CSF)
  - Dieses Rahmenwerk dient als Leitfaden zur Verwaltung und Minimierung von Sicherheitsrisiken in der IT-Infrastruktur. Es umfasst eine Vielzahl von Standards, Richtlinien und Praktiken, die für:
    - Die Prävention,
    - Erkennung und
    - Reaktion auf Cyberattacken benutzt werden können.[20]
- ISO: IEC 207001:2022 Information Security Management System (ISMS): Managementsystem für Informationssicherheit (ISMS)

[14] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.35.
[15] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.35.
[16] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.35.
[17] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.36.
[18] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.37.
[19] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.37.
[20] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Vgl. S.38.

  - Diese ISO beschreibt internationale ‚Best Practices' für ein ISMS. Die IEC 27001:2022 legt besonderen Wert auf einen risikobasierten Ansatz zur Informationssicherheit. Unternehmen werden dazu aufgefordert, ihre Risiken im Bereich Informationssicherheit zu erkennen und geeignete Maßnahmen zur Risikobewältigung zu ergreifen.[21]
- Center of Internet Security (CIS) Benchmarks: Benchmarks des Zentrums für Internetsicherheit (CIS)
  - Die Maßstäbe der CIS repräsentieren anerkannte ‚Best Practices', die in Zusammenarbeit entwickelt wurden und weltweit von Sicherheitsfachleuten verwendet werden, um ihre Cybersicherheitsabwehr zu stärken und zu verwalten.[22]

Laut irischem Recht bestehen keine speziellen Einschränkungen mit Blick auf den Import oder Export von Technologien zur Abwehr von Cyberangriffen. Der Export von Dual-Use-Produkten unterliegt europäischen und irischen Vorschriften und kann sowohl zivil als auch militärisch genutzt werden.[23]

3.3 Die Cyberbedrohungslage in Irland

In Irland hat die Rate an Cyberkriminalität in der Vergangenheit deutlich zugenommen. Diese Zunahme ist alarmierend, da Irland den führenden Markt für Datenhosting in Europa darstellt und mehr als 30% der europäischen Daten beherbergt. [24] Dies stellt nicht nur eine Bedrohung für Irland dar, sondern auch für ganz Europa. Einer der schwerwiegendsten Cyberangriffe auf Irland ereignete sich im Jahr 2021, als Hacker die irische Gesundheitsorganisation, Health Service Executive (HSE), attackiert haben. Dieser Angriff legte landesweit die IT-Systeme der HSE lahm. Es dauerte vier Monate, bis sich die Systeme wieder erholt hatten.[25]. Mehr als 100.000 Menschen waren von diesem Angriff betroffen, da ihnen persönlichen Daten gestohlen wurden[26]. Ein neueres Beispiel ereignete sich in der Luftfahrtindustrie bei AerCap Holdings, dem weltweit größten Flugzeug-Leasinggeber. Am 17. Januar 2024 wurde AerCap Opfer eines Ransomware Angriff. Auch wenn das Unternehmen keine finanziellen Verluste meldete, zeigt dieser Angriff, dass auch große Unternehmen, wie AerCap, die jährlichen Einnahmen von mehr als 6.4 Mrd. Euro vorweisen, Opfer von Cyberangriffen sein können. Dies verdeutlicht, dass nicht nur KMUs, sondern auch Großunternehmen von Cyberangriffen gefährdet sind und Lösungen brauchen, um sich zu schützen.[27]

Der Angriff auf das Gesundheitswesen verdeutlichte das Risiko von Cyberangriffen in Irland und führte zu einem größeren Bewusstsein der Cybersicherheit im Land. Des Weiteren zeigt eine Umfrage, an der 150 Fach- und Führungskräfte befragt wurden, dass irische Unternehmen Schwierigkeiten bei der Bewältigung von Cyberangriffen haben. Dazu haben 64% der Befragten angegeben, dass die Zunahme von Cyberangriffen der Hauptgrund dafür war, dass sie ihre Cyber-Resilienz nicht verbessern konnten. Ferner gaben 13% an, dass ein Mangel an internen Cyberfähigkeiten und -expertise besteht, während 9% veraltete Technologien und mangelnde Vorabinvestitionen in Lösungen als Hindernisse nannten. Hierbei könnten sich Chancen für deutsche Unternehmen ergeben, Lösungen anzubieten, um die genannten Hürden zu bewältigen. [28]

Laut dem Hiscox Cyber-Readiness Bericht (2023), der 5.005 Cybersicherheitsprofessionelle im Jahr 2023 befragte, waren irische Unternehmen am stärksten von Cyberangriffen betroffen, wobei mehr als sieben von zehn Unternehmen (71%) ins Visier genommen wurden. Die durchschnittlichen Kosten eines Cyberangriffs in Irland im Jahr 2023 betrugen etwa 9000 Euro. Des Weiteren berichteten 30% der befragten Unternehmen in Irland im Jahr 2023 von mindestens einem Ransomware-Angriff, im Vergleich zu 19% im Jahr 2022 und 16% im Jahr 2021. Darüber hinaus waren 77% der Opfer von Ransomware zahlungsbereit, im Vergleich zu 70% im Jahr 2022 und 75% im Jahr 2021. Dies zeigt, dass der Trend von Ransomware-Angriffen und die daraus resultierenden finanziellen Verluste in den letzten Jahren deutlich gestiegen sind und betont das Problem und die Gefahr von Cyberangriffen in Irland. In diesem Zusammenhang müssen dringend Schutzsysteme und andere innovative Sicherheitslösungen eingesetzt werden, um die Anzahl und Erfolg solcher Attacken zu reduzieren.[29]

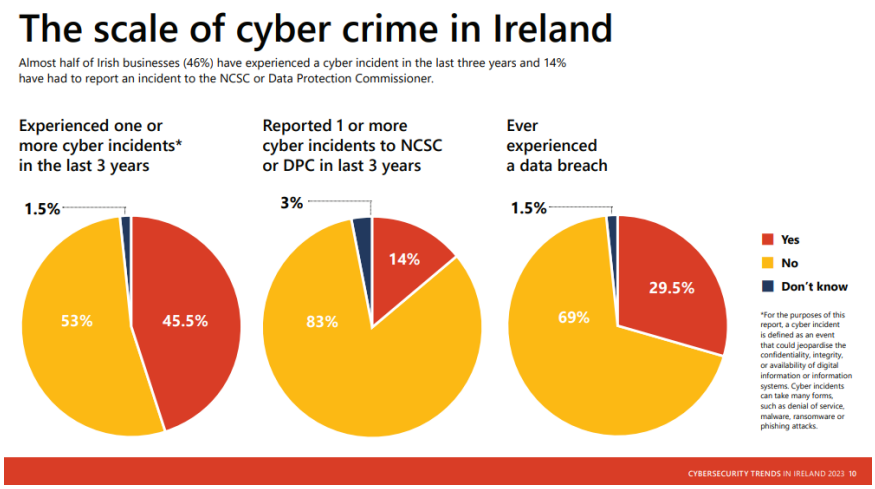
[21] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)". Vgl. S.37.
[22] Department of the Environment, Climate and Communications (2023). „Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)". Vgl. S.38.
[23] Finlay, A., Hughes, R., (2023). „Cybersecurity Laws and Regulations Ireland 2024".
[24] Cyber Ireland (2024). „Cluster Strategy 2024–2027". Vgl. S.3.
[25] U.S. Department of Health & Human Services (2022). „Lessons Learned from the HSE Cyber Attack.". Vgl. S.3.
[26] Jones, Horgan J., Wall, M., (2022). „HSE Cyberattack: More than 100,000 People Whose Personal Data Stolen to Be Contacted,".
[27] Irish Information Security Forum (2024) „Cybersecurity Attack on AerCap".
[28] Doyle, C. (2023). „Two Thirds of Irish Businesses to Increase Investment in Cyber Security,".
[29] Hiscox Ltd (2023). „Hiscox Cyber Readiness Report 2023". Vgl. S.16-17

Weiterhin ergab ein Bericht von Microsoft und Kieran McCorry (2023), der 200 C-Level-Führungskräfte in Irland zu den Cybersicherheitstrends befragte, dass 46% der Befragten in den letzten drei Jahren mindestens einen Cyberangriff erlebt haben, während 30% Opfer von Datenschutzverletzungen wurden. Etwa 14% der Befragten haben in den letzten drei Jahren einen oder mehrere Cybervorfälle dem National Cyber Security Centre (NCSC) oder dem Data Protection Commissioner gemeldet (siehe Abbildung 3). Darüber hinaus sind sich mehr als 70% der irischen Führungskräfte weder bewusst noch darauf vorbereitet, die NIS2-Richtlinie einzuhalten. Dies könnte das mangelnde Bewusstsein, die Unsicherheit über Meldeverfahren oder Sorgen hinsichtlich möglicher Auswirkungen auf den Ruf der Organisation zeigen. Ferner könnte die niedrige Meldequote auf Herausforderungen bei der Erfassung und Verfolgung von Cyberbedrohungen hinweisen und unterstreicht den Raum für Verbesserungen in der Cybersicherheitsbranche in Irland bezüglich der Infrastruktur.[30]

Des Weiteren sind die Auswirkungen von Cyberkriminalität auf die finanzielle Lage von Unternehmen signifikant. 20% der Befragten haben finanzielle Verluste aufgrund von Cyberangriffen gemeldet. Diese Verluste können auf verschiedene Cyberbedrohungen zurückzuführen sein. E-Mail-Kompromittierung sowie Phishing und Social Engineering wurden von 38% der Befragten genannt (siehe Abbildung 4). [31] Zudem führen weniger als die Hälfte (44%) regelmäßige Risikobewertungen durch. Dazu haben nur 38% eine mehrschichtige IT-Strategie implementiert, die Prävention, Erkennung, Reaktion und Wiederherstellung umfasst. Besorgniserregend ist, dass 26% der Unternehmen angegeben haben, im kommenden Jahr trotz der steigenden Bedrohungslage nicht in ihre IT-Sicherheitsinfrastruktur zu investieren.[32] Nichtsdestotrotz erhalten 57% weiterhin regelmäßiges Cybersicherheitstraining.[33] Dies unterstreicht die aktuelle Lage in Irland bezüglich Cyberangriffen und ihre Bedrohung für die irische Wirtschaft. Daher wird nach effektiven Lösungen und präventiven Maßnahmen gesucht, um die Infrastruktur in Irland zu schützen und finanzielle Verluste zu verhindern.

