Bundesverband Deutsche Startups e.V.

RAGSTIFTUNG

2020

Cyber security an der RUHR

Startups als Treiber digitaler Sicherheit

Herausgeber
Bundesverband Deutsche Startups e.V.

Partner und Förderer
RAG-Stiftung

Autoren
Dr. Alexander Hirschfeld
Jannis Gilde
Vanusch Walk

Design
Dina Wagasowa

ISBN
978-3-948895-05-1

RAGSTIFTUNG

Bundesverband Deutsche Startups e.V.

— 2020

Cyber security an der Startup-Front

Startups als Treiber digitaler Sicherheit

V O R W O R T

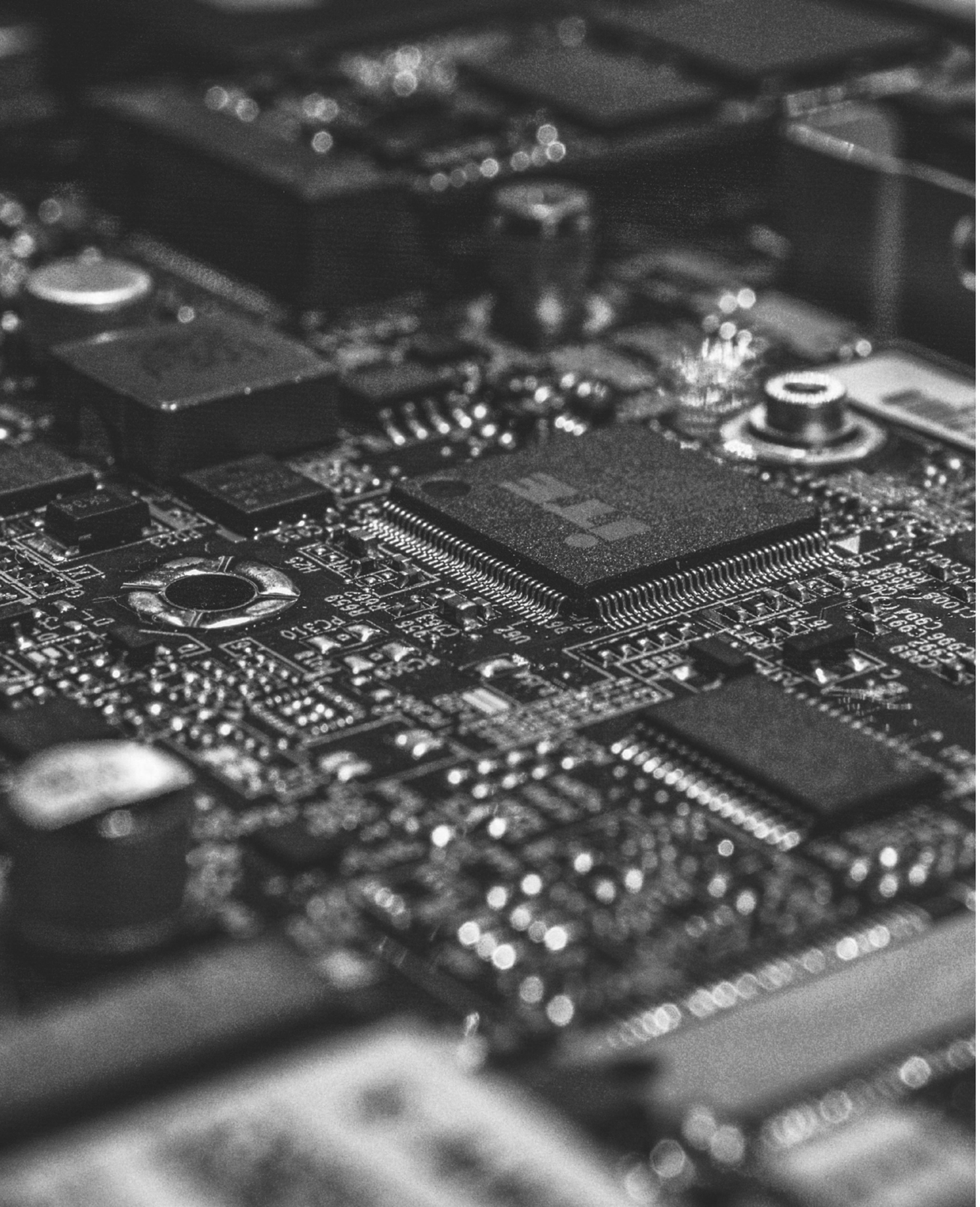
Dr. Jörg Goschin
Geschäftsführer KfW Capital

Die Welt der globalen Vernetzung ist ein milliardenschwerer Wachstumsmarkt, dessen Chancen weitreichend sind. Von neuen Produkten und Dienstleistungen sowie Effizienzgewinnen werden private und öffentliche Haushalte profitieren. Der Aufbau einer wirkungsvollen Cybersecurity wird dabei zur unabdingbaren Voraussetzung, um die deutlich zunehmenden Risiken der virtuellen Welt – von Datendiebstahl über Serviceunterbrechungen bis zum Kontrollverlust über ganze Prozesse – zu minimieren und beherrschbar zu machen.

Diese Studie dokumentiert auf eindrucksvolle Weise, dass bereits wertvolles Cybersecurity-Know-How an Forschungseinrichtungen und bei innovativen Unternehmen in Deutschland vorhanden ist. Sie belegt aber auch, dass innovative Technologieunternehmen schwierigere Finanzierungsbedingungen vorfinden als in anderen Ländern. Der deutsche VC-Markt hat sich zwar insgesamt positiv entwickelt; seit 2014 sind die jährlichen VC-Investitionen von 0,7 Milliarden Euro auf 1,9 Milliarden Euro gestiegen. In Relation zur nationalen Wirtschaftskraft zeigt sich jedoch ein differenziertes Bild: Um zu Großbritannien aufzuschließen, müssten deutsche Startups jährlich Zugang zu etwa doppelt so viel Venture Capital erhalten, um das US-Level zu erreichen, sogar das Zehnfache.

KfW Capital investiert in deutsche und europäische VC-Fonds mit Deutschlandbezug. Unser Ziel ist es, die Fondslandschaft so zu stärken, dass innovative Technologieunternehmen besseren Zugang zu Kapital auf ihrem Wachstumsweg erhalten. Über zehn Jahre investiert KfW Capital rund 2 Milliarden Euro. Darüber hinaus werden in 2020 durch das vom Bund beschlossene Corona-Start-up-Hilfsprogramm über die KfW, KfW Capital, den Europäischen Investitionsfonds und die Landesförderinstitute weitere 2 Milliarden Euro für innovative Technologieunternehmen bereitgestellt. Zum ersten Mal während einer Krise gibt es damit für diese Zielgruppe ein eigenes Hilfspaket. Die Regierungskoalition hat außerdem im Sommer 2020 den Zukunftsfonds und damit zusätzliche 10 Milliarden Euro zur Stärkung innovativer Technologieunternehmen beschlossen.

