Bundesamt
für Sicherheit in der
Informationstechnik

cyberagentur

Cyber Startup Landscape - Bay Area

Eine Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)

Bundesamt für Sicherheit in der
Informationstechnik (BSI)
Postfach 20 03 63
53133 Bonn
Germany
E-Mail: us-cooperation@bsi.bund.de
Internet: https://www.bsi.bund.de

Agentur für Innovation in der
Cybersicherheit GmbH (Cyberagentur)
Große Steinstraße 19
06108 Halle (Saale)
Germany
Tel.: +49 345 78288032
E-Mail: kontakt@cyberagentur.de
Internet: https://www.cyberagentur.de

Version 1.0, August 2024

Hinweis:

Die Mehrzahl der in der Studie verwendeten Personenbezeichnungen (wie z.B. „Investoren“, „Kunden“ oder „Branchenführer“) bezieht sich auf Unternehmen. Auf eine Doppelnennung und gegenderte Bezeichnungen wird daher zugunsten einer besseren Lesbarkeit verzichtet. Wo sich solche und ähnliche Bezeichnungen auf einzelne Personen beziehen, sind gleichermaßen weibliche, männliche und diverse Personen gemeint.

Management Summary

Die letzte Dekade führte zu einem erheblichen Wachstum des Cybersicherheitssektors und infolgedessen zu einem dynamischen Umfeld für Startups. Neue Trends, Innovationen und Technologien im Bereich der Cybersicherheit und den dazugehörigen Schlüsseltechnologien prägen somit die Zukunft maßgeblich.

Aus diesem Grund veröffentlichen das Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) und die Agentur für Innovation in der Cybersicherheit GmbH (kurz Cyberagentur) die vorliegende Studie „Cyber Startup Landscape - Bay Area“, mittels derer ein Überblick über die wichtigsten Startups, Technologien und Trends im Bereich der Cybersicherheit gegeben werden soll. Die im Rahmen dieser Studie veröffentlichte Landscape wurde mit Hilfe einer Reihe von Datenbanken erstellt, in denen sich relevante Informationen über die in der Bay Area ansässigen Startups fanden. Der Schwerpunkt der Datenerhebung lag auf den im Bereich der Cybersicherheit tätigen Startups mit einem starken Technologie-Fokus (kurz Cyber Startups). Dies bedeutet, dass im Gegensatz zu anderen Tätigkeitsbereichen wie z.B. der Anwenderforschung, neuartige Geschäftsmodelle oder Beratungsdienstleister, diese Startups erhebliche Ressourcen und Mittel für ihre technologische Forschung und Entwicklung erfordern.

Im Ergebnis unserer Analyse wurden 437 Startups, die diese Kriterien erfüllen, in die vorliegende Studie einbezogen. Dabei unterschieden sich diese teils erheblich in Hinblick auf ihre Eigenschaften wie Größe, Alter, Reife und technische Spezifikationen. Die in diese Landscape eingebundenen Startups wurden thematisch in vier Hauptcluster gegliedert: Digital Infrastructure Security, Personal Digital Security, Security Analytics, und Operational Technology & Application Security. Darüber hinaus wurde jedes Startup Subclustern (insgesamt 19 Stück) zugewiesen, die als Bottom-up-Struktur dem Zwecke der Navigation in dieser Landscape dienen. In einem weiteren Schritt wurden im Rahmen der durchgeführten Analysen sieben Schlüsseltechnologien identifiziert, die von den Startups in unterschiedlichem Maße genutzt werden. Im Einzelnen waren dies: Künstliche Intelligenz (KI) und maschinelles Lernen (ML), Bilderkennung, Blockchain-Infrastruktur, Internet der Dinge (IoT), Cloud-Technologie, Quantencomputing und Big Data. Neben der unter den Startups dominierenden Cloud-Technologie sind auch die beiden Schlüsseltechnologien KI und ML gleichmäßig in den wichtigsten Clustern verteilt. Dies spiegelt den in vielen Branchen beobachteten Trend der Bereitschaft zur zukünftigen Nutzung dieser leistungsstarken Technologie wider. Quantencomputing ist nach wie vor die Technologie, auf die am wenigsten verwiesen wird, was jedoch darauf hindeutet, dass trotz der geringen Reife die ersten geschäftlichen Anwendungen für diese Technologie bald auf dem Markt erscheinen werden.

Nachdem alle 437 Startups sortiert und mit relevanten Schlüsseltechnologien verbunden waren, wurden von uns insgesamt 44 Startups ausgewählt, um diese in unserer Landscape präsentieren zu können. Die Auswahl basierte dabei auf einer Vielzahl von Kriterien, von der Anzahl der angemeldeten Patente bis hin zu einzigartigen Technologiekombinationen innerhalb der angebotenen Lösung. Die ausgewählten 44 Startups spiegeln dabei sowohl die Bandbreite als auch die Vielfalt der Cybersicherheits-Perspektiven wider und sind somit Bestandteil der Hauptergebnisse dieser Studie.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

In den vergangenen zehn Jahren erlebte die Branche der Cybersicherheit ein beispielloses Wachstum, das durch die Covid-19-Pandemie noch erheblich beschleunigt wurde. Im Gegensatz zu vielen anderen Branchen beobachtete der Cybersicherheitssektor eine anhaltende Nachfrage und florierte in einem ansonsten schwierigen makroökonomischen Umfeld, was sich im Wachstum vieler börsennotierter Cybersicherheitsunternehmen deutlich widerspiegelt. Die wachsende Nachfrage fördert ein dynamisches Umfeld für Startups, um innovative Lösungen und modernste Technologien zu entwickeln.

Aus diesem Grund veröffentlichen das Bundesamt für Sicherheit in der Informationstechnik (kurz BSI) und die Agentur für Innovation in der Cybersicherheit GmbH (kurz Cyberagentur) die vorliegende Studie „Cyber Startup Landscape - Bay Area“, mittels derer ein Überblick über die wichtigsten Startups, Technologien und Trends im Bereich der Cybersicherheit gegeben werden soll. Mit dieser Studie setzen wir unseren Auftrag als zentrale Förder- und Koordinierungsstelle für Forschungsprojekte im Bereich der Cybersicherheit fort und unterstützen die Bundesregierung bei der gezielten Stärkung der Forschung im Bereich Cybersicherheit. Zudem tragen wir so zur technologischen Souveränität von übermorgen bei.

Die Wahl der Bay Area als Fokus dieser Studie liegt in der weltweit wahrgenommenen Reputation dieser Region als Hotspot und Geburtsstätte vieler Startup-Erfolgsgeschichten begründet. Die für den Erfolg notwendigen Akteure – Universitäten mit den jeweiligen Instituten, Tech-Giganten, Acceleratoren, Inkubatoren und Großinvestoren, einschließlich Risikokapitalgebern – befinden sich im direkten Umfeld dieser Unternehmen und tragen alle zu innovativen Lösungen bei. Im Fokus dieser Studie stehen Startups da diese oft Wegbereiter für neue Dienstleistungen und Produkte für den Markt sind und dabei mit dem Ziel der Veränderung des Status Quo als Innovationstreiber agieren.

Mit dieser Studie möchten wir einen Überblick über die Vielfalt der in der Bay Area ansässigen Cyber Startups geben. Nach einer allgemeinen Einführung folgen im Rahmen dieser Studie mehrere detaillierte Analysen, mit dem Ziel, einen Einblick in das Startup-Ökosysteme zu geben und deren Bedeutung für den Cybersicherheitssektor zu analysieren. Darüber hinaus wird ein tiefer Einblick in die Schlüsseltechnologien und den finanziellen Hintergrund der gescouteten Startups gewährt, wobei ressourcenintensive Bereiche hervorgehoben werden. Schlussendlich haben wir eine Reihe von Startups ausgewählt, die in Zukunft ein hohes Disruptionspotential aufweisen könnten. Diese Startups haben wir genauer analysiert und bezeichnen die Auswertung nachfolgend als Deep Dive Profil. Weitere Informationen zu diesen Profilen werden in **Anlage 3** dieser Studie bereitgestellt.

2 Methodik

Da Cyber Startups bereits Gegenstand zahlreicher Untersuchungen waren, scheint es wenig überraschend, dass wir eine Reihe von Studien anderer Organisationen ausmachen konnten, die bereits Einblicke in die Welt der Cyber Startups geben. Obwohl all diese Studien eine gewisse Ähnlichkeit vereint und auch Gemeinsamkeiten mit unserer Landscape bestehen, möchten wir dennoch in Hinblick auf die hier vorliegende Studie das Thema dieser abgrenzen und unseren Forschungsansatz sowie die im Rahmen der Analyse verwendeten Datenquellen transparent machen. In einem ersten Schritt erfolgt daher die Festlegung von Startups als Untersuchungsobjekt sowie der für die Aufnahme in die Studie von ihnen zu erfüllenden Kriterien. Danach erfolgt eine Vorstellung unserer Datenquellen und des der Studie zugrundeliegenden Methodik.

2.1 Definitionen und Aufnahmekriterien

In Vorbereitung unserer Cyber Startup Landscape erfolgt zunächst die Definition der Aufnahmekriterien, nämlich Startups aus dem geographischen Raum Bay Area, die Cybersicherheitslösungen im Bereich der Deep Tech anbieten. Im Anschluss präsentieren wir die bei der Auswahl der Unternehmen angewandten Prüflogik und erläutern die Aufnahmekriterien und Datenquellen.

2.1.1 Startups

Unsere Studie konzentriert sich auf die grundlegende Einheit unserer Forschung: Das Startup. Obwohl der Begriff in der Praxis alltäglich ist und wenig bis keinen Raum für Missverständnisse bietet, möchten wir unsere Begriffsdefinition darlegen, die sich von der von anderen Organisationen unterscheidet. Im Sinne unserer Studie definiert sich ein Startup durch die folgenden Eigenschaften: Bei einem Startup handelt es sich um ein nicht börsennotiertes privates Unternehmen („juristische Person“), das von seinen Gründern (d. h. natürliche Personen, nicht Unternehmen) kontrolliert wird. Dabei löst es mittels eines skalierbaren Produkts, das auf geschütztem, geistigem Eigentum (IP) basiert, ein relevantes Problem. Des Weiteren definieren wir Startups als Unternehmen, die im Allgemeinen durch Risikokapital (venture capital – VC) finanziert werden, wobei jedoch eine bestehende VC-Finanzierung keine Bedingung für das Vorliegen eines Startups ist. Die Studie umfasst auch Universitätsableger und neu gegründete Startups mit geringer Sichtbarkeit oder im „Stealth-Modus“, soweit ausreichende Daten verfügbar sind. Dies schließt börsennotierte oder aufgekaufte Unternehmen standardmäßig aus, da diese nicht die von uns geforderten Merkmale eines Startups erfüllen. Da diese Landscape sich auf die Gegenwart konzentriert, wurde der Beobachtungsraum auf einen Zeitraum von 10 Jahren beschränkt, so dass vor 2014 gegründete Startups nicht Bestandteil dieser Studie sind.

2.1.2 San Francisco Bay Area

Die im Rahmen dieser Studie erstellte Landscape konzentriert sich auf die San Francisco Bay Area und somit auf eine Region, die für ihre Vielzahl innovativer Startups, Unternehmen, Forschungsinstitute und Universitäten bekannt geworden ist. Als Kriterium für die Aufnahme in diese Studie gilt, dass die Startups ihren Hauptsitz oder zumindest einen Bürostandort in der Bay Area haben müssen. Dabei umfasst die Bay Area die elf Counties Alameda, Contra Costa, Marin, Napa, Sacramento, San Francisco, San Mateo, Santa Clara, Santa Cruz, Solano und Sonoma.

***Abbildung 1**: Übersicht über Bay Area Counties*

2.1.3 Cybersicherheit

Nach der Festlegung der Studienobjekte sowie der geografischen Abgrenzung gehen wir im Folgenden auf die thematische Ausrichtung unserer Studie ein. Der Schwerpunkt unserer Landscape liegt auf Startups aus dem Sektor der Cybersicherheit. Die von uns angewandte Definition für den Begriff der Cybersicherheit ergibt sich dabei aus dem im Jahr 2009 veröffentlichten „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" (kurz „BSI-Gesetz" oder auch „BSIG"). Das BSIG definiert Informationstechnik als „alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen". Darauf aufbauend bedeutet „Sicherheit der Informationstechnik" demnach die Einhaltung bestimmter Sicherheitsstandards für die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen durch Sicherheitsvorkehrungen in, und für die Nutzung von, informationstechnischen Systemen, Komponenten oder Verfahren." Diese Definition spiegelt auch die Überlegungen des National Institute of Standards and Technology (NIST) zu den zugrundeliegenden Werten der Verfügbarkeit, Integrität und Vertraulichkeit wider. In der NIST-Definition heißt es, dass Cybersicherheit ferner „die Verhinderung von Schäden an Computern, elektronischen Kommunikationssystemen, elektronischen Kommunikationsdiensten, drahtgebundener Kommunikation und elektronischer Kommunikation, einschließlich der darin enthaltenen Informationen, sowie deren Schutz und Wiederherstellung, um deren Verfügbarkeit, Integrität, Authentifizierung, Vertraulichkeit und Nichtabstreitbarkeit zu gewährleisten" bedeutet. Aufgrund der internationalen Ausrichtung unserer Studie und der US-Geografie eignet sich die erweiterte NIST-Definition für den Zweck dieser Untersuchung und stellt ein geeignetes Kriterium bei der Auswahl von den für unsere Landscape geeigneten Startups dar.

Zusätzlich zur allgemeinen Definition von Cybersicherheit werden wir uns im Rahmen der Studie häufig auf verschiedene Begriffe des NIST Cybersecurity Framework (CSF) 2.0 beziehen. Dieses bietet beides, eine Grundlage und eine Taxonomie, die es Organisationen aller Branchen ermöglicht, Cybersicherheitsfragen zu verstehen und entsprechend zu handeln. Insbesondere die zentralen Funktionen dieses Rahmenwerks sind für das Verständnis des Umfangs der Bemühungen zur Gewährleistung einer digital sicheren Wirtschaft und eines sicheren Betriebs von Bedeutung. Die Kernfunktionen des CSF sind „Govern", „Identify", „Protect", „Detect", „Respond" und „Recover", die im Folgenden kurz vorgestellt werden:

- Govern (GV): Die Strategie, die Erwartungen und die Richtlinien des Risikomanagements für die Cybersicherheit der Organisation werden festgelegt, kommuniziert und überwacht.
- Identify (ID): Die aktuellen Cybersicherheitsrisiken der Organisation werden verstanden.
- Protect (PR): Maßnahmen zum Schutz vor identifizierten Cybersicherheitsrisiken werden eingesetzt.
- Detect (DE): Mögliche Cybersicherheitsangriffe und -gefährdungen werden aufgespürt und analysiert.
- Respond (RS): Es werden Maßnahmen bezüglich eines erkannten Cybersicherheitsvorfalls ergriffen.
- Recover (RC): Vermögenswerte und Vorgänge, die von einem Cybersicherheitsvorfall betroffen sind, werden wiederhergestellt.

Für unsere Untersuchung orientierten wir uns daher an den kombinierten Definitionen von Cybersecurity und suchten nach Startups, deren Produkte und Dienstleistungen direkt oder indirekt darauf abzielen, Cyberbedrohungen und Angriffe auf Unternehmen, Regierungsorganisationen oder Einzelpersonen zu erkennen, zu verhindern, Schutz zu bieten und darauf zu reagieren. Dies umfasst sowohl zu entwickelnde Software- als auch Hardwareangebote.

2.1.4 Deep Tech

Die Studie konzentriert sich auf Startups, die im oder am Rande des Deep Tech Sektors angesiedelt sind. Im Rahmen unserer Studie bezieht sich dieser Begriff auf Technologien, die – im Gegensatz zu Bereichen wie z. B. Nutzerforschung, innovativen Geschäftsmodellen oder Beratungsdienstleistungen – einen erheblichen Einsatz von Ressourcen und Finanzmitteln für Forschung und Entwicklung erfordern. Die von den Startups angebotenen Lösungen erfordern ein hohes Maß an Innovationen auf technischer oder wissenschaftlicher Ebene, die potenziell bahnbrechend und – sofern in einem frühen Stadium erkennbar – transformativ sind. Erfüllt wird diese Voraussetzung entweder durch eine herausragende Finanzierung in den jeweiligen Runden oder durch bereits angemeldetes, geistiges Eigentum, das dem technischen Niveau zuzuordnen ist.

2.2 Methodik

Nach der Festlegung des Untersuchungsrahmens befasst sich das folgende Kapitel mit unserem Forschungsansatz, zeigt die verwendeten Datenquellen und das genutzte Analyseverfahren und legt Finanzierungs- und Produktreifebegriffe fest, die im Rahmen unserer Analyse genutzt werden.

2.2.1 Quellen und Prozesse

Die Studie stützt sich auf mehrere Datenbanken, die sowohl mengenmäßig als auch qualitativ Daten zu unserer Analyse beitrugen. Als Primärquelle wurden öffentlich zugängliche Datenbanken wie Tracxn, Pitchbook und Crunchbase genutzt, die ausführliche Informationen zu relevanten Startups bieten. Die entsprechend gewonnenen Daten wurden in der Folge zusammengefasst und vorab bewertet mit dem Ziel der Erstellung einer Projektkundendatenbank, die mehr als 30,000 vorbewertete Startups und anonymisierte Leistungsdaten enthält.

Neben diesen Primärquellen wurden drei zusätzliche Quellen für die weitere Analyse herangezogen. Zunächst haben wir Informationen aus dem uns zugänglichen Startup-Ökosystem eingeholt, zu dem Investoren aller Art, Acceleratoren und Inkubatoren, Veranstaltungen für Startups, VCs, oder auf relevante Szenen ausgerichtete Nachrichtenportale gehören. Zusätzlich dazu griffen wir auf ein privates Netzwerk von Unternehmern, Kunden und Partnern zu, darunter Mitarbeiter in für unsere Forschung relevanten Funktionen und Branchen. Ergänzt wurden sie durch akademische Kontakte mit Forschungsschwerpunkten in den Bereichen Startup-Ökosysteme, Innovation und strategisches Management. Schließlich verschafften uns unsere Verbindungen zur Industrie die Perspektive größerer, technologisch ausgerichteter Unternehmen sowie von Branchenführern und Experten in ihrem Kompetenzbereich und ihren Wettbewerbern.

Eine Übersicht über die Quellen findet sich in der folgenden **Abbildung 2**.

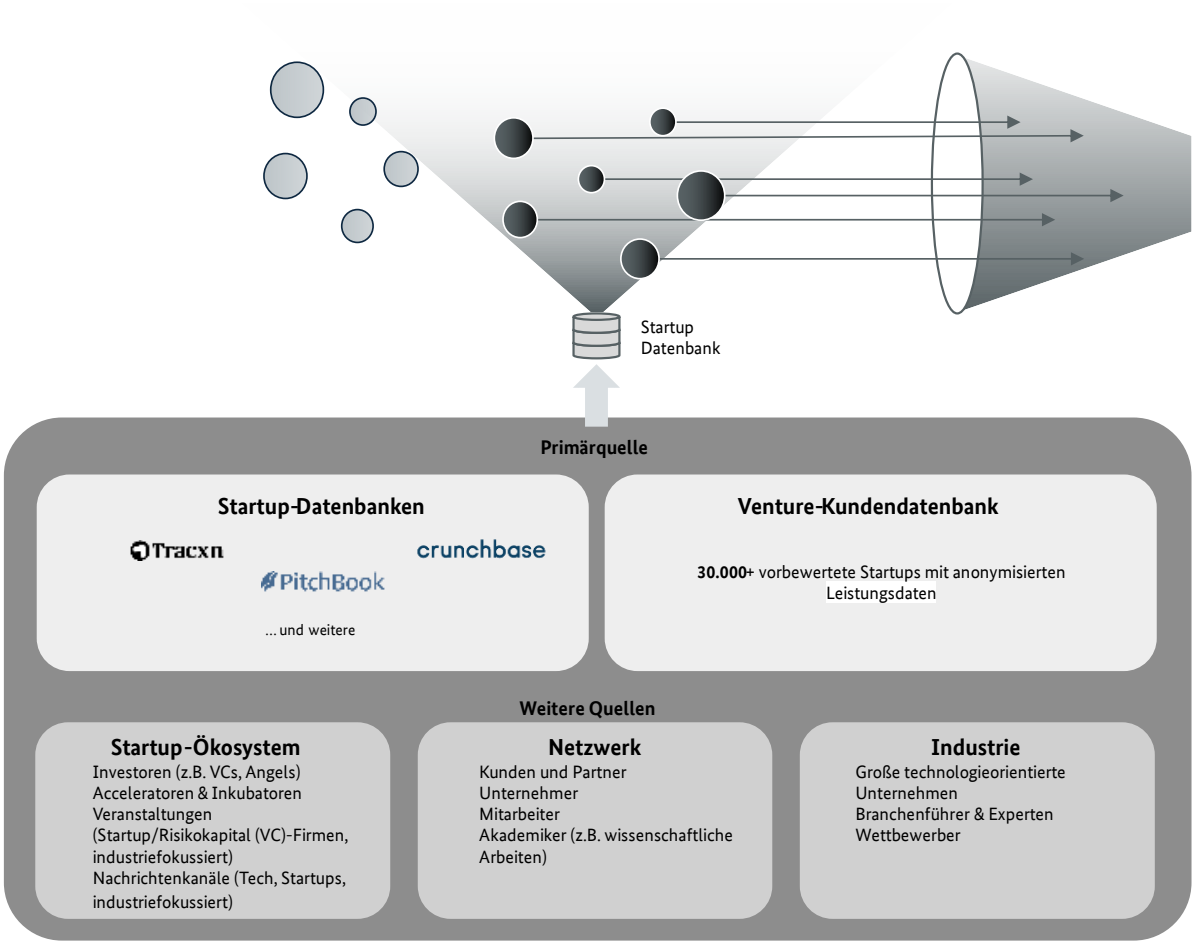

***Abbildung 2**: Struktur der Startup-Datenbank und Quellen*

Die Informationen aller genannten Quellen wurden in einer Datenbank zusammengeführt, welche die Filterung der Startups nach den in Kapitel 2.1 festgelegten Kriterien ermöglichte. Nach der Erstellung einer Liste von den in das Profil passenden Startups führten wir unter Bereinigung ggf. auftretender Inkonsistenzen eine Überprüfung der Daten durch, die dann als Grundlage für die Festlegung der thematischen Cluster diente.

Nach Schaffung und Sicherstellung der Datenqualität haben wir die Startups thematischen Clustern zugewiesen. Dafür wurden Gruppen von Startups basierend auf Gemeinsamkeiten der von ihnen angebotenen Cybersicherheitsanwendungen festgelegt. Insgesamt konnten so vier Hauptcluster und 19 Subcluster abgeleitet werden. Diese Cluster und Subcluster dienen von nun an der thematischen Ausrichtung unserer Landscape und der anschließenden Analyse.

2.2.2 Auswahlprozess der Deep Dive Startups

Unsere Liste umfasst insgesamt 437 Startups; im ersten Schritt haben wir, wie im **Kapitel 3** und **Kapitel 5** ausführlich beschrieben, zunächst die Cluster sowie die ihnen zugehörigen Daten analysiert. Anschließend haben wir eine Liste von 20 so genannten Deep Dive Startups erstellt, die wir genauer analysiert haben. Der Auswahlprozess umfasste dabei zwei Schritte. Zunächst erstellten wir eine erweiterte Liste potenzieller Deep Dive Startups und fügten dieser dann auf Grundlage der folgenden Kriterien weitere Startups hinzu:

- Die fünf Startups mit der höchsten durchschnittlichen jährlichen Finanzierung innerhalb jedes Clusters. Dies ermöglichte uns das Filtern nach ressourcenintensiven und somit dem Deep Tech Kriterium entsprechenden Startups.
- Die jeweils fünf Startups mit der höchsten Anzahl angemeldeter Patente, wobei das Augenmerk auf dem Innovationsergebnis lag.
- Die fünf Startups mit den höchsten Umsätzen, was darauf hinweisen kann, dass die Lösungen sowohl vom Markt nachgefragt werden als auch ein stabiles Ergebnis liefern.
- Es ist davon auszugehen, dass Startups, bei denen im Jahr 2024 Finanzierungsrunden stattgefunden haben, sich in den kommenden 12 Monaten weiterentwickeln, weswegen diese Startups für uns von Interesse sind.
- Die neu im Jahr 2024 gegründeten Startups, mit dem Ziel, diejenigen mit dem größten Potential zu finden.
- Startups, die in Subcluster passen, in welchen ein hohes Potenzial vermutet wird (insbesondere: Server Security, BYOD Security, Blockchain Security, Website Security, IoT Security, Threat Intelligence und Email Security).
- Startups, die von Investoren unterstützt wurden, die in dieser Studie wie in **Kapitel 5.4** beschrieben als Top-Investoren angesehen wurden und die entweder einen hohen Gesamtfinanzierungsbetrag oder eine hohe durchschnittliche jährliche Finanzierung aufwiesen.
- Weitere Gründe für eine Aufnahme in unsere Liste während der Analyse waren:
    - In einem Fall eine einzigartige Kombination von Schlüsseltechnologien.
    - In einem Fall ein fremdfinanziertes Startup mit einer Strategie zur Anmeldung von Patenten.
    - In einem Fall ein Startup, das nur von einem Forschungsinstitut unterstützt wird.