Ein Bericht von Grant Thornton (2023), berichtet, dass ein Drittel der betroffenen Unternehmen durchschnittlich 22.773 Euro Lösegeld an Cyberkriminelle gezahlt haben. Es wurde festgestellt, dass die Kosten für Cyberkriminalität etwa 9,6 Mrd. Euro betragen. Dies unterstreicht die Notwendigkeit, dass Unternehmen ein erhöhtes Bewusstsein für die Bedrohung entwickeln müssen.[34]

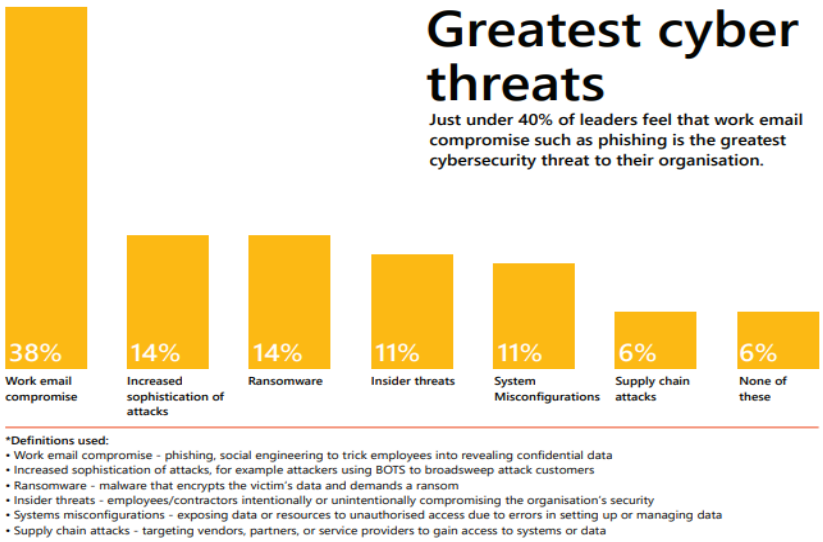
Abbildung 3: Die Cyberkriminalität in Irland



Quelle: McCorry, K. (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.10.[35]

[30] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.7.
[31] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.7.
[32] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.9.
[33] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.9.
[34] Harris, M., (2023). „Cyber-Security Remains a Priority for Irish Businesses, with Almost Half Likely to Increase Investment in Risk Mitigation“.
[35] McCorry, K. (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.10.

Abbildung 4: Die größten Cyberbedrohungen in Irland



Quelle: McCorry, K. (2023). „Cybersecurity Trends in Ireland 2023“. Vgl S.12.[36]

3.4 Künftige Entwicklungen in den relevanten Segmenten und Nachfragesektoren & Marktpotenziale und -chancen

3.4.1 Künftige Entwicklungen in den relevanten Segmenten und Nachfragesektoren

Die steigende Bedrohung von Cyberangriffen nicht nur in Irland, sondern weltweit, hat zu einer verstärkten Nachfrage nach fortschrittlichen Sicherheitslösungen geführt. Der Allianz Risk Barometer Bericht für das Jahr 2024, der mehr als 3.000 Teilnehmer aus 92 Ländern befragte, besagt, dass Cybervorfälle zum ersten Mal die größte globale Bedrohung darstellen, mit 36% der Befragten, die dies so sehen. Ein Angriff gehört zu den größten Risiken in Amerika, Afrika, dem Mittleren Osten, dem asiatisch-pazifischen Raum und Europa.[37]

Cyberattacken werden auch im Jahr 2024 weiter steigen. Zu den meist besorgniserregenden Cybervorfällen zählen Datenschutzverletzungen, Angriffe auf kritische Infrastruktur sowie Sachwerte und Ransomware.[38] Gemäß dem Nationalen Cyber Security Risk Assessment 2022, zitiert vom International Trade Administration des U.S. Department of Commerce (2024), spielt die Sicherheit der Lieferkette bei digitalen Technologien in wichtigen Branchen wie Energie, Verkehr, Finanzdienstleistungen, Gesundheitswesen, Telekommunikation sowie bei den IT-Systemen von Regierungen und des öffentlichen Sektors eine zunehmend wichtigere Rolle. Die führenden Endnutzersegmente umfassen Großunternehmen, den öffentlichen Sektor, KMU sowie Fernarbeiter und Privatkunden. Zusätzlich zu diesen wichtigen Segmenten wurden weitere Endnutzersegmente identifiziert, darunter die Biowissenschaften, das öffentliche Gesundheitswesen und die Finanzdienstleistungen.[39]

Diesbezüglich wird in Zukunft erwartet, dass Unternehmen vermehrt in ihre Cybersicherheitstechnologien investieren, um sie effektiver vor Cyberangriffen zu schützen. Laut der von Dell Technologies durchgeführten Umfrage, planen zwei Drittel der Unternehmen in ihre Cybersicherheitsstrategie zu investieren und 93% der Unternehmen haben in den letzten 12 Monaten bereits Schritte unternommen, um ihre Daten besser zu schützen. Zudem wird die Nachfrage nach qualifizierten Fachkräften im Bereich Cybersicherheit deutlich steigen, da derzeit ein Defizit besteht.[40]

Im Cyber Ireland Labour Market Report für das Jahr 2023 wurde ein Bericht des ISC2 zitiert, der besagt, dass der Fachkräftemangel vor allem in der Cybersicherheitsbranche spürbar ist. Etwa 70% der Befragten geben an, dass sie

[36] McCorry, K. (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.12.
[37] International Trade Administration U.S. Department of Commerce (2024). „Ireland - Cybersecurity“.
[38] Allianz Commercial (2023). „ Allianz Risk Barometer Identifying the major business risks for 2024“. Vgl. S. 7.
[39] International Trade Administration U.S. Department of Commerce (2024). „Ireland - Cybersecurity“.
[40] Doyle, C., (2023). „Two Thirds of Irish Businesses to Increase Investment in Cyber Security“.

nicht effektiv arbeiten können, da ihr Unternehmen nicht über genügend Cybersicherheitspersonal verfügt. Dieser Mangel an Fachkräften beeinträchtigt grundlegende Funktionen des Branche, wie Risikobewertung, Überwachung und Aktualisierung kritischer Systeme. Deshalb sollte Irland aktiv Anreize schaffen hochqualifizierte Fachkräfte für die Branche zu gewinnen, um diese Lücke zu schließen. Trotz des Wachstums in den letzten Jahren, insbesondere zwischen 2019 und 2020, könnte sich das Marktwachstum verlangsamen. Laut dem Morgan McKinley Quarterly Employment Monitor für das zweite Quartal 2023, der von Cyber Ireland zitiert wird, sind die Unternehmen bei der Einstellung von Mitarbeitern vorsichtiger geworden, was zu einem Rückgang der Zahl der offenen Stellen geführt hat.[41] Zukünftige Entwicklungen, die im Bereich Rekrutierung beachtet werden müssen, sind Verordnungen. Dies wurde als einer der wichtigeren Faktoren im Bereich Rekrutierung eingeordnet. Außerdem wurde laut dem im Cyber Ireland Labour Markt Bericht, zitiert von Morgan McKinley, ein Anstieg bei der Nachfrage von Cybersicherheitstalenten im Banken- und Finanzsektor identifiziert.[42]

Im Bericht „State of the Cyber Security Sector in Ireland" (2022) wurde jedoch eine Umfrage erwähnt, die ergab, dass 83% der Unternehmen in den nächsten 12 Monaten ein Wachstum ihres Cybersicherheit-Teams erwarten.[43] Dies unterstreicht die Dynamik und das Potenzial für Entwicklung in der Branche. Zudem zeigt es, dass Unternehmen in der Branche eine optimistische Haltung gegenüber dem Arbeitsmarkt haben.

Zunächst besteht gemäß dem Labour Market Report 2023 von Cyber Ireland eine weitere zukünftige Entwicklung, die bei der Priorisierung von Cybersicherheit in irischen Unternehmen notwendig ist. In dem bereits erwähnten Hiscox Cyber Readiness Report 2023 waren irische Unternehmen am stärksten von Cyberangriffen betroffen und verzeichneten eine hohe Zahl von Ransomware-Zahlungen, was die Dringlichkeit der Priorisierung von Cybersicherheit unterstreicht. Gemäß dem Bericht deutet dies darauf hin, dass Unternehmen in Irland einen Trend zeigen, bei dem ein zu geringes Bewusstsein für Cybersicherheit besteht und diese nicht ausreichend priorisiert wird.[44]

Eine weitere wichtige zukünftige Entwicklung, laut dem Microsoft Bericht von Kieran McCorry (2023), ist die Integration einer neuen Richtlinie in der Cybersicherheitsbranche. Die NIS2-Richtlinie, die im Oktober 2024 eingeführt wird, wird eine bedeutende Rolle bei der Verstärkung von Cybersicherheit in Unternehmen spielen. Das Ziel besteht darin, eine Basis von grundlegenden Sicherheitsmaßnahmen für Anbieter digitaler Dienste und Betreiber kritischer Infrastrukturen zu etablieren. Es soll dazu beitragen, das Risiko von Cyberangriffen zu verringern und die Cybersicherheit in der EU zu verbessern. Diese Richtlinie wird auch für irische Unternehmen zwingend erforderlich sein, um sich entsprechend darauf vorzubereiten.[45] Auch die neue regulatorische Initiative „DORA" (Digital Operational Resilience Act) zielt darauf ab, die Sicherheit und Widerstandsfähigkeit kritischer digitaler Infrastrukturen und Dienstleistungen in der EU zu verbessern. Beide Richtlinien werden Unternehmen daher dazu verpflichten, ihre Cybersicherheitsstrategie, -politik und -praxis an die neuen Normen und Erwartungen anzupassen.[46]