Auch wenn Deutschland bei der Finanzierung von wichtigen Schlüsseltechnologien Nachholpotenzial hat, sehe ich für den Bereich Cybersecurity positiv in die Zukunft: Schon heute ist die Technologiekompetenz auf einem sehr hohen Niveau, sodass entscheidende Beiträge für Innovation, Sicherheit und damit die Zukunftsfähigkeit Deutschlands und Europas zu erwarten sind. Dieser Report wird weitere wichtige Impulse hierfür sowie für den weiteren Ausbau des Cybersecurity-Clusters im Ruhrgebiet und darüber hinaus geben.



INHALTSVERZEICHNIS

KERN ERGEBNISSE

1 **Zukunftsmarkt und zentrale Infrastruktur:** Mit 5 Milliarden Euro an aktuellen Ausgaben und einem jährlichen Wachstum von 10 Prozent ist Cybersecurity einer der wichtigsten Wachstumsmärkte in Deutschland und stellt ein Kernelement unserer digitalen Infrastruktur dar.

2 **Deutschland mit Nachholbedarf bei Cyberinvestments:** Während in Israel pro Kopf 108 Euro in Startups im Bereich Cybersecurity investiert werden, liegt dieser Wert in Deutschland bei nur 83 Cent. Eine zentrale Rolle bei der Stärkung dieses Sektors spielt dabei die Unterstützung bestehender Cluster.

3 **Ruhrgebiet als Cybersecurity-Cluster:** Neben Berlin und München ist das Ruhrgebiet die dritte Kraft im Feld der Cybersicherheits-Startups – mit einem Anteil von 7,2 Prozent der deutschen Cybersecurity-Startups zeigt sich hier eine überdurchschnittlich hohe Gründungsaktivität.

4 **Ausgeprägter Forschungstransfer:** Das Cybersecurity-Cluster im Ruhrgebiet zeichnet sich vor allem durch seine Stärke an der Schnittstelle zwischen Wissenschaft und Startup-Gründung aus, in der sich ein spezialisiertes Ökosystem entwickelt hat.

5 **Synergien nutzen:** Der internationale Vergleich macht deutlich, dass Cybersecurity-Cluster vor allem von der engen Kooperation zwischen Forschung, Politik und Wirtschaft profitieren. Diese Voraussetzung ist im Ruhrgebiet deutlich gegeben. Mit Blick auf die Marktorientierung und hinsichtlich der Anbindung an staatliche Sicherheitseinrichtungen gibt es noch Entwicklungspotenziale.

KEY FINDINGS

1 **Future market and key infrastructure:** This year five billion euros were spent on the cybersecurity industry in Germany; this is an annual growth rate of 10 percent, making it one of our most important growth markets and a cornerstone of our digital infrastructure.

2 **Huge investment backlog:** Germany invests only 83 cents per capita in cybersecurity startups, a tiny amount compared with Israel where the figure stands at 108 euros. If the sector is to be strengthened, it is vitally important to support existing hubs.

3 **The Ruhr area as a cybersecurity hub:** The Ruhr area ranks third after Berlin and Munich in the field of cybersecurity startups. With a share of 7.2 percent of German startups, this sector is exceptionally lively here.

4 **Outstanding research transfer:** One outstanding feature of the cybersecurity hub in the Ruhr area can be seen in the strong ties between research and entrepreneurship where a specialized ecosystem has developed.

5 **Exploiting synergies:** Cybersecurity hubs benefit particularly from close cooperation between research, politics and business. A good foundation has already been established in the Ruhr area but there is still potential for development when it comes to market focus and collaboration with national security agencies.

1. HINTERGRUND

1.1. Ausgangspunkt und Zielsetzung

Spätestens seit Ausbruch der Corona-Pandemie ist das Thema Cybersicherheit bzw. Cybersecurity von der Peripherie ins Zentrum der wirtschaftlichen, öffentlichen und politischen Aufmerksamkeit gerückt. Im Kontext der Krise ist der massive Rückstand bei digitalen Lösungen und der Digitalausstattung in der Arbeitswelt sowie im Bildungs- und Gesundheitswesen deutlich geworden. Dabei wurde nicht nur das Fehlen dringend benötigter Hardware und Software sichtbar, sondern vor allem auch der Bedarf an einer sicheren digitalen Infrastruktur.

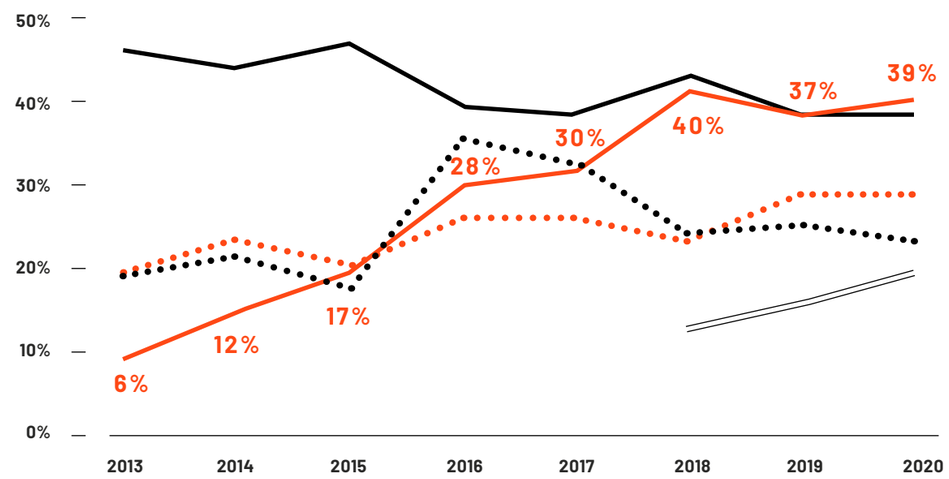
Cybersecurity ist elementar zur Wahrung von Geschäftsgeheimnissen, zur Sicherung sensibler Daten und damit für das Vertrauen der Kundinnen und Kunden in neue Technologien – etwa in den Bereichen E-Commerce, Internet of Things oder Cloud-Computing. Gleiches gilt für den Staat und das öffentliche Leben: So ist die Digitalisierung des staatlichen Bildungssystems oder der Gesundheitsversorgung ohne entsprechende Sicherheitstechnologien völlig undenkbar. Cybersicherheit ist damit die Basis unserer gegenwärtigen und zukünftigen gesellschaftlichen Entwicklung und gewinnt als Wirtschaftsfaktor zunehmend an Bedeutung.