Auf diese Weise konnten wir 44 Startups ermitteln, die als Kandidaten für unsere Deep Dive Startups in Frage kamen. Die Liste wurde in einer Schwerpunktgruppe diskutiert, welche aus allen an der Erstellung dieser Studie Beteiligten bestand. In Vorbereitung auf diese Besprechung wurde die erweiterte Liste den Gruppenmitgliedern eine Woche vor dem angesetzten Termin zur Verfügung gestellt und darum gebeten, die den eigenen Präferenzen am ehesten zusagenden Deep Dive Startups auszuwählen. Im Rahmen des gemeinsamen Termins wurden die von den einzelnen Mitgliedern ausgewählten Startups dann anhand verschiedener Kriterien gegeneinander abgewogen. Ziel war es, durch die Deep Dive Startups alle Facetten der Cyber Startup Landscape abzubilden, einschließlich solcher Faktoren wie Reifegrad, Finanzierung, Patente und Alter. Im Ergebnis entstand eine Liste von insgesamt 20 Deep Dive Startups, die daraufhin einer tiefergehenden Analyse unterzogen wurden. Das entsprechende Profil für die einzelnen Deep Dive Startups findet sich in **Anlage 3**.

2.2.3 Finanzierung der Startups und Produktreife

Als Grundlage für die weitere Kategorisierung und Analyse möchten wir im Folgenden die Finanzierung der Startups in Verbindung mit der Produktreife betrachten. Grundsätzlich folgen wir dabei den allgemein bekannten Abläufen der Finanzierungsrunden bei Startups, angefangen bei der (Vor-) Finanzierung über Finanzierungen für A, B, C und ggf. auch weiteren Serien bis hin zum Finanzierungsausstieg. Dabei geben wir Orientierung hinsichtlich der in den jeweiligen Runden zum Tragen kommenden Finanzierungsdaten, Unternehmen und Produktreife.

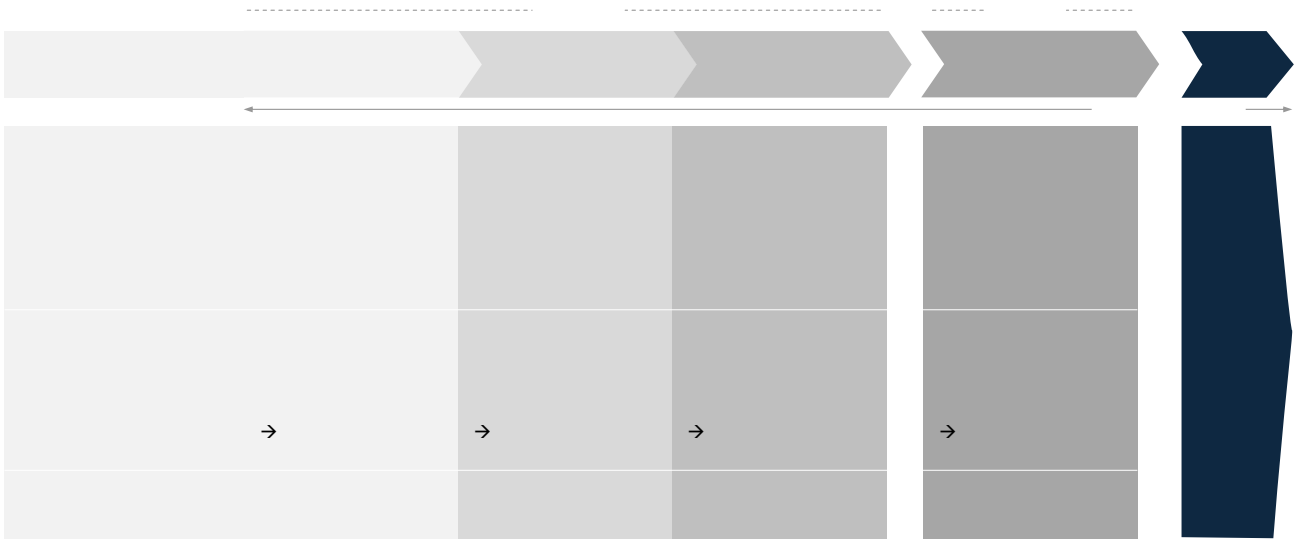

***Abbildung 3**: Startup-Reifegrad & Finanzierung*

Wie bereits erwähnt, leitet sich die Deep Tech Ausrichtung unserer Forschung aus der Untersuchung früher Stadien ab, in denen potenziell geschützte Technologien entwickelt und erhebliche Investitionen getätigt werden.

3 Strukturelle Analyse

Das folgende Kapitel analysiert die vier Startup-Cluster, in denen die identifizierten 437 Startups agieren und operieren. Die Aufteilung bildet die Struktur unserer Cyber Startup Landscape, um die Navigation durch die hohe Anzahl der identifizierten Startups zu erleichtern. Wir beginnen mit einer Analyse der Cluster und ihrer jeweiligen Subcluster, gehen dann auf die von uns identifizierten Schlüsseltechnologien ein und legen dar, wo diese innerhalb der Cluster eingeordnet werden können.

3.1 Startup Cluster – Übersicht

Unsere Analyse identifizierte vier wichtige Startup-Cluster innerhalb unserer Cyber Startup Landscape:

- Analytics
- Digital Infrastructure Security
- Operational Technology (OT) & Application Security
- Personal Digital Security

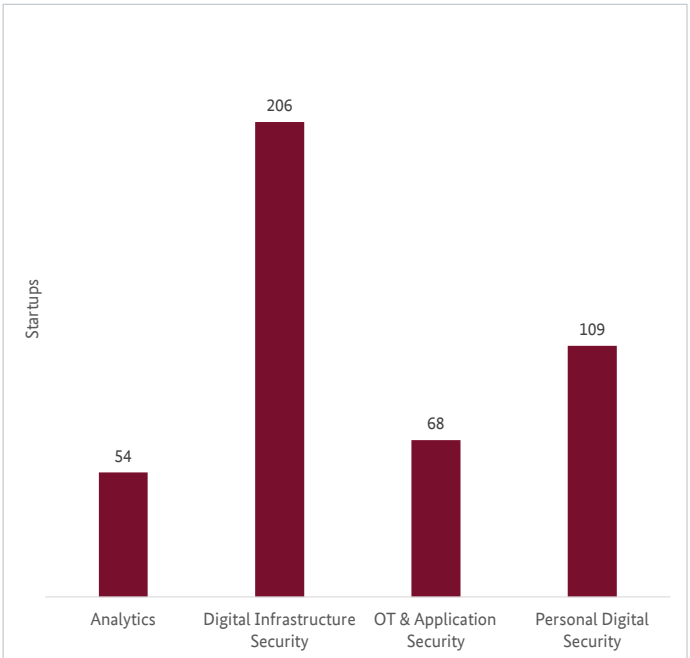

***Abbildung 4**: Anzahl der Startups pro Cluster*

Die Definition der Cluster basiert auf bestimmten Merkmalen der Startups. Diese Merkmale wurden für jedes einzelne Startup ermittelt, und Gruppen ähnlicher Merkmale wurden anschließend zu Mustern zusammengefasst. Diese Muster ermöglichten schließlich, Cluster und Subcluster auf der Grundlage gemeinsamer Merkmale und Schwerpunktbereiche zu definieren. Die Landscape spiegelt dabei die thematische Vielfalt der Startups in der Bay Area wider. Gemäß der aus dem BSI-Gesetz von 2009 und dem NIST Cybersecurity Framework (siehe **Kapitel 2.1.3**) abgeleiteten Definition des Begriffs Cybersicherheit, beleuchtet jedes Cluster die vielfältigen von Startups genutzten Ansätze mit denen Cybersicherheitsherausforderungen begegnet, digitale Umgebungen geschützt und Innovationen zum Schutz kritischer Systeme, persönlicher Geräte und industrieller Abläufe gefördert werden. Diese Rahmenwerke, die den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit von Informationen betonen, dienten als Grundlage bei der Identifizierung von Startups, die zur Erkennung und Verhinderung von Cyberbedrohungen und Cyberangriffen sowie zum Schutz vor solchen Bedrohungen und zur Reaktion im Falle ihres Auftretens beitragen.

Im Rahmen unserer Analyse wurden 206 Startups im Cluster Digital Infrastructure Security, 109 in Personal Digital Security, 54 in Security Analytics und 68 in OT & Application Security identifiziert, in Summe demnach 437 Startups. **Abbildung 4Abbildung 4**: Anzahl der Startups pro Cluster zeigt die ausführliche Verteilung unserer Landscape. Die folgenden Kapitel beleuchten die einzelnen Cluster näher und geben einen thematischen Überblick über die jeweiligen Subcluster.

3.1.1 Digital Infrastructure Security

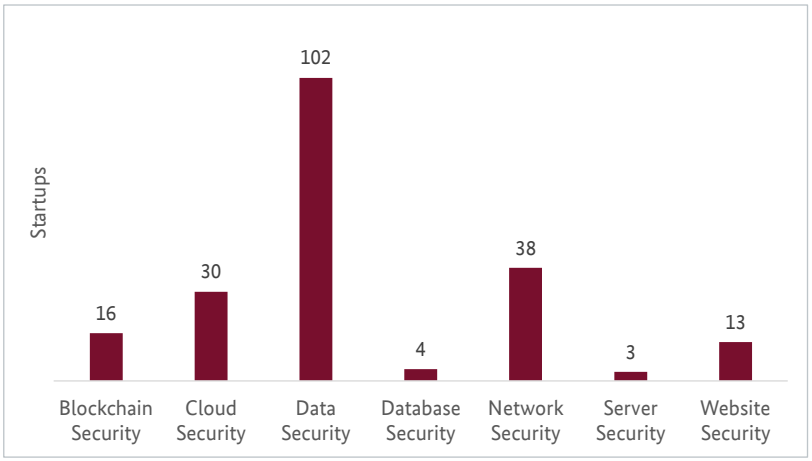

***Abbildung 5**: Verteilung der Subcluster – Cluster Digital Infrastructure Security*

Der Cluster Digital Infrastructure Security umfasst 206 Startups, die sich auf die Absicherung kritischer Systeme und Netzwerke in der digitalen Landschaft konzentrieren. Diese Startups setzen verschiedene Technologien ein, um den Schutz und die Integrität von Daten, Servern, Websites und Cloud-basierten Ressourcen zu gewährleisten. Zu den Schwerpunktbereichen des Clusters Digital Infrastructure Security gehören Network Security, Website-Security, Server Security, Database Security, Data Security, Cloud Security und Blockchain-Security. Durch die Stärkung der digitalen Infrastruktur können Unternehmen sich gegen Cyberbedrohungen wehren, eine zuverlässige und sichere Datenverwaltung fördern und die Einführung sicherer digitaler Technologien wie Blockchain unterstützen. Diese umfassenden Sicherheitsmaßnahmen sind entscheidend, um Risiken zu mindern und ein sicheres digitales Geschäftsumfeld zu schaffen. Die Verteilung der Startups ist in **Abbildung 5** dargestellt. Die Subcluster sind unterschiedlich groß, von Data Security mit 102 Startups bis hin zu Server Security mit nur drei Startups. Die Subcluster werden im Folgenden detailliert beschrieben.

3.1.1.1 Blockchain Security

Blockchain Security umfasst Maßnahmen, Verfahren und Technologien zum Schutz der Integrität und Vertraulichkeit der im Blockchain-Netzwerk gespeicherten Daten vor böswilligen Angriffen und unbefugtem Zugriff, wie z. B. die Echtzeitüberwachung von Blockchain-Protokollen, intelligente Verträge zur Erkennung von Bedrohungen und *SlowMist Hacked,* eine Datenbank, die Sicherheitsvorfälle im Blockchain-Bereich verfolgt.

3.1.1.2 Cloud Security

Cloud Security bezieht sich auf eine Reihe von Maßnahmen, Verfahren und Technologien zum Schutz von Daten, Anwendungen und Diensten, die in Cloud-Umgebungen gehostet werden. Die Cloud Technologie bietet zahlreiche Vorteile wie Skalierbarkeit, Flexibilität und Kosteneffizienz, birgt aber auch neue Herausforderungen und Sicherheitsrisiken. Sicherheitsmethoden wie homomorphe Verschlüsselung und Confidential Computing, Identitätszugriffsmanagement und Mehrfaktor-Authentifizierung sorgen dafür, dass Daten und Anwendungen sicher in der Cloud betrieben werden.

3.1.1.3 Data Security

Data Security umfasst Maßnahmen, Verfahren und Technologien, die dazu dienen, Daten im Gebrauch, bei der Übertragung und im Ruhezustand vor unberechtigtem Zugriff, Verlust, Manipulation und Diebstahl zu schützen. Dies kann beispielsweise durch den Einsatz von Festplattenverschlüsselung, Zugriffskontrolle, Backup und Transport Layer Security gewährleistet werden.

3.1.1.4 Database Security

Database Security bezieht sich auf Maßnahmen, Verfahren und Technologien zum Schutz von Datenbanken vor einer Vielzahl von Bedrohungen, z. B. Datenverlust und unberechtigtem Zugriff. Eine sichere Datenbank schützt die gespeicherten Daten sowohl vor internen als auch externen Bedrohungen. Dies kann unter anderem mit Hilfe von Zugriffskontrolltechnologien und -methoden sichergestellt werden, die es dem Benutzer ermöglichen, alle Änderungen an einer Datenbank durch Protokollierung von Ereignissen zu überwachen.

3.1.1.5 Network Security

Network Security bezieht sich auf Maßnahmen, Verfahren und Technologien, die dazu dienen, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Ressourcen in einem Netzwerk zu schützen. Dazu gehört der Schutz vor unbefugtem Zugriff, Missbrauch, Systemausfällen und Angriffen. Zu den Technologien, die für einen besseren Schutz eingesetzt werden, gehören Firewalls, Intrusion Detection Systeme, Web Application Firewalls und Endpoint Detection Systeme.

3.1.1.6 Server Security

Server Security bezieht sich auf Maßnahmen, Verfahren und Technologien zum Schutz von Serverumgebungen, Diensten und den auf den Servern gespeicherten Daten vor Cyberangriffen, unbefugtem Zugriff und Aktivitäten, Datenverlust, Unterbrechung von Diensten und Ausfallzeiten. Die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Servern ist entscheidend für den reibungslosen Betrieb von IT-Infrastrukturen und -Diensten. Serversicherheit wird unter anderem durch Betriebssystem-Härtung, Firewalls und VPN-Verbindungen erhöht.

3.1.1.7 Website Security

Website Security umfasst Maßnahmen, Verfahren und Technologien zum Schutz von Websites vor Cyberbedrohungen. Dazu gehört der Schutz von Daten, die Verhinderung unbefugter Zugriffe und die Gewährleistung der Verfügbarkeit der Website. Sicherheitszertifikate und die Verwendung von Sicherheits-Headern sind gängige Maßnahmen, um einen bestmöglichen Schutz zu gewährleisten.

3.1.2 Personal Digital Security

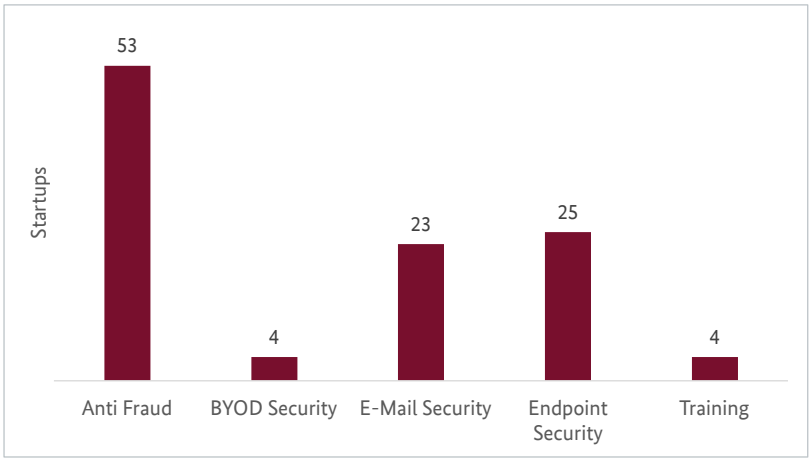

***Abbildung 6**: Verteilung der Subcluster – Cluster Personal Digital Security*

Personal Digital Security ist ein vielschichtiger Ansatz, der darauf abzielt, einzelne Nutzer vor Cyberbedrohungen auf verschiedenen digitalen Plattformen zu schützen. Dazu gehören der Schutz der E-Mail-Kommunikation (E-Mail Security), die Verwaltung des sicheren Zugriffs auf persönliche Geräte (BYOD Security), die Sicherung von Endgeräten (Endpoint Security) die Ausstattung von Einzelpersonen mit einem robusten Identitätsmanagement und die Aufklärung von Nutzern über Vorkehrungen zur Betrugsbekämpfung (Anti-Fraud) sowie Cybersicherheitstrainings. Dieser umfassende Ansatz sorgt für ein sicheres digitales Nutzererlebnis und mindert das Risiko von Datenschutzverstößen. Neben der Beschreibung zeigt **Abbildung 6** die Aufgliederung des Clusters Personal Digital Security in seine Subcluster und deren Größe. Mit 53 Startups enthält der Subcluster Anti-Fraud fast die Hälfte der Startups im Cluster Personal Digital Security. Email Security mit 23 und Endpoint Security mit 25 Startups sind mittelgroße Subcluster, während BYOD Security und Training jeweils nur vier Startups enthalten. Die Subcluster werden im Folgenden detailliert beschrieben.

3.1.2.1 Anti-Fraud

Anti-Fraud bezeichnet die Strategien, Maßnahmen und Technologien, die zur Verhinderung, Aufdeckung und Bekämpfung von betrügerischen Handlungen eingesetzt werden. Betrug kann viele Formen annehmen, darunter Finanzbetrug, Identitätsdiebstahl, Phishing, Insiderbetrug und Cyberbetrug. So sollen Schäden verhindert werden durch die Einführung interner Kontrollen, Schulungen von Mitarbeitern und Einsatz technischer Lösungen, die von Verhaltensanalysen über Lösungen zur Identitätsüberprüfung bis hin zu Betrugspräventions-, Aufdeckungs- und Reaktionssystemen reichen.

3.1.2.2 BYOD Security

BYOD (Bring Your Own Device) Security bezieht sich auf die von Mitarbeitern am Arbeitsplatz genutzten privaten Geräte wie Laptops, Smartphones und Tablets. BYOD bietet zwar zahlreiche Vorteile wie erhöhte Flexibilität, Produktivität und Kosteneinsparungen, birgt aber auch erhebliche Sicherheitsrisiken. Diese Risiken können z. B. durch den Einsatz von Mobile Device Management (MDM)-Lösungen, die Einrichtung von VPN-Verbindungen und Mitarbeiterschulungen gemindert werden.

3.1.2.3 Email Security

Email Security bezieht sich auf Maßnahmen, Verfahren und Technologien zum Schutz der E-Mail-Kommunikation vor verschiedenen Bedrohungen und unbefugtem Zugriff. Da die E-Mail ein primäres Kommunikationsmittel ist, ist ihre Sicherheit von entscheidender Bedeutung, um Datenlecks, Phishing-Angriffe, Infektionen mit Schadsoftware und andere Bedrohungen durch E-Mail-Verschlüsselungslösungen und Anti-Spam-Systeme zu verhindern.

3.1.2.4 Endpoint Security

Endpoint Security bezieht sich auf Maßnahmen, Verfahren und Technologien zum Schutz von Endpunkten oder Endgeräten wie Desktops, Laptops, Smartphones und Tablets, die mit einem Netzwerk verbunden sind. Da diese Geräte häufig Ziel von Cyberangriffen sind, ist ihre Sicherheit entscheidend für den Schutz der gesamten IT-Infrastruktur eines Unternehmens. Dieser Schutz kann unter anderem durch Anti-Viren- und Anti-Malware-Software, Endpunkt-Erkennung und -Reaktion, sowie Firewall- und Intrusion-Präventionssysteme gewährleistet werden.

3.1.2.5 Training

Training umfasst Maßnahmen, Programme und Kurse, die darauf abzielen, Mitarbeiter und Nutzer über Sicherheitsbedrohungen aufzuklären und ihnen die Fähigkeiten und Kenntnisse zu vermitteln, diese Bedrohungen zu erkennen und selbst abzuwehren. Sensibilisierung von Mitarbeitern durch IT-Sicherheitskampagnen oder Anti-Phishing-Kampagnen kann Teil dieser Maßnahme sein.

3.1.3 Analytics

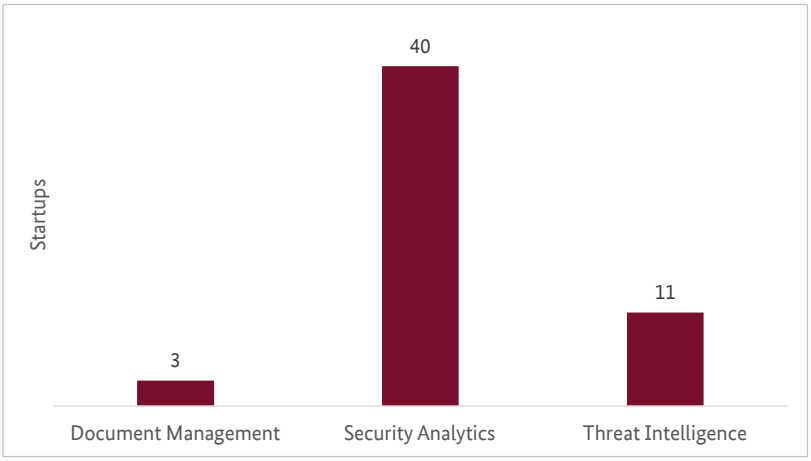

Abbildung 7: *Verteilung der Subcluster – Cluster Analytics*

Der Bereich Analytics umfasst den Einsatz modernster Technologien und Datenanalysen, um Cyberbedrohungen zu erkennen, sich vor solchen zu schützen und darauf zu reagieren. Bei diesem Ansatz werden Bedrohungsdaten mit virtuellen Cyberübungen kombiniert, Marktplätze von Anbietern von Tools und Dienstleistungen genutzt und widerstandsfähige Systeme zum Dokumentenmanagement eingesetzt, um umfassende und vorausschauende Cyberabwehrstrategien zu entwickeln. Mit diesem Ansatz können Unternehmen besser auf Sicherheitsverletzungen reagieren und künftige Schwachstellen effektiv mindern. Unsere Analyse identifizierte innerhalb des Analytics Cluster die folgenden Subcluster: Document Management, Security Analytics und Threat Intelligence.

Der Cluster Analytics ist mit 54 Startups der kleinste aller Cluster. Wie in **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellt, fallen die meisten Startups, genauer gesagt 40, in den Subcluster Security Analytics, der damit der größte Subcluster von Analytics ist. Die beiden verbleibenden Subcluster sind Threat Intelligence mit elf und Document Management mit drei Startups. Dies unterstreicht die Größe des Subclusters Security Analytics, da dieser mehr Startups enthält als die beiden anderen Subcluster in Summe. Eine Beschreibung der Subcluster findet sich im folgenden Abschnitt.