Außerdem hat sich gemäß dem „State of the Cyber Security Sector in Ireland" Cyber Ireland Bericht (2022) eine weitere Veränderung im Bereich der Cybersicherheit abgezeichnet, die die Rolle der Regierung betrifft. Diese ist bestrebt, die Branche durch verschiedene Maßnahmen wie Bewusstseinsbildung, Beschaffung und Unterstützung von Geschäftsaktivitäten zu fördern. Die erhöhte Beteiligung der Regierung in der Branche soll dazu beitragen, die nationale Widerstandsfähigkeit zu stärken. Der Angriff auf das Gesundheitswesen im Jahr 2021 unterstreicht die Bedeutung von Investitionen in Cybersicherheit und die Notwendigkeit entsprechende Praktiken verstärkt zu integrieren. Des Weiteren könnte das öffentliche Beschaffungswesen dazu beitragen, die Ausgaben für Cybersicherheit zu steigern und die nationale Widerstandsfähigkeit zu fördern.[47]

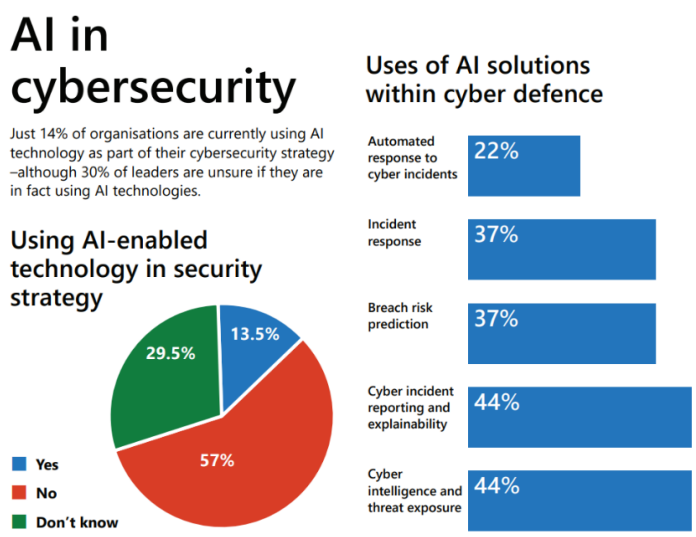
3.4.2 Marktpotenziale und -chancen

Gemäß dem Bericht von Cyber Ireland im Jahr 2022 gibt es ein großes Potenzial auf dem Arbeitsmarkt in der Cybersicherheitsbranche. Hinsichtlich der Arbeitskräfte könnte die Branche mit einer Wachstumsrate von über 10% pro Jahr expandieren. Es weist darauf hin, dass die Branche bis 2030 voraussichtlich eine Bruttowertschöpfung (BWS) von 2,5 Mrd. Euro generieren und mehr als 17.000 Cybersicherheitsexperten beschäftigen könnte. Der wachsende Markt

[41] Cyber Ireland (2023). „State of the Cyber Security Labour Market in Ireland". Vgl. S.42.
[42] Cyber Ireland (2023). „State of the Cyber Security Labour Market in Ireland". Vgl. S.43.
[43] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland". Vgl. S.54.
[44] Cyber Ireland (2023). „State of the Cyber Security Labour Market in Ireland". Vgl. S.45.
[45] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023". Vgl. S. 21.
[46] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023". Vgl. S. 23.
[47] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland". Vgl. S.10.

könnte neue Geschäftsmöglichkeiten für deutsche Unternehmen anbieten, um ihre Produkte und Dienstleistungen im Bereich Cybersicherheit einzuführen und von der erhöhten Nachfrage zu profitieren. Darüber hinaus erwähnt der Bericht den Angriff auf das Gesundheitssystem HSE im Jahr 2021, der zur Folge hatte, dass weitere Maßnahmen ergriffen wurden, um die öffentlichen Ausgaben für Cybersicherheitsdienste zu erhöhen. Zudem lässt eine Längsschnittanalyse darauf schließen, dass es zu einem Anstieg an staatliche Ausgaben kommen wird. Dies könnte den Markteintritt, die Ausweitung des Angebots und Partnerschaften zwischen größeren Unternehmen und KMU fördern. In diesem Zusammenhang bietet sich eine intensivere Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor zum Schutz der Infrastruktur an und der Unternehmen in der gesamten irischen Wirtschaft. Die erwartete Zunahme staatlicher Ausgaben könnte die Bildung von Partnerschaften zwischen deutschen Unternehmen und irischen KMU fördern. Mögliche Partnerschaften gewähren deutschen Unternehmen die Chance, gemeinsam innovative Lösungen zu entwickeln, um den Bedürfnissen des irischen Marktes gerecht zu werden.[48]

Abbildung 5: Künstliche Intelligenz im Bereich Cybersicherheit



Quelle: McCorry K. (2023). „Cybersecurity Trends in Ireland 2023“. S.17[49]

Ein weiteres Potenzial besteht bei der Nutzung künstlicher Intelligenz (KI). Laut dem Bericht von Microsoft und Kieran McCorry (2023), geben 14% der 200 Befragten an, KI bereits innerhalb ihrer IT-Sicherheitsstrategie einzusetzen. Gleichzeitig sind 30% der Führungskräfte unsicher, ob sie KI-Technologien für die Cyberabwehr einsetzen wollen. 57% nutzen keine KI in ihre Sicherheitsstrategie (siehe Abbildung 5). Aus diesem Grund existiert ein Potenzial, das Bewusstsein für KI in Irland zu steigern. Künstliche Intelligenz kann in verschiedenen Bereichen innerhalb der Cyberabwehr genutzt werden, wie etwa bei automatisierten Reaktionen auf Cyber-Vorfälle, der Vorhersage von Risiken von Sicherheitsverletzungen, Berichterstattung und Analyse von Cybervorfällen, sowie Cyber-Intelligenz und Bedrohungslagen (siehe Abbildung 5). Hierbei könnten sich Marktchancen ergeben, KI-Lösungen als Cyberabwehrsystem anzubieten, um potenzielle Risiken zu identifizieren und zu verhindern.[50]

Gemäß dem Bericht von Microsoft und Kieran McCorry (2023) haben über die Hälfte der Organisationen angegeben, dass ihnen die notwendige strategische Infrastruktur für eine entsprechende Cyberverteidigungsstrategie fehlt. Dazu gaben nur 21% der Befragten an, einen praktizierten IT Business Continuity- oder Cyber-Reaktionsplan mit Schulungen und Übungen zu haben. 30,5% haben ein internes Team von IT-Fachleuten, 38% haben eine IT-Strategie, die die Prävention, Erkennung, Reaktion und Wiederherstellung umfasst. Ebenfalls führen über 38% regelmäßige Risikobewertungen durch, um Schwachstellen zu erkennen. Zuletzt gaben 43,5% an, über keine dieser infrastrukturellen Anforderungen zu verfügen. Dies zeigt, dass es im Bereich Cybersicherheit ein Marktpotenzial für diese Art von Infrastrukturen gibt, um Unternehmen, die keine Verteidigungsstrategie haben, bei der Vorbereitung von Angriffen zu unterstützen und zu beraten. Der Bericht unterstreicht die Notwendigkeit von Aus- und Weiterbildungen im Bereich Cybersicherheit, da nur 21% der Organisationen diese praktizieren. Deshalb könnten sich Marktchancen im Bereich Schulungen bieten, um Mitarbeiter besser auf Cyberangriffe vorzubereiten. Phishing und Social Engineering stellen eine bedeutende Cyberbedrohung in Irland dar. Vermehrte Schulungen könnten dazu beitragen, diese Bedrohung zu

[48] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*”.* Vgl. S.64.
[49] Kieran McCorry (2023). „Cybersecurity Trends in Ireland 2023“. S.17.
[50] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023“. Vgl. S.17.

reduzieren, da Mitarbeiter ein größeres Bewusstsein für Cybersicherheit entwickeln und E-Mail-Kompromittierungen besser erkennen können.[51]

Ein weiteres Marktpotenzial eignet sich im Bereich Beratungsdienste. Wie in den vergangenen Abschnitten bereits erwähnt, sind laut dem von Microsoft und Kieran McCorry verfassten Bericht (2023) die Mehrheit der Führungskräfte in Irland entweder nicht darüber informiert, dass sie die NIS2-Richtline einhalten müssen, oder sie haben bisher keine entsprechenden Maßnahmen ergriffen. Dazu fehlt den Unternehmen die notwendige strategische Infrastruktur. Diesbezüglich könnten sich Chancen hinsichtlich der Beratungsdienste in Irland ergeben, um Unternehmen besser bei der Einhaltung der Richtlinien sowie zu angemessenen Strategien zu beraten.[52]

Die Berichte von Microsoft und Kieran McCorry (2023) sowie von Hiscox (2023) verdeutlichen die Präsenz von Cyberkriminalität in Irland und die damit verbundenen Risiken. Dies schafft bedeutende Chancen für deutsche Unternehmen, die effiziente Systeme und Lösungen zur Bekämpfung von IT-Sicherheitsrisiken und Cyberkriminalität bereitstellen. Insbesondere Dienste zum Schutz vor Ransomware, Anwendungen zur Minimierung von Cyberrisiken und Lösungen für Drittanbieter-Risiken sind gefragt.