Vor diesem Hintergrund hat das Ruhrgebiet als profilierter Standort im Bereich Cybersecurity gerade in der aktuellen Phase die Chance, die hier vorhandenen Potenziale auszuschöpfen und damit die Innovationskraft und wirtschaftliche Leistungsfähigkeit der Region insgesamt voranzubringen. Ziel dieser Studie ist es, die Stärken und Herausforderungen des Cybersecurity-Clusters im Ruhrgebiet herauszuarbeiten und zu generellen Trends in diesem Zukunftsmarkt in Beziehung zu setzen – dabei wird das Ruhrgebiet sowohl auf nationaler als auch auf internationaler Ebene verortet.

„Um für Startups und etablierte Unternehmen gute Voraussetzungen für Innovationen im Gesundheitssektor zu schaffen, brauchen wir eine sichere digitale Infrastruktur. Denn nur so können wir das Vertrauen der Menschen in digitale Lösungen gewinnen und weiter stärken. In diesem Kontext ist das Thema Cybersecurity elementar."

– Lina Behrens, Managing Director Flying Health und Vorstandsmitglied des Startup-Verbands

/ Abbildung 1: Unternehmerische Risiken im Zeitverlauf (Auswahl) 2013–2020 (Allianz 2020)



1.2. Aufstieg des Cybersecurity-Sektors

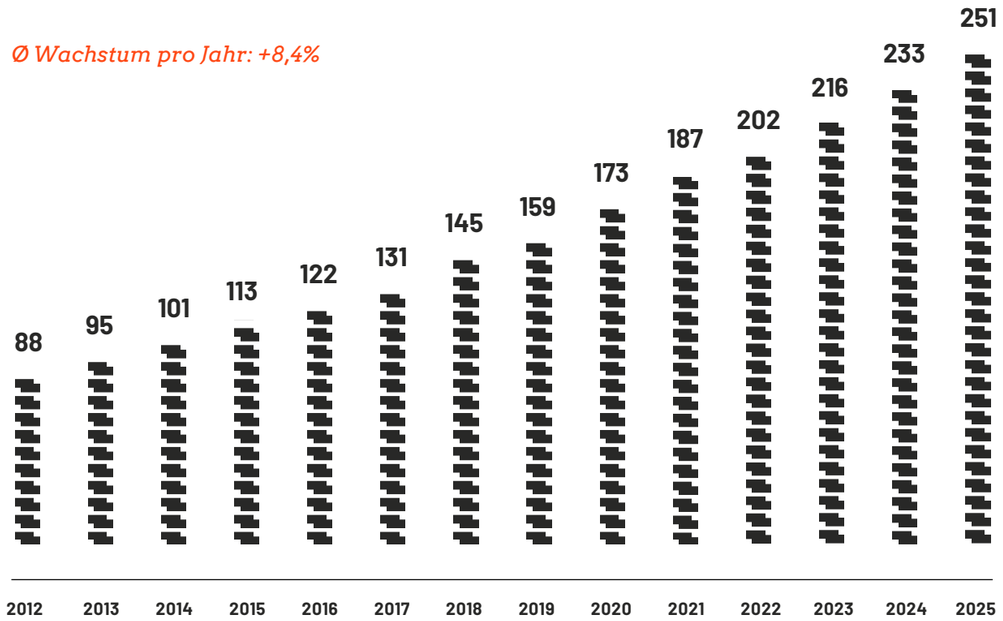
Digitale Sicherheitstechnologien werden für Unternehmen seit Jahren immer wichtiger: So haben sich Cyber-Vorfälle, beispielsweise durch Cyberkriminalität, den Ausfall der IT oder einen Datenverlust, laut Allianz Risk Barometer in den letzten Jahren von einem untergeordneten Faktor zum größten Wirtschaftsrisiko für Unternehmen entwickelt (Abbildung 1). Weltweit sind also Politik, Wirtschaft und Gesellschaft in einem nie da gewesenen Maße von Cyberangriffen bedroht, deren Auswirkungen von sozialen Problemen über enorme finanzielle Schäden bis hin zur Existenzbedrohung reichen.

Vor dem Hintergrund dieser neuen Herausforderungen sind die Ausgaben für Cybersicherheit stark angestiegen. Allein in Deutschland werden für das Jahr 2020 Aufwendungen in Höhe von mehr als 5 Milliarden Euro prognostiziert, mit einem jährlichen Anstieg von über 10 Prozent (Bitkom 2020). Das globale Marktvolumen des Sektors wird für 2020 auf über 170 Milliarden US-Dollar geschätzt – mit ähnlichen Wachstumsprognosen

(Abbildung 2). Das Potenzial liegt noch deutlich höher, worauf die steigenden Kosten von Cyberangriffen verweisen: Im globalen Maßstab werden mögliche Wertverluste im Zeitraum von 2018 bis 2023 auf insgesamt 5,2 Billionen US-Dollar geschätzt, was fast 6 Prozent der jährlichen Weltwirtschaftsleistung entspricht (Accenture 2019).

Neben den direkten wirtschaftlichen Schäden ist Cybersicherheit heute zentraler Bestandteil unserer zunehmend digitalen Infrastruktur: Vermehrte Angriffe auf Krankenhäuser und die damit verbundenen Gefahren für Patientinnen und Patienten, die zunehmende Bedeutung des mobilen Arbeitens und damit gewachsene Herausforderungen der Datensicherheit sowie die Auswirkungen manipulativer Eingriffe Dritter, zum Beispiel auf demokratische Prozesse und Institutionen, illustrieren hier die Bandbreite der Risiken (Deloitte 2019). Damit ist Cybersicherheit ein gesamtgesellschaftliches Thema, das durch die Corona-Pandemie und den damit einhergehenden Digitalisierungsschub noch einmal an Relevanz gewinnt. Deutschland und Europa stehen vor der Herausforderung, die Kontrolle über diese Infrastruktur und damit die digitale Souveränität mit dem dafür relevanten Know-how langfristig zu sichern.

/ **Abbildung 2: Geschätzte Ausgaben für Cybersecurity weltweit, in Mrd. US-Dollar (AustCyber 2019)**



„Startups sollen einfache und verständliche Lösungen entwickeln, die auch unbedarfte Nutzer besser verstehen. Cyber ist zu komplex und oftmals eine UX/UI-Hölle. Es gibt zwar viele Lösungen, aber die werden nicht gekauft, weil das Management der Firmen sparsam ist und fälschlich glaubt, dass einzig ihre Firma allein nicht zum Opfer von Cyberattacken wird."