3.1.3.1 Document Management

Document Management bezieht sich auf Richtlinien, Verfahren und Technologien zum Schutz sensibler Informationen innerhalb eines Dokumentenmanagementsystems (DMS). Dazu gehört sicherzustellen, dass nur autorisierte Benutzer auf die Dokumente zugreifen können, dass kein unberechtigter Zugriff erfolgen kann und dass die Integrität und Vertraulichkeit der Dokumente über ihren gesamten Lebenszyklus gewährleistet ist. Diese Festlegung von Zugriffsrechten, Workflows und Prüfpfaden stellt ein geeignetes System für die sichere Bereitstellung und Verarbeitung von Daten sicher.

3.1.3.2 Security Analytics

Security Analytics bezieht sich auf die systematische Untersuchung und Bewertung von Sicherheitsereignissen und -vorfällen. Sie zielt darauf ab, die Fähigkeit einer Organisation, Sicherheitsbedrohungen zu erkennen, darauf zu reagieren und solche zu verhindern, zu verbessern. Dabei werden verschiedene Techniken und Tools zur Analyse sicherheitsbezogener Daten eingesetzt mit dem Ziel, Muster, Trends und Anomalien zu erkennen, die potenzielle Sicherheitsbedrohungen oder -verletzungen anzeigen können. Geeignete Maßnahmen sind beispielsweise SIEM (Security Information & Event Management) oder der Betrieb eines Zentrums für Sicherheitsmaßnahmen (kurz SOC für Security Operation Centre).

3.1.3.3 Threat Intelligence

Threat Intelligence bezeichnet die Sammlung, Analyse und Interpretation von Informationen über aktuelle und potenzielle Bedrohungen für die IT-Sicherheit eines Unternehmens. Das Hauptmerkmal von Threat Intelligence ist die Fähigkeit, Rohdaten in verwertbare Erkenntnisse umzuwandeln, die es Unternehmen ermöglichen, Bedrohungen vorherzusehen und aufzuspüren sowie proaktive und fundierte Entscheidungen zu treffen und wirksamer auf auftretende Bedrohungen reagieren zu können. Maßnahmen wie Datenanalyse, Echtzeitüberwachung und Schwachstellenanalyse können bei der Umsetzung von Threat Intelligence helfen.

3.1.4 OT & Application Security

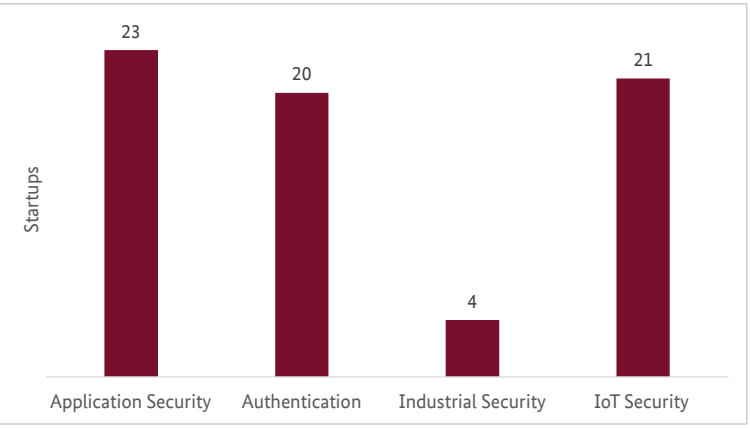

***Abbildung 8**: Verteilung der Subcluster – Cluster OT & Application Security*

Das vierte identifizierte Cluster ist Operational Technology & Application kurz OT & Application Security), welches sich auf Software und Hardware zum Schutz aller Geräte, Personen und Systeme bezieht, die für die Durchführung von Prozessen erforderlich sind. Dieser Cluster beschränkt sich nicht nur auf physische Geräte, die für die Wertschöpfung in einer Organisation erforderlich sind, sondern umfasst auch eine Vielzahl digitaler Berührungspunkte. Die Sicherheit der Schnittstellen zwischen mehreren digitalen oder zusätzlichen physischen Punkten im System ist in diesem Cluster von besonderem Interesse, da Organisationen auf effiziente und sichere Abläufe in ihrem internen und externen Netzwerk angewiesen sind. Zu den Schwerpunktbereichen innerhalb des OT & Application Security Clusters gehören Authentication, IoT-Sicherheit, Application Security und Industrial Security. OT & Application Security spielt eine fundamentale Rolle für die Widerstandsfähigkeit und Kontinuität sowie beim Schutz von Informationen, Aufrechterhaltung der Vertraulichkeit und Sicherstellung der Integrität von Systemen.

Abbildung 8 zeigt die Verteilung der Startups innerhalb des OT & Application Security-Clusters. Der Subcluster Industrial Security ist der kleinste Subcluster und umfasst insgesamt nur vier Startups. Im Vergleich dazu sind die übrigen drei Subcluster jeweils ähnlich groß. Application Security ist mit 23 Startups der größte der drei Subcluster, gefolgt von IoT Security mit 21 und Authentication mit 20 Startups. Interessanterweise ist der OT & Application Security Cluster der Einzige, der keinen größenmäßig herausstechenden Subcluster enthält. Die Subcluster werden im Folgenden detailliert beschrieben.

3.1.4.1 Application Security

Application Security bezieht sich auf Maßnahmen, Verfahren und Technologien, die darauf abzielen, die Vertraulichkeit, Integrität und Verfügbarkeit sowohl der Softwareanwendung selbst als auch der von ihr verwalteten Daten zu wahren. Da Anwendungen häufig als Einstiegspunkte für Angriffe dienen, ist es von entscheidender Bedeutung, Sicherheitsmaßnahmen in den gesamten Lebenszyklus von Anwendungen zu integrieren. Hohe Sicherheitsanforderungen während der Entwicklung (Sicherheit durch Design) sowie Codeanalysen, kontinuierliche Schwachstellenanalysen und die Bewertung der Sicherheit von Komponenten von Drittanbietern, die in die Anwendung integriert sind, tragen dazu bei, Anwendungen über ihren gesamten Lebenszyklus vor Bedrohungen und Schwachstellen zu schützen.

3.1.4.2 Authentication

Authentication bezeichnet Maßnahmen, Verfahren und Technologien, die die Identität von Benutzern, Geräten oder Systemen verifizieren und gleichzeitig vor unbefugtem Zugriff und Identitätsdiebstahl schützen sollen. Dies lässt sich beispielsweise mit Passwörtern, Smartcards und über biometrische Merkmale realisieren.

3.1.4.3 Industrial Security

Industrial Security bezeichnet Maßnahmen, Verfahren, Technologien und Strategien, die erforderlich sind, um industrielle Systeme, Anlagen und Prozesse vor Bedrohungen, Angriffen und Störungen zu schützen. Diese Sicherheitsdisziplin umfasst sowohl physische Sicherheit als auch Cyber-Sicherheit und ist für den Schutz kritischer Infrastrukturen von entscheidender Bedeutung. Die Sicherheit kann durch Netzwerksegmentierung, Verschlüsselung und Zugriffskontrollen gewährleistet werden.

3.1.4.4 IoT Security

Das Internet der Dinge (IoT)[1] bezeichnet ein Netzwerk miteinander verbundener Geräte, Sensoren und Maschinen, die Daten sammeln, austauschen und verarbeiten. Da IoT-Geräte zunehmend in verschiedenen Bereichen wie Smart Homes, Industrie 4.0, Gesundheitswesen und Smart Cities eingesetzt werden, gewinnt

[1] Im Deutschen existiert keine Abkürzung für „Internet der Dinge“, sodass im Rahmen dieser Studie auf die englische Abkürzung zurückgegriffen wird.

die Sicherheit dieser Geräte zunehmend an Bedeutung. Wichtige Sicherheitsmaßnahmen können die Implementierung von Zugriffskontrollmechanismen, die Verwendung sicherer Protokolle sowie fortlaufende Sicherheitsupdates und Patches umfassen.

3.2 Identifizierte Schlüsseltechnologien

Anhand der Liste mit 437 Startups und den von diesen offengelegten Produktinformationen (Produktbeschreibung und öffentliche Website-Informationen) haben wir sieben Schlüsseltechnologien identifiziert, die von den aufgeführten Startups in unterschiedlichem Maße genutzt werden. Dieses Kapitel widmet sich den Schlüsseltechnologien sowie deren Verknüpfung mit den Clustern und Subclustern.

3.2.1 Künstliche Intelligenz (KI) und maschinelles Lernen (ML)

Wir definieren den Begriff „Künstliche Intelligenz“ sowohl als Technologie als auch als wissenschaftliche Disziplin, die mehrere Ansätze und Techniken wie maschinelles Lernen, maschinelles Denken und Robotik umfasst. KI-Systeme sind Software- und Hardwaresysteme, die Künstliche Intelligenz nutzen, um sich in der physischen oder digitalen Dimension rational zu verhalten. Auf der Grundlage ihrer Wahrnehmung und Analyse ihrer Umgebung handeln diese Systeme mit einem gewissen Grad an Autonomie, um bestimmte Ziele zu erreichen.

3.2.2 Bilderkennung

Wir definieren Bilderkennung als die Fähigkeit von Software, Menschen, Objekte, Schriften und Bewegungen in digitalen Bildern zu identifizieren. Diese Technologie ermöglicht es Computern, Elemente zu erkennen und zu kategorisieren, was den ersten Schritt zum Verständnis von Bildern darstellt. Die Bilderkennung im Bereich der Bildverarbeitung wird in einer Vielzahl von Anwendungsfällen wie Fotobibliotheken, Gesichtserkennung und öffentlicher Überwachung, aber auch in einem industriellen Kontext wie der Qualitätskontrolle eingesetzt. Die Bilderkennung erfordert ein hohes Verständnis für kontextbezogenes Wissen und parallele Verarbeitung. Während die Leistung des Menschen bisher überlegen war, könnte die schnelle Entwicklung von KI diese Überlegenheit in Zukunft verringern.

3.2.3 Blockchain-Infrastruktur

Blockchain ist eine technische Lösung, um Daten aus zwischen Nutzern vereinbarten Transaktionen in einer verteilten Infrastruktur ohne zentrale Instanz transparent und fälschungssicher zu verwalten. Blockchain ermöglicht die vertrauenswürdige und transparente Überprüfung von Transaktionen (z. B. im Zahlungsverkehr mit Kryptowährungen) ohne zentrale Instanz. Der Name Blockchain leitet sich von der Art der Dokumentation ab: Blöcke von Datensätzen werden aneinandergereiht und miteinander verknüpft, um eine kontinuierlich wachsende Blockchain zu bilden. Alle Knoten im Netz einigen sich im Rahmen eines Konsensverfahrens auf einen einheitlichen Status der Blockchain. Kryptografische Mechanismen sorgen

unter anderem dafür, dass Daten, die einmal in der Blockchain gespeichert sind, praktisch nicht mehr verändert werden können.

3.2.4 Internet der Dinge (IoT)

Das Internet der Dinge (IoT) bezeichnet eine vernetzte Welt intelligenter Geräte. Diese IoT-Geräte verhalten sich wie Computer und sind über das Internet mit einem lokalen Netzwerk oder mit anderen Geräten verbunden. Sie sollen unseren Alltag einfacher, komfortabler und effizienter machen, indem sie beispielsweise die Temperatur und Helligkeit in einem Raum messen und eine ganze Reihe von Prozessen automatisieren, die auf diesen Informationen basieren. Sie können die gesammelten Daten auch durch andere hilfreiche Informationen ergänzen. Oft sendet das Gerät im Rahmen dieser Tätigkeit Daten an eine Cloud, wo sie verarbeitet und zur Verfügung gestellt werden oder als Grundlage für andere Dienste dienen.

3.2.5 Cloud-Technologie

Im Anschluss an den Cloud Computing Compliance Criteria Catalog (C5) definieren wir Cloud Computing als einen bedarfsgerechten Ansatz für die dynamische Bereitstellung, Nutzung und Abrechnung von IT-Services über ein Netzwerk. Diese Services werden ausschließlich über definierte technische Schnittstellen und Protokolle angeboten und genutzt. Wir erweitern diese Definition um die im Rahmen des Cloud Computing angebotenen Dienstleistungen auf das gesamte Spektrum der Informationstechnologie, darunter Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

3.2.6 Quantum Computing (Quantencomputing)

Die heutigen Computer verarbeiten Informationen nach den Gesetzen der klassischen Physik: Register und Speicherinhalte haben immer einen einzigen Wert. Dies gilt unabhängig davon, ob die Komponenten eines Computers, z. B. Transistoren, auf den Gesetzen der Quantenphysik beruhen. In einem Quantencomputer wird die Information selbst quantenmechanisch behandelt: Register und Speicherinhalte können mehrere Werte gleichzeitig in Überlappung enthalten, und Maschinenbefehle beeinflussen alle diese Werte gleichzeitig. Das bedeutet, dass selbst ein einzelner Quantenprozessor mit einem hohen Maß an intrinsischer Parallelität arbeitet, ohne dass parallelisierte Hardware wie mehrere Prozessorkerne erforderlich ist. Damit ist es prinzipiell möglich, eine Quantenbeschleunigung, auch Quantenüberlegenheit genannt, zu erreichen. Dies meint die Fähigkeit eines Quantencomputers, Berechnungen durchzuführen, deren Reproduktion für klassische Computer äußerst teuer ist.

3.2.7 Big Data

In Anlehnung an das NIST Big Data Interoperability Framework (Volume 1) bezeichnen wir Big Data als ein Unvermögen herkömmlicher Datenarchitekturen, die neuen Datensätze effizient zu verarbeiten. Merkmale von Big Data, die neue Architekturen erzwingen, sind das Volumen (d. h. die Größe des Datensatzes), die Vielfalt (d. h. Daten aus verschiedenen Repositorien, Domänen oder Typen), die Geschwindigkeit (d. h. die Flussrate) und die Variabilität (d. h. die Veränderung anderer Merkmale). Diese Merkmale – Volumen, Vielfalt, Geschwindigkeit und Variabilität – werden umgangssprachlich als Big Data „Vs" (abgeleitet von den englischen Begriffen) bezeichnet. Obwohl Big Data noch viele weitere V's zugeschrieben werden, sind nur die vier genannten Gründe ausschlaggebend für den Wechsel zu neuen, parallelen Architekturen für datenintensive Anwendungen. Dieser Wechsel erfolgt mit dem Ziel, eine aus Kostensicht effektivere Leistung zu erreichen. Diese Big-Data-Merkmale diktieren den Gesamtentwurf eines Big-Data-Systems, was mit dem Ziel des Erreichens der erforderlichen Effizienz zu unterschiedlichen Architekturen für Datensysteme oder unterschiedlichen Verfahrensordnungen im Lebenszyklus der Daten führt.

3.3 Beziehung zwischen Schlüsseltechnologien und Clustern

Wir haben die Startups auf Verweise zu Schlüsseltechnologien untersucht und konnten dabei die sieben in **Kapitel 3.2** eingeführten Technologien identifizieren**.** Wie in **Abbildung 9** dargestellt, können somit Beziehungen zwischen Schlüsseltechnologien und Clustern abgeleitet werden. Bezüglich unseres Datensatzes ist darauf hinzuweisen, dass wir keine Aussage zur genauen Nutzung von Technologien durch die Startups treffen können. Nicht alle Informationen zu bestimmten Technologieanwendungen sind bei Startups im Stealth Modus öffentlich verfügbar. Trotz dieser Einschränkungen gelang es uns, 585 Verweise auf verwendete Schlüsseltechnologien zu finden. Einige Startups berichten von der Nutzung mehrerer Technologien, während andere lediglich die Anwendung einer einzelnen oder keiner identifizierten Technologien angeben. Dennoch wurde jedes Cluster, Subcluster und Schlüsseltechnologie mindestens einmal erwähnt.

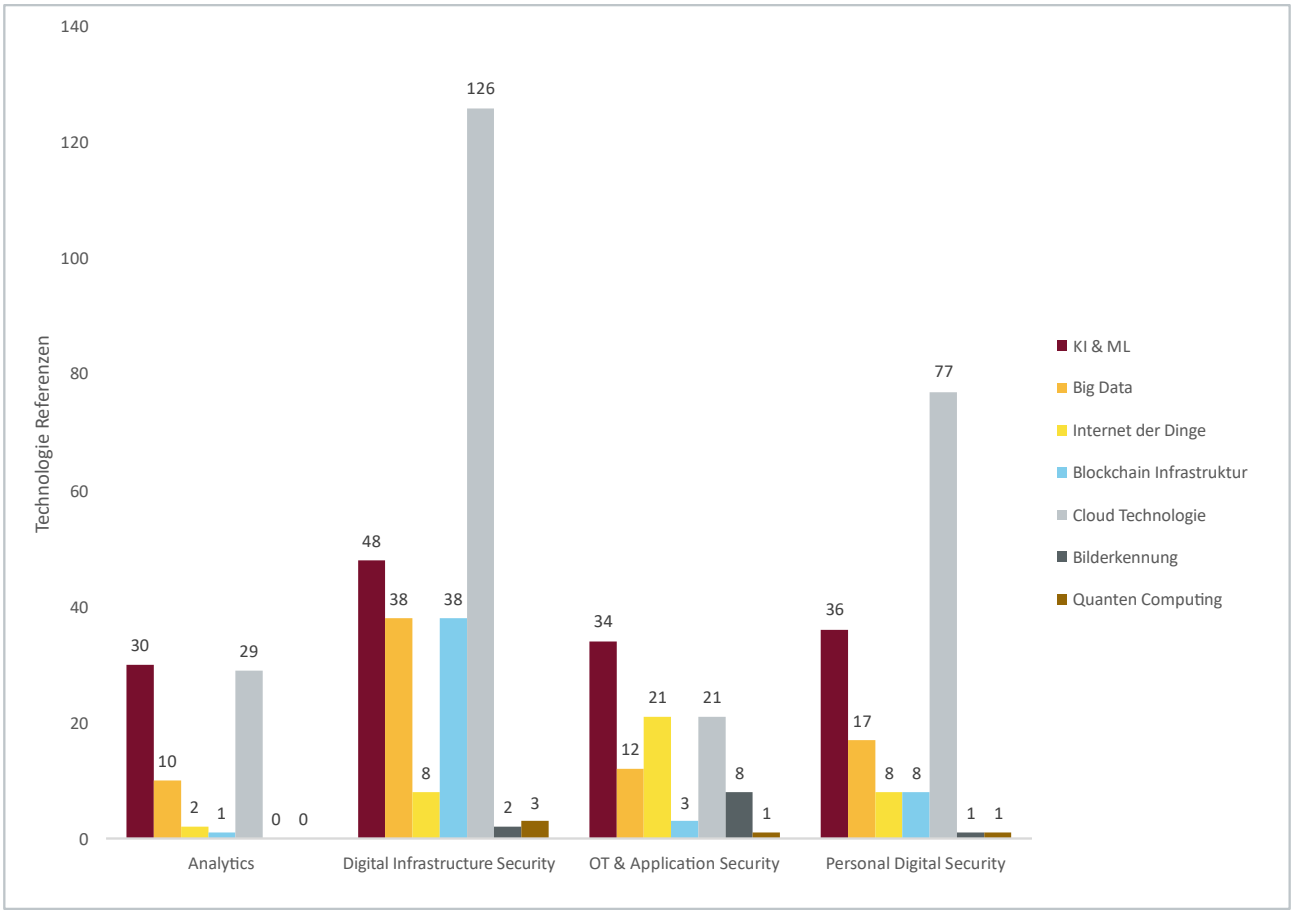

***Abbildung 9**: Technologie-Referenzen je Cluster*

Die am häufigsten genannte und in unserer Landscape genutzte Technologie ist die Cloud-Technologie. Da 58 % der Startups in unserem Umfeld den Einsatz dieser Technologie erwähnen, ist sie von wesentlicher Bedeutung für den Cybersicherheitssektor. Dies ist nachvollziehbar, da ein Großteil des Online-Datenverkehrs über Cloud-Dienste abgewickelt wird oder mit ihnen in Verbindung steht. Dieser Hypothese folgend, wird die Cloud-Technologie in 72 % der Startups im Cluster Personal Digital Security erwähnt, und entspricht somit der höchsten Referenzquote einer Technologie über alle Cluster hinweg. Grund für diese Vormacht ist unserer Ansicht nach die zunehmende Menge an Cloud-basierten Verbraucherdiensten, da der Schutz personenbezogener Daten in diesem Bereich mittlerweile eine Grundanforderung darstellt.

Die nach der Cloud-Technologie am zweithäufigsten genutzte Technologie ist die Künstliche Intelligenz und das Maschinelle Lernen, die von 34 % der Startups genannt wird. Den höchsten Anteil hier hält der Analytics Cluster, in dem 56 % der Startups angeben, KI zu nutzen. Dies ist nicht überraschend, da sich die Technologie für viele analytische Anwendungsfälle eignet und den großen Vorteil bietet, große Datenmengen verarbeiten zu können und daraus aussagekräftige Erkenntnisse zu gewinnen. Tatsächlich hat der Security Analytics-Subcluster die höchste Referenz aller Subcluster, mit 26 Erwähnungen der Technologie – 65 % der Startups dieses Subclusters verweisen auf diese Technologie.

Nach Künstlicher Intelligenz und Cloud-Technologie rangiert Big Data mit insgesamt 18 % an dritter Stelle der am häufigsten genannten Technologien in unserer Studie. In den meisten Subclustern wird Big Data von

33 % genannt, mit Ausnahme des Subclusters Database. Hier erwähnen 75 % den Einsatz von Big Data, aber mit einer Subclustergröße von nur vier Startups und einem thematischen Match ist dieser Ausreißer sehr einfach zu erklären. Der Subcluster mit den meisten Erwähnungen von Big Data insgesamt ist der Subcluster Data Security mit 22 Erwähnungen, was 22 % der Startups in diesem Subcluster entspricht.

Überraschenderweise liegt die Zahl der Verweise auf die Blockchain-Infrastruktur bei 11 % in der gesamten Landscape. Angesichts des Hypes um die Technologie in den späten 2010er Jahren hätte man erwarten können, dass diese in der Bay Area stärker vertreten ist. Wir vermuten, dass der Cybersicherheitsaspekt der Technologie noch nicht vollständig erkannt worden ist. Die meisten Verweise gibt es mit Nennungen durch 38 Startups im Cluster Digital Infrastructure Security. Dies unterstreicht die Ambitionen der Blockchain-Technologie als künftiger Infrastrukturanbieter für das Web3-Zeitalter. Die häufigsten Nennungen erfolgten im Subcluster Data Security mit 18 und Blockchain Security mit 15 Nennungen. Angesichts der Tatsache, dass Blockchains fälschungssichere Daten für Transaktionen versprechen, ist dies keine Überraschung und unterstreicht die Ambitionen der Blockchain-Technologie, in Zukunft eine Kerntechnologie zu werden.

Insgesamt erwähnen 9 % der Startups die Verwendung des Internets der Dinge (IoT) in ihren Lösungen. Ähnlich wie bei Blockchain haben wir es hier mit einer vergleichsweise selten im Cluster genutzten Technologie zu tun, die vor allem im Cluster OT & Application Security zum Einsatz kommt, wo insgesamt 21 Startups – das sind 30 % des Clusters – sie nutzen. Wir glauben, dass die Einführung dieser Lösung mit einer höheren Entwicklungsrate der Hardwarelösung in diesem Cluster zusammenhängt. Unsere Daten erlauben es uns jedoch nicht, dies schlüssig zu beweisen.

Die am wenigsten erwähnten Technologien in der Startup-Landscape sind schließlich die Bilderkennung mit 3 % und das Quantencomputing mit 1 %. Die Bilderkennung ist im Cluster OT & Application Security am beliebtesten, da sie fast ausschließlich im Subcluster Authentication eingesetzt wird. Mit Gesichtserkennung und Netzhautscans erfüllt die Technologie diesen Zweck, wird aber von den in unserer Liste geführten Startups nicht großflächig genutzt. Aufgrund der begrenzten Erwähnung von nur fünf Startups, die Quantencomputing nutzen, können wir kein klares Muster von Anwendungsfällen oder Vorteilen ableiten, die diese Technologie einem Cluster oder Subcluster bietet. Unsere Untersuchung hat ergeben, dass die geringe Zahl der Nennungen darauf zurückzuführen ist, dass es sich um die am wenigsten ausgereifte Technologie mit potentiellen zukünftigen Anwendungsmöglichkeiten handelt.