Die Beteiligung des öffentlichen Sektors ist von wesentlicher Bedeutung für die Formgebung der Cybersicherheitsbranche und spielt eine bedeutende Rolle als Abnehmer für entsprechende Produkte und Dienstleistungen. Die von Cyber Ireland zitierte Analyse zu den Ausschreibungen von Etenders 2022 zeigt die Nachfrage nach Cybersicherheitsdiensten zwischen 2012 und 2021. Die Anzahl der öffentlich ausgeschriebenen Aufträge ist in dem Zeitraum drastisch gestiegen. Im Jahr 2012 wurde ein Projekt verzeichnet, während es im Jahr 2021 schon 53 waren. Innerhalb von zehn Jahren hat sich die Anzahl der ausgeschriebenen Projekte verzehnfacht.[53] Darüber hinaus waren die am meisten nachgefragten Dienste:

- Unterstützung bei der Bereitstellung/Entwicklung von Sicherheitssoftwarepaketen
- Softwarepakete für Datensicherheit
- Entwicklungsdienste für Datensicherheitssoftware
- Dienstleistungen zur Entwicklung von Sicherheitssoftware
- Softwarepakete für Datensicherheit.[54]

Dies verdeutlicht die Nachfrage nach Cybersicherheitsdiensten und das Potenzial des Marktes diese anzubieten. Die wachsende Möglichkeit im Bereich der öffentlichen Beschaffung sollten genutzt werden.[55]

Der Bericht „State of the Cyber Security Sector in Ireland" (2022) hat verschiedene erwartete Wachstumschancen aufgezeigt. Dazu gehört die Erweiterung von Dienstleistungen durch die Einstellung von Hochschulabsolventen und die Erweiterung der Marktanforderungen, wie zum Beispiel der verstärkte Einsatz von Technologien. Des Weiteren werden größere Projekte, Fusionen und Übernahmen kleiner Unternehmen als weitere Möglichkeiten zur Expansion betrachtet. Insbesondere wurden mindestens 14 Übernahmen von inländischen Unternehmen identifiziert, die sich auf Cybersicherheitsdienstleistungen spezialisieren. Schließlich wird die Nutzung der internationalen Präsenz Irlands als Chance betrachtet, um weitere internationale Investitionen anzuziehen.[56] Im selben Bericht wurde allerdings festgestellt, dass die Spezifikationen für Ausschreibungen restriktiv und schwer zu erfüllen sind. Infolgedessen schlägt Cyber Ireland vor, das Potenzial für eine verstärkte Zusammenarbeit mit KMU im Bereich Cybersicherheit zu nutzen, um exklusive und wirkungsvolle Ausschreibungsmöglichkeiten gemeinsam zu entwickeln. Diese Partnerschaft könnte dazu beitragen, dass KMU ihre Aktivitäten im Inland weiter ausweiten können.[57]

Cyber Ireland schlägt außerdem vor, dass Irland seine bestehende Expertise und seine derzeitige Attraktivität als Standort für Cybersicherheit nutzen sollte, um externe Unternehmen zu ermutigen, verstärkt in den Ausbau ihrer Fähigkeiten und Kapazitäten im Bereich der Cybersicherheit zu investieren. Zudem besteht Potenzial für die Entwicklung von Unterstützungsmaßnahmen, die als Chance für deutsche Unternehmen betrachtet werden können.

[51] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023". Vgl. S.13.
[52] McCorry, K., (2023). „Cybersecurity Trends in Ireland 2023". Vgl. S.17.
[53] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S. 58.
[54] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S. 59.
[55] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S.59.
[56] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S.54.
[57] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S.10.

Enterprise Ireland, wie von Cyber Ireland zitiert, betonen in ihrem European Cybersecurity Market Opportunity Mapping Exercise, dass diese Entwicklung darauf abzielt, das Engagement auf europäischen Märkten zu fördern.[58]

3.5 Irlands Strategie für Cybersicherheit/Aktuelle Vorhaben, Projekte und Ziele

Die National Cyber Security Strategy (NCSS) hat derzeit eine, noch bis dieses Jahr 2024, laufende Cybersicherheitsstrategie. Die Strategie wurde im Jahr 2019 veröffentlich und zielt darauf ab, die Sicherheit und Widerstandsfähigkeit der Regierungssysteme und die kritische nationale Infrastruktur zu verbessern. Dies ist von wichtiger Bedeutung für Irland, da die kritische nationale Infrastruktur mit ihren komplexen Systemen und Datenströmen anfällig für Cyberangriffe ist. Die Strategie stützt sich auf drei Säulen:

- „Protect“ (den Staat, die Bevölkerung, sowie die kritische nationale Infrastruktur vor Cyberbedrohungen zu schützen)[59]
- „Develop“ (die Fähigkeit des Staates, von Forschungseinrichtungen, Unternehmen, dem öffentlichen Sektor und der Bevölkerung zu entwickeln)[60]
- „Engage“ (national, als auch international strategisch zu agieren, um einen freien, offenen, friedlichen und sicheren Cyberspace zu fördern).[61]

Die Cybersicherheitsstrategie der NCSC setzt dabei bestimmte Ziele voraus. Darunter fallen:

- Die Fähigkeit das Sicherheitssystem weiter auszubauen, um auf Cybervorfällen zu reagieren und sie zu bewältigen. Dies bedeutet, dass die Regierung besser in der Lage sein sollte, auf Cyberangriffe zu reagieren, um die nationale Sicherheit zu schützen und die daraus resultierenden Auswirkungen zu minimieren.[62]
- Die Regierung soll die kritische Infrastruktur identifizieren und schützen, indem sie Maßnahmen ergreift, um ihre Widerstandsfähigkeit gegen Cyberangriffe zu stärken. Dies umfasst die Sicherstellung, dass Betreiber von wesentlichen Diensten angemessene Notfallpläne haben.[63]
- Die Widerstandsfähigkeit und Sicherheit der IT-Systeme stärken, um sowohl Daten als auch Dienstleistungen besser zu schützen.[64]
- In Bildungsinitiativen investieren, um Arbeitskräfte auf Berufe im Bereich fortgeschrittene IT und Cybersicherheit vorzubereiten.[65]
- Das Bewusstsein der Unternehmen für ihre Verantwortung bei der Sicherung eigener Infrastruktur schärfen. Gleichzeitig zielt die Regierung darauf ab, die Forschung und Entwicklung in der irischen Cybersicherheitsbranche zu fördern.[66]
- Weiterhin mit internationalen Partner und Organisationen zusammenarbeiten, um sicherzustellen, dass der Cyberspace für alle offen, sicher, einheitlich und frei bleibt, sowie dazu beitragen, die wirtschaftliche und soziale Entwicklung zu fördern.[67]
- Das Bewusstsein und die Fähigkeiten von Privatpersonen im Bereich Cyberhygienepraktiken verbessern, durch die Bereitstellung unterstützender Schulungen.[68]

Das nationale Cluster für die Cybersicherheitsbranche, Cyber Ireland, hat 2024 eine neue Clusterstrategie für den Zeitraum 2024 bis 2027 veröffentlicht. Die Strategie zielt darauf ab, das Wachstum in der Branche bis 2030 zu fördern.[69] Zu den Komponenten der Strategie gehören:

[58] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ”. Vgl. S.11.
[59] Department of the Environment Climate and Communications (2023). „National Cyber Security Strategy 2019-2024 Mid-Term Review“. Vgl. S.5.
[60] Department of the Environment Climate and Communications (2023). „National Cyber Security Strategy 2019-2024 Mid-Term Review“. Vgl. S.5.
[61] Department of the Environment Climate and Communications (2023). „National Cyber Security Strategy 2019-2024 Mid-Term Review“. Vgl. S.5.
[62] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[63] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[64] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[65] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[66] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[67] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[68] Government of Ireland (2019). „National Cyber Security Strategy”. Vgl. S.13.
[69] Cyber Ireland (2024). „Cluster Strategy 2024–2027”. Vgl. S.4.

1. Zusammenarbeit und Kooperation von Wirtschaft, Politik, öffentlichen Trägern und Kultur in Form von Clustern.[70]
2. Förderung des Unternehmenswachstums durch Unterstützung von Unternehmen bei ihrem Wachstum und der Entwicklung neuer Innovationen und Lösungen. Hierbei liegt ein besonderer Fokus auf der Unterstützung von Start-ups und KMU, um das Wachstum der Branche zu fördern.[71]
3. Entwicklung des Arbeitskräftepotenzials durch die Unterstützung einer nachhaltigen Deckung des Fachkräftebedarfs, um den Anforderungen und Bedürfnissen der Branche gerecht zu werden.[72]
4. Befürwortung und Förderung durch die Vertretung der Interessen der Branche, um die Mitglieder zu unterstützen und den Markt durch Partnerschaften mit privaten und öffentlichen Interessenträgern zu stärken.[73]

Des Weiteren hat Ossian Smyth, der Staatsminister im Ministerium für Umwelt, Klima und Kommunikation, die Schaffung eines neuen nationalen Cybersicherheits-, Koordinations- und Entwicklungszentrumprojekt (NCC-IE) für Irland begrüßt. Dieses Projekt ist innerhalb des Nationalen Cybersicherheitszentrums (NCSC) angesiedelt. Der Start des Cybersicherheitsprojekts erfolgte im Mai 2023, mit einer Finanzierung von 4,2 Mio. Euro und zielt darauf ab, KMU Mittel für Forschung, Innovation und erhöhte Widerstandsfähigkeit bereitzustellen[74]. Das 2-jährige Projekt wird mit 2 Mio. Euro von der EU und 2,2 Mio. Euro vom Ministerium für Umwelt, Klima und Kommunikation finanziert.[75]

Cyber Ireland begrüßt die jüngsten Maßnahmen der Regierung sowie die starke Unterstützung von Finanzminister McGrath für die Cybersicherheit und den Technologiesektor Irlands im Budget 2024. Laut dem Artikel von Cyber Ireland, wurde dem nationalen Cybersicherheitszentrum (NCSC) eine beträchtliche Investition von 10,7 Mio. Euro zugesprochen. Diese erhebliche Investition in Cybersicherheit, Verteidigung und Industrieunterstützung wird die Stärkung der irischen Cybersicherheitsbranche und die nationale Cyber-Resilienz vorantreiben. Zudem wurde der Minister für öffentliche Ausgaben und Reformen, Paschal Donohoe, zitiert, der die Regierungsbemühungen hervorhob, den Schutz der Bürger, ihrer Daten sowie der digitalen Infrastruktur und Dienstleistungen zu gewährleisten. Das neue Budget für 2024 soll dazu beitragen, die Cybersicherheit zu stärken und die Widerstandsfähigkeit zu erhöhen, die Qualifikationslücke im IT-Bereich zu schließen und die Branche weiterzuentwickeln.[76] Zusätzlich werden in Cork weitere Investitionen im Bereich Cybersicherheit getätigt. Die Initiative von 7 Mio. Euro für die Munster Technological University in Cork (MTU) zielt darauf ab, eine neue Generation von Cybersicherheitsexperten zu fördern. Über einen Zeitraum von sechs Jahren wird das Cyber Innovate Projekt der MTU die Innovation und das Unternehmertum in Irland antreiben, neue Unternehmen gründen und mehr Arbeitsplätze schaffen. Das Projekt soll jedes Jahr 12-15 Teilnehmern die erforderlichen Fähigkeiten vermitteln, um neue Produkte und Dienstleistungen in der Branche zu entwickeln, und damit zur Gründung neuer kommerzielle Start-ups und forschungsnahe Hochschulausgründungen beitragen könnte.[77]

3.6 Wettbewerbssituation und Key Players

Es gibt viele wesentliche Beteiligte auf dem irischen Cybersicherheitsmarkt wie eine Vielzahl von inländischen und ausländischen Cybersicherheitsunternehmen, Verbände, Regulierer, sowie Behörden, die den Markt ausmachen. Der Wettbewerb in der irischen Cybersicherheitsbranche ist intensiv, Irland verfügt über eine große Zahl von IT-Unternehmen, von denen allein in Dublin mehr als 734 ansässig sind.[78] Der Markt wird gemäß Cyber Ireland (2022) von den 489 Unternehmen wie folgt aufgeteilt:

- 44% sind Großunternehmen,
- 12% sind Mittelgroße,
- 16% sind Kleine und
- 28% sind Mikrounternehmen.