– Sven Weizenegger, Leiter Cyber Innovation Hub der Bundeswehr

1.3. Startups als Innovationstreiber und Wirtschaftsfaktor

Startups sind für die wirtschaftliche Erneuerung und digitale Transformation elementar. Aktuell sind 7 der 10 wertvollsten Firmen weltweit Digitalunternehmen, von denen bis auf Apple und Microsoft keines älter als 30 Jahre ist (Murphy et al. 2020). Aufgrund der dargestellten Dynamik der Cybersecurity-Branche hängt der Erfolg in diesem Bereich daher nicht zuletzt von der Existenz eines aktiven und leistungsstarken Startup-Ökosystems ab, das in diesem Sektor neue Unternehmen hervorbringt und für existierende Startups die nötigen Wachstumsimpulse schafft.

Während in der deutschen Startup-Szene häufig vor allem Berlin und München durch bekannte Erfolgsgeschichten und eine hohe Gründungsaktivität im Fokus stehen, hat sich im Ruhrgebiet

ein spezialisiertes Cybersecurity-Ökosystem etabliert. Dieses Cluster zeichnet sich vor allem durch die gezielte Verbindung exzellenter Forschung mit einer fokussierten Gründungsförderung aus. Hier können bestehende Stärken ausgebaut und damit das Startup-Ökosystem in der Region insgesamt entscheidend vorangebracht werden.

Der Fokus des Reports liegt daher neben der generellen Entwicklung des Cybersecurity-Sektors im Ruhrgebiet auf der Analyse des Startup-Ökosystems. Dabei wird auf die definitorischen Kriterien des Deutschen Startup Monitors zurückgegriffen (Kollmann et al. 2020): Startups sind jünger als 10 Jahre, mit ihrer Technologie und/oder ihrem Geschäftsmodell innovativ und haben beziehungsweise planen ein signifikantes Mitarbeiter- und/oder Umsatzwachstum. Sie sind damit eine besondere Form des wesentlich breiteren Feldes der Existenzgründung, unter der üblicherweise jede Form der beruflichen Selbstständigkeit verstanden wird (Metzger 2020).

2. BACKGROUND SUMMARY

The Coronavirus pandemic has put the spotlight on cybersecurity in public discourse as well as in business and politics. Cybersecurity plays a key role in the protection of individual privacy and thus in building customer trust in innovative fields such as E-commerce, the Internet of Things or Cloud Computing. Furthermore, companies now rate the risks associated with cyber incidents as the number one threat worldwide, greater even than business interruptions caused by supply chain issues or market turbulences, for example.

This has led to a sharp increase in the cybersecurity market with roughly five billion euros spent in Germany this year and an annual growth rate of 10 percent. Current global revenue of around 173 billion US dollars as well as the tremendous costs related to cybercrime point to the vast opportunities and needs within this field. Startups and cybersecurity hubs such as the Ruhr area play a crucial role in leveraging these potentials.

Cybersecurity

2. CLUSTER AN DER RUHR

2.1. Cybersecurity-Startups in Deutschland

Innovative Wachstumsunternehmen entstehen häufig in bereits etablierten und aktiven Ökosystemen: Erstens können hier erfolgreiche Startup-Unternehmerinnen und -Unternehmer mit Erfahrungen, Expertise und Netzwerken unterstützen und damit die Bedingungen für neue Gründungen verbessern. Zweitens haben solche Hotspots eine hohe Attraktivität für Talente und Kapitalgeber, wodurch sich eine hohe Konzentration an relevanten Ressourcen und Humankapital ergibt (Mason & Brown 2014). Das Silicon Valley und Standorte wie London, Tel Aviv oder Shanghai sind prominente internationale Beispiele dieser Effekte – in Deutschland gilt Ähnliches für Berlin und München.

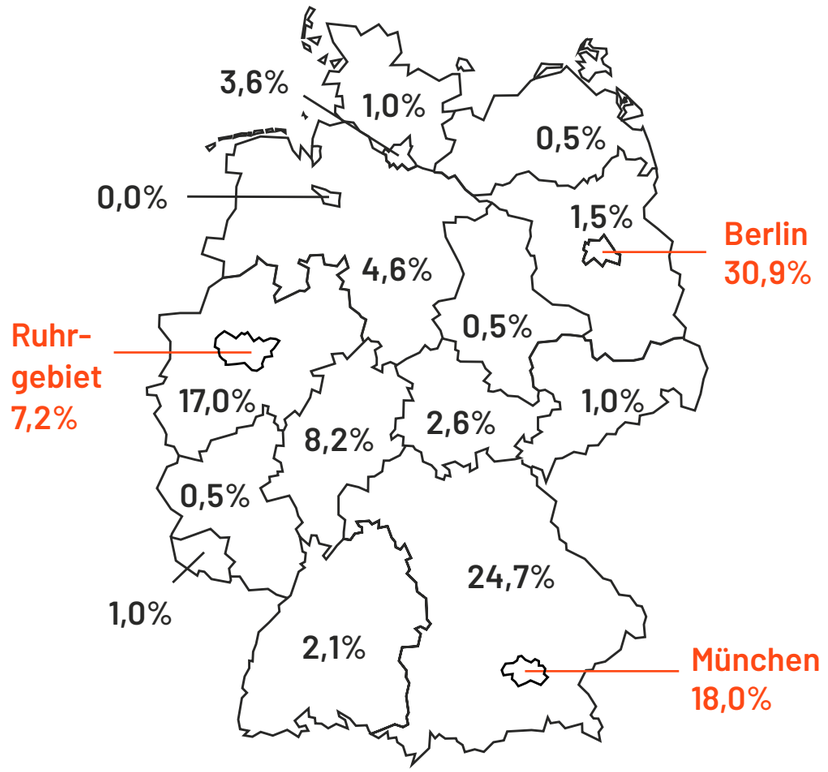
Hotspots bieten die Möglichkeit, generelle Synergien zu nutzen, andere Standorte haben dagegen das Potenzial, sich zu spezialisieren – gerade im Bereich forschungs- und technologieintensiver Gründungen (Hirschfeld & Gilde 2020). Zur Identifikation derartiger Konzentrationen im Feld Cybersicherheit wurden die knapp 200 auf der Plattform Dealroom gelisteten Cybersecurity-Startups auf ihren Unternehmenssitz hin analysiert (Abbildung 4). Dabei zeigt sich, dass Berlin und München fast die Hälfte der Startups auf sich vereinen. In Schlagdistanz zu den beiden Hotspots bildet das Ruhrgebiet hinsichtlich des Anteils an Cybersecurity-Startups in Deutschland die dritte Kraft.