4 Cyber Startup Landscape

Wie bereits in der Einleitung ausgeführt, hat die wachsende Anzahl von größtenteils digitalen Bedrohungen, Unternehmen und Regierungen dazu gezwungen, ihre IT-Infrastrukturen zu verbessern. In der Folge entstanden mehr als 400 Startups in der Bay Area, in denen bahnbrechende Technologien entwickelt werden und welche in hohem Maße attraktiv für Risikokapitalgeber sind. **Kapitel 4** beleuchtet diese Startups näher, mit dem Ziel einen kurzen Überblick über die gesamte Cyber Startup Landscape der Bay Area, einschließlich der geografischen Streuung der Startups, zu vermitteln.

4.1 Cyber Startup Landscape

In diesem Kapitel wird die gesamte Cyber Startup Landscape in der Bay Area dargestellt. Ausgehend von einer Liste aller 437 Unternehmen wurden auf der Grundlage öffentlich verfügbarer Informationen (z. B. Produktbeschreibungen, Website-Daten, Startup-Datenbanken) Cluster für bestimmte Anwendungsfälle gebildet, um den Markt zunächst zu segmentieren. Diese Segmentierung soll einen besseren Überblick über bestimmte Technologietrends und finanzielle Zuwendungen, d. h. Risikokapitalfinanzierung, vermitteln. Die tragenden Säulen dieser Studie sind die vier Hauptcluster, denen die Startups zugewiesen werden. Aufgrund der sehr umfangreichen Liste von Startups in dieser Landscape erfolgte zur weiteren Kategorisierung der Unternehmen die Aufsplittung der Hauptcluster in weitere Subcluster. Mittels des in **Kapitel 2.2.2** beschriebenen Prozesses wurden die 44 betrachteten Startups, einschließlich der jeweiligen Marken (siehe **Abbildung 10**), aus der Gesamtheit von 437 Startups ausgewählt, da die in Summe mehr als 400 Logos zu viel für eine einzige Seite gewesen wären.

Cyber Startup Landscape Bay Area

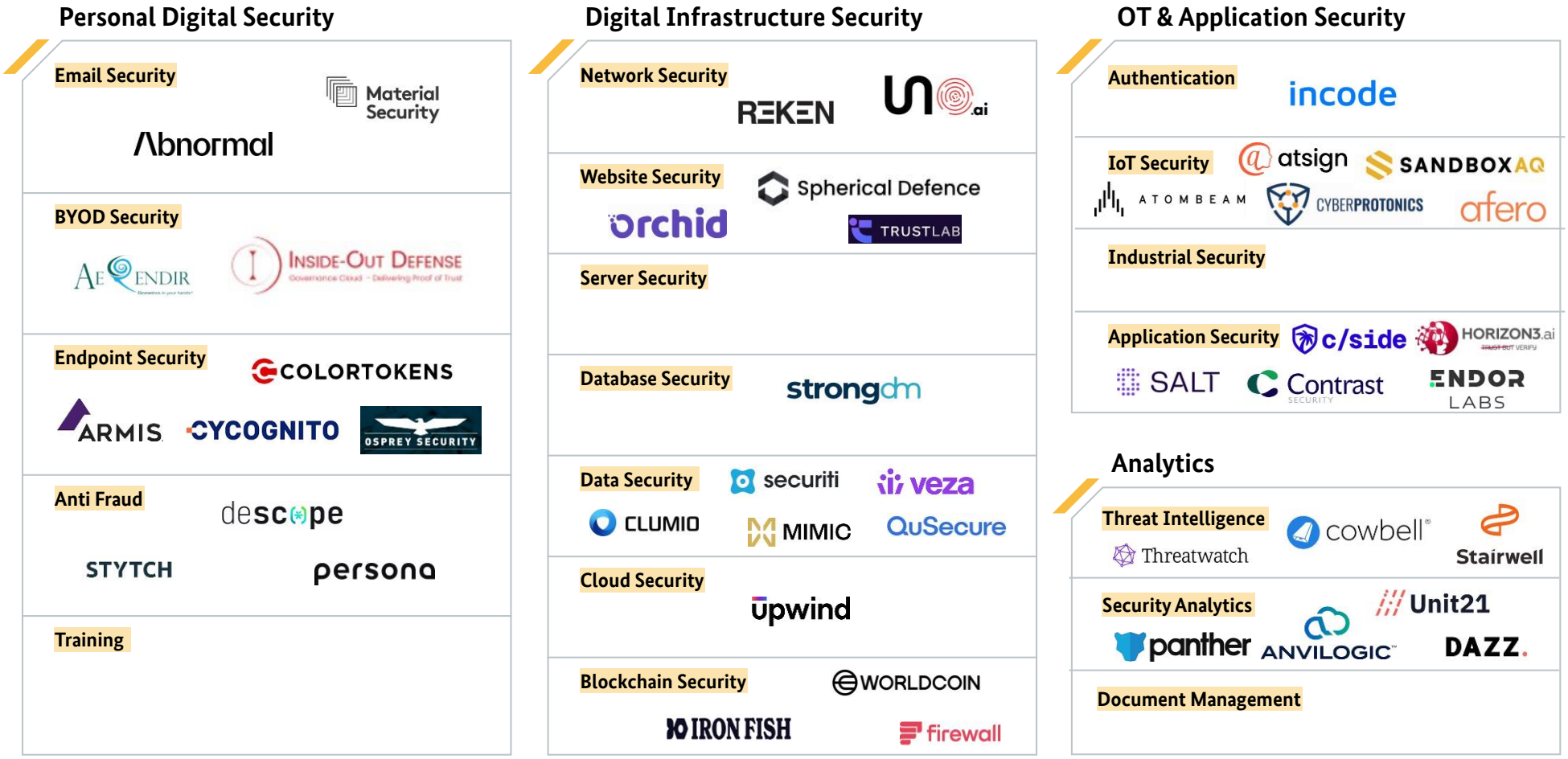

***Abbildung 10**: Cyber Startup Landscape - Bay Area, Quelle der Logos: Hersteller-Webseiten*

4.2 Lage in der Bay Area

Neben der allgemeinen thematischen Analyse wurde auch eine bemerkenswerte geografische Verteilung von Startup-Hauptsitzen festgestellt. In der gesamten Bay Area können wir einen Fokus auf San Francisco County mit 182 Startups und Santa Clara County mit 180 Startups beobachten. Insgesamt finden sich somit in diesen beiden Counties 83 % der in unserer Landscape angesiedelten Startup-Zentralen. Dieser Trend kann vor allem durch die hohe Bevölkerungsdichte in diesen Counties und ihre Nähe zu Hightech-Unternehmen, Universitäten und anderen Akteuren im Ökosystem erklärt werden. Darüber hinaus machen potenzielle Kunden und kurze Wege zu den Zulieferern diese beiden Counties zu einer beliebten Wahl für die Ansiedlung der Zentralen innovativer Startups, was unsere Datenerhebung einmal mehr belegt.

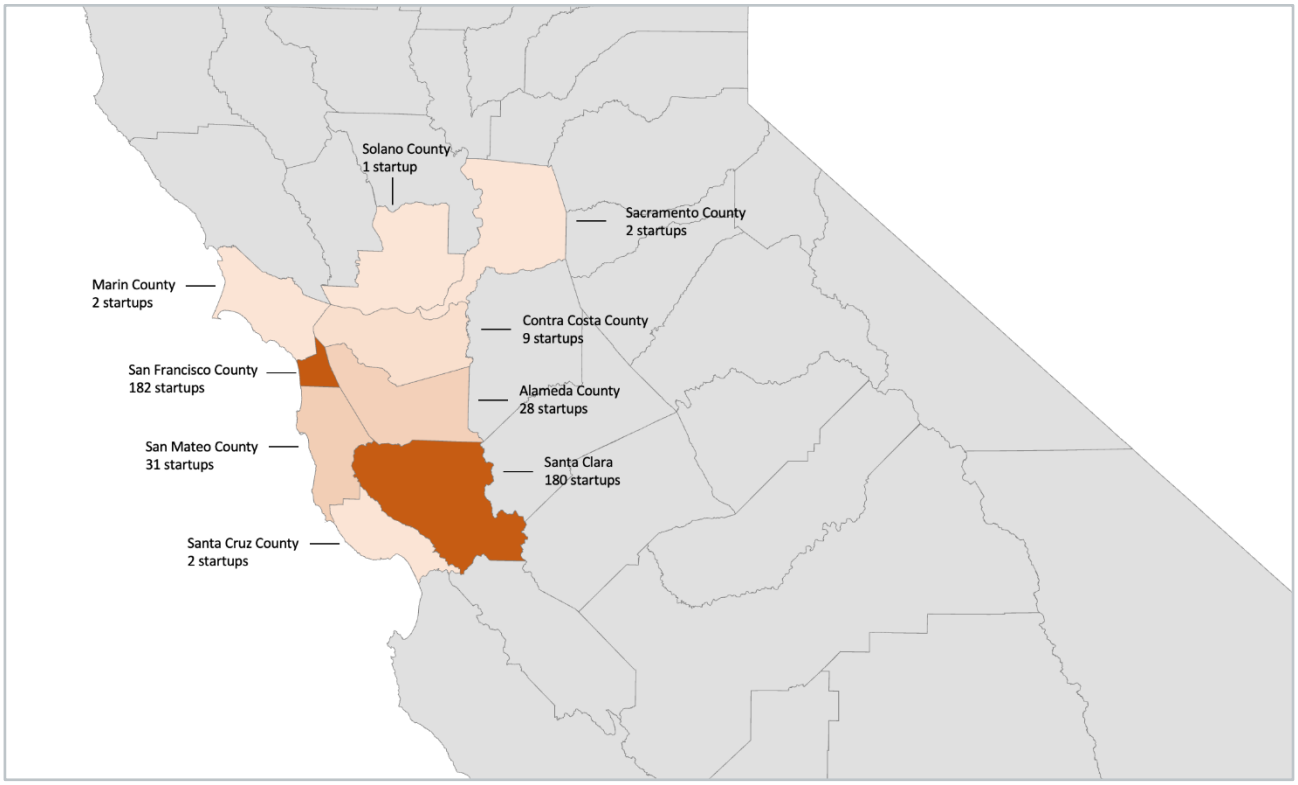

***Abbildung 11**: Bay Area Heatmap – Hauptsitz oder Bürostandort der Startups*

5 Landscape-Analyse

In diesem Kapitel möchten wir die Cluster im Hinblick auf ihre Größe, ihre Finanzierung und, im Rahmen unserer Analyse herausgearbeiteten, auffälligen statistischen Merkmale beleuchten. Wir beginnen mit einer allgemeinen Charakterisierung der Bay Area, bevor wir den Prozess der Analyse innerhalb der in **Kapitel 3** abgeleiteten Struktur der Cluster und Subcluster wiederholen.

5.1 Allgemeiner Überblick über Startups in der Bay Area

Die Bay Area bietet einen einzigartigen Hintergrund für Startups und ein Ökosystem, in dem diese gedeihen können. Unsere Landscape enthält daher Hunderte von potenziellen neuen Unternehmen, von denen wir annehmen, dass sie den Cybersicherheitsbereich in verschiedenen Bereichen beeinflussen werden. Bevor wir die einzelnen Cluster im Detail analysieren, möchten wir die allgemeinen Trends und Gegebenheiten darlegen. Dies beinhaltet den Trend bei den Neugründungen und Investitionen sowie die lokale Streuung in der Region. Basierend auf den in **Kapitel 2** dargestellten Kriterien haben wir 437 Startups identifiziert, die bis heute aktiv sind. Der 10-Jahres-Beobachtungszeitraum ermöglicht uns eine stärkere Eingrenzung des Zeitraums, in dem sich die aktuelle Landscape entwickelt hat. Das Balkendiagramm in Fehler! Verweisquelle konnte nicht gefunden werden. zeigt dabei die jährliche Anzahl der neu gegründeten Cyber-Startups in der Bay Area (rot hervorgehoben) im Vergleich zu den entsprechenden weltweiten Zahlen.[2]

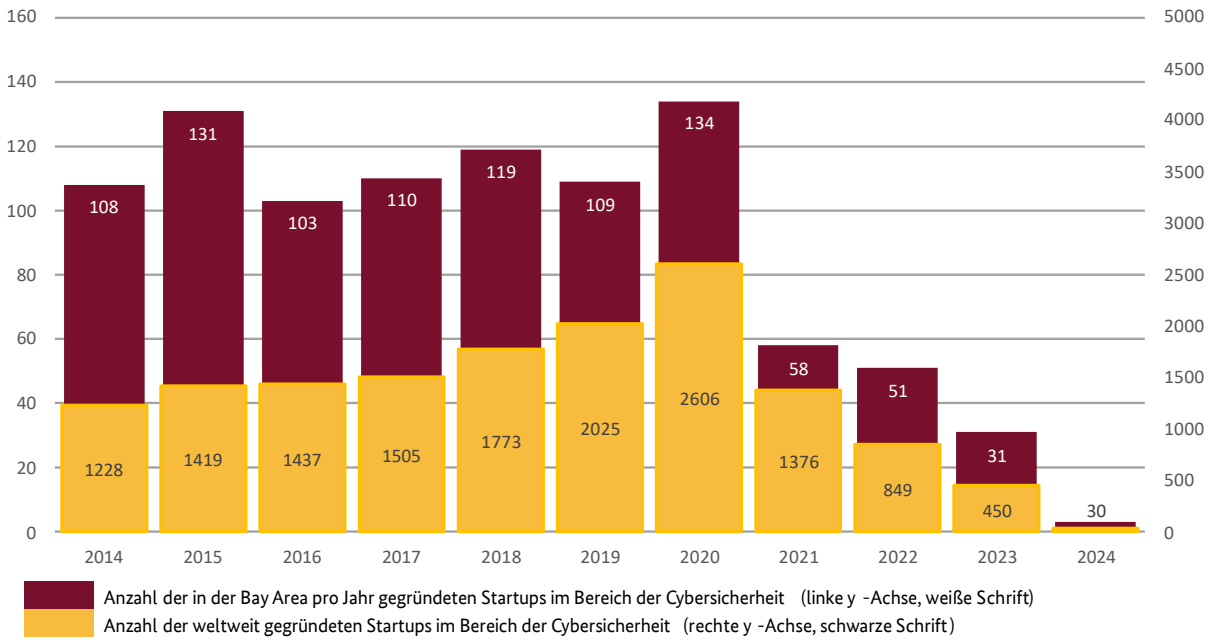

***Abbildung 12**: Marktentwicklung der Startups*[3]

[2] Der Vergleich erfolgt auf globaler Ebene, wobei 140 Länder (siehe **Anlage 4**) mit mindestens einem Startup im Bereich Cybersicherheit ermittelt wurden.

[3] 2024: Bay Area: Drei Startups; Weltweit: 30 Startups

Während sich die Zahl der Neugründungen in der Bay Area zwischen 2014 und 2019 nicht wesentlich änderte, erreichte sie 2020 ihren Höhepunkt und ging mit 58 Neugründungen im Jahr 2021 stark zurück. Seitdem ist die Zahl der neu gegründeten Cyber-Startups stetig zurückgegangen und könnte im Jahr 2024 einen neuen Tiefstand erreichen. Die globale Entwicklung zeigte einen ähnlichen Trend, einschließlich eines starken Rückgangs im Jahr 2021. Dies lässt den Schluss zu, dass die Entwicklung der Neugründungen im Vergleich mit den globalen Zahlen nicht durch den Standort Bay Area beeinflusst wurde. Es ist jedoch zu beachten, dass die Grafik nur die Zahl der neu gegründeten Startups umfasst, von denen einige mittlerweile erfolgreiche Exits vorgenommen oder ihr Geschäft aufgegeben haben. Erfolgsquoten oder ähnliche Faktoren im Hinblick auf die zukünftige Entwicklung eines Unternehmens werden also nicht berücksichtigt. Ein wichtiger Faktor, der den Erfolg von Startups beeinflusst, ist die Verfügbarkeit von Risikokapital zur Finanzierung der technologischen Entwicklung. Dies wird durch die in Abbildung 13 hervorgehobenen Investitionen pro Förderstufe und der Gesamtzahl der durchgeführten Investitionsrunden verdeutlicht.

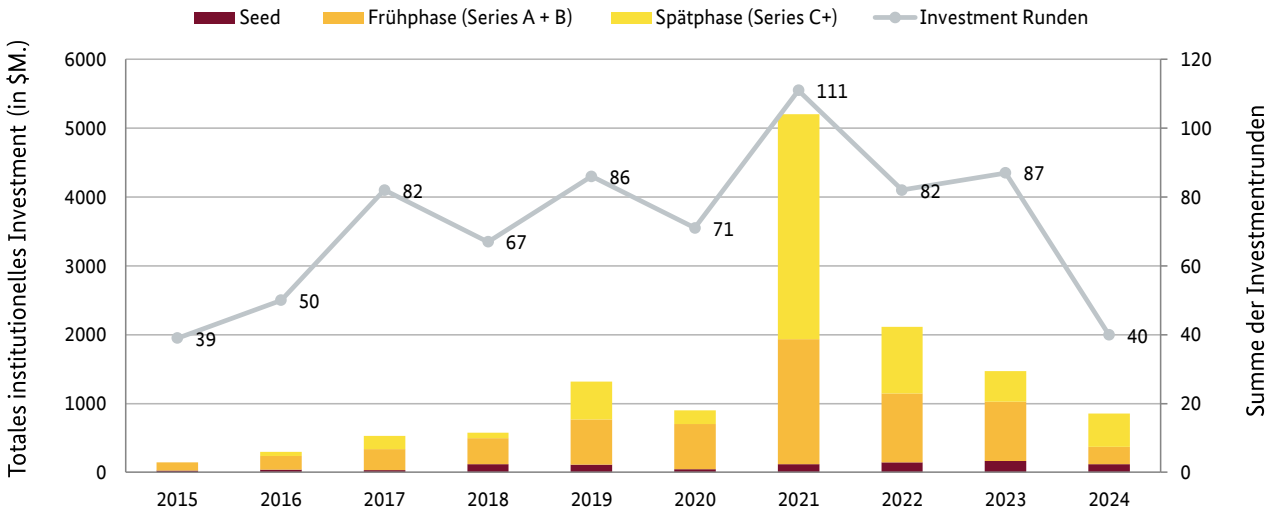

***Abbildung 13**: Trend bei Startup-Investitionen nach Phase*

Während bis zum Jahr 2019 ein allgemeiner Aufwärtstrend für das gesamte Investitionskapital beobachtet werden kann, kam es im Jahr 2020 vermutlich aufgrund der Pandemiesituation zu einem kurzfristigen Rückgang auf rund Mio. USD 902 und 71 Finanzierungsrunden. Das Jahr 2021 zeigt jedoch eine rasante Trendwende mit einem fast sechsmal so hohen Investitionsvolumen von rund Mrd. USD 5,2 und 111 Finanzierungsrunden. Wie bei den in **Fehler! Verweisquelle konnte nicht gefunden werden.** gezeigten Neugründungen sind die Gesamtinvestitionen und Finanzierungsrunden seither stetig zurückgegangen.

Wie **Abbildung 13** zeigt, verzeichnet das Jahr 2021 das höchste Investitionsvolumen für Tech-Startups in der Bay Area. Unsere Untersuchung identifizierte mehrere mögliche Faktoren für diese Entwicklung. Zum einen hat die COVID-19-Pandemie dazu geführt, dass viele physische Räume wie Büros, Schulen oder Gemeinschaftsplattformen durch Online-Kommunikation ersetzt wurden. Dies verstärkte den Bedarf an Cybersicherheitslösungen, was gleichzeitig mehr Investoren anlockte und das Wachstum des Cybersicherheitsmarktes unterstrich. Darüber hinaus war das Jahr 2021 durch niedrige Zinssätze

gekennzeichnet, um die Wirtschaft nach der Covid-19-Pandemie zu stützen. Dadurch wurden zusätzliche Mittel freigesetzt, was eine mögliche Erklärung für den starken Anstieg der Investitionen im Jahr 2021 darstellt. Obwohl diese Hypothesen vernünftig erscheinen, möchten wir darauf hinweisen, dass unsere Forschung diese Zusammenhänge nicht nachweisen kann. Darüber hinaus haben wir eine Analyse der am höchsten dotierten Finanzierungsrunden für unseren Datensatz durchgeführt und mehrere große Finanzierungsrunden einzelner Startups identifiziert, die zusätzlich zum Investitionsboom im Jahr 2021 beigetragen haben. **Abbildung 14** zeigt die zehn größten Finanzierungsrunden in unserem Beobachtungszeitraum. Sechs Finanzierungsrunden fanden im Jahr 2021 statt, wobei es sich durchweg um Investitionen in der Spätphase handelte (Serie C oder höher). Dies unterstreicht die Verfügbarkeit von Investitionsmitteln zu diesem Zeitpunkt. Darüber hinaus hat ein einzelnes Startup, *Lacework,* im Jahr 2021 rund ein Drittel aller Mittel gewonnen. Im Rahmen einer Finanzierungsrunde der Serien D und D+ erhielt *Lacework* insgesamt Mrd. USD 1,825. Zum Vergleich: Diese Finanzierung allein hätte die Gesamtinvestitionen in jedem einzelnen Jahr im Beobachtungszeitraum 2015 bis 2024 übertroffen.

Finanzierungsrunde	Startup	Series	Finanzierung in $
18.11.2021	Lacework	Serie D	1,300.000.000
7.1.2021	Lacework	Serie D	525.000.000
14.2.2023	SandboxAQ	Serie A	500.000.000
29.11.2021	Armis Security	Serie D	300.000.000
14.1.2019	Rubrik	Serie E	261.000.000
7.12.2021	Incode	Serie B	220.000.000
7.3.2022	Abnormal Security	Serie C	210.000.000
8.9.2021	Aviatrix	Serie E	200.000.000
28.4.2017	Rubrik	Serie D	180.000.000
15.9.2021	Persona	Serie C	150.000.000

***Abbildung 14**: Wichtige Finanzierungsrunden*

Für unsere Startup Landscape und die anschließende Analyse ist es wichtig zu berücksichtigen, dass dieser Bereich bereits erhebliche Fördermittel erhalten hat. Dies garantiert nicht die Reife aller Subcluster, die wir antreffen, aber im Allgemeinen ist die Bay Area wahrscheinlich die Heimat sowohl etablierter Akteure, die auf einen erfolgreichen Ausstieg hinarbeiten, als auch von Newcomern, die diese Region bewusst gewählt haben, um dieselbe Art von Investitionen anzuziehen.

5.2 Clusteranalyse

Nach der bereits erfolgten allgemeinen Analyse der Landscape beschäftigt sich dieses Kapitel detaillierter mit den in **Kapitel 3** eingeführten Clustern und Subclustern. Die Analyse folgt dabei derselben Struktur und hebt verschiedene statistische Anomalien mit Hypothesen für ihr Auftreten hervor. Im Anschluss an die aktuelle Analyse geben wir einen Ausblick, in welchem Maße die Startups der jeweiligen Subcluster zukünftige Auswirkungen auf die Cybersicherheit haben könnten.

5.2.1 Digital Infrastructure Security

Die Startup-Landscape für die Sicherheit digitaler Infrastrukturen erfährt derzeit eine erhebliche Expansion und umfasst ein breites Spektrum an Startups, die sich auf Bereiche wie Netzwerksicherheit, sichere Cloud-Infrastrukturen, Datenverschlüsselung sowie Identity and Access Management spezialisiert haben. Der Cluster zeichnet sich durch eine hohe Aktivitätsrate und eine durchschnittliche Investition von Mio. USD 14 je Startup aus – dies entspricht dem niedrigsten Wert aller Hauptcluster. Es ist bei weitem der Cluster mit den meisten aktiven Startups von zum Zeitpunkt unserer Datenerhebung 206 Unternehmen in Summe. Hinzu kommen 67 Exits durch Übernahmen oder Börsengänge und 92 Startups, die ihre Geschäftstätigkeit aufgegeben haben, sodass der Cluster insgesamt 365 Startups umfasst. Startups, die sich mit der Sicherheit digitaler Infrastrukturen beschäftigen, ziehen weltweit beträchtliche Investitionsmittel an. Mehrere Risikokapitalgeber und Investoren haben aufgrund des innovativen Potenzials und der Bedeutung in der heutigen digitalen Welt Interesse an diesem Cluster gezeigt, wobei Risikokapitalgeber aus den USA deutlich dominieren. Dieser Investitionstrend unterstreicht die wachsende globale Bedeutung des Sektors und dessen Fähigkeit, Finanzmittel anzuziehen.