Das heißt, dass 56% dieser Branche aus KMU besteht.[79]

[70] Cyber Ireland (2024). „Cluster Strategy 2024–2027". Vgl. S. 10.
[71] Cyber Ireland (2024). „Cluster Strategy 2024–2027". Vgl. S. 11.
[72] Cyber Ireland (2024). „Cluster Strategy 2024–2027". Vgl. S. 12.
[73] Cyber Ireland (2024). „Cluster Strategy 2024–2027". Vgl. S.13.
[74] Department of the Environment, Climate and Communications (2023). „Minister Smyth welcomes establishment of €4.2 million National Cybersecurity Coordination and Development Centre (NCC-IE) project".
[75] O'Regan, E., (2023). „€4.2m project aims to provide cybersecurity funds for small firms".
[76] Cyber Ireland (2023). „Cyber Ireland welcomes investment in Cyber Security in Budget 2024".
[77] Ó Liatháin, C., (2024). „New Cork initiative set to train next generation of cyber security experts".
[78] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S.29.
[79] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland ". Vgl. S.23.

Laut dem Cyber Ireland 2022 Bericht sind 240 der 489 Unternehmen inländische Anbieter. Die ausländischen Anbieter werden wie folgt aufgeteilt:

- 139 kommen aus den USA,
- 53 sind aus dem Vereinigten Königreich (ohne Nordirland),
- 9 aus Frankreich,
- 8 aus Nordirland,
- 8 aus Deutschland,
- 6 aus Japan,
- 5 aus Kanada und
- 21 aus anderen Ländern.[80]

Des Weiteren teilte Cyber Ireland (2022) die Unternehmen nach Unternehmensgrößen auf:

- 217 Großunternehmen, die 250 Vollzeitäquivalente oder mehr haben (194 oder 89% ausländische Unternehmen/23 oder 11% inländische Anbieter).
- 58 mittlere Unternehmen mit 50 bis 249 Vollzeitäquivalenten (17 oder 29% sind ausländische Anbieter/41 oder 71% sind Inländische).
- 77 kleine Unternehmen mit 10 bis 49 Vollzeitäquivalenten (23 oder 30% ausländische Anbieter/54 oder 70% Inländische).
- 137 Mikro-Unternehmen mit 1 bis 9 Vollzeitäquivalenten (15 oder 11% ausländische Anbieter/122 oder 89% sind Inländische)[81].

Cyber Ireland (2022) beschreibt, dass von den 489 Unternehmen in Irland folgende Leistungen angeboten werden:

- 174 oder 36% bieten Managed Security Service Provision (MSSP) und Advisory Services an,
- 151 oder 31% bieten auf Securing Applications, Networks und Cloud Environments an,
- 138 oder 28% bieten Risk, Compliance und Fraud an,
- 129 oder 27% bieten Threat intelligence, Monitoring, Detection und Analysis an,
- 64 oder 13% bieten Operational Technology (OT) Security und Connected Devices an,
- 56 oder 11% bieten Identification, Authentication und Access Control an, und
- 92 oder 19% bieten sonstige Dienstleistungen, wie Interne Forschung, Entwicklung, und Rekrutierung an.[82]

Es ist ersichtlich, dass ein bedeutender Anteil der Cybersicherheitsbranche in Irland auf die Bereitstellung von Dienstleistungen ausgerichtet ist.

Außerdem hat der Bericht „State of the Cyber Security Sector in Ireland*"* von Cyber Irland (2022) die Unternehmen entweder als „Dedicated (Pure-Play)" oder „Diversified" kategorisiert. „Dedicated" Unternehmen sind solche, deren Einnahmen zu 75% oder mehr aus der Bereitstellung von Cybersicherheit stammen. Diese Unternehmen bieten spezifische Produkte oder Dienstleistungen für die Cybersicherheitsbranche an. Andererseits bezieht sich die Kategorisierung von „Diversified" Unternehmen auf Firmen, die Cybersicherheitsdienstleistungen als Teil einer breiten Geschäftsstruktur anbieten, wie zum Beispiel dem Finanz-, Versicherungs- oder Verteidigungssektor. Die Aufteilung ist wie folgt:

- 160 oder 33% der Unternehmen „Dedicated" (Pure-Play) und
- 329 oder 67% der Unternehmen „Diversified".[83]

Darüber hinaus hat derselbe Bericht die bedeutungsvollsten Unternehmen in der irischen Cybersicherheitsbranche erwähnt. Die größten Unternehmen Irlands befinden sich in Dublin. Die Hauptstadt beherbergt 397 Cybersicherheitsbüros und damit die meisten im Land. Dort sind Cybersicherheit-Teams von Unternehmen wie Microsoft, Amazon, Zurich und Threatlocker ansässig. Es gibt eine starke Basis von KMU, insbesondere Managed Security Service Providers (MSSPs), wie Integrity 360 und Ward Solutions, die Fachkräfte von Universitäten in Dublin rekrutieren. Die Technological University Dublin, das University College Dublin, und die Dublin Business School

[80] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"*. Vgl. S.25.
[81] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"*. Vgl. S.26.
[82] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"*. Vgl. S.27.
[83] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"*. Vgl. S.23 ff.

bieten spezielle Cybersicherheitskurse an. Sie haben Forschungseinrichtungen wie das Centre of Applied AI CeADAR, Centre for Cybersecurity und Cybercrime Investigation an der University College Dublin (UCD), sowie das Collaboratory an der Technological University Dublin. Das National Cyber Security Centre (NCSC) ist auch in Dublin beheimatet. [84]

Ferner ist Cork, mit seinen 129 Cybersicherheitsunternehmen, ebenfalls ein bedeutender Standort, besonders für US-Unternehmen, wie zum Beispiel das McAfees Centre of Excellence und das EMEA-Headquarter von Trend Micro. Das nationale Cybersicherheit-Cluster Cyber Ireland, ist ebenfalls in Cork ansässig. Die Region um Galway, mit 39 Cybersicherheitsbüros, ist die Heimat vom Hewlett-Packard's Global Cyber Defence Centre. Die Region um Limerick, mit 30 Cybersicherheitsbüros, ist die Heimat der University of Limerick und Lero, Irish Software Research Centre. Weitere bedeutungsvolle Standorte, die entweder Standorte oder Akademische Institute beheimaten in der Cybersicherheitsbranche sind: Clare, Kildare, Waterford, Louth, Donegal, Kerry, Carlow, Athlone, Sligo, Letterkenny und Dundalk.[85]

Es gibt wichtige Verbände und Regulierer sowie Behörden im Sicherheitsbereich, die bei einer Betrachtung des Marktes beachtet werden müssen. Zu den wichtigsten Verbänden in der irischen Cybersicherheitsbranche zählt das nationale Cluster Cyber Ireland. Die wichtigste staatliche Einrichtung ist der National Cyber Security Centre (NCSC). Die Hauptaufgabe der NCSC besteht darin, bei der Bewältigung großer Cybersicherheitsvorfälle die Führung zu übernehmen. Es bietet Bürger und Unternehmen Orientierungshilfen und Ratschläge im Bereich Cybersicherheit an. Außerdem arbeitet der NCSC daran, die mit der Cybersicherheit verbundenen Risiken für wichtige Dienste zu minimieren.[86]

Ein Regulierer, mit der Befugnis zur Untersuchung von Cyberkriminalität und anderen relevanten Vorfälle ist die Garda Síochána, die nationale Polizei. Darüber hinaus verfügt die Garda über das National Cyber Crime Bureau, eine spezialisierte Abteilung der Polizei, über die Befugnis zur Untersuchung von Cyberkriminalität. Eine weitere regulierende Behörde mit Untersuchungsbefugnissen ist die Zentralbank Irlands. Diese Behörde kann prüfen, ob die von ihnen regulierten Unternehmen im Finanzdienstleistungssektor nach einem Vorfall im Cybersichrheitsbereich, die geltenden Gesetze und Vorschrifte befolgt haben.[87] Die Data Protection Commission (DPC) ist eine weitere bedeutende Behörde in der irischen Cybersicherheitsbranche. Sie ist eine nationale unabhängige Behörde und hat die Aufgabe, die persönlichen Daten der Einzelpersonen in der EU zu schützen. Zudem überwacht die DPC die Umsetzung der Datenschutz-Grundverordnung (DSGVO) in Irland und hat auch Zuständigkeiten im Zusammenhang mit anderen wichtigen regulatorischen Rahmenbedingungen, wie den irischen ePrivacy-Vorschriften von 2011 und der EU-Richtlinie (Law Enforcement Directive).[88]