Die dargestellte Verteilung zeigt einerseits, dass die generelle Attraktivität der Hotspots auch im Bereich Cybersecurity ihre Wirkung entfaltet. Gleichzeitig ist der Effekt der Spezialisierung deutlich erkennbar: In vielen Regionen finden sich kaum Startups in diesem Feld – dagegen sticht das Ruhrgebiet als Cybersecurity-Cluster klar hervor. Noch deutlicher wird diese Konzentration im Vergleich zur generellen Startup-Aktivität in der Region: Laut Dealroom und den Daten des Deutschen Startup Monitors liegt der Anteil deutscher Startups aus dem Ruhrgebiet zwischen knapp 2 und 4 Prozent – im Cybersecurity-Sektor ist dieser Wert dagegen mit über 7 Prozent um ein Vielfaches höher.

„Das Cybersecurity-Ökosystem im Ruhrgebiet ist Weltklasse und hat sich als führender Standort im Feld etabliert. Wir verfügen hier über ein in Europa einzigartiges Netzwerk von Universitäten und Forschungseinrichtungen auf dem Gebiet der Cybersecurity. Auch eCAPITAL ist mit ihrem in Deutschland einzigartigen Fonds, der nur auf Cyber-Unternehmen ausgelegt ist, ein wichtiger Bestandteil dieses Ökosystems. Und an starken Ausgründungen für Investitionen mangelt es im Ruhrgebiet nicht – u.a. Zynamics, Escrypt, Syrrix, isits, Cure53, Kasper & Oswald, HackmanIT, VMRay, Cyber Defence, Physec, forthmind, emproof, Cardcoin, Bitbuckler, xignsys, aware7 und RIPS Technologies."

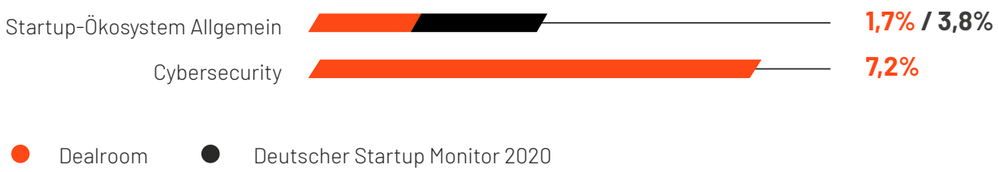
– Willi Mannheims, Managing Partner bei eCAPITAL

/ **Abbildung 3: Verteilung der Cybersecurity-Startups in Deutschland (Dealroom)** [1]



[1] Es konnten bei Dealroom 194 Startups (max. 10 Jahre alt inkl. Ortsangabe) im Bereich „Security" identifiziert werden.

Abbildung 4: Anteil Startups aus dem Ruhrgebiet im Startup-Ökosystem allgemein und im Bereich Cybersecurity (Dealroom & DSM 2020)

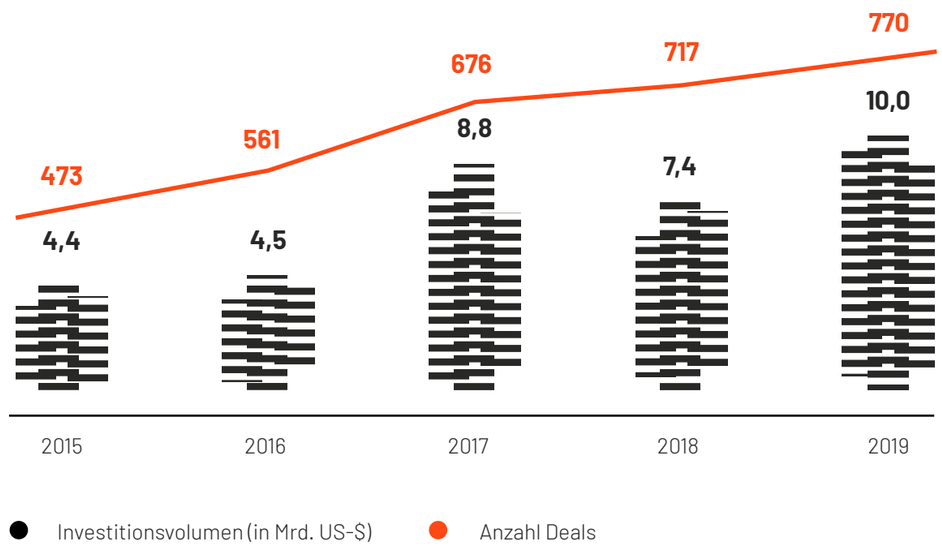


2.2. Entwicklungen und aktuelle Chancen im Ruhrgebiet

Mit der Gründung der heutigen G DATA CyberDefense im Jahr 1985 in Bochum und der Entwicklung des wohl ersten kommerziellen Antivirusprogramms hat das Ruhrgebiet bereits vor mehr als 30 Jahren echte Pionierarbeit im Bereich Cybersecurity geleistet. Seitdem hat sich die Region zu einem wichtigen Standort auf diesem Gebiet entwickelt: 2002 wurde an der Ruhr-Universität Bochum das Horst-Görtz-Institut für Sicherheit in der Informationstechnik (HGI) gegründet, das heute mit ca. 1.000 Studierenden zu den größten Ausbildungsstätten für IT-Sicherheit in Europa gehört. Dabei profitiert die Region nicht nur von der Forschungsstärke, sondern auch von einer langen Historie der engen Verbindung von Theorie und Praxis.

Seit der Gründung des HGI sind mehr als 20 Startups im Umfeld

Abbildung 5: Investitionen in Cybersecurity-Startups weltweit (CBInsights 2020)



des Instituts entstanden. Oft wird dabei von zwei Gründungswellen gesprochen: Zur ersten Generation erfolgreicher Cybersecurity-Startups gehören Unternehmen wie ESCRYPT, Sirrix und Zynamics. Ihr Erfolg wird auch daran sichtbar, dass diese Startups von der Bosch-Gruppe, Rohde & Schwarz und Google übernommen wurden. Solche Exits haben langfristig eine enorm wichtige Funktion in Startup-Ökosystemen: Denn erfolgreiche Gründerinnen und Gründer bringen neben dem erwirtschafteten Kapital auch ihr Know-how wieder in den Finanzierungs- und Innovationskreislauf ein. Diese frühen Erfolgsgeschichten bilden die Grundlage für die zweite und damit aktuelle Gründungswelle an der Schnittstelle von Forschung und unternehmerischer Praxis im Cybersicherheitssektor, was sich im hohen Anteil an Cybersecurity-Startups im Ruhrgebiet niederschlägt.

Die wachsende ökonomische Bedeutung des Cybersecurity-Sektors ist also auch im Ruhrgebiet klar erkennbar. So hat sich etwa der Aktienwert des Essener IT-Sicherheits-Unternehmens Secunet in den vergangenen zehn Jahren fast verdreißigfacht. Auch die Bedingungen für junge Unternehmen sind sehr gut: Weltweit wurden 2019 knapp 10 Milliarden US-Dollar in Cybersecurity-Startups investiert, wobei sich der Wert seit 2015 mehr als verdoppelt hat. Von diesem Trend konnten auch Unternehmen im Ruhrgebiet, wie beispielsweise das Startup VMRay profitieren. Gleichzeitig sind größere Finanzierungsrunden für deutsche Cybersecurity-Startups bisher noch eine Seltenheit: Während es bisher kein deutsches Cybersecurity-Unicorn – also ein Startup mit einem Unternehmenswert von mindestens einer Milliarde Euro – gibt, steht das britische Unicorn DarkTrace kurz vor seinem Börsengang. Perspektivisch kommt dem Cluster im Ruhrgebiet für den Wirtschaftsstandort Deutschland damit eine besondere Bedeutung im internationalen Wettbewerb zu.

„Cybersecurity ist das Querschnittsthema, welches alle Bereiche der Digitalisierung erfasst. Diese Vielfältigkeit der Anwendungen spiegelt das Ruhrgebiet wider und ermöglicht einen erfolgreichen Transfer von der Forschung in die Praxis."

– Dr. Heiko Koepke, Co-Founder und Geschäftsführer PHYSEC GmbH

2.3. Entstehung des Cybersecurity-Ökosystems

In den vergangenen Jahren hat sich das Cybersecurity-Cluster im Ruhrgebiet zu einem umfassenden Startup-Ökosystem entwickelt. Hervorzuheben ist der Aufbau des Inkubators Cube 5 am HGI, mit dem die Gründungspotenziale an der Schnittstelle zwischen Forschung und Praxis im Bereich Cybersecurity gezielt adressiert werden. Ein wichtiger Baustein, um Studierenden das Gründen näherzubringen, sind dabei Vorbilder – erfolgreiche Startups wie beispielsweise die Gewinner des Gründerpreises NRW Physec zeigen Interessierten, welche Möglichkeiten sie haben, ihre eigenen Ideen in der Wirtschaft zu realisieren.
Die fachspezifische Exzellenz universitärer sowie außeruniversitärer Forschungseinrichtungen sind das Erfolgsrezept des Cybersecurity-Clusters im Ruhrgebiet. Mit dem 2019 in Bochum gegründeten Max-Planck-Institut für Cybersicherheit und Schutz der Privatsphäre wird die Forschungsstärke der Region weiter ausgebaut. Die dichte Hochschullandschaft, bei der auch das 2005 am Standort

Gelsenkirchen der Westfälischen Hochschule geschaffene Institut für Internet-Sicherheit eine wichtige Rolle spielt, bringt nicht nur Innovationen hervor, sondern auch viele Fachkräfte. Die damit einhergehende Verfügbarkeit von qualifiziertem Personal vor Ort – gerade im Bereich Informatik – ist ein wichtiger Wettbewerbsvorteil der Region.
Mit dem bereits genannten Inkubator Cube 5 existiert im Ruhrgebiet ein einzigartiges Unterstützungsprogramm an der Schnittstelle zwischen Wissenschaft und Gründung. Hervorzuheben ist dabei, dass sowohl für gründungsinteressierte Studierende als auch für frühphasige Startups branchenspezifische Angebote gemacht werden. Dazu gehört auch die Beratung zum Förderprogramm StartUpSecure des Bundesministeriums für Bildung und Forschung – als einer von vier Standorten in Deutschland – sowie das Accelerator-Programm Liftoff. Im Finanzierungsbereich ist der Wagniskapitalgeber eCapital aus Münster mit einem dezidierten Fonds für den Bereich Cybersecurity im Ruhrgebiet präsent. Insgesamt ist in der Region also ein umfassendes Ökosystem mit einer besonderen Stärke im Forschungstransfer entstanden.

/ Abbildung 6: Cybersecurity-Ökosystem im Ruhrgebiet

„Der zentrale Vorteil des Cybersecurity-Ökosystems in Bochum besteht darin, dass wir es seit 2001 kontinuierlich weiterentwickelt haben. Mit mehr als 1000 Studierenden verfügen wir heute über Europas führendes akademisches Ausbildungsprogramm im Feld und sind weltweit in Sachen Forschungsoutput unter den Top-3. Daneben können wir auf 15 Jahre Erfahrung beim Aufbau von Cybersecurity-Startups zurückblicken, die sich heute in unserem Inkubator Cube 5 bündelt. All das macht uns zu einem der attraktivsten Standorte im Cybersecurity-Bereich."

– Christof Paar, Leiter Max Planck Institut für Cybersicherheit und Schutz der Privatsphäre an der Ruhr-Universität Bochum

Cyber Security

2. CLUSTER RUHR AREA SUMMARY

Startup ecosystems evolve around talent and capital and this tends to concentrate in certain locations. In Germany, startups are currently thriving most in Berlin and Munich, while specialized hubs are also evolving in other regions. With 7.2 percent of Germany's cybersecurity startups, the Ruhr area is an important hub in this sector with a particular strength in research transfer.

The Ruhr hub has its origins back in 1985 when the Bochum-based antivirus software developer G Data CyberDefense was founded, marking a pioneering move in the cybersecurity market. Since then the cybersecurity sector has been continuously developed around the Ruhr-University Bochum, most notably with the creation of the Horst Görtz Institute for IT Security in 2002. Today the institute offers specialized degree programs to more than a thousand students and runs the cybersecurity incubator Cube 5. Important players alongside these initiatives are the Institute for Internet Security in Gelsenkirchen or the Essen-based cybersecurity company Secunet.

Das Ruhrgebiet

3. IM INTERNATIONALEN WETTBEWERB

3.1. Internationale Cybersecurity-Hotspots

Das Cybersecurity-Cluster im Ruhrgebiet stärkt die Wirtschaftskraft der Region, schafft zukunftssichere Arbeitsplätze und ist wichtiger Bestandteil einer positiven Entwicklung des Innovationsstandorts Deutschland. Dies belegen nicht zuletzt auch die bereits etablierten Cybersecurity-Unternehmen des Ruhrgebiets: G DATA beschäftigt heute 500, Secunet sogar fast 600 Mitarbeitende. Im internationalen Vergleich der Investitionen in diese Zukunftstechnologie ist jedoch ein deutlicher Nachholbedarf sichtbar. Israel ist bei der Allokation von Wagniskapital weltweiter Spitzenreiter, was neben der Stärke des dortigen Startup-Ökosystems auch mit der besonderen Historie und geopolitischen Situation des Landes zusammenhängt. Doch auch in Großbritannien, mit dessen Startup-Ökosystem sich Deutschland durchaus messen kann, wird pro Kopf etwa 7-mal so viel VC-Kapital in den Bereich Cybersecurity investiert (Abbildung 7).

Dieser Rückstand Deutschlands hängt eng mit dem Fehlen international sichtbarer Hotspots im Bereich Cybersicherheit zusammen. Solche leistungsstarken Cluster haben sich neben dem Silicon Valley unter anderem um Boston und in Israel etabliert. Ähnlich wie das Ruhrgebiet zeichnen sich beide Ökosysteme durch erstklassige Forschungs- und Lehreinrichtungen aus, die sich früh auf den Bereich Cybersecurity spezialisiert haben. Gleichzeitig existieren jedoch auch relevante Unterschiede: Während das Ökosystem in Boston vom direkten Zugang zum nordamerikanischen (Finanz-) Markt profitiert, verfügt Israel in diesem Bereich über eine einzigartige staatliche Förderstruktur, die durch einen guten Zugang zum VC-Markt ergänzt wird (Start-Up Nation Central 2019).

Neben Ausbildung und Kapitalausstattung ist die Vernetzung zur Sicherheitswirtschaft und staatlichen Sicherheitseinrichtungen ein entscheidendes Merkmal beider Ökosysteme. In Israel sammeln Cybersecurity-Gründerinnen und -Gründer praktische Erfahrungen im militärischen Kontext und werden bei der Umsetzung erworbener Fähigkeiten und Kenntnisse in geschäftsfähige Anwendungen gezielt unterstützt. Das Cluster um Boston kann mit den IBM Security Command Centers auf etablierte Unternehmen setzen, ist über die Center of Academic Excellence aber gleichzeitig auch mit nationalen Sicherheitsbehörden wie der NSA und dem FBI eng verbunden (MassCyberCenter 2020).

Abbildung 7: VC-Investitionen pro Kopf im Bereich Cybersecurity im internationalen Vergleich 2019 (Dealroom)

The COVID crisis has caused cybercrime to grow dramatically and the economic and financial damage is estimated to reach $6 Trillion USD annually by 2021. Companies, banks, insurance companies, governments and cities all need to work together, on both a national and international level, to cooperate and create an international cyber alliance, where countries such as Germany, the United States and Israel can share information and best practices. The cyber threat also creates an opportunity for new ideas, startups and companies to provide new solutions that will enable free trade, and will protect the integrity of information, democracies, and individual rights. By working with young entrepreneurs and collaborating with Israeli and American startups, leading universities and research institutions - Germany can bring additional groundbreaking innovation to its ecosystem and be a part of a strong international cyber alliance.

– Erel Margalit, Founder & Chairman of JVP and Margalit Startup City

3.2. Potenziale und Herausforderungen im Ruhrgebiet

Der internationale Vergleich zeigt, dass im Cybersecurity-Cluster des Ruhrgebiets entscheidende Erfolgsfaktoren bereits angelegt sind: Das Ökosystem profitiert von einer für dieses Feld sehr langen unternehmerischen Tradition, weltweit anerkannter Forschungsexpertise und einer leistungsfähigen Gründungsförderung. Die Stärken des Standorts werden auch von den Gründerinnen und Gründern des Ruhrgebiets im Deutschen Startup Monitor bestätigt: 87,7 Prozent bewerten die Nähe zu den Universitäten vor Ort positiv – ein Wert, der weit über dem Bundesschnitt liegt (Abbildung 8).

Gleichzeitig wird deutlich, dass die genannten internationalen Hotspots bezüglich der Einbettung in globale Märkte, der Sichtbarkeit für internationale Geldgeber und der Verbindung zu nationalstaatlichen Sicherheitssystemen über klare Standortvorteile verfügen. Im Bereich der Finanzierung braucht das Cybersecurity-Cluster Ruhr eine Stärkung von Business Angels und vor allem von VC-Investoren. Dies dient nicht zuletzt der Incentivierung der Gründerinnen und Gründer, ihre Ideen von Beginn an gezielt vom Markt und der Skalierbarkeit her zu denken (Hellmann & Puri 2002).

Neben den Herausforderungen in den Bereichen Marktnähe und Investitionen steckt auch die Verzahnung des Cybersecurity-Ökosystems mit staatlichen Sicherheitsstrukturen hierzulande noch in einer frühen Entwicklungsphase. Im Jahr 2017 wurden mit dem Cyber Innovation Hub der Bundeswehr in Berlin sowie der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) in München neue Institutionen geschaffen. Aktuell befindet sich außerdem die Agentur für Innovation in der Cybersicherheit in Halle im Aufbau. Hier ergeben sich für die Zukunft erhebliche Potenziale zur besseren Vernetzung zwischen dem Staat und Cybersecurity-Startups, die allerdings gezielt adressiert werden müssen. Auch in NRW hat die Landesregierung den Bereich Cybersecurity – insbesondere in der Forschung – gestärkt und befindet sich damit ebenfalls auf dem Weg, die Schnittstelle von Innovation und Sicherheit auszubauen. Gerade im Bereich Cybersicherheit können Startups und Staat wechselseitig stark voneinander profitieren: Hierfür braucht es klarere Zuständigkeiten, die Öffnung öffentlicher Beschaffungsprozesse für junge Unternehmen und auch mehr staatliche Investitionen.

Abbildung 8: Positive Bewertung der Nähe zu Universitäten (DSM 2020)

„Die Relevanz des Themas Cybersecurity ist inzwischen überall angekommen. Das ist eine echte Chance für das Ruhrgebiet: Hier ist ein europaweit führendes Ökosystem mit internationaler Spitzenforschung, mittlerweile etablierten Unternehmen und spannenden Startups entstanden. Um im globalen Wettbewerb noch erfolgreicher zu sein, brauchen wir in Deutschland aber mehr Investoren, die auch bereit sind, größere Finanzierungsrunden in diesem Bereich zu machen."

– Dr. Carsten Willems, Co-Founder und CEO VMRay

„In jüngster Vergangenheit hat die Politik – insbesondere in NRW – bewiesen, dass sie die rasanten Entwicklungen sowie Herausforderungen im Kontext der Digitalisierung erkennt und entsprechend handelt. Der Kompetenzausbau im Bereich IT-Sicherheit in unserer Region bekommt damit eine starke Rückendeckung und kann so weiter vorangetrieben werden – gemeinsam mit den hier ansässigen Hochschulen, Instituten und IT-Sicherheitsfirmen, den Sicherheits-Clustern sowie mit der Unterstützung der kommunalen Wirtschaftsförderungen."

– Christine Skropke, Leiterin Public Affairs bei secunet

3.3. Chancen und Perspektiven des Ruhr-Clusters

Für das Cybersecurity-Cluster Ruhr gilt es nun, die Incentivierung unternehmerischen Handelns aus dem universitären Umfeld heraus weiter auszubauen. Da die Wachstumsorientierung der Startups für Investoren das zentrale Entscheidungskriterium darstellt, sind entsprechende Motive – Stichworte: Skalierbarkeit und „groß denken" – und erfolgreiche Vorbilder für die Weiterentwicklung der Gründungskultur sowie des Ökosystems entscheidend. Eine Stärkung der Investmentseite ist auch wichtig, um im internationalen Wettbewerb zu bestehen: Hier gilt es sowohl Talente langfristig vor Ort zu halten als auch potenzielle Gründerinnen und Gründer sowie IT-Fachkräfte für das Ruhrgebiet zu gewinnen.

Um die bestehenden Stärken des Cybersecurity-Clusters im Ruhrgebiet weiter auszubauen, sollten die bestehenden Forschungseinrichtungen als Standorte der internationalen Spitzenforschung, auch mit starken Anreizen für Top-Forscherinnen und -Forscher, kontinuierlich gefördert werden. Dieser Ausbau vorhandener Kompetenzen ist zur Profilierung und Forcierung der internationalen Sichtbarkeit sowie Wettbewerbsfähigkeit fundamental. Hier ist die Politik gefragt, den Standort Ruhr im Sinne einer nachhaltigen Hochschul- und Wirtschaftspolitik strategisch zu gestalten. Denn wie die internationalen Hotspots zeigen, profitiert der Hightech-Bereich Cybersecurity maßgeblich von digitalen sicherheitspolitischen Projekten und Initiativen.

Insgesamt heißt es im Kontext des aktuellen Digitalisierungsschubs, das Momentum zu nutzen. Dabei bieten sich auch vor dem Hintergrund der zunehmenden Bedeutung der digitalen Souveränität innerhalb Deutschlands und Europas neue Chancen für das Cybersecurity-Cluster im Ruhrgebiet. Hier sind einerseits die Stärkung des europäischen Binnenmarktes und andererseits der Ausbau staatlicher Förderinstrumente unabdingbar. Das spezialisierte Ökosystem im Ruhrgebiet befindet sich in einer sehr guten Position, um diesen Markt nachhaltig zu besetzen. Dazu bedarf es der Anbindung an die im Ausbau befindlichen digitalen Sicherheitsstrukturen des Staates, der stärkeren Vernetzung in die Praxis und der weiteren Steigerung der Attraktivität des Clusters für Investoren.

„Wir haben im Ruhrgebiet tolle Bedingungen im Cybersecurity-Bereich. Mit unseren Hochschulen bilden wir nicht nur Fachkräfte aus, sondern sind auch in der Forschung in diesem Bereich führend. Hiervon profitieren wir als junges Unternehmen enorm. Wir müssen aber noch stärker daran arbeiten, dass man das Ruhrgebiet nicht nur mit einer starken Industrie verbindet, sondern auch mit seinen erfolgreichen Cybersecurity-Unternehmen."

– Matteo Große-Kampmann, Co-Founder und Geschäftsführer AWARE7

The Ruhr Area

3 INTERNATIONAL COMPARISON SUMMARY

International cybersecurity hubs such as Israel showcase important characteristics of successful ecosystems and point to the strengths and opportunities of the Ruhr area. As in the Ruhr area, the Israeli ecosystem has a strong research focus. However, there are also crucial differences: In Israel, private investments in cybersecurity startups amount to 108 euros per capita, whereas in Germany the figure stands at only 83 cents. Alongside financial resources, strong cooperation with national security agencies also accelerates the growth of the ecosystem.

Access to capital and cooperation with national security agencies are the two vital ingredients if the Ruhr area is to continue its development as a cybersecurity hub. To achieve this, the ecosystem needs to promote the transfer of scientific innovation into scalable business models and to strengthen the visibility for investors. Cross-links between startups and state players in cybersecurity are another key factor.

LITERATUR VERZEICHNIS

Accenture (2019): The Cost of Cybercrime – Ninth Annual Cost of Cybercrime Study. URL: https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Allianz (2020): Allianz Risk Barometer 2020 – Identifying the major business risks for 2020. URL: https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-de.html

AustCyber (2019): Australia's Cyber Security Sector Competitiveness Plan 2019. URL: https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019

Bitkom (2020): Markt für IT-Sicherheit auf Allzeithoch. URL: https://www.bitkom.org/Presse/Presseinformation/Markt-fuer-IT-Sicherheit-auf-Allzeithoch

CBInsights (2020): 2020 Cyber Defenders. URL: https://www.cbinsights.com/research/report/cyber-defenders-2020/

Dealroom (2020): Global Data Platform. URL: https://dealroom.co/

Deloitte (2019): Cyber Security Report 2019 Teil 1: Fake News und Schlüsseltechnologien – wachsende Herausforderungen. URL: https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html

Hellmann, T. / Puri, M. (2002): Venture Capital and the Professionalization of Start-Up Firms: Empirical Evidence, Journal of Finance. URL: https://onlinelibrary.wiley.com/doi/10.1111/1540-6261.00419

Hirschfeld, A. / Gilde, J. (2020): Innovationsreport Ruhr. URL: https://deutschestartups.org/wp-content/uploads/2020/04/Innovationsreport-Ruhr.pdf

MassCyberCenter (2020): Massachusetts Cybersecurity – Global Leadership Through Talent, Resources, and Investment. URL: https://masstech.org/sites/mtc/files/documents/PitchDecks/Cyber%20Security%20Pitch%20Deck-10-29-2019.pdf

Mason, C. / Brown, R. (2014): Entrepreneurial Ecosystems and Growth Oriented Entrepre-neurship. URL: https://www.oecd.org/cfe/leed/entrepreneurial-ecosystems.pdf

Murphy, A. / Tucker, H. / Coyne, M. / Touryalai, H. (2020): Global 2000 – The World's Largest Public Companies. URL: https://www.forbes.com/global2000/#15c8c177335d

Kollmann, T. / Jung, P. / Kleine-Stegemann, L. / Ataee, J. / de Cruppe, K. (2020): Deutscher Startup Monitor (DSM) 2020, Berlin. URL: https://deutschestartups.org/wp-content/uploads/2020/09/20200929_Deutscher-Startup-Monitor-2020.pdf

Metzger, G. (2020): KfW-Start-up-Report 2019: Zahl der Start-ups in Deutschland steigt weiter, Frankfurt am Main. URL: https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/KfW-Start-up-Report/KfW-Start-up-Report-2019.pdf

Start-up Nation Central (2019): Finder Insights Series – Israeli Cybersecurity Industry in 2018. URL: http://mlp.startupnationcentral.org/rs/663-SRH-472/images/Start-Up%20Nation%20Central%20Cybersecurity%20Report%202019.pdf