Digital Infrastructure Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
365	206	67	92

Neu gegründete Startups:
(in 2023 - 2024)
16

Gesamtinvestment:
$2.89 Milliarden

Durchschnittliche Investition pro aktivem Startup:
$14 Million

Jüngste Finanzierungsrunden:
Mimic ($25.2 M, 2.5.2024, Seed)
Elisity ($41.9 M, 29.4.2024, Series B)
StrongDM ($37.8 M, 22.4.2024, Series C)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
126	48	38

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
38	8	2	3

***Abbildung 15**: Cluster Digital Infrastructure Security*

5.2.1.1 Network Security

***Abbildung 16**: Subcluster Network Security*

Mit insgesamt 66 Startups hat sich der Teilcluster Network Security maßgeblich für die Bereitstellung von Plattformen zur Sicherheitsüberwachung, Erkennung und Verhinderung von unberechtigtem Zugriff und Missbrauch von Unternehmensnetzwerken eingesetzt. Die Präsenz von 38 aktiven Startups deutet darauf hin, dass etwa die Hälfte aller Startups ihren Geschäftsbetrieb aufrechterhalten konnte. Der erfolgreiche Exit von 17 Startups unterstreicht die Attraktivität von Network Security für Investoren. Allerdings haben auch 11 Startups ihr Geschäft aufgegeben, was darauf hinweist, dass es zwar erhebliche Aktivitäten und Investitionen gibt, der Markt aber auch von starkem Wettbewerb und Herausforderungen gekennzeichnet ist. Das Auftauchen von vier neu gegründeten Unternehmen in den vergangenen zwei Jahren könnte darauf hinweisen, dass es in diesem Bereich noch Raum für Innovationen und neue Lösungen gibt. Im Vergleich zu den anderen Subclustern spiegeln die durchschnittlichen Investitionen in Höhe von Mio. USD 11,39 einen moderaten, aber stetigen Kapitalzufluss wider, was auf ein ausgewogenes Vertrauen der Investoren in das Wachstumspotenzial von auf Netzwerksicherheit spezialisierten Startups schließen lässt. Die beträchtliche Anzahl von Exits und die jüngsten Finanzierungsrunden unterstreichen die anhaltende Innovation in diesem Sektor. Angesichts des Zukunftspotentials der digitalen Infrastruktur erscheint dies nur logisch.

Potenzielle Auswirkungen

Die Bedeutung der Vertraulichkeit und Integrität von Daten und Ressourcen innerhalb eines Netzwerks wächst mit jedem neuen Element in einem Netzwerk, von dem die meisten stetig wachsende Cloud-Systeme bilden. Mit der zunehmenden Nutzung von Cloud-Services zur Speicherung und Verarbeitung von Daten wird Netzwerksicherheit zum entscheidenden Faktor, um Daten während der Übertragung zu schützen und unbefugten Zugriff zu verhindern. Sicherheitsmaßnahmen wie die Verwendung von Zero Trust Architekturen, Firewalls der nächsten Generation, VPNs für Verschlüsselung, Zugriffskontrollen und die Überwachung mit einem SOC/SIEM sind unerlässlich. Darüber hinaus ermöglichen künstliche Intelligenz und maschinelles Lernen zukünftige Netzwerksicherheitsdienste, die eine erweiterte Erkennung von Anomalien, die Automatisierung von Sicherheitsmaßnahmen und eine proaktive Abwehr von Angriffen ermöglichen.

5.2.1.2 Website Security

Website Security

Startups:

Total	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
18	13	3	2

Neu gegründete Startups:
(in 2023 - 2024)
0

Gesamtinvestment:
$73.39 Million

Durchschnittliche Investition pro aktivem Startup:
$5.65 Million

Jüngste Finanzierungsrunden:
Orchid (unveröffentlicht, 29.1.2024)
Trust Lab ($13.9 M, 15.1.2023)
Lokker ($4.7 M, 20.4.2022, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	Big Data
5	5	2

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
3	0	1	0

***Abbildung 17**: Subcluster Website Security*

Der Subcluster Website Security umfasst insgesamt 18 Startups, von denen 13 derzeit aktiv sind. Diese Startups befassen sich mit der Sicherheit von Websites und Webdiensten und deren Schutz vor internetweiten Angriffen. Während es drei erfolgreiche Ausstiege durch Börsengänge oder Übernahmen gab, haben zwei Startups ihr Geschäft aufgegeben. Dies könnte auf einen Nischenmarkt oder einen möglicherweise langsameren Wachstumskurs im Vergleich zu anderen Subclustern hindeuten. Die durchschnittliche Investitionssumme von Mio. USD 5,65 je Startup ist im Vergleich zu anderen Subclustern eher niedrig, was darauf hindeutet, dass Startups im Bereich Website-Sicherheit möglicherweise keine großen finanziellen Ressourcen benötigen. Insgesamt sind die meisten der identifizierten Startups noch aktiv, und nur eine Minderheit hat sich zurückgezogen oder den Betrieb eingestellt. Dies zeigt, dass in Zukunft ein hohes Potenzial für signifikante Entwicklungen besteht. Dieses Argument wird auch durch die Tatsache unterstützt, dass es in den letzten Jahren mehrere Finanzierungsrunden gegeben hat, um Startups zu finanzieren, die Lösungen zum Schutz von Websites und Webdiensten vor Angriffen anbieten. Allerdings gibt es zwischen 2023 und 2024 einen Mangel an neu gegründeten Startups, was eine beginnende Sättigung des Marktes anzeigen könnte.

Potenzielle Auswirkungen

Am wichtigsten ist jedoch, dass ein Mangel an Website-Sicherheit zur Implementierung von schädlichem Code, zum Sammeln vertraulicher Daten, zum Fälschen von Websites für Phishing-Angriffe oder zum Herunterfahren des externen Netzwerks einer Organisation durch „Denial-of-Service“-Angriffe führen und den Inhabern der Seiten oder deren Nutzern somit größeren Schaden zufügen könnte. Da Datenschutz und Datenintegrität in der Gesellschaft immer mehr an Bedeutung gewinnen, müssen Websitebetreiber wirksame Sicherheitsmaßnahmen ergreifen, um Datenlecks und unbefugten Zugriff zu verhindern. Sie können aus einer Vielzahl von Lösungen wie TLS-Verschlüsselung, Web Application Firewalls (WAF) oder rollenbasierter Zugangskontrolle wählen. Die Zahl der erfolgreichen Exits in diesem Cluster zeigt, wie sehr sich diese Dienste auf dem Markt durchgesetzt haben.

5.2.1.3 Server Security

Die Anzahl der Startups, die Lösungen für die Sicherheit und die Absicherung von Servern anbieten, um unbefugten Zugriff und Angriffe auf Schwachstellen zu verhindern, ist im Vergleich zu anderen Subclustern relativ gering. Mit derzeit nur drei aktiven Startups deutet dies auf einen Nischenmarkt mit weniger Markteinsteigern und potenziell spezialisierten Lösungen hin. Dies wird auch durch den Mangel an in den vergangenen zwei Jahren neu gegründeten Startups unterstrichen. Darüber hinaus ist die durchschnittliche Investition pro Startup eher gering (Mio. USD 0,23), was auf den speziellen Fokus dieser Startups innerhalb des Server Security Bereichs zurückzuführen sein könnte. Im Vergleich zu den anderen Subclustern unserer Landscape fehlt es diesem Subcluster an Dynamik. Wir sind der Meinung, dass dies darauf zurückzuführen ist, dass die vorliegende Spezialisierung aufgrund der zunehmenden Abdeckung von Serversicherheitsaspekten im Rahmen von Cloud-Sicherheitslösungen nicht mehr benötigt wird.

***Abbildung 18**: Subcluster Server Security*

Potenzielle Auswirkungen

Obwohl es sich um eine Nische zu handeln scheint, hat der Subcluster Serversicherheit den Grundstein für moderne Serversicherheitsstandards gelegt. Bei jeder Operation mit derartigen Auswirkungen gewährleistet die Implementierung von Redundanzen und Failover-Mechanismen die öffentliche und private Sicherheit, während sich die Lösungen weiterentwickeln. Automatisiertes Patch-Management ist ein wesentlicher Bestandteil der zukünftigen Systemhärtung auf Firmware-Ebene. Angesichts der zunehmenden Verbreitung von Blockchain-Technologie und Kryptowährungen ist der Schutz von Servern, die Blockchain-Netzwerke und -Transaktionen verwalten, für die Verhinderung von Betrug und die Aufrechterhaltung der Systemintegrität von entscheidender Bedeutung.

5.2.1.4 Database Security

In unserer Analyse konnten wir 16 Startups ausfindig machen, die sich mit der Bereitstellung von Lösungen für die Zugriffskontrolle, Prüfung, Verschlüsselung, Integritätskontrolle und Sicherung von Datenbanken befassen. Während nur vier davon noch aktiv sind, gibt es acht Startups, die sich durch Börsengänge oder Übernahmen erfolgreich aus dem Markt zurückgezogen haben, und vier Startups, die ihr Geschäft aufgegeben haben. Diese Zahlen könnten Indikatoren für einen stark umkämpften Markt sein, in dem erfolgreiche Startups ein beträchtliches Wachstum erzielen oder von größeren Unternehmen übernommen werden. Die durchschnittliche Investitionssumme von Mio. USD 33,78 ist im Vergleich zu anderen Subclustern signifikant. Hohe durchschnittliche Investitionen deuten häufig auf eine starke Marktnachfrage und überzeugende Geschäftsmodelle hin, die Investoren anziehen und sie zur Anlage erhebliche Investitionsbeträge ermutigen. Die jüngsten Finanzierungsrunden unterstreichen das anhaltende Vertrauen der Investoren in Lösungen für die Datenbanksicherheit und Investitionen in die Serie C und frühere Runden.

Database Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
16	4	8	4

Neu gegründete Startups:
(in 2023 - 2024)
0

Gesamtinvestment:
$135.10 Million

Durchschnittliche Investition pro aktivem Startup:
$33.78 Million

Jüngste Finanzierungsrunden:
StrongDM ($37.8 M, 22.4.2024, Series C)
Opaque ($20.8M, 28.6.2022, Series A)
TrustLogi ($3.1 M, 23.6.2021)

Technologie-Referenz:

Cloud	*KI & ML*	Big Data
1	2	3

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
1	0	0	0

***Abbildung 19**: Subcluster Database Security*

Potenzielle Auswirkungen

Das Vertrauen der Investoren könnte auch darin begründet sein, dass die Datenbanksicherheit immer wichtiger wird, nicht nur, weil die Bedrohungen immer raffinierter werden, sondern auch angesichts der zunehmenden Integration von IoT-Geräten und der Zunahme von Big Data, die die Komplexität und den Umfang von Datenbanken erhöhen. Mit der Einführung von künstlicher Intelligenz und Algorithmen des maschinellen Lernens können moderne Anwendungen eine Art “rote Linie” für Datenbankaktivitäten erstellen, wobei jede Abweichung von dieser, egal ob außerhalb oder innerhalb eines Unternehmens, eine potenzielle Sicherheitsbedrohung darstellt. In Zukunft muss Database Security quantenresistente Algorithmen zum Schutz vor Quantenangriffen verwenden. Brute-Force-Angriffe mit Quantencomputern könnten Passwörter oder Verschlüsselungen, die zur Sicherung von Datenbanken verwendet werden, viel schneller knacken. Die Datenbanksicherheit muss quantenresistente Algorithmen zum Schutz vor Quantenangriffen einsetzen, z. B. mit der Blockchain-Technologie.

Brute-Force-Angriffe mit Quantencomputern könnten Passwörter oder Verschlüsselungsschlüssel, die zur Sicherung von Datenbanken verwendet werden, viel schneller knacken. Die Datenbanksicherheit muss quantenresistente Algorithmen zum Schutz vor Quantenangriffen einsetzen. So können beispielsweise Cloud-Anbieter Post-Quantum-Kryptografie (PQC) zur Verschlüsselung von Daten einsetzen. Diese

Algorithmen sind so konzipiert, dass sie selbst von Quantencomputern nicht leicht geknackt werden können. Beispiele sind gitterbasierte Kryptosysteme oder hashbasierte Signaturen.

5.2.1.5 Data Security

***Abbildung 20**: Subcluster Data Security*

Der Subcluster Data Security umfasst insgesamt 184 Startups, von denen 102 derzeit aktiv sind. In diesem Subcluster gab es 17 Abgänge durch Börsengänge oder Übernahmen und 65 Startups, die ihre Geschäftstätigkeit eingestellt haben. Dies deutet auf ein wettbewerbsintensives und unbeständiges Marktumfeld hin, in dem eine beträchtliche Anzahl von Startups Schwierigkeiten hat, ihre Geschäftstätigkeit aufrechtzuerhalten. Seit 2023 gab es acht Neugründungen, und es wurden beträchtliche Investitionen getätigt – Mrd. USD 1,49 in Summe bzw. durchschnittlich Mio. USD 14,65 je Startup. Dieses Investitionsniveau deutet auf Vertrauen in das Wachstum des Marktes hin und unterstreicht die große Bedeutung von Datensicherheitslösungen. Die kontinuierliche Gründung neuer Startups zeigt, dass der Markt für Datensicherheitslösungen noch nicht gesättigt ist und neue Marktteilnehmer auch weiterhin an neu auftretenden Bedrohungen oder Schwachstellen arbeiten.

Potenzielle Auswirkungen

Mit der fortschreitenden Digitalisierung in allen Lebensbereichen, von Smart Cities bis hin zum Internet der Dinge (IoT), nimmt die Zahl der verbundenen Geräte und Systeme exponentiell zu. Jedes dieser Geräte kann anfällig für Angriffe sein, weshalb der Subcluster Data Security auch weiterhin Wachstum zeigt. Ransomware-Angriffe machen Backups unerlässlich. Cloud-Backups ermöglichen eine schnelle und kostengünstige räumliche und netzwerktechnische Trennung. Die hohe Anzahl von Verweisen auf Schlüsseltechnologien, die in unserer Studie identifiziert wurden, unterstreicht die Vielfalt an Lösungen, die in diesem Bereich angeboten werden, von Biometrie für den Zugang zu Systemen bis hin zu quantensicherer Verschlüsselung in der Zukunft.

5.2.1.6 Cloud Security

Cloud Security stellt ein durchschnittliches Subcluster innerhalb der Digital Infrastructure Security dar, dies wird durch folgende Zahlen untermauert: Von den 58 Startups sind 30 noch aktiv, und es werden durchschnittlich Investitionen in Höhe von etwa 15,77 Millionen USD pro Startup getätigt. Es gibt einen signifikanten Anteil erfolgreicher Exits (21 von 58 Startups) durch Börsengänge oder Übernahmen, was die höchste Anzahl von Exits im gesamten Cluster darstellt. Dafür kann es mehrere Gründe geben, wir vermuten jedoch als ausschlaggebenden Grund, dass die hohe Akzeptanz der Cloud-Technologie in fast allen Branchen einen wachsenden Markt darstellt, auf dem verschiedene Lösungen gedeihen können. Dieses Argument wird auch durch die Tatsache gestützt, dass nur sieben Startups ihr Geschäft aufgegeben haben. Auf den ersten Blick scheint der Subcluster daher recht ausgereift zu sein, aber mit drei neuen Startups im vergangenen Jahr hat der Erfolg des Subclusters möglicherweise neue Wettbewerber für die Branche angezogen.

Cloud Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
58	30	21	7

Neu gegründete Startups:
(in 2023 - 2024)
3

Gesamtinvestment:
$473.05 Million

Durchschnittliche Investition pro aktivem Startup:
$15.77 Million

Jüngste Finanzierungsrunden:
Arch0 ($1.2 M, 3.4.2024, Seed)
P0 Security ($44.7 M, 11.1.2023, Seed)
Discern Security ($27.8 M, 14.10.2023, Seed)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
23	9	6

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
0	1	0	0

***Abbildung 21**: Subcluster Cloud Security*

Potenzielle Auswirkungen

Mit dem Einzug der Cloud-Technologie in den Mainstream gewinnt natürlich auch die Cloud-Sicherheit an Bedeutung. Dies beginnt mit Diensten, die über adaptive Cloud-Konfigurationen laufen, und wächst mit jedem angeschlossenen IoT-Gerät. Cloud-Sicherheitsprotokolle umfassen häufig die Verschlüsselung von Daten im Ruhezustand, in der Verwendung und während der Übertragung, um sicherzustellen, dass Daten auch dann nicht lesbar sind, wenn sie ohne Autorisierung abgefangen oder abgerufen werden. Darüber hinaus umfassen Cloud Security-Services in der Regel erweiterte Überwachungs- und Analysetools, die Bedrohungen in Echtzeit erkennen und darauf reagieren können, was die Fähigkeit eines Unternehmens verbessert, Cyberbedrohungen schnell zu mindern. In Zukunft könnte die Entwicklung von Algorithmen der künstlichen Intelligenz und des maschinellen Lernens sowie die Blockchain-Technologie die Sicherheit erhöhen und verbessern, indem sie unveränderliche und dezentralisierte Aufzeichnungen für Transaktionen und Datenintegrität bereitstellt. Darüber hinaus wird ein Architekturmodell, das Netzwerksicherheitsfunktionen wie Secure Web Gateway, Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS) und Zero Trust Network Access (ZTNA) in einer einzigen Cloud-Plattform integriert, in Zukunft wahrscheinlich zum Standard werden.

5.2.1.7 Blockchain Security

Blockchain Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
20	16	1	3

Neu gegründete Startups:
(in 2023 - 2024)
1

Gesamtinvestment:
$283.47 Million

Durchschnittliche Investition pro aktivem Startup:
$17.72 Million

Jüngste Finanzierungsrunden:
Firewall ($3.4 M, 6.3.2024, Seed)
PrimeVault (unveröffentlicht, 5.9.2023)
Ancilia ($0.1 M, 20.6.2023)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
1	1	0

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
15	0	1	0

***Abbildung 22**: Subcluster Blockchain Security*

Der Subcluster Blockchain Security besteht aus insgesamt 20 Startups, von denen 16 noch aktiv sind und nicht übernommen wurden. Mit Mio. USD 17,72 liegen die Investitionen je Startup etwas über dem Gesamtdurchschnitt der Subcluster, was die Hypothese höherer technologischer Anforderungen in diesem Bereich unterstützt. Mit nur einem erfolgreichen Exit haben die Startups und Lösungen in den Subclustern noch nicht die nötige Aufmerksamkeit für eine Übernahme auf sich gezogen oder es fehlt ihnen der Kundenstamm für langfristige Pläne eines Börsengangs. Die niedrige Ausstiegs- und Misserfolgsrate deutet darauf hin, dass zwar ein erhebliches Interesse am Thema Blockchain Security besteht und Investitionen getätigt werden, der Markt sich aber noch stabilisiert, da sich viele Startups noch in einem frühen Stadium der Entwicklung befinden und ihre Rentabilität unter Beweis stellen müssen. Die Gründung eines neuen Startups im vergangenen Jahr spiegelt das anhaltende Interesse am Bereich Blockchain-Security wider, wobei die überschaubare Zahl auf einen vorsichtigen, aber stetigen Zustrom neuer Akteure schließen lässt. Wir gehen davon aus, dass der Subcluster weiter reifen und sowohl Kunden als auch Investoren anziehen wird, je mehr Startups hier auf Fortschritte hinarbeiten. Dies wird wahrscheinlich sowohl die Zahl der erfolgreichen Exits als auch die Zahl der Startups, die ihr Geschäft aufgeben, erhöhen, da die stärksten Akteure ihre Position festigen werden.

Potenzielle Auswirkungen

Blockchain ist aufgrund seiner inhärenten Merkmale – Transparenz und Dezentralisierung – derzeit besonders interessant. Blockchain automatisiert die regulatorische Berichterstattung und ermöglicht so die Überwachung der Einhaltung regulatorischer Anforderungen in Echtzeit und in der Vergangenheit, was eine absolute Transparenz und Rechenschaftspflicht ermöglicht. In Zukunft werden IoT-Daten auf Blockchains gespeichert, und durch die Nutzung von künstlicher Intelligenz und maschinellem Lernen werden sie vertrauenswürdige, effiziente und kollaborative Umgebungen für Benutzer, Betreiber und Regulierungsbehörden gleichermaßen schaffen.

5.2.2 Personal Digital Security

***Abbildung 23**: Cluster Personal Digital Security*

Die Cyber Startup Landscape ist im Bereich von Personal Digital Security stark gewachsen und zieht eine Vielzahl von Startups an, die sich auf verschlüsselte Kommunikation, Identitätsschutz und Datenschutzlösungen konzentrieren. Mit insgesamt 157 Startups, von denen 109 noch aktiv sind, zeigt der Cluster großes Potenzial für die Zukunft. Mit 24 Startups, die erfolgreich aus dem Markt ausschieden, und 24 Startups, die ihr Geschäft aufgaben, zeigten Investoren ein großes Vertrauen in diesem Cluster im Vergleich zu den normalen Erfolgsraten von Startups. Die durchschnittliche Investitionssumme von Mio. USD 21,2 entspricht in etwa dem Gesamtdurchschnitt der Studie, und auch die vier kürzlich in den Markt eingetretenen Unternehmen lassen auf zukünftige Rentabilität schließen. Insgesamt ist ein breites Spektrum spezialisierter Unternehmen entstanden, die sich mit einer Vielzahl persönlicher digitaler Sicherheitsbedürfnisse und -dienste befassen, von verschlüsselter Kommunikation über Identitätsschutz bis hin zu Sensibilisierungsmaßnahmen. Dieser kollektive Fokus von Startups bildet ein Cluster, der sich der Verbesserung der persönlichen digitalen Sicherheit widmet und wichtige Entwicklungen für die Branche insgesamt beiträgt.

5.2.2.1 Endpoint Security

***Abbildung 24**: Subcluster Endpoint Security*

Der Subcluster Endpoint Security umfasst insgesamt 42 Startups, von denen 25 derzeit Plattformen für die Cybersicherheit unternehmenseigener Endgeräte bereitstellen. Zehn Startups haben sich durch Börsengänge oder Übernahmen aus dem Markt zurückgezogen, was im Vergleich zu anderen Subclustern beachtlich ist, während nur sieben ihre Geschäftstätigkeit aufgegeben haben. Die hohen Gesamtinvestitionen in den Bereich Endpoint Security (Mio. USD 830,92) unterstreichen dessen Bedeutung und das Vertrauen der Investoren in sein Wachstumspotenzial. Die durchschnittliche Investition je Startup ist die höchste unter den verglichenen Subclustern, was auf eine erhebliche finanzielle Unterstützung für Unternehmen in diesem Bereich hindeutet. Allerdings wurde zwischen 2023 und 2024 nur ein neues Startup gegründet, was auf hohe Eintrittsbarrieren aufgrund der fortgeschrittenen Entwicklung, bereits etablierter Akteure und des Wettbewerbs auf dem Markt hindeuten könnte. Dies könnte auch auf ein geringeres Innovationstempo hindeuten, da es weniger bahnbrechende Ideen gibt, die die Gründung neuer Startups rechtfertigen würden. Die Tatsache, dass Daten zu den jüngsten Finanzierungsrunden nicht veröffentlicht wurden, könnte ein Hinweis auf eine gewisse wettbewerbsbedingte Sensibilität und strategische Diskretion bei Startups und Investoren sein, was auf ein stark umkämpftes und strategisch nuanciertes Marktumfeld schließen lässt.

Potenzielle Auswirkungen

Endpoint Security bietet bereits wesentlichen Schutz vor modernen Bedrohungen wie Ransomware-Angriffen und unerwünschten Datenlecks durch bösartigen Code, unterstützt Remote- und Cloud-basiertes Arbeiten und gewährleistet durch BYOD-Richtlinien die Einhaltung von Vorschriften und den Datenschutz. Darüber hinaus spielt die Zero-Trust-Architektur eine entscheidende Rolle bei der Endpunktsicherheit, da sie sicherstellt, dass alle Endpunkte unabhängig von ihrem Standort oder ihrem vorherigen Vertrauensstatus einer kontinuierlichen Überprüfung, strengen und dynamischen Zugriffskontrollen und der Überwachung des Endpunktverhaltens unterliegen.

5.2.2.2 BYOD Security

BYOD Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
4	4	*0*	0

Neu gegründete Startups:
(in 2023 - 2024)
0

Gesamtinvestment:
$6 Million

Durchschnittliche Investition pro aktivem Startup:
$1.5 Million

Jüngste Finanzierungsrunden:
SnippetSentry ($1.1 M, 26.3.2024, Seed)
Swif (unveröffentlicht, 6.11.2023, Seed)
Inside-Out Defense (unveröffentlicht, 12.4.2023)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
2	2	1

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
0	1	*0*	*0*

***Abbildung 25**: Subcluster BYOD Security*

Der Cluster BYOD Security besteht aus vier Startups, die derzeit alle aktiv sind, ohne dass es zu Ausstiegen oder Misserfolgen kam. Die begrenzte Anzahl von Startups in diesem Sektor deutet auf eine Nische innerhalb der größeren Cybersicherheitslandschaft hin, die durch spezifische geschäftliche Anforderungen an die Sicherung von am Arbeitsplatz verwendeten persönlichen Geräten angetrieben wird. Die Tatsache, dass alle Startups noch aktiv sind, deutet jedoch auf Stabilität und Widerstandsfähigkeit innerhalb dieser Nische hin. Das Fehlen von Ausstiegen oder Misserfolgen könnte darauf hindeuten, dass sich die Unternehmen entweder in einem frühen Entwicklungsstadium befinden oder stetig wachsen, ohne sich um Übernahmen oder Börsengänge zu bemühen. Die Gesamtinvestitionen in Höhe von Mio. USD 6 mit einem Durchschnitt von Mio. USD 1,5 je Startup deuten darauf hin, dass der Sektor zwar finanzielle Unterstützung erhält, diese aber im Vergleich zu anderen Bereichen relativ bescheiden ist. Dies könnte auf ein frühes Entwicklungsstadium hindeuten, in dem die Startups noch dabei sind, ihr Wertversprechen zu beweisen und ihre Lösungen zu skalieren.

Potenzielle Auswirkungen

Unabhängig von der geringen Zahl der Startups wird die Sicherheit von BYOD ein integraler Bestandteil künftiger IT-Strategien sein, und zwar nicht nur aufgrund des Bedarfs an allgemeiner Flexibilität oder der zunehmenden Remote-Arbeit, die die Verwendung einer größeren Vielfalt von Geräten wie Smartphones, Tablets, Laptops und Wearables umfasst. Aufgrund der zunehmenden Nutzung von Cloud-Services müssen BYOD-Geräte jedoch nahtlos in die Sicherheitsmaßnahmen der Cloud integriert werden. Dies ermöglicht einen sicheren Zugriff auf Cloud-Anwendungen und schützt die in der Cloud gespeicherten Daten vor unerwünschtem Datenlecks sowie vor Vermischung geschäftlicher und persönlicher Daten. Ebenso wird das Auftreten und die Einführung fortschrittlicher Technologien wie künstliche Intelligenz und maschinelles Lernen dazu beitragen, ungewöhnliche Verhaltensmuster und Bedrohungen in Echtzeit zu erkennen, Sicherheitsreaktionen zu automatisieren und so die umfassende und adaptive Sicherheitsinfrastruktur zu schaffen, die für die Einführung von BYOD erforderlich ist.

5.2.2.3 Email Security

In unserer Analyse haben wir insgesamt 31 Startups identifiziert, die sich auf die Bereitstellung eines sicheren Gateways und die Verschlüsselung von E-Mail-Kommunikationssystemen konzentrieren. Von diesen sind 23 derzeit aktiv, vier haben sich durch Börsengänge oder Übernahmen erfolgreich aus dem Markt zurückgezogen und vier haben ihr Geschäft aufgegeben. Wie in den meisten anderen Sektoren wurde auch hier in den vergangenen Jahren nur ein neues Unternehmen gegründet. Es wurden beträchtliche Investitionen in den E-Mail-Sicherheitssektor getätigt – in Summe Mio. USD 577,2 bzw. durchschnittlich Mio. USD 25.1 je Startup – was die Bedeutung einer sicheren E-Mail-Kommunikation und das Vertrauen der Investoren in das Potenzial dieser Startups widerspiegelt. In den letzten Investitionsrunden hat das Unternehmen Abnormal einen beträchtlichen Betrag von Mio. USD 83,9 einbringen können, was darauf hindeutet, dass es als führendes oder vielversprechendes Unternehmen in diesem Bereich wahrgenommen wird. Die jüngsten mit hohen Beträgen arbeitenden Finanzierungsrunden zeigen, dass es ein erhebliches Marktpotenzial für E-Mail-Sicherheitslösungen im Allgemeinen gibt.

Email Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
31	23	*4*	4

Neu gegründete Startups:
(in 2023 - 2024)
1

Gesamtinvestment:
$577.20 Million

Durchschnittliche Investition pro aktivem Startup:
$25.1 Million

Jüngste Finanzierungsrunden:
Abnormal ($83.9 M, 1.5.2024)
DataKrypto ($2.8 M, 26.3.2024, Seed)
Infisical ($2.6 M, 3.7.2023, Seed)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
21	4	2

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
2	*0*	*0*	1

***Abbildung 26**: Subcluster Email Security*

Potenzielle Auswirkungen

Dieses Potenzial erscheint angesichts der Relevanz von E-Mails in der modernen Kommunikation logisch. E-Mail-Sicherheit ist für den Schutz der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen sowohl in Unternehmen als auch in der Gesellschaft von entscheidender Bedeutung. Zusätzlich zu bereits etablierten Lösungen und Technologien wird erwartet, dass Technologien wie Maschinelles Lernen und KI eingesetzt werden, um ausgeklügelte Phishing-Versuche zu erkennen und zu blockieren, die durch herkömmliche Filter nicht gefunden werden. In Zukunft werden fortschrittliche Verschlüsselungsmethoden für den Schutz der sensiblen Natur und des Inhalts von E-Mails während des Transports und der Speicherung von grundlegender Bedeutung sein, so dass auch das Quantencomputing in Zukunft einen größeren Einfluss haben dürfte.

5.2.2.4 Training

***Abbildung 27**: Subcluster Training*

Im Subcluster Training befinden sich insgesamt sechs Startups, die Plattformen für Cybersicherheitstrainings anbieten. Während vier noch aktiv sind, ist einer aufgrund eines Börsengangs oder einer Übernahme ausgeschieden und ein Startup hat sein Geschäft aufgegeben. Die geringe Anzahl von Startups deutet auf einen Nischenmarkt hin, was auf die spezielle Art von Cybersicherheitstraining zurückzuführen sein könnte, die ein erhebliches Fachwissen erfordern, um effektive Trainingsprogramme und -plattformen zu entwickeln. Außerdem könnte das Fehlen von Neugründungen in den vergangenen zwei Jahren darauf hindeuten, dass bestehende Unternehmen die Nachfrage nach Cybersicherheitstrainings wirksam decken. Die durchschnittliche Investition pro Startup ist mit Mio. USD 23,82 relativ hoch, was darauf hindeutet, dass die Investoren die Bedeutung und die potenzielle Rendite in diesem Bereich erkennen. Die umfangreichen Finanzierungsrunden für Unternehmen wie SafeBreach unterstreichen den wahrgenommenen Wert und das Wachstumspotenzial des Bereichs Cybersicherheitstraining. Dieses hohe Investitionsniveau pro Unternehmen legt nahe, dass Investoren bereit sind, weniger, aber vielversprechendere und wirkungsvolle Startups in dieser Nische zu unterstützen („Qualität über Quantität“), um der steigenden Anzahl an Cyberbedrohungen zu begegnen.

Potenzielle Auswirkungen

Angesichts der wachsenden Zahl anspruchsvollerer und komplexerer Cyberbedrohungen ist es fraglich, inwieweit die bestehende Anzahl von Startups die Marktnachfrage nach Cybersicherheitstraining erfüllen kann. Der Trend verstärkt die Notwendigkeit regelmäßiger und verbesserter Trainings, da Mitarbeiter oft als das schwächste Glied innerhalb der Kette der Cybersicherheitsverteidigungen eines Unternehmens angesehen werden. Effektive Schulungsprogramme können diese Schwachstelle in eine Stärke umwandeln, indem sie Mitarbeiter befähigen. Dies schafft Vertrauen und eine sicherheitsbewusste Kultur innerhalb einer Organisation, wodurch die Wahrscheinlichkeit von Phishing- oder Social-Engineering-Versuchen und -Angriffen verringert wird. Außerdem können diese Trainings auch zu erheblichen Kosteneinsparungen für Organisationen jeder Größenordnung führen.

5.2.2.5 Anti-Fraud

Der Cluster Anti-Fraud ist mit 74 Startups, von denen 53 noch aktiv sind, der größte der untersuchten Cybersicherheitscluster. Dies deutet auf ein großes Interesse und einen hohen wahrgenommenen Bedarf an Lösungen für die Bereiche Betrug, Identitätsdiebstahl, Zahlungsbetrug und Telefonbetrug hin. Dies könnte darauf zurückzuführen sein, dass die Betrugstaktiken immer ausgefeilter werden und einen erheblichen finanziellen Schaden bzw. Rufschaden verursachen können, was auf einen dynamischen und wettbewerbsorientierten Markt mit vielen Möglichkeiten für Innovation und Differenzierung hindeutet. Der Sektor hat erste erfolgreiche Ausstiege erlebt, was darauf hindeutet, dass Startups zur Betrugsbekämpfung attraktive Übernahmeziele sind. Aufgrund des möglicherweise wettbewerbsintensiven Charakters des Marktes, der raschen Entwicklung und der hohen Anforderungen haben jedoch bereits 12 Startups ihr Geschäft aufgegeben. Gleichzeitig könnte die geringe Zahl neu gegründeter Unternehmen auf einen Sättigungspunkt des Marktes hindeuten, an dem es für neue Marktteilnehmer schwierig ist, sich zu differenzieren oder eine Finanzierung zu sichern. Dieser Trend könnte darauf hindeuten, dass der Schwerpunkt eher auf der Skalierung bestehender Startups als auf der Gründung neuer Unternehmen liegt. Die jüngsten Seed-Finanzierungsrunden, einschließlich einer beträchtlichen Finanzierung für Opal, zeigen das anhaltende Interesse der Investoren und das Vertrauen in das Potenzial neuer und aufstrebender Lösungen.

Anti-Fraud

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
74	53	9	12

Neu gegründete Startups:
(in 2023 - 2024)
2

Gesamtinvestment:
$803.43 Million

Durchschnittliche Investition pro aktivem Startup:
$15.16 Million

Jüngste Finanzierungsrunden:
Opal ($20.38 M, 1.3.2024, Seed)
Rupt (unveröffentlicht, 8.2.2024, Seed)
Doppel ($12.77 M, 23.1.2024, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
33	22	10

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
4	2	1	0

Abbildung 28: *Subcluster Anti-Fraud*

Potenzielle Auswirkungen

Dieses Interesse beruht wahrscheinlich darauf, dass moderne Betrugstaktiken immer ausgefeilter werden, was die Integration fortschrittlicher Technologien zur Betrugsbekämpfung erforderlich macht, um in Zukunft eine robuste Sicherheitslage zu schaffen. Zur weiteren Verbesserung der Betrugsbekämpfung wird die Technologie künstliche Intelligenz & maschinelles Lernen immer wichtiger, da sie riesige Datenmengen analysieren und ungewöhnliche Muster und potenzielle Betrüger erkennen kann. Weitere Instrumente sind die Mehrfaktor-Authentifizierung (MFA) oder die biometrische Authentifizierung, die es Betrügern erschweren, sich als legitime Nutzer auszugeben.

5.2.3 Analytics

Der Startup-Markt im Bereich Security Analytics verzeichnet ein schnelles und signifikantes Wachstum, wobei 2021 zahlreiche sich im Frühstadium befindliche Startups entstanden. Diese Unternehmen, die sich auf datengesteuerte Sicherheitserkenntnisse und die Erkennung von Bedrohungen spezialisiert haben, unterstreichen die dynamische Landschaft der Branche und den Trend zu innovativeren, KI-gesteuerten Lösungen. Insgesamt werden 88 Startups in diesem Sektor identifiziert. Davon sind 54 noch im Geschäft und sechs wurden im vergangenen Jahr gegründet. Dies unterstreicht das Potenzial des Sektors, zumal bereits 17 erfolgreiche Exits stattgefunden haben. Die durchschnittliche Investition pro Startup liegt bei Mio. USD 19,3, was dem Durchschnitt unserer gesamten Datenbank entspricht. Trotz vieler neu gegründeter Startups und des Frühstadiums, in dem sich diese befinden, weist dieser Cluster einen hohen Reifegrad auf, was das beschleunigte Entwicklungstempo unterstreicht. Interessant ist auch die Vielfalt der beobachteten Geschäftsmodelle, die von "Software as a Service" (SaaS) bis hin zu maßgeschneiderten Beratungsleistungen reichen. Bei SaaS handelt es sich um ein Cloud-basiertes Lizenz- und Vertriebsmodell, bei dem Software über das Internet bereitgestellt wird und von einem Drittanbieter gehostet wird. Anstatt die Software auf dem eigenen Computer oder Server zu installieren und zu betreiben, greifen die Nutzer über das Internet darauf zu.

Analytics

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
88	54	17	17

Neu gegründete Startups:
(in 2023 - 2024)
6

Gesamtinvestment:
$1.04 Milliarden

Durchschnittliche Investition pro aktivem Startup:
$19.3 Million

Jüngste Finanzierungsrunden:
Prophet Security ($10.2 M, 23.4.2024, Seed)
Anvilogic ($41.7 M, 17.4.2024, Series C)
Reach Security ($18.5 M, 7.3.2024, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
29	30	10

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
1	2	0	0

***Abbildung 29**: Cluster Analytics*

5.2.3.1 Document Management

***Abbildung 30**: Subcluster Document Management*

Mit insgesamt vier Startups ist der Subcluster Document Management der kleinste des Clusters Analytics. Dies könnte darauf hindeuten, dass Dokumentenverwaltung ein Nischenbereich innerhalb des Cybersicherheitsbereichs ist. Die Gesamtinvestition in die Startups innerhalb dieses Teilclusters beträgt Mio. USD 25,18, mit einer durchschnittlichen Investition von Mio. USD 8,39 je Startup. Letzteres ist im Vergleich zu anderen Subclustern innerhalb von Analytics relativ bescheiden und liegt sogar unter dem Durchschnitt aller Subcluster. Dies kann als Indikator dafür angesehen werden, dass die Investoren dieses Feld als weniger vielversprechend ansehen, auch aufgrund jüngster Fortschritte bei Generativer KI, die innerhalb der letzten zwei Jahre viele der im Subcluster angebotenen Fähigkeiten übertroffen hat. Darüber hinaus könnte das Fehlen jüngster Finanzierungsrunden darauf hindeuten, dass die Investoren derzeit zögern, neue oder bestehende Startups in diesem Bereich zu finanzieren.

Potenzielle Auswirkungen

Es besteht ein grundlegender Bedarf an Dokumentenmanagement, der dadurch unterstrichen wird, dass Unternehmen weiterhin eine große Anzahl digitaler Dokumente erzeugen, die effektiv und sicher geschützt werden müssen. Es wird erwartet, dass die Systeme dieses Subclusters in Zukunft in größeren Ökosystemen aufgehen werden, die wahrscheinlich fortschrittliche Verschlüsselungstechnologien wie Ende-zu-Ende-Verschlüsselung, Zero-Trust-Architektur und quantenresistente Algorithmen beinhalten werden, um sensible Daten sowohl im Ruhezustand als auch bei der Nutzung und bei der Übertragung zu schützen.

5.2.3.2 Security Analytics

Security Analytics

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
69	40	14	15

Neu gegründete Startups:
(in 2023 - 2024)
4

Gesamtinvestment:
$783.41 Million

Durchschnittliche Investition pro aktivem Startup:
$19.56 Million

Jüngste Finanzierungsrunden:
Prophet Security ($10.2 M, 23.4.2024, Seed)
Anvilogic ($41.7 M, 17.4.2024, Series C)
Reach Security ($18.5 M, 7.3.2024, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
20	26	9

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
0	1	0	0

***Abbildung 31**: Subcluster Security Analytics*

Der Subcluster Security Analytics ist mit insgesamt 69 Startups, von denen 40 noch aktiv sind, der größte Subcluster. Diese hohe Zahl deutet auf eine starke Nachfrage nach Sicherheitsanalyselösungen hin und spiegelt die Bedeutung der Analyse von und Reaktion auf Cybersicherheitsbedrohungen in Echtzeit wider. Da immer noch eine große Anzahl von Startups aktiv ist, deutet dies auf ein hohes Aktivitätsniveau und einen dynamischen Markt mit fortlaufender Entwicklung und Bereitstellung neuer Lösungen hin. Die Tatsache, dass in den vergangenen zwei Jahren vier Startups gegründet wurden, unterstreicht dieses Argument. Während sich 14 Startups erfolgreich aus dem Markt zurückgezogen haben, hat eine hohe Zahl von 15 Startups ihr Geschäft aufgegeben. Dies könnte ein Indikator dafür sein, dass die Startups möglicherweise attraktive Ziele für Übernahmen oder Börsengänge werden können, sobald die Einzigartigkeit ihres Angebots offensichtlich wird. In Summe wurde ein erheblicher Betrag von Mio. USD 783,41 investiert bei einer durchschnittlichen Investition von Mio. USD 19,6 je Startup. Dies deutet auf ein starkes Vertrauen der Investoren in diesen Bereich hin und auf die generell optimistische Annahme eines weiteren Wachstums des Sektors.

Potenzielle Auswirkungen

Dies erscheint angesichts der Vielzahl neuer Angriffe und der damit verbundenen Notwendigkeit Informationen über die eigene Organisation einzuholen nur logisch. Angesichts dieser Bedrohungen wird erwartet, dass Security Analytics die Art und Weise, in der Unternehmen Cyberbedrohungen erkennen, auf sie reagieren und sie entschärfen, verändern wird, indem es durch Verhaltensanalysen und die Nutzung von Technologien tiefere Einblicke in Sicherheitsvorfälle liefert. Security Analytics wird Künstliche Intelligenz und Algorithmen des maschinellen Lernens nutzen, um ausgefeilte Bedrohungen wie Zero-Day-Exploits, Advanced Persistent Threats (APTs) und komplexe Malware zu erkennen und auf sie zu reagieren. Da das Internet der Dinge (IoT) weiterwächst, wird Security Analytics eine entscheidende Rolle bei der Überwachung und dem Schutz verbundener Geräte spielen und dadurch Anomalien und potenzielle Bedrohungen innerhalb des riesigen Netzwerks von IoT-Geräten identifizieren.

5.2.3.3 Threat Intelligence

Threat Intelligence

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
15	11	3	1

Neu gegründete Startups:
(in 2023 - 2024)
2

Gesamtinvestment:
$236.34 Million

Durchschnittliche Investition pro aktivem Startup:
$21.49 Million

Jüngste Finanzierungsrunden:
Cowbell ($23.7 M, 1.11.2023, Seed)
Ridge Security ($2.9 M, 20.10.2023, Seed)
ProjectDiscovery ($24.5 M, 17.8.2023, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
7	4	1

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
0	0	0	0

***Abbildung 32**: Subcluster Threat Intelligence*

Der Subcluster Threat Intelligence besteht aus 15 Startups, von denen 11 noch aktiv sind und drei erfolgreiche Exits absolviert haben. Dies zeigt eine eher moderate Austrittsrate, was darauf hindeutet, dass innerhalb des Sektors noch viel Bewegung ist und somit eine weitere Entwicklung erwartet werden kann. Mit nur einer Geschäftsaufgabe ist die Abbruchrate eher gering. Dies deutet auf eine stabile Nachfrage nach Threat-Intelligence-Lösungen hin, mittels derer Unternehmen evidenzbasiertes Wissen über vorhandene und neue Bedrohungen und Schwachstellen in ihrer Umgebung aufbauen können. Darüber hinaus weist der Subcluster Threat Intelligence mit Mio. USD 21,49 je Startup im Vergleich aller Subcluster des Analytics Clusters die höchsten durchschnittlichen Investitionswerte auf. Dies spiegelt das starke Vertrauen der Investoren wider, verdeutlicht aber auch, dass Threat-Intelligence-Startups erhebliches Kapital für die Entwicklung und Skalierung ihrer Lösungen benötigen. Die Kombination aus einer hohen Überlebensrate, einer moderaten Ausstiegsrate und beträchtlichen Investitionen in jüngster Zeit lässt auf einen dynamischen und vielversprechenden Markt schließen, gestützt durch die Tatsache, dass dieser Bereich eine entscheidende Rolle bei der Verbesserung von Cybersicherheitsmaßnahmen spielt.

Potenzielle Auswirkungen

Da Cyberbedrohungen immer ausgefeilter und häufiger werden, wird die Bedeutung von Threat Intelligence für die Stärkung der modernen Cybersicherheit wahrscheinlich noch zunehmen. Das Potenzial zur Verbesserung der Threat Intelligence ist enorm und umfasst Fortschritte in den Bereichen Technologie, Prozesse und Zusammenarbeit. Das Hauptmerkmal von Threat Intelligence ist die Fähigkeit, Rohdaten in verwertbare Erkenntnisse umzuwandeln, die es Unternehmen ermöglichen, Bedrohungen vorherzusehen, zu erkennen und effektiver darauf zu reagieren. Durch die Integration von Threat Intelligence in SIEM-Systeme (Security Information and Event Management) erhalten Unternehmen kontextbezogene Warnmeldungen, die zur Unterscheidung zwischen falsch positiven und echten Bedrohungen beitragen und zu wirksameren Reaktionen führen. Dies kann auch erweiterte Maßnahmen wie Vulnerability Scanning, Threat Feeds und Malware-Analyse umfassen.

5.2.4 OT & Application Security

Das Startup-Ökosystem für OT & Application Security in der Bay Area umfasst insgesamt 109 Startups, die sich auf fortschrittliche Sicherheitsanalysen, industrielle Kontrollsysteme und den Schutz digitaler Infrastrukturen spezialisiert haben. Bemerkenswert ist, dass der Reifegrad dieser Startup-Lösungen bereits hoch ist: 68 Startups sind noch aktiv, im Vergleich zu 17 erfolgreichen Exits und 24 Geschäftsaufgaben. Mit einem Wert von Mio. USD 29,12 je Startup belaufen sich die Investitionsbeträge hier fast auf den doppelten Wert der durchschnittlichen Investitionen je Startup in unserer Landscape. Die Gründe dafür können variieren, wir gehen jedoch davon aus, dass sie zumindest teilweise in einer verstärkten Einbindung von Hardware liegen. Die Geschäftsmodelle der Startups im Bereich der OT & Application Security sind sehr unterschiedlich. Die meisten Startups konzentrieren sich auf IoT-Lösungen, wobei der Anteil der Startups, die Soft- und Hardware für die Authentifizierung anbieten, gleich groß ist.

OT & Application Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
109	68	17	24

Neu gegründete Startups:
(in 2023 - 2024)
3

Gesamtinvestment:
$1.98 Milliarden

Durchschnittliche Investition pro aktivem Startup:
$29.12 Million

Jüngste Finanzierungsrunden:
c/side ($1.6 M, 16.5.2024)
AtomBeam ($6.46 M, 12.3.2024, Seed)
Turant ($0.1 M, 7.3.2024, Seed)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
21	34	12

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
3	21	8	1

***Abbildung 33**: Cluster OT & Application Security*

5.2.4.1 Application Security

Application Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
42	23	12	7

Neu gegründete Startups:
(in 2023 - 2024)
2

Gesamtinvestment:
$865.27 Million

Durchschnittliche Investition pro aktivem Startup:
$37.62 Million

Jüngste Finanzierungsrunden:
c/side ($1.6 M, 16.5.2024)
Traceable ($28 M, 1.4.2024, Series B)
Leen (unveröffentlicht, 22.3.2024)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
15	13	6

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
0	1	0	0

***Abbildung 34**: Subcluster Application Security*

Der Subcluster Anwendungssicherheit umfasst insgesamt 42 Startups und ist damit der größte Subcluster im Cluster OT & Application Security. Mit 23 Startups ist fast die Hälfte der Startups des Subclusters immer noch aktiv. Zwei neu gegründete Startups spiegeln die anhaltende Dynamik in diesem Subcluster wider. Mit 12 erfolgreichen Exits und nur sieben Geschäftsaufgaben zeigt sich ein erfolgreicher Subcluster Application Security, der eine gewisse Reife erreicht hat. In Summe wurden Mio. USD 865,27 investiert, was ca. der Hälfte der Investitionen des Clusters entspricht. Pro Startup wurden im Schnitt Mio. USD 37,62 investiert. Dies macht ihn zu einem sehr ressourcenintensiven Subcluster.

Potenzielle Auswirkungen

Da sich Cyberbedrohungen immer weiterentwickeln und stetig zunehmen, wird der Bedarf an innovativen technischen Lösungen im Bereich der Anwendungssicherheit wahrscheinlich zunehmen und diese zu einem wichtigen Aspekt für Unternehmen, Startups und Investoren machen. Der Schwerpunkt liegt dabei auf der Einführung von DevSecOps, der Absicherung von Daten und Anwendungen in verteilten Netzwerken (z. B. Cloud), dem Schutz des riesigen Netzwerks verbundener Geräte und der Absicherung von Drittanbieterkomponenten einer Software (z. B. Supply Chain Security).

5.2.4.2 Industrial Security

Industrial Security ist mit insgesamt acht Startups der kleinste Subcluster im Cluster OT & Application Security. Mit einer Investition von durchschnittlich Mio. USD 39,12 je Startup, weist er den höchsten Wert aller Subcluster innerhalb dieser Studie auf. Dies deutet sowohl auf eine ressourcenintensive Entwicklung in diesem Bereich als auch auf einen höheren Reifegrad als bei anderen Subclustern hin. Gestützt wird diese Annahme auch durch das Fehlen von Neuzugängen in diesem Subcluster, in dem im vergangenen Jahr keine Startups gegründet wurden. Die Tatsache, dass drei Startups ihr Geschäft aufgeben mussten und nur ein Unternehmen erfolgreich aus dem Markt austrat, könnte der Grund für die fehlenden Neuzugänge sein, insbesondere in Anbetracht der hohen Investitionen, die in diesem Subcluster erforderlich sind.

***Abbildung 35**: Subcluster Industrial Security*

Potenzielle Auswirkungen

Auch wenn eine vergleichsweise geringe Anzahl von Startups im Bereich der industriellen Sicherheit tätig ist, wird erwartet, dass dieser Bereich zunehmend an Bedeutung gewinnt. Es gibt einen zunehmenden Bedarf an industriellen Sicherheitslösungen für IoT-Geräte, die als entscheidend für die Sicherheitsarchitektur gelten. Diese Lösungen konzentrieren sich auf die Sicherung der Kommunikation, die Gewährleistung der Integrität der Geräte und den Schutz der Daten, die zwischen Geräten und Steuerungssystemen übertragen werden.

Auch wenn eine vergleichsweise geringe Zahl von Startups im Bereich der industriellen Sicherheit tätig ist, wird erwartet, dass dieser Bereich zunehmend an Bedeutung gewinnen wird. Industrien werden stärker miteinander vernetzt. Sie entwickeln sich auch weiter und integrieren fortschrittliche Technologien. Darüber hinaus gibt es einen wachsenden Bedarf an industriellen Sicherheitslösungen für IoT-Geräte, die als entscheidend für die Sicherheitsarchitektur angesehen werden. Diese Lösungen konzentrieren sich auf die

Sicherung der Kommunikation, die Gewährleistung der Integrität der Geräte und den Schutz der Daten, die zwischen Geräten und Kontrollsystemen übertragen werden. Im nächsten Kapitel wird der Subcluster IoT Security näher beleuchtet.

5.2.4.3 IoT Security

IoT Security

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
25	21	3	1

Neu gegründete Startups:
(in 2023 - 2024)
1

Gesamtinvestment:
$632.36 Million

Durchschnittliche Investition pro aktivem Startup:
$30.11 Million

Jüngste Finanzierungsrunden:
AtomBeam ($6.46 M, 12.3.2024, Seed)
Swif (unveröffentlicht, 6.11.2023, Seed)
SandboxAQ ($0.2 M, 29.6.2023, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
4	5	2

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
1	17	0	1

***Abbildung 36**: Subcluster IoT Security*

Der Subcluster IoT Security zeigt eine hohe Aktivitätsrate: 21 von 25 Startups sind noch aktiv und ein neues Startup wurde im vergangenen Jahr gegründet. In Verbindung mit der zweitniedrigsten durchschnittlichen Investitionssumme pro Startup des Clusters OT & Application Security gehen wir davon aus, dass dies der am wenigsten ausgereifte der vier Subcluster ist. Dies könnte damit zusammenhängen, dass sich das Internet der Dinge noch nicht voll entfaltet hat. Die drei erfolgreichen Exits und die Tatsache, dass nur ein Startup den Betrieb einstellte, zeigen das zukünftige Potenzial in diesem Bereich. Wir nehmen an, dass die Startups dieses Subclusters mehr Zeit benötigen, um ihre Lösungen vollständig zu entwickeln, da sie die Anforderungen an Software und Hardware in größerem Umfang als andere in unserer Landscape harmonisieren und anpassen müssen.

Potenzielle Auswirkungen

Die Anzahl der IoT-Geräte wächst exponentiell. Im Jahr 2023 wurden 16,1 Milliarden aktive IoT-Geräte registriert, eine Zahl, die bis 2033 vermutlich auf 39,9 Milliarden und somit um ca. 10 % jährlich steigen wird.[4] Mit der Verbreitung von IoT-Geräten hat sich die Angriffsfläche drastisch erhöht. Die Sicherung dieser Geräte ist von entscheidender Bedeutung, um zu verhindern, dass sie als Einstiegspunkte für Cyberangriffe genutzt werden können. IoT-Geräte sind stark auf drahtlose Kommunikation aller Art angewiesen, die anfällig für verschiedene Angriffe ist. Fortschrittliche kryptografische Lösungen können diese Kommunikationskanäle schützen, um Abhören/ Lauschangriffe, Man-in-the-Middle-Angriffe und Datenverstöße zu verhindern. Durch die Nutzung der KI-Fähigkeiten bei der Erkennung von Anomalien, der automatischen Reaktion, der prädiktiven Analyse und der adaptiven Sicherheit kann die KI-Technologie zu einer umfassenden und robusten Verteidigung gegen die sich entwickelnde Landschaft der IoT-Sicherheitsbedrohungen beitragen.

[4] Quelle: Global IoT connections forecast to reach 40 billion in 2033 - Transforma Insights

5.2.4.4 Authentication

Authentication

Startups:

Gesamt	*Aktiv*	*Exit (IPO/Akq.)*	*Out of Business*
34	20	1	13

Neu gegründete Startups:
(in 2023 - 2024)
0

Gesamtinvestment:
$329.09 Million

Durchschnittliche Investition pro aktivem Startup:
$16.45 Million

Jüngste Finanzierungsrunden:
Turant ($0.1 M, 7.3.2024, Seed)
Red Vector ($1.9 M, 1.1.2024, Seed)
Spec ($14.18 M, 18.10.2023, Series A)

Technologie-Referenz:

Cloud	*KI & ML*	*Big Data*
2	14	3

Blockchain	*IoT*	*Bilderkennung*	*Quantum*
2	0	8	0

***Abbildung 37**: Subcluster Authentication*

Der Subcluster Authentication umfasst 34 Startups, von denen 20 derzeit aktiv sind. Mit einer durchschnittlichen Investition von Mio. USD 16,45 je Startup liegt dieser Wert nahe am Gesamtdurchschnitt unserer Landscape, ist aber der niedrigste Wert aller Subcluster im Cluster OT & Application Security. Das auffälligste Merkmal dieses Subclusters ist jedoch die hohe Anzahl von Startups, die den Betrieb eingestellt haben. Mit gescheiterten 13 Unternehmen und nur einem, das erfolgreich aus dem Markt ausgeschieden ist, könnte dies auch ein Grund dafür sein, warum im vergangenen Jahr kein neues Startup gegründet wurde. Die verbleibenden Startups, die etwa ein Drittel der Gesamtanzahl ausmachen, eröffnen zumindest die Möglichkeit für weitere erfolgreiche Startups. Die hohe Rate fehlgeschlagener Startups könnte in der allgemeinen Weiterentwicklung der Authentifizierungsmethoden über Smartphones und andere Geräte begründet sein. Weitere Gründe könnten die hohen Implementierungskosten und die komplexe Integration in die bestehende Infrastruktur sein; insbesondere gilt dies für biometrische Authentifizierungstechnologien. Es könnte auch sein, dass einige Konzepte bei der Markteinführung schlecht durchdacht waren; diese Annahme ist jedoch momentan durch unsere Daten nicht zu belegen. Unabhängig von den Gründen für die hohe Anzahl an Geschäftsaufgaben erwarten wir eine starke Zurückhaltung von Investoren in diesem Bereich und somit eine baldige Verringerung der Aktivitäten.

Potenzielle Auswirkungen

Der angenommene Trend niedriger Erfolgsraten steht dabei im Widerspruch zur gestiegenen gesellschaftlichen Nachfrage nach digitaler Authentifizierung. Außerdem ist zu erwähnen, dass ein Mangel an starker Authentifizierungssicherheit weitreichende und schwerwiegende Folgen haben kann, darunter Datenschutzverletzungen, Finanzbetrug, Identitätsdiebstahl und -betrug, Betriebsunterbrechungen, Rufschädigung und rechtliche Folgen. Da der Bedarf an digitaler Authentifizierung wächst, müssten sich Wissenschaft und Wirtschaft auf die Stärkung und Ausweitung des Sektors der Authentifizierungssicherheit konzentrieren. Allerdings sollten auch die Grenzen und Schwächen biometrischer Authentifizierungsmethoden berücksichtigt werden, wie Spoofing, Fälschungen, falsche Akzeptanz- oder Ablehnungsraten und die Speicherung biometrischer Daten, die Anreize für Cyberkriminelle bieten können.

5.3 Größe der Startups nach Mitarbeitern

Nach Abschluss des vorigen Kapitels werden wir uns nun auf die Größe der Unternehmen, gemessen an der Zahl der Beschäftigten, konzentrieren. Mit über 400 Unternehmen, die sich alle in unterschiedlichen Reifephasen befinden und unterschiedliche Strategien verfolgen, können Mitarbeiter einen soliden Indikator für die Gesamtreife eines (Sub-) Clusters liefern. Für die Zwecke dieser Studie haben wir die Startups nach ihrer Größe in fünf Gruppen eingeteilt und eine Kategorie für Startups hinzugefügt, für die die Anzahl der Mitarbeiter nicht erfasst werden konnte. Die detaillierten Tabellen finden sich in **Anlage 2.**

5.3.1 Digital Infrastructure Security

Wie in **Abbildung 38** gezeigt, sind im Cluster Digital Infrastructure Security Unternehmen aller Größen vertreten. Angesichts der Größe des Clusters ist dies nicht überraschend, aber die Verteilung innerhalb des Clusters ist leicht zugunsten kleinerer Unternehmen verzerrt. Da etwa 46 % der Startups keine Beschäftigungsdaten offengelegt haben, haben wir daher die niedrigsten relativen Daten aller Cluster genutzt.

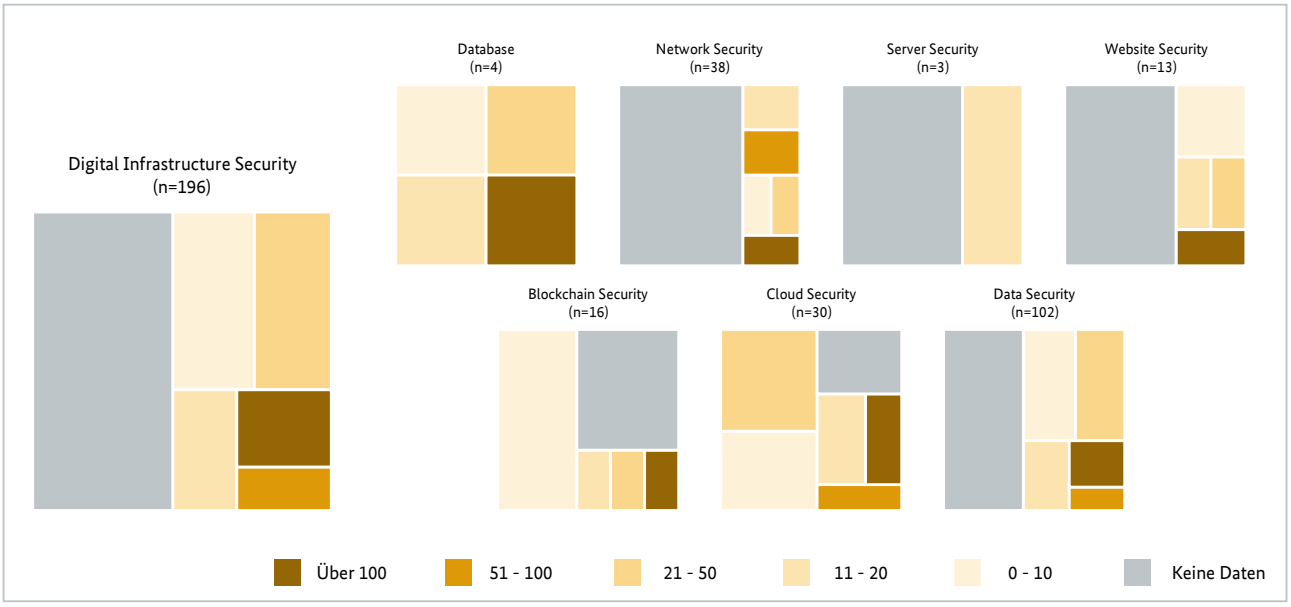

Abbildung 38: *Mitarbeiterstatistik im Cluster Digital Infrastructure Security*

Die Subcluster präsentieren sich unterschiedlich, denn nur drei von sieben Subclustern – namentlich Cloud Security, Data Security und Network Security – enthalten mindestens einen Startup jeder Kategorie. Im Subcluster Network Security haben mehr als 50 % der Startups keinen gültigen Datenpunkt. Dies gilt auch für den Subcluster Website Security, der zwar zahlenmäßig kleiner ist, aber mit 13 Startups dennoch eine bedeutende Gruppe darstellt. Die Startups, für die Daten gesammelt werden könnten, neigen jedoch zu einer kleineren Anzahl von Mitarbeitern, mit Ausnahme eines Unternehmens, das über 100 Mitarbeiter beschäftigt. Interessanterweise spiegelt sich diese Struktur auch im Blockchain-Subcluster wider, der noch stärker auf Startups mit weniger als zehn Mitarbeitern ausgerichtet ist. Auch der Blockchain-Subcluster weist eine geringere Quote an Startups ohne Daten auf.

5.3.2 Personal Digital Security

Der Cluster Personal Digital Security, bestehend aus 103 Startups, ist relativ gleichmäßig über alle Größenkategorien verteilt. Dies deutet darauf hin, dass der Cluster weder besonders reif noch sehr jung ist. Dies scheint sich in den Subclustern mit kleineren Abweichungen als für unsere Stichprobe zu erwarten war fortzusetzen. Des Weiteren zeigt **Abbildung 39**, dass BYOD Security im Vergleich zum Cluster in stärkerem Maße aus kleineren Startups zu bestehen scheint. Die Größe des Subclusters erlaubt jedoch keinen Rückschluss auf die Gründe für diese Datenlage. Das gleiche gilt für den Subcluster Training, da auch dieser nur vier Startups umfasst und nur für zwei davon Mitarbeiterstatistiken vorliegen.

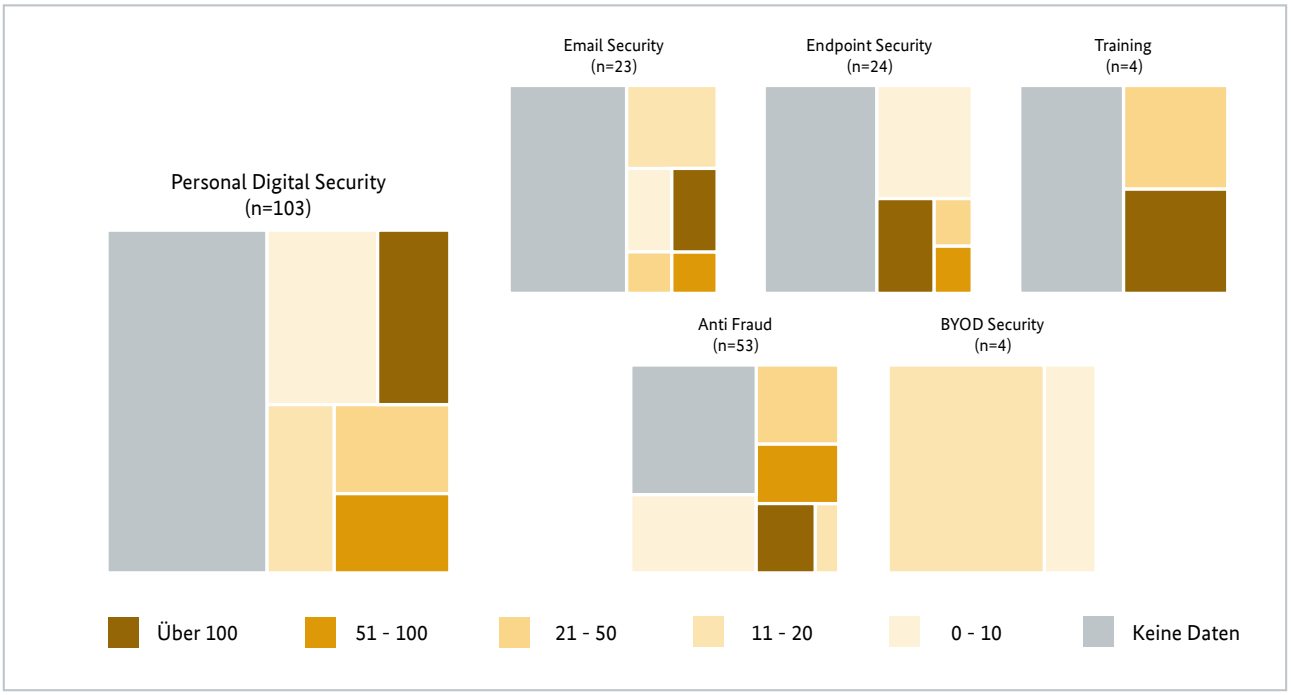

***Abbildung 39**: Mitarbeiterstatistik im Cluster Personal Digital Security*

5.3.3 Analytics

Von den vier in dieser Landscape identifizierten Clustern umfasst der in **Abbildung 40** gezeigte Cluster Analytics die geringste Anzahl von Subclustern. Dennoch konnten wir von über 62 Prozent der Startups valide Daten zu ihren Mitarbeiterzahlen erheben. Während die meisten Startups etwa 21 bis 50 Mitarbeiter haben, sind hier sowohl die größte Kategorie (100+ Mitarbeiter) als auch die kleinste Kategorie (unter zehn Mitarbeiter) mit acht bzw. sieben Startups vertreten. Der größte Subcluster, Security Analytics, bestimmt die Verteilung des Clusters, wobei der Schwerpunkt hier auf kleinen oder großen Startups liegt. Die häufigste Unternehmensgröße in diesem Subcluster ist die Kategorie 21 bis 50 Mitarbeiter, in die neun Startups fallen. Die elf Startups im Subcluster Threat Intelligence sind ähnlich verteilt, nur die Kategorie 11 bis 20 Mitarbeiter ist hier nicht vertreten. Der Subcluster Document Management umfasst schlussendlich drei kleinere bis mittelgroße Startups, was die bereits in **Kapitel 3.1.3** genannte These eines Nischenangebots unterstreicht.

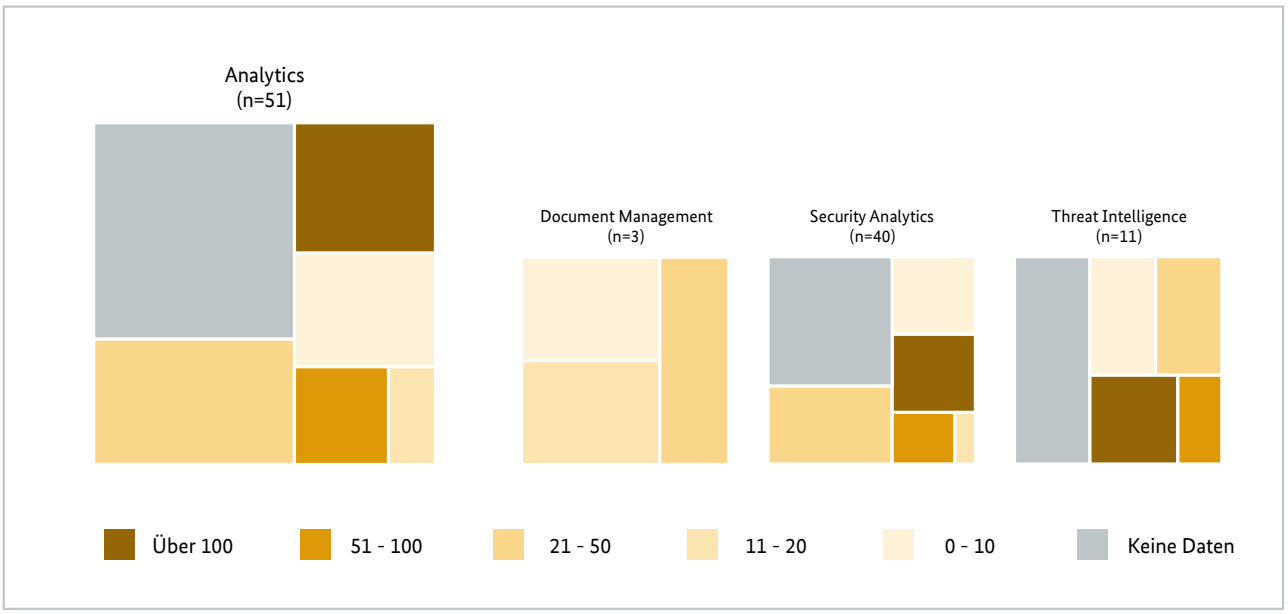

***Abbildung 40**: Mitarbeiterstatistik in Analytics*

5.3.4 OT & Application Security

Im Cluster OT & Application Security, der in **Abbildung 41** dargestellt ist, können wir eine hohe Datenverfügbarkeit beobachten: Nur bei 25 % der Startups liegen keine Daten vor, um diese in eine Kategorie einsortieren zu können. Mit Ausnahme der Kategorie 51 bis 100 Mitarbeiter, in die nur vier Startups fallen und die somit die kleinste Kategorie darstellt, verteilen sich die Startups relativ gleichmäßig auf alle anderen Kategorien. Auf Ebene der Subcluster unterscheidet sich hingegen die Verteilung innerhalb der einzelnen Subcluster. Während die Startups im Subcluster Application Security recht gleichmäßig verteilt sind, zeigen sowohl der Subcluster Authentication als auch der Subcluster IoT Security größtenteils Unternehmen mit weniger Mitarbeitern. Der Subcluster Industrial Security besteht nur aus vier Startups, davon jedoch zwei mit mehr als 100 Mitarbeitern. Auch dies kann als Indikator dafür gesehen werden, dass die Abdeckung industrieller Räume einen abweichenden Ansatz bei der Ressourcenverteilung, einschließlich der des Personals, erfordert.

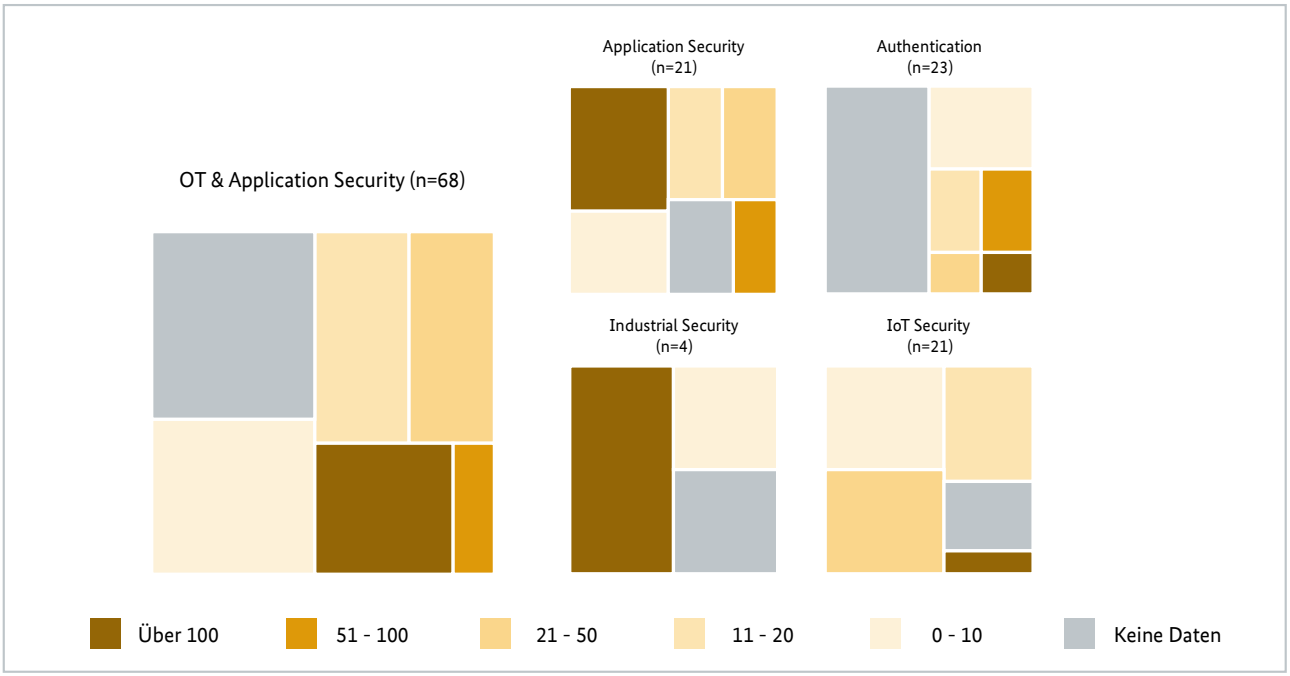

***Abbildung 41**: Mitarbeiterstatistik im Cluster OT Security*

5.4 Investoren und Acceleratoren

In diesem Kapitel konzentrieren wir uns auf eine andere Gruppe von Akteuren in der Bay Area, die die Landscape und die Startups beeinflussen – Investoren und Acceleratoren. Wir beginnen damit, in diesem Zusammenhang zwischen verschiedenen Arten von Organisationen zu unterscheiden und folgen dann mit einer eingehenden Untersuchung der erfolgreichsten Akteure in diesem Bereich.

5.4.1 Definition von Startup-Investoren

Bevor eine detaillierte statistische Analyse der Investoren durchgeführt wird, lohnt es sich, die verschiedenen Anlagemodelle zu erläutern. Acceleratoren bereiten Unternehmen im Frühstadium auf die Markteinführung ihrer Produkte oder Prototypen vor und kümmern sich um relevante Fragen der strategischen Planung, des Betriebs und des Managements. Im Gegensatz zu Inkubatorprogrammen, die sich über Jahre erstrecken können, verbringen Startups in der Regel nur wenige Monate in einem Acceleratorprogramm. Einige Acceleratoren, z. B. *Y Combinator* oder *Plug and Play*, fungieren als Mikroinvestoren und finanzieren ihre Startups im Rahmen des Programms mit Investitionen von weniger als Mio. USD 1. Diese Organisationen, die den Accelerator verwalten und finanzieren, erhalten als Gegenleistung für ihre Beiträge eine geringe Kapitalbeteiligung (etwa <6 %).

Risikokapital (VC)-Firmen sind eine Form der Finanzierung, bei der Geld in Startups angelegt wird, um im Gegenzug Anteile an diesem Unternehmen zu erhalten. Im Bereich des Risikokapitals entspricht diese Beteiligung oft einem großen Anteil, der jedoch immer noch eine operative Kontrolle von 50 % oder weniger des Unternehmens bedeutet, welches die Kapitalspritze erhält. VCS stehen häufig hinter den am besten finanzierten und berühmtesten Startups und deren Ausstiege, z. B. Facebook, Cisco, Oracle oder Google. Im Gegensatz dazu operieren Corporate Venture Capital (CVC)-Firmen in der Regel im Rahmen eines großen, etablierten Unternehmens, z. B. Cisco Investments, BMW iVentures, Robert Bosch Venture Capital. Viele CVC-Unternehmen erhalten Betriebsmittel von ihrer Muttergesellschaft, und im Gegensatz zu ihren traditionellen VC-Partnern streben CVC-Teams eine Minderheitsbeteiligung an dem Startup an (oft <5 %).

5.4.2 Investorenanalyse

Für unsere Investorenanalyse haben wir die sechs am stärksten involvierten Anleger in unserer Landscape (= Anzahl der Investitionen) identifiziert. Die Ergebnisse sind in **Abbildung 42** dargestellt.

Investor	Plug and Play Tech Center	Y Combinator	Insight Partners	Accel	Andreessen Horowitz	Sequoia Capital
Investortyp	*Accelerator/ Frühphase-VC-Investor (micro-inv.)*	*Accelerator/ Frühphase-VC-Investor (micro-inv.)*	*Früh- bis Spätphasen-VC-Investor in Softwaretechnologie*	*Früh- bis Spätphasen-VC-Investor*	*Phasenagnostischer VC-Investor*	*Früh- bis Spätphasen-VC-Investor*
Sitz	Sunnyvale, USA	Mountain View, USA	New York, USA	Palo Alto, USA	Menlo Park, USA	Menlo Park, USA
Portfolio-Startups	**1.501**	**4.717**	**797**	**1.057**	**966**	**1.578**
Portfolio Akquisitionen	**140**	**467**	**223**	**344**	**204**	**383**
Durchschnittl. Akquisitionsrate	9.3 %	9.9 %	27.9 %	32.5 %	21.1 %	24.2 %
Landscape Bezug	**23**	**22**	**10**	**10**	**10**	**9**
Top Cluster	Personal Digital Sec. **(8)**	Digital Infrastr. Sec. **(9)** Personal Digital Sec. (**9**)	Digital Infrastr. Sec. **(5)**	Digital Infrastr. Sec. **(4)**	Digital Infrastr. Sec. **(6)**	Digital Infrastr. Sec. **(4)**
Top Subcluster	Anti-Fraud **(6)**	Anti-Fraud **(5)**	Data Security (**2**) & Network Security **(2)**	Cloud Security (**2**) & Anti Fraud **(2)**	Anti-Fraud **(4)**	Security Analytics **(2)**

***Abbildung 42**: Übersicht der 6 am stärksten involvierten Anleger*

Wie gezeigt, fallen innerhalb der Gruppe insgesamt 84 Investments in unsere Suchparameter. Im Durchschnitt haben diese Investoren eine Erwerbsquote von 16,6 %, was bedeutet, dass etwa eines von sechs Startups, in die sie investieren, später gekauft wird. Die Gesamtzahl der Startups in ihrem Portfolio beläuft sich auf 10.616 in verschiedenen Ländern und Branchen. Diese Tatsache, kombiniert mit der oben genannten Erwerbsquote, zeigt, dass alle im Folgenden aufgeführten institutionellen Anleger über eine große Erfahrung verfügen.

Während die allgemeine Aktivität solcher Investoren und Acceleratoren darauf hindeutet, dass unsere Schwerpunktbranche und unser Schwerpunktbereich ein hohes Potenzial für die Zukunft haben, sind einige Punkte eine genauere Betrachtung wert. So sticht *Y Combinator* mit der größten Anzahl von Startups im Portfolio, insgesamt 4.717, hervor. Im Cybersicherheitssektor in der Bay Area sind sie jedoch selektiv (22). Wir vermuten, dass dies auf die Tatsache zurückzuführen ist, dass viele Startups im Cybersicherheitssektor umfangreiche Finanzmittel benötigen, was nicht mit *Y Combinator's* traditionellem Mikroinvestor-Ansatz übereinstimmt, der darin besteht, eine hohe Anzahl von Startups mit kleineren Volumina zu finanzieren. Ein weiterer Mikroinvestor führt mit 23 Anlagen die sechs größten Investitionen an: *Plug and Play Tech Center*. Interessanterweise ist dieses Unternehmen auch der einzige Investor und Accelerator in den Top 6, der mit insgesamt acht Investitionen die meisten Anlagen im Cluster Personal Digital Security getätigt hat. Obwohl der Unterschied nicht groß ist, ist er spürbar und könnte auf ein besonderes Interesse in diesem Bereich oder eine allgemeine Anlagestrategie des Accelerators/ Mikroinvestors zur Differenzierung seines Portfolios hinweisen. Im Vergleich dazu ist *Insight Partners* der Anleger mit den wenigsten Investitionen (797) in unserer

Top-Sechs-Liste. Seine Gesamtübernahmequote ist höher als die der vorangegangenen Acceleratoren, aber der Schwerpunkt als Früh- bis Spätphasen-VC-Investor im Bereich Softwaretechnologie ist ebenfalls ein anderer. Das Portfolio ist breit über die Subcluster gestreut, wobei Data Security und Network Security mit jeweils nur zwei Investitionen die Spitzenreiter sind. *Accel* ist mit 32,5 % der erfolgreichste Investor unter den börsennotierten Investoren (u.a. Cybersicherheit). Er investiert in Startups in der Früh- und Spätphase mit Schwerpunkt auf dem Cluster Digital Infrastructure Security (vier Investitionen) und dem Subcluster Cloud-Security und Anti-Fraud (zwei Investitionen). Der Subcluster Cloud Security zeigt deutlich einen anderen, stärker fokussierten Ansatz von *Accel* im Vergleich zu den anderen Investoren in diesem Subcluster. Die zehn Landscape-bezogenen Investitionen von *Accel* werden von *Andreesen Horowitz*, mit einer im Gesamtportfolio ebenfalls leicht überdurchschnittlichen Erfolgsquote von 21,1 %, ergänzt. Die Investitionen wurden überwiegend in den Cluster Digital Infrastructure Security (6) getätigt. Was dieses von den anderen sechs führenden Unternehmen unterscheidet, ist ein eher stufenunabhängiger Ansatz im Rahmen und Kontext dieser Studie. *Sequoia Capital* schließlich hat die geringste Anzahl von Investitionen (9), liegt aber immer noch nahe an der Gruppe von *Insight Partners, Accel und Andreessen Horowitz*. Mit einer Akquisitionsrate von 24,2 % verfügt Sequoia über die drittbeste Portfolioerwerb-Rate unter den sechs größten Investoren. Am besten im Cluster Digital Infrastructure Security zeigt sich Sequoia mit vier Investitionen.

Die sechs größten Investoren bevorzugen das Cluster Digital Infrastructure Security. Mit fünf von sechs Investoren, die die meisten ihrer Investitionen in diesem Cluster haben, ist dies bezeichnend; bedenkt man jedoch, dass fast die Hälfte der aktiven Startups diesem Cluster zugewiesen sind, folgt dieses Ergebnis der allgemeinen Verteilung der Startup Landscape. *Plug and Play Tech Center* investierte entgegen dieser Verteilung in verschiedene Cluster, wobei Personal Digital Security das Cluster mit den meisten Investitionen war. Bei der Untersuchung der Subcluster-Ebene wird deutlich, dass Anti-Fraud der bevorzugte Subcluster von vier der sechs größten Investoren ist. Mit nur 12 % der aktiven Startups in diesem Bereich ist dieser Fokus recht bedeutsam. Wir interpretieren dies als ein Bedürfnis nach Vertrauen im digitalen Raum. Das etablierte Vertrauen zwischen Transaktionsparteien ist die Grundlage eines jeden Wirtschaftssystems, und wir glauben, dass dies eines der Motive für den Fokus der sechs größten Investoren ist. Auf gesellschaftlicher Ebene könnten die hohen Investitionen in den Anti-Fraud Cluster auch eine Antwort auf die Ära der alternativen Fakten und der hybriden Kriegsführung im Zusammenhang mit Fake News sein, aber diese Motive sind lediglich Theorien für das Verhalten der Investoren und ihr hohes Interesse an dem Subcluster Betrugsbekämpfung.

Anlage 1

Startup-Verweise zu Schlüsseltechnologien pro Cluster:

Cluster	KI & ML[5]	Big Data	Internet der Dinge (IoT)	Blockchain-Infrastruktur	Cloud-Technologie	Bild-erkennung	Quanten-computing
Analytics	30	10	2	1	29	0	0
Digital Infrastructure Security	48	38	8	38	126	2	3
OT & Application Security	34	12	21	3	21	8	1
Personal Digital Security	36	17	8	8	77	1	1

[5] Künstliche Intelligenz (KI) und maschinelles Lernen (ML)

Startup-Verweise auf Schlüsseltechnologien pro Subcluster:

Subcluster	KI & ML[6]	Big Data	Internet der Dinge (IoT)	Blockchain-Infrastruktur	Cloud-Technologie	Bild-erkennung	Quanten-computing
Document Management	0	0	1	1	2	0	0
Security Analytics	26	9	1	0	20	0	0
Threat Intelligence	4	1	0	0	7	0	0
Blockchain Security	1	0	0	15	1	1	0
Cloud Security	9	6	1	0	23	0	0
Data Security	23	22	1	18	64	0	3
Database	2	3	0	1	1	0	0
Network Security	7	4	6	0	31	0	0
Server Security	1	1	0	1	1	0	0
Website Security	5	2	0	3	5	1	0
Application Security	13	6	1	0	15	0	0
Authentication	14	3	0	2	2	8	0
Industrial Security	2	1	3	0	0	0	0
IoT Security	5	2	17	1	4	0	1
Anti-Fraud	22	10	2	4	33	1	0
BYOD Security	2	1	1	0	2	0	0
Email Security	4	2	0	2	21	0	1
Endpoint Security	7	4	4	2	17	0	0
Training	1	0	1	0	4	0	0

[6] Siehe **Fußnote 4**

Anlage 2

Mitarbeiterstatistik pro Cluster:

Cluster	1 bis 10	11 bis 20	21 bis 50	51 bis 100	Über 100	Keine Daten
Analytics	9	2	12	4	8	19
Digital Infrastructure Security	37	21	31	9	16	92
OT & Application Security	15	11	11	4	10	17
Personal Digital Security	21	10	11	8	11	48

Mitarbeiterstatistik pro Subcluster:

Subcluster	1 bis 10	11 bis 20	21 bis 50	51 bis 100	Über 100	Keine Daten
Document Management	1	1	1	0	0	0
Security Analytics	6	1	9	3	6	15
Threat Intelligence	2	0	2	1	2	4
Blockchain Security	7	1	1	0	1	6
Cloud Security	7	4	9	2	3	5
Data Security	18	10	17	4	8	45
Database	1	1	1	0	1	0
Network Security	2	3	2	3	2	26
Server Security	0	1	0	0	0	2
Website Security	2	1	1	0	1	8
Application Security	4	4	4	2	6	3
Authentication	4	2	1	2	1	10
Industrial Security	1	0	0	0	2	1

Subcluster	1 bis 10	11 bis 20	21 bis 50	51 bis 100	Über 100	Keine Daten
IoT Security	6	5	6	0	1	3
Anti-Fraud	12	2	8	6	5	20
BYOD Security	1	3	0	0	0	0
Email Security	2	4	1	1	2	13
Endpoint Security	6	1	1	1	3	13
Training	0	0	1	0	1	2

Anlage 3

Die ausgewählten Deep Dive Profile wurden in einer separaten Datei in Ergänzung zu dieser Studie dargestellt. Anfragen zu den Profilen können an das BSI oder die Cyberagentur gerichtet werden.

Nachstehend sind die 20 ausgewählten Deep Dive Startups - wie in **Kapitel 2.2.2** erwähnt - abgebildet.

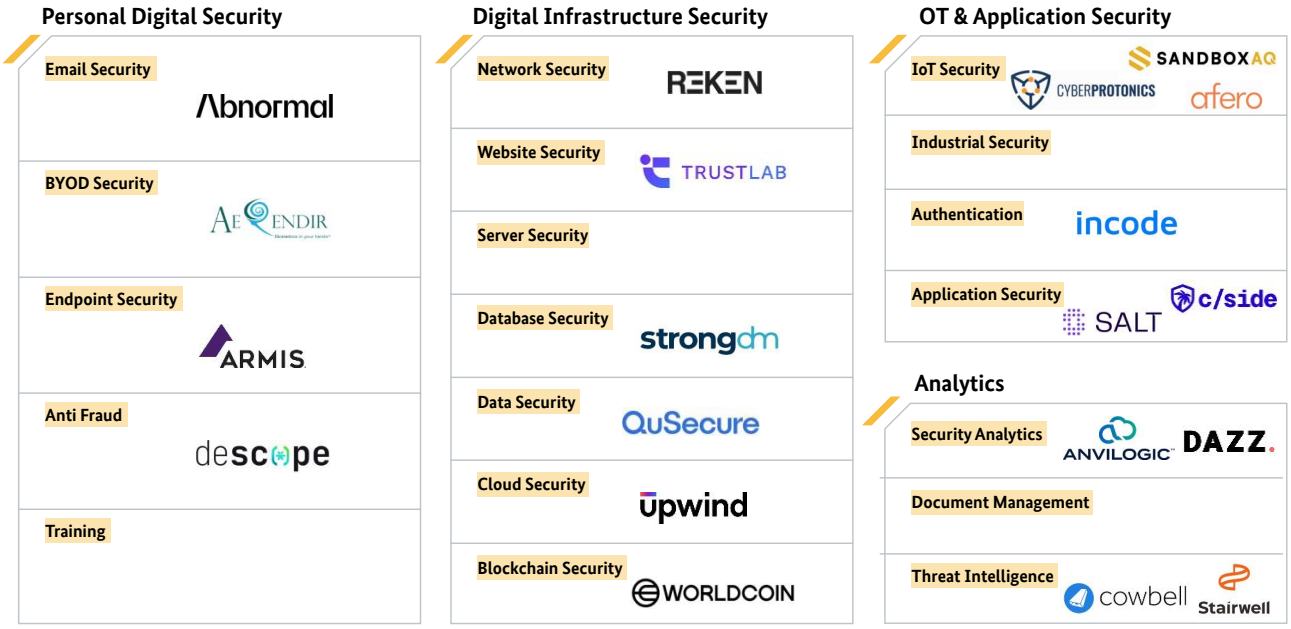

***Abbildung 43**: Cyber Startup Landscape Bay Area – 20 Deep Dive Startups*

Das unten abgebildete Bild dient zur Erläuterung eines exemplarisch abgebildeten Deep Dive Profils, wie sie in der oben genannten Datei vorzufinden ist.

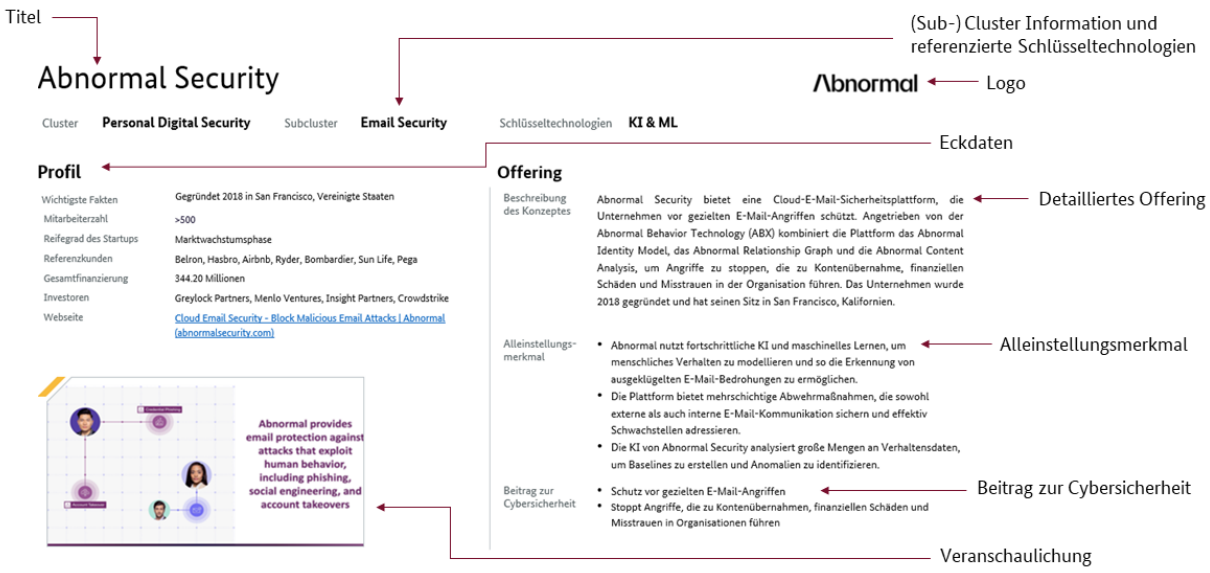

***Abbildung 44**: Struktur des Deep Dive Profils*

Anlage 4

Übersicht der Anzahl an gesichteten Startups pro Land:

Land	Gesamtzahl der Unternehmen (Mitte 2024)
United States	4561
United Kingdom	1218
India	989
Israel	488
China	480
Canada	443
Germany	403
France	363
Australia	309
Singapore	258
Netherlands	248
Spain	177
Switzerland	169
Turkey	155
Russia	144
Italy	136
South Korea	125
Brazil	108
Estonia	105
Japan	100
United Arab Emirates	96
Panama	95
Sweden	95
South Africa	92
Ireland	80
Indonesia	72
Belgium	70
Poland	70
Cyprus	59
Austria	59
New Zealand	59

Land	Gesamtzahl der Unternehmen (Mitte 2024)
Ukraine	54
Czech Republic	54
Malaysia	54
Romania	54
Denmark	54
Iceland	53
Philippines	52
Taiwan	46
Norway	46
Nigeria	44
Portugal	43
Finland	40
Vietnam	39
Thailand	36
Mexico	36
Lithuania	33
Colombia	30
Bulgaria	28
Pakistan	26
Bangladesh	26
Malta	25
Luxembourg	24
Argentina	22
Hungary	21
Chile	20
Slovenia	19
Slovakia	19
Greece	17
Iran	17
Egypt	17
Bahamas	16
Saudi Arabia	16
Anguilla	15
Cayman Islands	14

Land	Gesamtzahl der Unternehmen (Mitte 2024)
Serbia	14
Kenya	13
Latvia	12
Peru	11
Armenia	11
Belarus	11
Montenegro	11
Belize	9
Georgia	9
Lebanon	9
Nepal	8
Croatia	8
Sri Lanka	8
Saint Kitts And Nevis	8
Kazakhstan	7
Morocco	7
Seychelles	7
Bahrain	7
Tunisia	7
Gibraltar	7
Ghana	6
Oman	6
Puerto Rico	5
Mauritius	5
Liechtenstein	4
Uruguay	4
Bosnia And Herzegovina	4
Jersey	4
Albania	4
Saint Vincent And The Grenadines	3
Somalia	3
Costa Rica	3
Kuwait	3
Venezuela	3

Land	Gesamtzahl der Unternehmen (Mitte 2024)
Palau	3
Algeria	3
Ecuador	3
Curacao	3
Trinidad And Tobago	3
Uzbekistan	3
Barbados	3
Uganda	3
Paraguay	2
Guatemala	2
Zambia	2
Andorra	2
Jordan	2
Palestine	2
Azerbaijan	2
Turks And Caicos Islands	2
Cameroon	2
Mozambique	2
Moldova	2
Marshall Islands	1
Iraq	1
Isle Of Man	1
North Macedonia	1
Jamaica	1
Yemen	1
Fiji	1
Channel Islands	1
Mauritania	1
Saint Lucia	1
Guernsey	1
Myanmar	1
Monaco	1
Vanuatu	1
Macedonia	1

Land	Gesamtzahl der Unternehmen (Mitte 2024)
Haiti	1
Bolivia	1
Qatar	1
Martinique	1
Reunion	1
Dominican Republic	1
Dominica	1