Das Department of Communications, Climate Action and Environment (DCCAE), das Ministerium für Kommunikation, Klimaschutz und Umwelt, nimmt in Irland eine weitere wesentliche Rolle ein. Es hat die Aufgabe, Vorschriften und Programme in verschiedenen Bereichen umzusetzen und sicherzustellen, dass alle Aktivitäten den Verpflichtungen den EU- und internationalen Abkommen entsprechen.[89]

Weitere wichtige Akteure in der Branche sind Einrichtungen der Forschung und Aus- und Weiterbildung, wie Universitäten oder Instituten. Es gibt viele Anbieter von Aus- und Weiterbildungsmaßnahmen im Bereich der Cybersicherheit, die durch eine starke Wettbewerbssituation geprägt sind. Die Ausbildung von Cybersicherheit in Irland wird von vielen Universitäten und Institutionen entweder als Bachelor, Master sowie Zertifikatskursen, und anderen Programme angeboten. In Dublin gibt es zahlreiche Universitäten, Hochschulen oder Institutionen die Cybersicherheit als Studiengang anbieten, darunter das National College of Ireland, das Irish Management Institute, die Technological University Dublin, das University College Dublin, die Dublin Business School, und der „Fasttrack into Information" Technology, oder auch FIT Dublin genannt. In Cork sind die Munster Technological University, das University College Cork, der FIT Cork und Cyber Skills, eine Organisation im Technologiesektor angesiedelt. In Limerick befinden sich die University of Limerick, die Lehrlingsausbildung und Bachelor oder Master sowie spezialisierte Auszeichnungsprogramme im Bereich der Cybersicherheit anbietet. Weitere bedeutungsvolle Ausbildungsstätte sind

[84] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland". Vgl. S.29 ff.
[85] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland". Vgl. S.31.
[86] Department of the Environment, Climate and Communications (2023). „Cyber Security".
[87] Finlay, A., Hughes, R., (2023). „Cybersecurity Laws and Regulations Ireland 2024".
[88] Dataprotection Commission. „The Data Protection Commission".
[89] Department of the Environment, Climate and Communications (2019). „About the Department of the Environment, Climate and Communications".

der Chevron College in Wexford, die Technological University of the Shannon, die South East Technological University in Carlow und Waterford, sowie das Education and Training Board in Sligo, Mayo, und Leitrim.[90]

Siehe Tabelle 1, um einen Überblick über die aktuellen Anbieter von Cybersicherheitskompetenzen in Irland zu erhalten, die von Cyber Ireland identifiziert wurden.

Tabelle 1: Anbieter von Cybersicherheitskompetenzen

Anbieter	Kurze Beschreibung
Advance Centre UCD (University College Dublin) & ATU (Atlantic Technological University)	Blended Learning Optionen sind verfügbar für postgraduierte Studierende, Hochschulabsolventen, Erwachsene, Fachleute aus der Industrie und KMU/MNU. Das Programm umfasst Module im Bereich Digital Manufacturing sowie Workshops und Fernunterricht, um Fachkräfte im Bereich Cybersicherheit und angrenzenden Branchen weiterzubilden und deren Entwicklung zu unterstützen. Dazu zielt das Programm darauf ab, den Fachkräftemangel im Bereich Cybersicherheit zu verringern, indem es hochwertige, praxisrelevante Schulungen für professionelle Lernende anbietet, um deren Fähigkeiten zu verbessern und den Bedarf der Industrie zu decken. Der Bericht von Cyber Ireland besagt, dass das Programm einen Mehrwert für verschiedene Arten von Unternehmen oder Behörde hat wie KMU, MNU, Unternehmen, Regierungen und staatliche Institutionen, Verteidigungskräfte und viele mehr. Es hat einen Mehrwert, da es Beschäftige für neue Aufgaben weiterqualifiziert, damit sie ihre entsprechenden Organisationen schützen könne.
Cyber Analyst Bootcamp-itag Skillnet	Es handelt sich um einen Onlinekurs, der gezielt auf Arbeitssuchende mit einem IT-Hintergrund abzielt. Angesichts der kontinuierlich wachsenden Nachfrage nach Cybersicherheitskompetenzen bietet das itag Skillnet ein 8-wöchiges Programm an, in dem die Teilnehmer die Möglichkeit haben, mit Industrieexperten zusammenzuarbeiten. Es fördert eine verstärkte Kooperation zwischen der Industrie, Akademikern, INtreo und Skills Connect bei der Entwicklung und Durchführung.
Cyber Skills	Es handelt sich um ein nationales Programm, das für postgraduierte Studierende, Hochschulabsolventen, Arbeitssuchende, Fachleute aus der Industrie und KMU/MNU konzipiert ist. Es zielt darauf ab, den Mangel an Fachkräfte im Bereich Cybersicherheit in Irland anzugehen. In Zusammenarbeit mit sämtlichen Universitäten in Irland, entwickeln und liefert es höhere Bildungs-Mikro-Zertifikate und -Wege, die darauf abzielen, die von der Industrie benötigten Fähigkeiten zu vermitteln. Das Programm bietet den Studierenden das Wissen, die Fähigkeiten und das Training, das benötigt wird, um sich weiterzuentwickeln und die Karriere im Bereich Cybersicherheit voranzutreiben. Sie suchen nach Industrieengagement, um ihre Programme zu gestalten und durchzuführen.
Cyber Quest- IT@Cork Skillnet & CJHNetwork	Cyber Quest ist für postgraduierte Studierende, Hochschulabsolventen und Arbeitssuchende konzipiert. Es handelt sich hierbei, um eine Online-Trainingsinitiative, die Schulungen zur Sensibilisierung, Entwicklung von Fähigkeiten und fortgeschrittenen Trainingsmöglichkeiten für Arbeitslose und diejenigen, die von Covid-19 betroffen wurden, anbietet. Das Ziel der Initiative ist es, Menschen dabei zu helfen, Beschäftigung in der Branche zu finden. Sie haben auch die Abdeckung von Fachkräften im Bereich der Cybersicherheit erweitert und das Bewusstsein für Schwachstellen im Allgemeinen geschärft.
Enterprise Ireland Leadership Development Programmes	Hierbei werden irische Führungskräfte motiviert, den Mut, das Selbstbewusstsein und die Kompetenz zu entwickeln, ihre Unternehmen global zu erweitern. Das Programm hilft dabei, die Anforderungen ihrer Kunden durch eine Auswahl von maßgeschneiderten Führungs- und Managementwicklungsprogramme zu erfüllen.
Future in Tech- Technology Ireland ICT Skillnet	Das Programm wurde konzipiert, um Arbeitssuchenden, die keinen IT-Hintergrund haben, neue digitale Fähigkeiten zu entwickeln und ihnen den Zugang zu neuen Arbeitsmöglichkeiten zu ermöglichen. Der Kurs ist auch für Berufseinsteiger geeignet, die eine Karriere in der IT-Sicherheit anstreben, und bietet ihnen das nötige Wissen und die erforderliche Kompetenz, um in der Branche Fuß zu fassen.
IBM Skillsbuild- IBM & Technology Ireland Skillnet	Es ist eine innovative Online-Plattform von IBM, die leicht zugänglich ist und grundlegende technische Lerninhalte bietet, die auf bestimmte gefragte technische Rollen und Karrieremöglichkeiten ausgerichtet ist. Dadurch können Lernende ihre technische Karriereziele erreichen oder sich weiterqualifizieren und umschulen.

[90] Cyber Ireland. „course-finder".

ICT Associate Apprenticeship Cyber Security- FIT	Das Programm nutzt ein "Learning-by-Doing"-Format zur Entwicklung von IKT-Fähigkeiten, womit das Konzept einer praxisorientierten Hochschulbildung verstanden und angewendet wird.
IDA Ireland Training Grant	Für die IDA ist es wichtig und Teil der Strategie, dass Kundenunternehmen in Schulungen investieren, um ihre Unternehmen zu modernisieren und für die Zukunft zu stärken.
UL Cybersecuritys Practitioner Apprenticeship BSc (Hons)- University Limerick & Online	Dieses Berufsbildungsprogramm fördert die Entwicklung des Wissenstandes in Cybersicherheit für Fachkräfte in Organisationen, indem es praktische Umsetzung am Arbeitsplatz mit gemischtem Lernen an der University of Limerick kombiniert. Es zielt darauf ab, den Mangel an Fachkräften in der Cybersicherheit zu adressieren und eine Talent-Pipline für die Industrie bereitzustellen.
UL Principal Engineer Apprenticeship Deng- University of Limerick & Online	Das Doktoratsstudium bereitet Kandidaten auf eine akademische Laufbahn vor, indem es sie darauf trainiert, wissenschaftliche Probleme gründlich anzugehen.
Cyber Security Academy- Cyber Skills, Cyber Ireland & MTU	Die Akademie konzentriert sich darauf, jungen Menschen technische Schulungen anzubieten, um sie auf zukünftige Karrieren im Bereich der Cybersicherheit vorzubereiten. Die Studierenden erhalten eine Einführung in wichtige technische Fähigkeiten wie Penetrationstests, ethisches Hacking und Kryptographie, die ihnen helfen, auf Sicherheitsvorfälle zu reagieren und Systeme zu schützen.

Quelle: Eigene Darstellung; basierend auf Informationen von Cyber Ireland. „CYBER SECURITY SKILLS PROVIDERS". Vgl. S. 1-22[91]

Es gibt verschiedene themenspezifische Messen im Laufe des Jahres. Ein Beispiel ist die Cyber Ireland National Conference die am 26. und 27. September 2023 in Galway stattgefunden hat. Bei der Messe haben 400 Cybersicherheitsexperten von mehr als 150 Unternehmen teilgenommen.[92]

3.7 Stärken und Schwächen des Marktes für die Branche Cybersicherheit

Ein Großteil der Unternehmen im Bereich der digitalen Sicherheit, welche sich in Irland niederlassen, entwickeln Produkte und Dienstleistungen, um diese ins Ausland zu exportieren. Irland selbst stellt vergleichsweise einen recht kleinen Markt dar, der allerdings durch den Zustrom an Unternehmen stetig wächst. Viele Großkonzerne eröffnen in Irland einen Unternehmenssitz als EU-Niederlassung oder aus steuerlichen Gründen. Von diesen Unternehmen stellen viele ein High-Value-Ziel für Hacker dar, weshalb die Unternehmen bereit sind, mehr für ihre Sicherheit zu investieren. Dies stellt hohe Margen in Aussicht. Dass ein erfolgreicher Hackerangriff Milliarden kosten kann, hat die Vergangenheit gezeigt. Der über Jahrzehnte anhaltende Zuwachs multinationaler Unternehmen führte zu starken Preis- und Lohnanstiegen in den urbanen Räumen Irlands, insbesondere in Dublin. Hohe Mieten und Gehälter in Irland macht die Etablierung einer Unternehmensniederlassung vergleichsweise kapitalintensiv. Die niedrige Besteuerung von Unternehmen reduziert diese finanziellen Belastungen zwar stark, jedoch könnte diese Erleichterung durch die Einführung der globalen Mindeststeuer in Zukunft schwinden.[93]

Des Weiteren herrscht ein Fachkräftemangel im Bereich der Cybersicherheit; vor allem bei Fachkräften mit mehrjähriger Berufserfahrung. Unternehmen in dieser Branche konkurrieren um diese gut ausgebildeten Arbeitskräfte, weshalb dieses Problem kurzfristig noch bestehen bleiben wird. Um diesen Mangel zu bekämpfen wird die Entwicklung einer Deckung der Fachkräfte sowie mehr Umschulungen bzw. Weiterbildungen ins Auge gefasst. Zielgruppe dieser Maßnahmen sind nicht nur lokale Arbeitskräfte, sondern auch Irland im Bereich der Cybersicherheit als Studienstandort, um so zukünftige Arbeitskräfte aus dem Ausland anzuwerben. Daraus resultiert mittel- bis langfristig ein hoher Bedarf an gut ausgebildeten Fachkräften für Cybersicherheit.[94]

Durch den Hackerangriff auf den Health Service Executive (2021) entstand ein stärkeres Bewusstsein für die Notwendigkeit von Cybersicherheit in Regierungsinstitutionen und zum Schutz von digitaler Infrastruktur. Vorfälle wie dieser bieten die Aussicht auf lukrative Staatsaufträge, vor allem im derzeitigen internationalen diplomatischen Klima, in welchem auch digitale Grenzen geschützt werden müssen. Da Irland im Bereich der Cybersicherheit eher Nachholbedarf hat, besteht hier eine große Chance für deutsche Unternehmen. Deutschland verfügt dank starker Spezialisierung seiner Unternehmen in vielen Nischen wettbewerbsfähige und innovative Unternehmen, daher ist es ihnen möglich, im irischen Markt selbstbewusst aufzutreten und mehr Qualität auf den Markt zu bringen. Lediglich

[91] Cyber Ireland. „CYBER SECURITY SKILLS PROVIDERS". Vgl. S. 1-22.
[92] Cyber Ireland (2023). „Cyber Ireland National Conference 2023".
[93] Cyber Ireland. „CYBER SECURITY SKILLS PROVIDERS". Vgl. S. 1-22.
[94] Cyber Ireland (2023). „Cyber Ireland National Conference 2023".

33%, der im Bereich der Cybersicherheit tätigen Unternehmen in Irland, sind im genannten Bereich auch spezialisiert. Die Mehrzahl, also 67%, sind Unternehmen oder gar Konzerne mit einem diversifizierten Portfolio, welche Cybersicherheitsdienstleistungen und -produkte lediglich als Teil ihrer Leistungen anbieten. Dies eröffnet spezialisierten Unternehmen die Chance, in den irischen Markt einzutreten und gezielt Nischen und Branchen maßgeschneidert zu bedienen. 28% aller in der Cybersicherheit in Irland tätigen Unternehmen sind Mikrounternehmen, von denen wiederum 61% in einem oder mehreren Bereichen der Cybersicherheit spezialisiert sind.[95] So ist es eine denkbare Option, durch die Akquise eines kleinen, spezialisierten Unternehmens in den irischen Markt einzutreten.

3.7.1 SWOT-Analyse der irischen Cybersicherheitsbranche

Abbildung 6: SWOT-Analyse der irischen Cybersicherheitsbranche vom Jahr 2022

Strengths (Stärken)	**Weaknesses (Schwächen)**
• Mehr als 7.300 Beschäftigte in der Branche • Umsatz von mehr als 2,1 Mrd. Euro pro Jahr • 1,1 Mrd. Euro Bruttowertschöpfung pro Jahr für die Wirtschaft • Die Produktivität der Arbeitskräfte in Irland ist mit die höchste der EU bei einer Bruttowertschöpfung von 150.000 Euro pro Beschäftigten • Größte Konzentration von Führungskräften im Bereich Cybersicherheit weltweit • Multinationale Unternehmen nutzen Irland gern als Tor zur EU • Irland bietet ein unternehmerfreundliches Ansiedlungsumfeld sowie attraktive Unterstützung der Startup-Landschaft • Einziges englischsprachiges Flächenland der EU • Europäischer Hub für multinationale Cybersicherheitsoperationen[96] • Immer mehr heimische Start-ups und etablierte Unternehmen exportieren ihre Produkte und Dienstleistungen weltweit[97] • Irland hat mit einem Anteil von über 30% an den europäischen Daten eine führende Position im Markt für Datenhosting in Europa[98]	• In manchen Teilbranchen starke Wettbewerbslage von Top-Unternehmen • Fachkräftemangel und stark steigende Löhne • Jedes Jahr fehlen rund 10.000 Personen in Cybersicherheitsberufen • Nachholbedarf, Talente auf der Einstiegsebene weiter zu fördern, um die Qualifikationslücke zu schließen
Opportunities (Chancen)	**Threats (Risiken)**
• Irland als internationaler Zielort für Cyberkriminalität- und Sicherheit • Die Möglichkeit sich innerhalb der globalen Cybersicherheitslieferkette zu positionieren und zu internationalisieren, da multinationale Unternehmen in Irland überwiegen • Geschätzte jährliche Wachstumsrate der Branche von 10% • Die Branche könnte eine jährliche Bruttowertschöpfung von etwa 2,5 Mrd. Euro bis 2030 erreichen • Die Branche hat das Potenzial mehr als 17,000 Stellen bis 2030 zu benötigen • Irlands Handels- und Investitionspolitik trägt weiter dazu bei, multinationale Unternehmen anzuziehen • Der Cyberangriff auf das Gesundheitssystem (HSE) wird dazu führen, dass weitere Maßnahmen ergriffen werden und das Bewusstsein für Cybersicherheitsdienste zu erhöhen • Starke öffentliche Unterstützung für Start-ups	• Bewusstsein für Cyberbedrohungen in der irischen Unternehmenslandschaft ist ausbaufähig • Multinational ausgerichtete Branche mit Einstiegshürden – jedoch großes Potenzial sich weit über den nationalen Markt hinaus stark zu positionieren • Mangelnde Schulungsangebote für nicht-technische Mitarbeiter und hochqualifizierte Cybersicherheitsfachkräften • Der Markt für Cybersicherheit ist stark abhängig von ausländischen Direktinvestitionen (Big-IT, Pharma, Medizintechnik, Finanzwesen)

Quelle: Eigene Darstellung; basierend auf Informationen von Cyber Ireland/Zarah Rios (2022), „State of the Cyber Security Sector in Ireland*"*. Vgl. S.64.[99]

[95] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"* Vgl. S.23 ff.
[96] Cyber Ireland (2024) „Cluster Strategy 2024–2027". Vgl. S.3.
[97] Cyber Ireland (2024) „Cluster Strategy 2024–2027". Vgl. S.3.
[98] Cyber Ireland (2024) „Cluster Strategy 2024–2027". Vgl. S.3.
[99] Cyber Ireland (2022). „State of the Cyber Security Sector in Ireland*"*. Vgl. S. 64.

4 Kontaktadressen

Name	Kurzprofil	Webseite
National Cybersecurity Centre (NCSC)	Das NCSC berät und informiert Anbieter von Regierungsinformatik und kritischen nationalen Infrastrukturen über aktuelle Bedrohungen und Schwachstellen im Zusammenhang mit der Netzinformationssicherheit.	https://www.ncsc.gov.ie/
Irish Computer Society (ICS)	Das ICS ist ein Mitgliedernetzwerk bestehend aus IT-Fachpersonal. Sie bieten eine Reihe von Dienstleistungen und Ressourcen für Fach-personal.	https://www.ics.ie/
Cyber Ireland	Cyber Ireland ist ein irisches Cluster im Bereich der Cybersicherheit. Ihr Ziel ist es, Innovation, Wachstum und Wettbewerbsfähigkeit im Bereich Cybersicherheit in Irland zu verbessern.	https://cyberireland.ie/
Information Systems Security Association (ISSA)	Die ISSA ist eine internationale not-for-profit Organisation von Fachleuten im Bereich der Informationssicherheit. Sie bieten Bildungsforen und Möglichkeiten zum gegenseitigen Austausch, um das Wissen und die Fähigkeiten ihrer Mitglieder zu verbessern.	https://www.issa.org/
Irish Information Security Forum (IISF)	Das IISF ist ein Zusammenschluss von Sicherheitsexperten, IT- und Cybersicherheitsfachleuten aus einer Vielzahl unterschiedlicher Branchen.	https://www.iisf.ie/
Cloud Security Alliance (CSA)	Die CSA ist eine not-for-profit Organisation, welche Verfahren entwickelt und anbietet, die die Cybersicherheit von Cloud-Diensten erhöht.	https://cloudsecurityalliance.org/
Centre for Secure Information Technologies (CSIT)	Das CSIT ist ein britisches Innovations- und Wissenszentrum für Cybersicherheit und befindet sich an der Queens Universität in Belfast.	https://www.qub.ac.uk/ecit/CSIT/
TeleTrusT Bundesverband IT-Sicherheit e.V.	Der Bundesverband IT-Sicherheit e.V. ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft, sowie thematisch verwandte Partnerorganisationen umfasst.	https://www.teletrust.de/startseite/
Allianz für Cyber-Scherheit	Die Allianz für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik hat das Ziel, die Widerstandsfähigkeit des Standortes Deutschland gegenüber Cyberangriffen zu stärken.	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html
Cyber-Sicherheitsrat Deutschland e.V.	Der Cybersicherheitsrat Deutschland hat das Ziel, Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cybersicherheit zu beraten und im Kampf gegen Cyberkriminalität zu stärken.	https://cybersicherheitsrat.de/
eco Verband der Internetwirtschaft	eco fördert die Entwicklung neuer Technologien, Infrastrukturen und Märkte. In ihrem Netzwerk befinden sich wichtige Fachleute aus der Internetwirtschaft.	https://www.eco.de/
IT-Sicherheitscluster e.V.	Der IT-Sicherheitscluster e.V. fördert die Weiterentwicklung und Erforschung von Datenschutz, IT-Sicherheit und Informations-sicherheit.	https://www.it-sicherheitscluster.de/
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)	Das BBK ist eine Bundesbehörde, die für den Bevölkerungsschutz, die Katastrophenhilfe und die zivile Verteidigung in Deutschland verantwortlich ist.	https://www.bbk.bund.de/
Verband für Sicherheitstechnik e.V.	Der VfS ist ein Fachverband, der sich mit Sicherheitstechnik beschäftigt. Er setzt sich für die Förderung von Sicherheitstechnologien ein, die dazu beitragen, zivile Sicherheit zu gewährleisten.	https://www.vfs-hh.de/

5 Literaturverzeichnis

Allianz Commercial (2023). „Allianz Risk Barometer Identifying the major business risks for 2024“. Allianz Commercial. Abgerufen am 23.März 2024 von: https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/economic-research/publications/specials/en/2024/january/Allianz_Risk_Barometer-2024.pdf.

Cyber Ireland. “About Cyber Ireland”. Abgerufen 13. Februar 2024, von Cyber Ireland: https://cyberireland.ie/about-us/.

Cyber Ireland (2024). “Cluster Strategy 2024–2027”. Abgerufen am 17 Februar 2024, von Cyber Ireland: https://cyberireland.ie/wp-content/uploads/2024/01/Cyber-Ireland-Cluster-strategy-2024-2027.pdf.

Cyber Ireland. “course-finder”. Abgerufen am 19. Februar 2024, von Cyber Ireland: https://cyberireland.ie/course-finder/.

Cyber Ireland (17. Oktober 2023). “Cyber Ireland National Conference 2023”. Abgerufen am 14 Februar 2024, von Cyber Ireland: https://cyberireland.ie/cyber-ireland-national-conference-2023-blog/.

Cyber Ireland (12. Oktober 2023). “Cyber Ireland welcomes investment in Cyber Security in Budget 2024”. Abgerufen am 14. Februar 2024 von Cyber Ireland: https://cyberireland.ie/cyber-ireland-cyber-security-in-budget-2024/.

Cyber Ireland. „CYBER SECURITY SKILLS PROVIDERS”. Abgerufen am 20. Februar 2024, von Cyber Ireland: https://cyberireland.ie/wp-content/uploads/2022/11/Talent-and-Skills-Brochure.pdf ; S. 1-22.

Cyber Ireland (September 2023). „State of the Cyber Security Labour Market in Ireland”. Abgerufen am 20. Februar 2024 von Cyber Ireland: https://cyberireland.ie/wp-content/uploads/2023/09/Cyber-Labour-Market-Report-2023.pdf.

Cyber Ireland (29. April 2022). „State of the Cyber Security Sector in Ireland”. Abgerufen am 21. Februar 2024, von Cyber Ireland: https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Report.pdf.

Data Protection Commission. “The Data Protection Commission”. Abgerufen am 22. Februar 2024, von Data Protection Commission: https://www.dataprotection.ie/.

Department of Public Expenditure NDP Delivery and Reform/Office of Government Procurement (25. Oktober 2023). “Public Procurement Guidelines for Goods and Services”. Abgerufen am 25. Februar 2024, von Office of Government Procurement: https://assets.gov.ie/274554/f2343b55-9615-4708-b7d8-717fff330f1d.pdf.

Department of the Environment, Climate and Communications (12. September 2019). “About the Department of the Environment, Climate and Communications”. Abgerufen am 03. April 2024, von Gov.ie: https://www.gov.ie/en/organisation-information/about-the-department-of-the-environment-climate-and-communications/.

Department of the Environment, Climate and Communications (Juni 2023). “Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)”. Abgerufen am 20. Februar 2024, von Department of the Environment, Climate and Communications: https://www.ncsc.gov.ie/pdfs/Guidelines_on_Cyber_Security_Specifications.pdf.

Department of the Environment, Climate and Communications (25. Mai 2023). „Minister Smyth welcomes establishment of €4.2 million National Cybersecurity Coordination and Development Centre (NCC-IE) project“. Department of the Environment, Climate and Communications. Abgerufen am 25. Februar 2024, von Department of the Environment, Climate and Communication: https://www.gov.ie/en/press-release/69ad2-minister-smyth-welcomes-the-establishment-of-new-42m-national-cybersecurity-coordination-and-development-centre-ncc-ie-project/.

Department of the Environment Climate and Communications (2023). „National Cyber Security Strategy 2019-2024 Mid-Term Review”. Abgerufen am 16. Februar 2024, von Government of Ireland: file:///C:/Users/GIC11/Downloads/261971_356d743c-b154-4a5f-b7ae-eb6714c2d011.pdf.

Department of the Environment, Climate and Communication (01. Juni 2023). “Cyber Security”. Abgerufen am 12. Februar 2024, von Gov.ie: https://www.gov.ie/en/policy-information/5e101b-network-and-information-security-cyber-security/#:~:text=National%20Cyber%20Security%20Centre,-The%20National%20Cyber&text=The%20role%20of%20the%20NCSC,related%20risks%20to%20key%20services.

Doyle, C. (8. November 2023). TechCentral.ie, “Two Thirds of Irish Businesses to Increase Investment in Cyber Security”. Abgerufen am 07. Februar 2024, von TechCentral.ie: https://www.techcentral.ie/two-thirds-of-irish-businesses-to-increase-investment-in-cyber-security/.

Finlay, A., Hughes, R., (14. November 2023). International Comparative Legal Guides International Business Reports. “Cybersecurity Laws and Regulations Ireland 2024.” Abgerufen am 07. Februar 2024, von International Comparative Legal Guides International Business Reports: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/ireland.

Germany Trade & Invest. (2023) „Wirtschaftsdaten kompakt- Irland“. Abgerufen am 21. Februar 2024 von GTAI: https://www.gtai.de/resource/blob/14996/074cdfcca828f38ace6af1eaf395222d/Wirtschaftsdaten_Dezember_2023_Irland.pdf

Germany Trade & Invest (11. Dezember 2023). Germany Trade & Invest „Wirtschaftsdaten kompakt- Deutschland“. Abgerufen am 12. Februar 2024, von GTAI: https://www.gtai.de/resource/blob/9074/a1f3d29eecc53e2305216fe1201ed431/Wirtschaftsdaten_Dezember_2023_Deutschland.pdf.

Government of Ireland (Dezember 2019). “National Cyber Security Strategy”. Abgerufen am 15. Februar 2024, von Government of Ireland: https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf.

Harris, M. (09. März 2023). Grant Thornton Ireland. “Cyber-Security Remains a Priority for Irish Businesses, with Almost Half Likely to Increase Investment in Risk Mitigation,”. Abgerufen am 03. Februar 2024, von Grant Thornton Ireland: https://www.grantthornton.ie/news-centre/cyber-security-remains-a-priority-for-irish-businesses-with-almost-half-likely-to-increase-investment-in-risk-mitigation/.

Hiscox Ltd. (2023). „Hiscox Cyber Readiness Report 2023“. Abgerufen am 28. Februar 2024, von Hiscox Ltd.: https://www.hiscox.ie/sites/ireland-new/files/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf.

International Trade Administration U.S. Department of Commerce (25. Januar 2024). „Ireland – Cybersecurity”. Abgerufen am 27. Februar, von International Trade Administration U.S. Department of Commerce: https://www.trade.gov/country-commercial-guides/ireland-cybersecurity.

Irish Information Security Forum (22. Januar 2024). “Cybersecurity Attack on AerCap”. Abgerufen am 13. Februar 2024, von Irish Information Security Forum: https://www.iisf.ie/Cybersecurity-Attack-AerCap.

Jones, Horgan J., Wall, M. (7. November 2022). The Irish Times. “HSE Cyberattack: More than 100,000 People Whose Personal Data Stolen to Be Contacted“. Abgerufen am 28. Februar 2024 von The Irish Times. https://www.irishtimes.com/health/2022/11/07/over-100000-people-whose-personal-data-stolen-in-hse-cyberattack-to-be-contacted/.

Lehnfeld, M., (15. Dezember 2022). Germany Trade & Invest. „Irland Irisches Geschäftsmodell zeigt sich krisenfest“. Abgerufen am 25. Februar 2024, von GTAI: https://www.gtai.de/de/trade/irland/wirtschaftsumfeld/irisches-geschaeftsmodell-zeigt-sich-krisenfest-590314.

McCorry, K., (2023). Microsoft Ireland. „Cybersecurity Trends in Ireland 2023“. Abgerufen am, von Microsoft Ireland: https://pulse.microsoft.com/wp-content/uploads/2023/12/Cybersecurity-Trends-Ireland-2023.pdf.

Ó Liatháin, C., (03. Februar 2024). EchoLIVE.ie. “New Cork initiative set to train next generation of cyber security experts”. Abgerufen am 11. Februar 2024, von EchoLIVE.ie: https://www.echolive.ie/corknews/arid-41338184.html.

O'Regan, E., (26. Mai 2023). Irish Examiner. „€4.2m project aims to provide cybersecurity funds for small firms”. Abgerufen 26. Februar, von Irish Examiner: https://www.irishexaminer.com/business/companies/arid-41148547.html.

U.S. Department of Health & Human Services, Office of Information Security (02. März 2022). “Lessons Learned from the HSE Cyber Attack.”. Abgerufen am 22. Februar 2024, von HHS Cybersecurity Program https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf.