DER GRÜNDUNGSINKUBATOR STARTUPSECURE | ATHENE

EIN VERBUNDPROJEKT ZWISCHEN TU DARMSTADT UND FRAUNHOFER SIT

Ein Rückblick auf die letzten 5 Jahre

StartUp Secure
ATHENE

August 2024

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Impressum / Herausgeber

StartUpSecure | ATHENE
Sprechereinrichtung:
Technische Universität Darmstadt
Lehrstuhl Wirtschaftsinformatik |
Software & Digital Business
Hochschulstraße 1
64289 Darmstadt

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft für ihre beiden Darmstädter Institute Fraunhofer Institut für Sichere Informationstechnologie (SIT) und Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) unter Beteiligung der Goethe-Universität Frankfurt/Main, der Technischen Universität Darmstadt und der Hochschule Darmstadt.

VORWORT

Liebe Leser*innen,

die rasanten Entwicklungen in der Digitalisierung revolutionieren unsere Wirtschaft und Gesellschaft. Prozesse werden effizienter, neue Anwendungsfelder entstehen, neue digitale Technologien und Lösungen kommen auf den Markt. Diese positive Entwicklung führt allerdings auch zu einem Anwachsen der Cyberkriminalität: Digitalisierung führt zu mehr und lohnenderen Angriffsmöglichkeiten. Cyberkriminalität ist schon heute eine alltägliche Bedrohung, die Unternehmen, öffentliche Einrichtungen und Privatpersonen gleichermaßen betrifft. Der Branchenverband BITKOM schätzt den jährlichen Schaden durch Cyberangriffe in Deutschland auf über 200 Milliarden Euro – eine horrende Summe. (Quelle: BITKOM)

Die Bedeutung von Cybersicherheit nimmt daher stetig zu. Neue Technologien wie die Künstliche Intelligenz (KI) eröffnet Cyberkriminellen neue Angriffsmöglichkeiten. Daher muss sich die Cybersicherheit mindestens ebenso schnell und umfassend weiterentwickeln wie die Informations- und Kommunikationstechnologien im Zuge der fortschreitenden Digitalisierung. Um den neuen Bedrohungen wirksam entgegenzuwirken, sind kontinuierliche Innovationen im Bereich der Cybersicherheit unerlässlich. Diese Innovationen müssen zudem marktfähig und mit einem soliden Geschäftsmodell verbunden sein.

Das Bewusstsein für die Notwendigkeit von Innovationen in der Cybersicherheit wird durch den Gründungsinkubator StartUpSecure | ATHENE gestärkt. Wir fördern Startups mit innovativen Geschäftsideen und bieten ihnen maßgeschneiderte Unterstützung, Fachexpertise und Netzwerkmöglichkeiten im Bereich Cybersicherheit. Wir tun dies im Verbund mit drei weiteren Inkubatoren aus dem StartUpSecure Programm des Bundesministeriums für Bildung und Forschung (BMBF). Ein großer Dank gilt allen Beteiligten und Unterstützenden, die dazu beigetragen haben, dass der Gründungsinkubator StartUpSecure am ATHENE Zentrum ermöglicht wurde und sich so erfolgreich entwickeln konnte. Seit Beginn des Inkubators im Jahr 2018 ist unsere Arbeit geprägt von neuen Ideen aus der Forschung und zahlreichen Inspirationen, die die Bedeutung und das Potenzial von Innovationen im Bereich der Cybersicherheit verdeutlichen.

Wir laden Sie ein, sich mit uns auf diese Rückschau zu begeben und die spannende Dynamik sowie das transformative Potenzial der Gründungsprojekte von StartUpSecure kennenzulernen. Wir hoffen, dass diese Broschüre nicht nur informiert, sondern Sie auch inspiriert, gemeinsam mit uns eine sicherere digitale Zukunft zu gestalten.

Prof. Dr. Peter Buxmann
Lehrstuhlinhaber
Wirtschaftsinformatik an der TU Darmstadt

Herzliche Grüße

Prof. Dr. Peter Buxmann
Co-Leiter des Gründungsinkubators StartUpSecure | ATHENE

DIE VIER STARTUPSECURE-INKUBATOREN

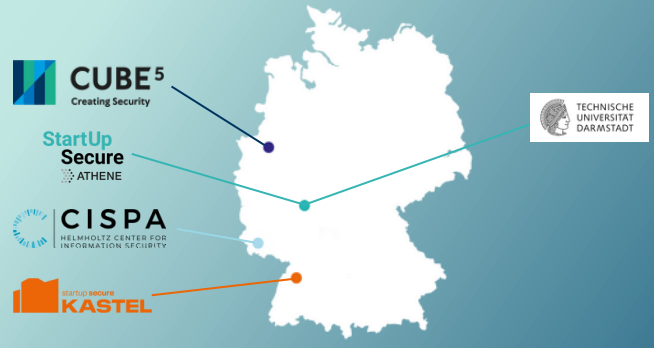
Förderinitiative für Gründungsinteressierte und Startups

Forschungsteams an deutschen Hochschulen oder in der Industrie sind mit ihren Ideen und unkonventionellen Ansätzen häufig Vorreiter neuer Entwicklungen. Um gute Ideen schneller in die Anwendung zu bringen, hat das Bundesministerium für Bildung und Forschung (BMBF) im Jahr 2018 die Initiative StartUpSecure gestartet.

Inkubatoren bringen Startups auf den Weg

Es gibt vier Standorte: CISPA in Saarbrücken, ATHENE in Darmstadt und KASTEL in Karlsruhe sowie CUBE 5 in Bochum.

Der Gründungsinkubator StartupSecure | ATHENE in Darmstadt wurde von der Technischen Universität Darmstadt und dem Fraunhofer-Institut für Sichere Informationstechnologie (SIT) ins Leben gerufen. Nach über fünf Jahren erfolgreicher Zusammenarbeit wird der Inkubator in das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE verstetigt. Diese Verstetigung unterstreicht die Bedeutung und den Erfolg des Inkubators, der als zentrale Anlaufstelle für innovative Startups im Bereich der Cybersicherheit dient und weiterhin ein wichtiger Knotenpunkt im Netzwerk der deutschen Gründungs- und Innovationslandschaft sein wird.



Der Standort Darmstadt

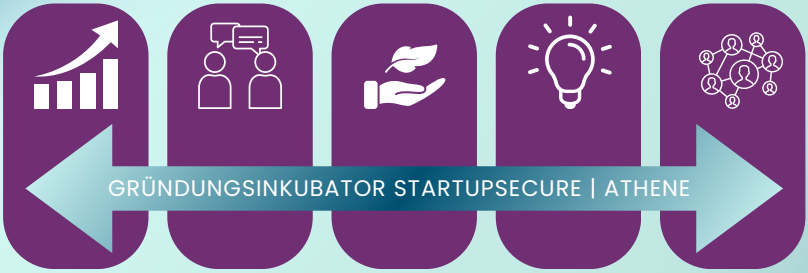
Eine aktuelle Untersuchung des Startup-Verbandes zu Neugründungen im Jahr 2023 zeigt, dass Darmstadt sich als herausragender Gründungsstandort etabliert hat und den dritten Platz in Deutschland belegt.

Mehr dazu...

findet sich auf der Webseite des Bundesministeriums für Bildung und Forschung.

StartUpSecure

Förderinitiativen



Der Gründungsinkubator StartUpSecure | ATHENE stützt sich auf Maßnahmen-Säulen, welche die fokussierten Bereiche des Inkubators verdeutlichen.

"Sichtbarkeit": Die Säule Sichtbarkeit ist von entscheidender Bedeutung, da sie durch gezielte Maßnahmen sicherstellt, dass der Gründungsinkubator als zentrale Anlaufstelle für Cybersicherheitsgründungen wahrgenommen wird und somit die Reichweite für Innovationen im Bereich Cybersicherheit erhöht. Sie umfasst alle Maßnahmen, die den Gründungsinkubator als zentrale Anlaufstelle für Gründungen im Bereich Cybersicherheit positioniert haben. Dazu gehören u.a. Wissenskommunikation, Austausch zwischen den relevanten Akteuren und Wissenschaftstransfer der Bedeutung von Innovationen im Bereich Cybersicherheit.

***"Beratung"*:** Die Beratung hat sich dabei an Gründer*innen und Gründungsinteressierte, Studierende, Wissenschaftler*innen sowie Fachkräfte aus dem ATHENE-Umfeld und darüber hinaus Externe gerichtet. Im Rahmen einer Sprechstunde fand eine technische und fachliche betriebswirtschaftliche Beratung zur Cybersicherheit sowie Beratung unter anderem zu Besonderheiten des Marktes im Bereich IT-Sicherheit statt. Die Beratung wurde nicht nur in der Anfangsphase der Gründungsprojekte genutzt, sondern auch in späteren Phasen. Zudem wurden diese Beratungsgespräche zur Begleitung der Antragsstellung für das Förderprogramm des BMBF für Projekte in der Entwicklungsphase (Phase 1) und Gründungsphase (Phase 2) genutzt.

***"Sensibilisierung"*:** Um aus technischen Lösungen marktfähige Produkte zu entwickeln, bedarf es an weiterem Know-How wie z.B. Nutzen, Nachfrage und Bedarfe von Anwender*innen. Dazu wurde insb. das Accelerator Programm SpeedUpSecure ins Leben gerufen, das im Mai/Juni 2024 das vierte Mal stattfand. Darüber hinaus wurden in der Lehre verschiedene Lehrformate angeboten, bei denen sich Studierende mit der Thematik Entrepreneurship & Innovationen im Cybersicherheits-Umfeld auseinandersetzen konnten, die aber auch den Gründer*innen im StartUpSecure-Umfeld eine Plattform boten, um Talente für ihre Gründungsprojekte zu akquirieren.

***"Ideen-Pooling"*:** Unter dieser Säule wurden Maßnahmen gebündelt, die darauf abzielten, dass neue Ideen entwickelt werden, die im Idealfall in Unternehmensgründungen münden. Dazu gehören: Impulse für die Ideengenerierung, Einsammeln von Gründungsideen, Ideenverfolgung und Analyse von Gründungsideen im Hinblick auf den Markt. Hierzu findet in einer sehr frühen Phase eine Markt- und Wettbewerbsanalyse, eine Überprüfung von Marktchancen und möglichen Geschäftsmodellen statt, sodass sich potenzielle Gründer*innen strategischer bei der Entwicklung von Ideen aufstellen.

***"Vernetzung"*:** Hier wurden insbesondere gründungsrelevante Veranstaltungen/Formate organisiert, um die Vernetzung innerhalb des Ökosystems voranzutreiben. Die StartUpSecure Community besteht unter anderem aus den anderen Partner-Inkubatoren hier in Deutschland und wird ergänzt durch internationale Kontakte. Des Weiteren wurden die Gründer*innen mit Mentor*innen und relevanten Stakeholdern vernetzt.

BERATUNG UND BEGLEITUNG VON GRÜNDUNGSPROJEKTEN IM BEREICH CYBERSICHERHEIT

Seit Beginn des Inkubators bis heute haben wir Gründungsvorhaben – kostenlos, vertraulich und individuell - beraten und begleitet.

Mit dem Inkubator StartUpSecure wurden Gründungsinteressierten und Gründungsteams in einer frühen Phase eine umfassende, individuelle Begleitung und Beratung mit spezifischem Bezug zur IT-Sicherheit angeboten. Aufgebaut wurde der Inkubator im Rahmen eines Verbundprojekts vom Fachgebiet Wirtschaftsinformatik | Software & Digital Business der Technischen Universität Darmstadt und dem Fraunhofer SIT.

Der Inkubator StartUpSecure | ATHENE hat alle notwendigen Faktoren für eine erfolgreiche Existenzgründung eingehend analysiert und dabei besondere Aufmerksamkeit auf die individuellen Bedürfnisse gelegt. Seit dem Start der Initiative des BMBFs wurden bereits 23 geförderte Projekte erfolgreich unterstützt. Diese werden auf den folgenden Seiten vorgestellt.

TU Darmstadt

Die Technische Universität Darmstadt steht für exzellente und relevante Wissenschaft. Globale Transformationen – von der Energiewende über Industrie 4.0 bis zur Künstlichen Intelligenz – fordern sie heraus. Diese tiefgreifenden Veränderungsprozesse gestalten sie durch herausragende Erkenntnisse und zukunftsweisende Studienangebote entscheidend mit. Nicht zuletzt mit dem Forschungsfeld Information and Intelligence (I + I). Dieses bündelt Forschung in den Themen Cybersicherheit, Künstliche Intelligenz, Kognitionswissenschaft, komplexe vernetzte Systeme und Datenschutz.

Fraunhofer SIT

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) zählt zu den weltweit führenden Forschungseinrichtungen für Cybersicherheit und Privatsphärenschutz. Das Institut beschäftigt sich mit den zentralen Sicherheitsherausforderungen in Wirtschaft, Verwaltung und Gesellschaft und betreibt praxisorientierte Spitzenforschung. ATHENE ist hier verankert.

DIE STARTUPSECURE- FÖRDERUNG

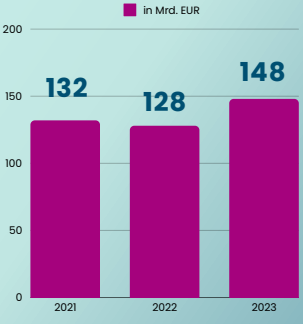
Für die Entwicklungs- und Gründungsphase von innovativen Ideen im Bereich Cybersecurity.

Das BMBF unterstützt dabei in zwei Förderphasen: In einer ersten Phase, **der Entwicklungsphase**, wird erarbeitet, wie die Idee technisch umgesetzt werden kann. Begleitend erstellt das Team ein Geschäftsmodell, um damit den Markt zu evaluieren. Mit der Gründung des Unternehmens startet die zweite Phase, **die Gründungsphase**. Dadurch erfolgt der Transfer in die Wirtschaft, die Erprobung erster Anwendungsszenarien und die Umsetzung des zuvor entwickelten Geschäftsmodells. Weiterhin sind kreative Vermarktung- und Vertriebsstrategien für einen erfolgreichen Unternehmensstart gefragt.

> "Es ist eindeutig ein Aushängeschild von dem Bundesministerium für Bildung und Forschung (BMBF) gefördert zu sein."
>
> Hendrik Amler, Co-Gründer von Polycrypt

> Unser StartUpSecure Projekt war ein wichtiger Baustein für unsere Firmenentwicklung. Die professionelle und hervorragende Unterstützung durch das ATHENE-Team in der Antragsphase hat uns diesen Schritt deutlich erleichtert.
>
> Dr. Kevin Füchsel, Gründer von Quantum Optics Jena

Cyberangriffe sind zur größten Sorge der Unternehmen geworden.



Durch Cyberangriffe entstandene Schäden in Deutschland (Quelle: Bitkom)

TRANSFER IN DIE LEHRE

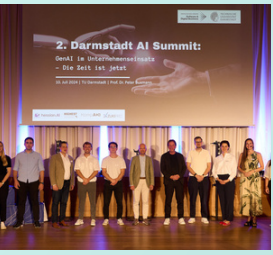
Im Rahmen der Tätigkeiten des Gründungsinkubators wurde eine breite Palette an Lehrformaten angeboten, um innovative Cybersicherheit-Ideen zu entwickeln und junge Talente für diesen wichtigen Bereich zu sensibilisieren. Diese Formate umfassten Praktika, Seminare und Abschlussarbeiten, die speziell darauf ausgelegt waren, praxisnahe Kenntnisse und Fähigkeiten im Kontext von Entrepreneurship & Innovationen im Cybersicherheits-Umfeld zu vermitteln.

Ein zentrales Element unserer Lehrangebote war die Einbindung von Startups mit Projekten, welche von StartUpSecure gefördert werden. Diese Startups dienten als Vorbilder für die Studierenden und boten wertvolle Einblicke in die realen Herausforderungen und Erfolge in der Cybersicherheits-Branche. Die Startups teilten ihre Erfahrungen und Best Practices, was den Studierenden half, ein tieferes Verständnis für die Cybersicherheits-Branche zu entwickeln und sich inspirieren zu lassen.

Darüber hinaus wurde regelmäßig im Rahmen der Blockveranstaltung sowohl theoretisches Wissen vermittelt als auch ein praktischer Teil angeboten, der relevante Kenntnisse im Bereich Cybersicherheits-Startups vermittelt. Dabei wurde der Prozess der Unternehmensgründung von der initialen Idee bis zur Realisierung eines umsetzbaren Startups durchgespielt. Zu Beginn erhalten die Teilnehmenden Impulsvorträge, auf deren Grundlage sie in Teams (bestehend aus 3-4 Personen) arbeiten. Die Konzepte und Inhalte, die während der Veranstaltung behandelt werden, sollen auf die individuellen Startup-Ideen der Teilnehmenden angewendet werden. Des Weiteren werden spezifische Aspekte der Unternehmensgründung in der IT-Sicherheitsbranche diskutiert.

IMPRESSIONEN AUS DEN COMMUNITY-VERANSTALTUNGEN

In den letzten Jahren wurden regelmäßig gründungsrelevante Veranstaltungen für die Community organisiert und durchgeführt.



FOUNDERSXCHANGE

Erfahrungsaustausch und ein gut ausgebautes Netzwerk sind entscheidend für den Erfolg einer Gründung.

Deshalb bietet der foundersXchange allen Gründer*innen und Gründungsinteressierten die Möglichkeit, sich in regelmäßigen Abständen mit Gleichgesinnten auszutauschen, in lockerer Atmosphäre wertvolle Kontakte zu knüpfen und spannende Impulsvorträge und Best Practice Erfahrungsberichte von Gründer*innen sowie Expert*innen zu erleben.

Gemeinsam haben der Gründungsinkubator StartUpSecure | ATHENE, das Technologie- und Gründerzentrum HUB31, das hessische Forschungszentrum für Künstliche Intelligenz hessian.AI, das Centrum für Satellitennavigation Hessen cesah, YUBIZZ die Gründungsinitiative der h_da und das Innovations- und Gründungszentrum HIGHEST den foundersXchange zu wechselnden aktuellen Themenschwerpunkten veranstaltet.

Das fXc Orga-Team

CESAH · hessian.AI · StartUp Secure ATHENE · HIGHEST Innovations- & Gründungszentrum Technische Universität Darmstadt · HUB31 Technologie- und Gründerzentrum Darmstadt · YUBIZZ.DE Die Gründungsinitiative der h_da

foundersXchange Cybersecurity-Special im Juni 2024

Kontakt

gude@foundersxchange.de

ACCELERATOR PROGRAMM SPEEDUPSECURE

Intensives Programm für Cybersecurity-Startups

Das Accelerator-Programm SpeedUpSecure wurde ins Leben gerufen, um die geförderten Projekte, die eine innovative Lösung bieten und sich in einer frühen Phase der Gründung befinden, mit vielfältigen Ressourcen sowie Qualifizierungs- und Vernetzungsangeboten zu unterstützen.
Ausgerichtet wird der Accelerator von StartUpSecure | ATHENE mit Unterstützung der Partner-Inkubatoren am CISPA, StartUpSecure KASTEL und Cube 5.

Accelerator

Module

- Trainings durch spezialisierte Referent*innen
- Begleitung & Beratung durch erfahrene Mentor*innen aus der Wirtschaft
- Austausch mit der Community, anderen Gründer*innen und Alumni
- Impulsvorträge von Gründer*innen von Cybersicherheits-Startups und Expert*innen
- Speed-Dating mit potentiellen Investor*innen
- Zugriff auf ein starkes Netzwerk

Der Final Pitch Day ist das Abschlussevent des Programms, bei dem die Startups ihre Lösung einem Fachpublikum aus der Industrie vorstellen. Die Jury kürt die Sieger*innen des Pitch Events.

Gewinner-Teams

1.Batch	2.Batch	3.Batch	4.Batch
Sanctuary	Quantum Optics Jena	Sanctuary	Trustlens
Bitahoy	DeepSign	Validaitor	InputLab
Aimino	LocateRisk	Lubis EDA	VISS

> Wir haben uns riesig über den Sieg beim Final Pitch Day gefreut und bedanken uns herzlich bei allen Unterstützern. Die Expertensessions haben uns unglaublich viele neue Einblicke verschafft und das Netzwerken beim Kick-off sowie heute beim Final Pitch Day war absolut gewinnbringend.
>
> Philipp Dewald, Gründer Trustlens
> (1. Platz SpeedUpSecures 2024)

> Mit seinem hoch qualitativen und überregionalen Netzwerk hat der Accelerator zum Erfolg von LocateRisk beigetragen. Die zahlreichen Tipps und Tricks - sei es zu Pitch, Investments oder dem Aufbau von Teams - haben uns in der frühen Phase sehr geholfen.
>
> Lukas Baumann, Gründer von LocateRisk
> (3. Platz SpeedUpSecures 2022)

Weitere Informationen

Webseite: www

COMMUNITY & NETZWERK

von StartUpSecure | ATHENE

Ein starkes Netzwerk ist nicht nur für unsere Startups von unschätzbarem Wert. In einer dynamischen und oft unsicheren Umgebung kann das richtige Netzwerk den entscheidenden Unterschied machen, um innovative Gründungsprojekte im Bereich Cybersicherheit in erfolgreiche Unternehmen zu verwandeln. Die hier präsentierten Logos stehen für die Partner und Unterstützenden, die unser Netzwerk zu einem Katalysator für Erfolg machen.

INTERVIEWS MIT UNSEREN MENTOREN

Die Mentor*innen sind Unternehmer*innen und/oder ausgewiesene Expert*innen aus der Wirtschaft. Sie unterstützten mit ihrem Wissen und ihren Erfahrungen sowie dem eigenen Netzwerk. Bei vielfältigen Fragen rund um das individuelle Gründungsvorhaben stehen unsere Mentor*innen Startups mit Rat und Tat zur Seite. Im Folgenden werden sie von ihren persönlichen Erfolgsgeheimnissen und Lebensweisheiten berichten.

Vom Sprung ins kalte Wasser – Ein Interview mit unserem Mentor Guenter Kraft

Guenter Kraft,
Xavira Ventures

Guenter Kraft ist nicht nur Mentor der ersten Stunde für unsere Startups, sondern unterstützt auch den Inkubator selbst, zum Beispiel durch Beratung, als Mitglied der Jury oder durch Zugriff auf sein Netzwerk. Studiert hat er Informatik an der Hochschule Darmstadt, danach ging er zu Cisco Systems, damals Anfang der 90er Jahre noch ein Startup. Zuständig für das Netzwerkmanagement - als Netzwerke gerade erst gebaut wurden - reiste er für das Unternehmen durch ganz Europa. [...]

Zum Interview

Risikobereitschaft im Land der Dichter und Denker - Ein Interview mit unserem Mentor Tolga Yilmaz

Tolga Yilmaz,
Schwarz Digits

Zur Cybersicherheit fand Tolga Yilmaz bereits während des Studiums der Wirtschaftsinformatik durch Neugierde und erste Berührungspunkte mit der Hackerszene im „Wilden-Web". Seit über 20 Jahren arbeitet Tolga Yilmaz in verschiedenen Bereichen – von First Line of Defence bis zu Third Line of Defence – in Unternehmen wie HSBC, MAN Truck & Bus / Volkswagen und aktuell bei Schwarz Digits. Ihm war es dabei immer wichtig, einen breiten Blickwinkel auf die Cybersicherheit zu erhalten. Seit 15 Jahren begleitet Tolga Yilmaz zudem Studierende und Gründerinnen und Gründer als Mentor. [...]

Zum Interview

Von Gründer zu Gründer*innen: Praktische Ratschläge für den Sprung ins kalte Wasser - Ein Interview mit unserem Mentor David Kelm

David Kelm,
Business Angel

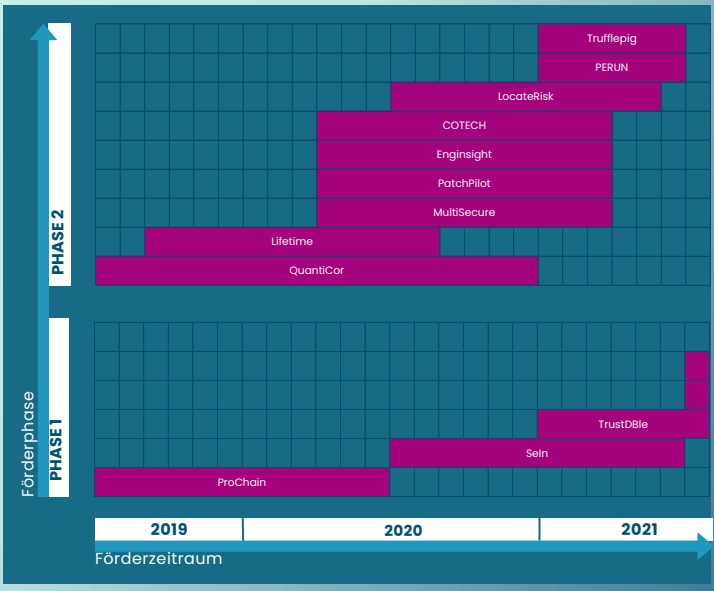
David Kelm ist einer der Gründer der IT-Seal GmbH (StartUpSecure Förderung Phase I). Als CEO hat er das Unternehmen durch mehrere Finanzierungsrunden bis zum EXIT geführt. Er ist mittlerweile als Mentor und Business Angel unterwegs und unterstützt vielversprechende Startups unter anderem im Bereich Go2Market & Growth Strategie, Organisationsaufbau, Equity Story und Finanzierungsrunden – Dinge also, die im Alltagsgeschäft oft liegen bleiben, weil sie nur wichtig, und nicht dringend genug sind. [...]

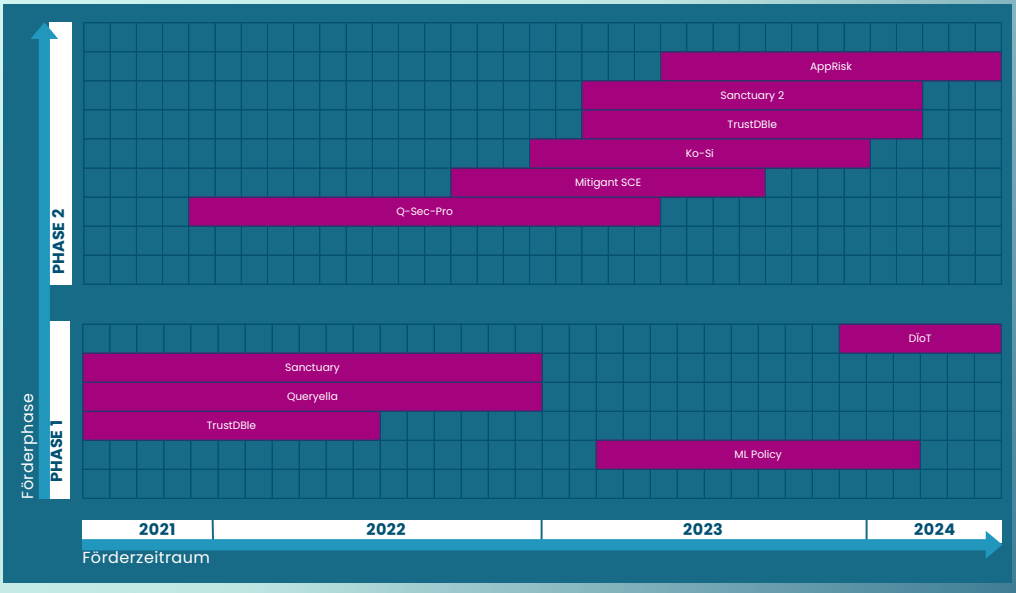
Zum Interview

AUF EINEN BLICK: UNSERE GEFÖRDERTEN PROJEKTE 2019 - 2024

In den letzten Jahren hat der Gründungsinkubator zahlreiche Teams mit innovativen Ideen im Bereich der Cybersicherheit insbesondere aus der Forschung bei ihrer Ausgründung aus Hochschulen und Institutionen begleitet.

In der folgenden Abbildung werden die StartUpSecure geförderten Projekte der Startups am Standort Darmstadt in ihrer Laufzeit und Förderphase dargestellt.





In den folgenden Seiten werden die einzelnen Gründungsprojekte detailliert vorgestellt.

Hinweis: Es besteht keine Gewährleistung für die Richtigkeit, Vollständigkeit oder Aktualität der nachfolgenden Informationen.

PROJEKTE: PROCHAIN UND PERUN
POLYCRYPT GMBH

2020	ca. 720 Tsd.€	ca. 798 Tsd.€	Darmstadt
Gründungsjahr	Fördersumme Phase I	Fördersumme Phase II	Standort

Motivation & Beschreibung der Projekte

Die Verschlüsselung von Datensätzen durch kryptographische Verfahren ist von großer gesellschaftlicher Bedeutung. Denn Kryptographie ist wesentlich, um Datensicherheit sowohl in Unternehmen als auch bei Bürgerinnen und Bürgern zu ermöglichen. Ein vielversprechender Ansatz in diesem Zusammenhang ist die Blockchain-Technologie. Diese integriert als besonderes Merkmal eine verschlüsselte Historie, etwa von Transaktionen mit digitalen Zahlungsmitteln wie die sogenannten Kryptowährungen. Zudem sind an der Verschlüsselung mehrere Computer an verschiedenen Standorten beteiligt. Dieser Verzicht auf eine zentrale Organisationseinheit führt zu einer höheren Sicherheit und Zuverlässigkeit gegenüber Angriffen aus dem Internet. [...]

Startup-Vorstellung

PolyCrypt ist eine Ausgründung aus dem Fachgebiet Angewandte Kryptographie der TU Darmstadt. Die Mission des Startups ist es, neue Innovationen der modernen Kryptografie von der Forschung in die Praxis zu überführen. Hierbei spielen dezentrale Technologien eine große Rolle, die eine Alternative zu großen zentralisierten Lösungen am Markt bieten sollen. Nutzer*innen sollen so wieder mehr Selbstbestimmung über ihre Daten bekommen.

Anerkennungen

2. Preis beim Ideenwettbewerb der TU Darmstadt (2019) | Finalist beim Up@it-sa Award (2019) | Nominiert für den IT-Sicherheitspreis 2020 & Durchsetzung bis zur Preisverleihung | Gewinner ETHGlobal Hackathon (2020)

Anwendungsgebiete

Anwendungen der Technologie finden sich vorwiegend im Web3 Sektor wie beispielsweise die Ausführung von Kleinstbeträgen ohne Gebühren (Micropayment-Networks), der Tausch von Kryptowährungen (Swaps), im Bereich Decentralized Finance (DeFi) oder der Transfer von Sammelgegenständen (Collectibles) zu anderen Ökosystemen/ Marktplätzen im Gaming-Sektor. Darüber hinaus gibt es Anwendungen im Sektor Industrie 4.0, um Zahlungen zwischen IoT Geräten in einem Smart-Factory Szenario zu ermöglichen sowie im Bereich digitale Identitäten (Self-Sovereign-Identity), um sichere Zahlungen für das Ausstellen von Zertifikaten (Credentials) zu ermöglichen.

13
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Web3

Kontakt

Webseite:
polycrypt
info@polycry.pt

BMBF Projektseiten:
Phase I & Phase II

PROJEKT: QUANTICOR
QUANTICOR SECURITY GMBH

2019	ca. 784 Tsd.€	Darmstadt
Projektjahr	Fördersumme Phase II	Standort

Motivation & Beschreibung des Projekts

Gegenwärtige Verfahren für den sicheren digitalen Informationsaustausch beruhen auf komplexen mathematischen Problemen. Diese sind mit konventionellen Rechnern nicht in angemessener Zeit lösbar. Momentan in der Entwicklung befindliche Quantencomputer werden diese Probleme aber deutlich schneller lösen können. Dies bedeutet, dass der Schutz den derzeit verwendete Verschlüsselungsverfahren bieten, außer Kraft gesetzt wird. Abgehörte Datenströme könnten von Quantencomputern entschlüsselt und die Inhalte gelesen werden. Davon ist der überwiegende Teil der vertraulichen und nachvollziehbaren Kommunikation betroffen, insbesondere also auch der Datenaustausch im Internet der Dinge. Eine schnelle Umsetzung praktisch nutzbarer Quantencomputer-resistenter kryptografischer Verfahren ist daher notwendig.

Startup-Vorstellung

Die QuantiCor Security GmbH ist einer der weltweit führenden Entwickler und Hersteller von Quantencomputer-resistenten Sicherheitslösungen für IT-Infrastrukturen und das Internet der Dinge (IoT). Als Partner von großen IT-Unternehmen stattet QuantiCor Security mittelständische und große Unternehmen mit Sicherheitslösungen der nächsten Generation aus.

Anerkennungen

Sieger des Accenture Innovation Awards (2018) | Embedded World Award (2020) | Preisträger des bundesweiten Wettbewerbs „Digitale Innovationen"

Anwendungsgebiete

Das Leistungsspektrum erstreckt sich von der Analyse über die Beratung, Konzeption, Entwicklung und Integration von Software-Lösungen bis hin zu Schulung und Support. Um den Anspruch der nationalen und internationalen Kund*innen im Zeitalter des fortlaufenden Wandels im Bereich IT-Sicherheit gerecht zu werden, forscht QuantiCor Security kontinuierlich im Bereich „Next Generation Cyber Solutions" und agiert aufgrund dessen auch als Partner großer Allianzen wie der Quantum Internet Alliance , welche unter anderem das Ziel der Entwicklung eines Quantum Internets verfolgt.

11+
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/ Internet/ Web 2.0

Kontakt

Webseite:
quanticor-security
info@quanticor-security.de

BMBF Projektseite:
Phase II

PROJEKT: LIFETIME
IT-SEAL GMBH

2016
Gründungsjahr

ca. 720 Tsd.€
Fördersumme
Phase II

Darmstadt
Standort

Motivation & Beschreibung des Projekts

Immer öfter versenden Kriminelle betrügerische E-Mails um an vertrauliche Informationen der Empfänger zu gelangen oder aber schadhafte Software zu verteilen. Diese Nachrichten wirken in ihrer Gestaltung täuschend echt. Selbst erfahrene Empfänger können oft nur sehr schwer feststellen, ob es sich um eine authentische E-Mail handelt. Werden Anhänge dieser Nachrichten geöffnet oder auf Verweise im Text geklickt, werden Passwörter an Kriminelle gesendet oder Schadprogramme auf dem Gerät des Empfängers installiert. Dieses Vorgehen, Phishing genannt, ist ein wichtiges Thema für viele Unternehmen. Der deutschen Wirtschaft entsteht durch diese Art der Angriffe jährlich ein erheblicher Schaden. [...]

Startup-Vorstellung

Als Teil der Hornetsecurity-Gruppe ist IT-Seal auf die Durchführung von IT-Security-Awareness-Trainings spezialisiert. Mit innovativen Technologien trainiert IT-Seal Mitarbeiter*innen von mittelständischen und großen Unternehmen, Risiken im Bereich der IT-Sicherheit effektiv zu erkennen und abzuwehren. Mit innovativen Technologien trainieren sie die Mitarbeiter*innen der Kund*innen im Autopiloten – bedarfsgerecht und kennzahlenbasiert. Ihre wissenschaftliche und patentierte Security-Awareness-Kennzahl ESI® macht das IT-Sicherheitsbewusstsein messbar und somit vergleichbar.

1.Platz
UP 18@it-sa
ATHENE Startup Award

Anerkennungen

Erhält Patent für den Employee Security Index (ESI®) | Bestes Cybersecurity Start-up (2018) | Gewinner des Preises UP18@itsa | 2. Platz als Awareness Security Initiative of the Year - Information Security Days (2018) | Top 10 Cyber Security Startup Europa | Gewinner des europaweiten Social Engineering Award

40+
aktuelle Teamgröße in 2024

Anwendungsgebiete

Das vollautomatische Security Awareness Training ist benutzerfreundlich und bietet maßgeschneiderte On-Demand-Schulungen, die Mitarbeitende in die Lage versetzen, selbst die raffiniertesten Angriffe zu erkennen.

Anwendungs-Branchen:

- IT/Internet/Web 2.0

Kontakt

Webseite:
it-seal
kontakt@it-seal.de

BMBF Projektseite:
Phase II

PROJEKT: MULTISECURE
MESHCLOUD GMBH

meshcloud

2017	ca. 527 Tsd. €	Frankfurt a.M.
Gründungsjahr	Fördersumme Phase II	Standort

Motivation & Beschreibung des Projekts

Unternehmen verschiedenster Industriezweige stehen unter einem hohen Digitalisierungsdruck. Neben Kompetenzen in der Software-Entwicklung ist vor allem die Nutzung von Cloud-Technologien eine Basis für die Entwicklung innovativer digitaler Geschäftsmodelle. Fehlkonfigurationen von Cloud-Plattformen führen jedoch immer wieder zu schwerwiegenden Sicherheitsvorfällen. Ursachen dafür sind meist mangelnde Kontrolle und Transparenz in Bezug auf Organisationsstrukturen und Cloud-Zugriffe. Für Unternehmen ein Dilemma: Auf der einen Seite erfordern moderne Entwicklungsmethoden eine hohe Agilität und eine freie Technologiewahl. Andererseits müssen IT-Infrastrukturen zuverlässig kontrolliert und sicher konfiguriert werden, um Sicherheitsrisiken zu vermeiden. Letzteres soll möglichst die Kreativität und die Effizienz der Mitarbeiter*innen nicht einschränken.

Startup-Vorstellung

Mit meshclouds Lösungen können Unternehmen Cloud-Plattformen sicher und skalierbar betreiben. Entwicklerteams können im Self-Service Accounts erstellen und absichern, Zugriffe verwalten, Kosten abrechnen und weitere Services beziehen. Die zentrale IT in Unternehmen kann alle Cloud-Plattformen in einem System administrieren. Dezentrale Teams können eigene Plattformen aufbauen und einbringen.

40+
aktuelle Teamgröße in 2024

Anerkennungen

Founder Competition (2017) | Hauptpreis Digital Innovation (2017) | Zweiten Platz beim Frankfurter Gründerpreis (2018) | Gewinn des edw Maleki Venture Award for Cyber auf der ersten European Digital Week (2019)

Anwendungs-Branchen:

- Chemie/Pharma
- Energie
- IT/Internet/Web 2.0
- Maschinen- und Fahrzeugbau
- Umwelt/Wasser
- Handel
- Finanzen
- Elektrotechnik/ Telekommunikation

Kontakt

Webseite: www

meshcloud

info@meshcloud.io

BMBF Projektseite: Phase II

PROJEKT: PATCHPILOT
SYNAMIC TECHNOLOGIES

2018
Gründungsjahr

ca. 662 Tsd.€
Fördersumme
Phase II

Darmstadt
Standort

Motivation & Beschreibung des Projekts

Die Nachrichten über Cyberangriffe auf Organisationen nehmen nicht ab. Dabei zählen schon lange nicht nur privatwirtschaftliche Unternehmen zu den Opfern. Auch Krankenhäuser, Kammergerichte und Stadtverwaltungen sind mittlerweile immer häufiger betroffen. Organisationen sind mit der zunehmenden Digitalisierung auch steigenden Risiken durch Cyberangriffe ausgesetzt. IT-Sicherheitsverantwortliche werden mit einer Flut von Informationen konfrontiert, die potenzielle und tatsächliche Angriffe beschreiben. Dabei den Überblick zu behalten, ist eine komplexe Aufgabe, die vielen schwerfällt. Durch den Fachkräftemangel in der IT-Sicherheit fehlen häufig die Kapazitäten und Kompetenzen, um adäquate Verteidigungsmaßnahmen festzulegen. Gerade kleine und mittelständische Unternehmen trifft es dabei besonders hart.

Startup-Vorstellung

Synamic Technologies wurde 2018 als Startup mit dem Ziel gegründet, Prozesse im Bereich der Cybersicherheit zu automatisieren. Das Startup ist auf semantische Technologien und Expertensysteme spezialisiert. Der Cyber Security Knowledge Graph beinhaltet Expertise im Schwachstellen- und Bedrohungsmanagement und bildet die Grundlage für unser Produkt CISOSCOPE.

Anerkennungen

Nominiert für den it-sa Award | Funding vom ELISE-Konsortium für Künstliche Intelligenz für das Projekt SCR.AI | Aktuell wird die Weiterentwicklung des Produktes unter DISTR@L gefördert

Anwendungsgebiete

CQgraff behält die aktuellen Schwachstellen, Risiken und Patches für die Kund*innen im Auge. Der Cyber Security Knowledge Graph unterstützt bei der Identifizierung und Behebung von Schwachstellen in der IT-Infrastruktur mit Hilfe von KI.

3
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/ Internet/ Web 2.0
- Maschinen- und Fahrzeugbau
- Finanzen und Energie

Kontakt

Webseite:
synamic
sven@synamic-technologies.com

BMBF Projektseite:
Phase II

PROJEKT: ENGINSIGHT
ENGINSIGHT GMBH

ENGINSIGHT

2017	ca. 638 Tsd. €	Jena
Gründungsjahr	Fördersumme Phase II	Standort

Motivation & Beschreibung des Projekts

Die voranschreitende Digitalisierung eröffnet neue Möglichkeiten: Innovationen und zukunftsweisende technische Lösungen entstehen binnen kürzester Zeit und revolutionieren ganze Märkte. Doch je mehr Systeme vernetzt werden und Daten „ins Netz fließen", desto interessanter werden diese Systeme für Hacker. Gleichzeitig bedeutet mehr Digitalisierung auch mehr Komplexität und damit mehr mögliche Angriffsflächen. Hierdurch wird es für Unternehmen immer schwieriger, eine adäquate Kontrolle über ihre IT-Systeme zu behalten. Als Ergebnis dieser Entwicklungen werden sowohl große als auch mittlere und kleine Unternehmen mit zunehmender Häufigkeit Opfer von Cyberangriffen.

Startup-Vorstellung

Enginsight bietet eine Vielzahl von Funktionen, darunter Schwachstellen-Scans, Netzwerk- und Anwendungssicherheitsanalysen, Risikobewertungen, Compliance-Checks, Datenanalyse und mehr. Die Plattform ist einfach zu bedienen und bietet Unternehmen eine benutzerfreundliche Oberfläche, die es ihnen ermöglicht, ihre Sicherheitsstrategien zu planen, zu implementieren und zu überwachen.

Anerkennungen

Thüringer Gründerpreis (2017) | Nominierungen für den upAward der it-sa (2018, 2019 & 2020)

40+
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- Chemie/Pharma
- Energie
- IT/Internet/Web 2.0
- Maschinen- und Fahrzeugbau
- Bildungssektor
- Medizintechnik
- Elektrotechnik/ Telekommunikation
- Handel

Kontakt

Webseite:
enginsight
hello@enginsight.com

BMBF Projektseite:
Phase II

PROJEKT: COTECH
HEYLOGIN GMBH

2017
Gründungsjahr

ca. 702 Tsd.€
Fördersumme
Phase II

Braunschweig
Standort

Motivation & Beschreibung des Projekts

Passwörter gelten als eine der größten Sicherheitslücken in Unternehmen. Viele Technologiekonzerne sind deshalb schon längst zum Einsatz einer elektronischen Karte zur Identifizierung übergegangen, einem sogenannten Security Key. Missbräuchliche Zugriffe auf die unternehmensinternen Nutzerkonten können damit verhindert werden. Für große Technologiekonzerne ist es mittlerweile kein Problem mehr, Nutzende in der eigenen Software mittels Security Keys zu authentifizieren. Die benötigte Sicherheitssoftware lässt sich in der eigenen IT-Abteilung schnell fertigen. Doch bereits Großunternehmen aus anderen Branchen fehlt es an Expertise, um eine solche Aufgabe zu bewältigen. [...]

Startup-Vorstellung

IT-Sicherheit muss nicht kompliziert sein, da ist man sich bei heylogin einig. Deshalb entwickelt heylogin, den ersten Passwortmanager ohne Masterpasswort. Angefangen hat alles mit den Gründern Dominik und Vincent. Beide beschäftigten sich schon während ihrer Forschungszeit mit Verschlüsselung und arbeiteten bereits an Alternativen zum Passwort. Als Sicherheitsberater erlebten sie schließlich die harte Realität im Tagesgeschäft ihrer Kund*innen: unsichere Passwörter auf Post-Its oder in Excel-Tabellen, alles frei geteilt und offen zugänglich ohne Kontrolle für Admins oder Management. Das war der Moment, in dem die Idee von heylogin geboren wurde. Die Confidential Technologies GmbH (COTECH) ist jetzt die heylogin GmbH.

11
aktuelle Teamgröße in 2024

Anerkennungen

Nominierung DEKRA Award (2022) | Nominierung Sparkasse Braunschweig Gründungspreis (2022) | 1. Platz Cybersecurity Summit Juni (2024) | Pre-Seed Runde mit deutschen Business Angels und Mozilla Ventures aus den USA (Sep 2022)

Anwendungs-Branchen:

- Bauwesen/ Architektur/Planung
- Energie
- IT/Internet/Web 2.0
- Maschinen- und Fahrzeugbau
- Umwelt/Wasser
- Biotechnologie
- Marketing/Medien Soziales/Gesundheit
- Elektrotechnik/ Telekommunikation
- Verschiedene Branchen, in denen IT und Internet zum Einsatz kommen.

Anwendungsgebiete

Die Entwicklung von heylogin vereinfacht die Arbeit, indem es das Passwort durch einen Wisch auf dem Smartphone ersetzt. Nach einmaliger Freischaltung kann sich ein Mitarbeitende dann mit nur einem Klick auf jeder beliebigen Website einloggen.

Kontakt

Webseite:
heylogin
hey@heylogin.com

BMBF Projektseite:
Phase II

PROJEKT: LOCATERISK
LOCATERISK GMBH

2020	ca. 728 Tsd.€	Darmstadt
Gründungsjahr	Fördersumme Phase II	Standort

Motivation & Beschreibung des Projekts

In Zeiten zunehmender Digitalisierung aller Arbeitsprozesse sollte IT-Sicherheit höchste Priorität in der Managementebene haben, denn die Digitalisierung birgt auch neue Gefahren. Um der Managementebene schnelle Handlungsempfehlungen geben zu können, muss das fachlich komplexe Thema übersichtlich und kompakt aufbereitet werden. Nur so können Gefährdungssituationen verstanden und die notwendigen Maßnahmen vom Management angewiesen werden. Möglich wird dies durch den Einsatz von Leistungskennzahlen, die bereits in anderen Sparten als Basis von Kommunikation und Planung Anwendung finden. Dieser Ansatz soll im Projekt LocateRisk auf die IT-Sicherheit übertragen werden.

Startup-Vorstellung

Entscheidungen zur Datensicherheit und zum Datenschutz erfordern messbare Informationen. LocateRisk deckt potenzielle IT-Risiken in der externen Angriffsfläche von Organisationen auf und liefert Funktionen zur schnellen Minimierung. Auf Basis der Analysen lassen sich fundiertere Geschäftsentscheidungen treffen und sicherheitskritische Prozesse verbessern.

Anerkennungen

Ausreifung der Technologie | Erfolgreiche Studiendurchführung | Legung der Grundlage für den späteren Unternehmenserfolg | Mitglied der Allianz für Cyber-Sicherheit des BSI | Trägt das Zeichen "IT Security made in Germany" des Bundesverbandes IT-Sicherheit | Best of Technology Award 2024

Anwendungsgebiete

Einfache Prüfung der unternehmensweiten IT-Landschaft auf Sicherheitsrisiken und Datenschutzverletzungen sowie Reduzierung der Lieferkettenrisiken im Unternehmen durch automatische Überwachung von Drittanbietern.

Gewinner 3. Platz des Accelerator 2022

19
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Consulting

Kontakt

Webseite:
locaterisk
info@LocateRisk.com

BMBF Projektseite:
Phase II

PROJEKT: TRUFFLEPIG
TRUFFLEPIG IT-FORENSICS GMBH

2020
Gründungsjahr

ca. 770 Tsd.€
Fördersumme
Phase II

Pfaffenhofen
Standort

Motivation & Beschreibung des Projekts

Aufgrund der zunehmenden Verbreitung leistungsfähiger Geräte wie Smartphones, Tablets und Computer gewinnen IT-forensische Auswertungen an Bedeutung. Viele wichtige Erkenntnisse können durch die Analyse des Arbeitsspeichers gewonnen werden, die oft in der „Incident Response" von Unternehmen sowie von Strafverfolgungsbehörden genutzt wird, etwa zur Identifikation von Schadsoftware oder zur Sicherung von Beweisen. Arbeitsspeicheranalysen sind jedoch aufwendig, da sie verschiedene technische Systeme und Konfigurationen sowie fortgeschrittene Systemkenntnisse erfordern. Dies verlangsamt die Analyse und macht sie fehleranfällig.

Startup-Vorstellung

Trufflepig Forensics ist ein Spezialist für IT-Sicherheit und IT-Forensik.Das Startup hilft Unternehmen bei der Abwehr und Aufarbeitung von Cyberangriffen mit ihrem Incident Response Team und ihren Expert*innen für IT-Forensik. Daneben führen sie Pentests durch und bereiten Unternehmen mit Incident Response Plänen auf den Ernstfall vor. Zudem entwickeln und vertreiben sie die Forensiksoftware Trufflepig.

Spezialgebiete

Durchführung von Risikoprüfungen für das IT-System des Kunden, Abgabe von Empfehlungen und Handeln in unmittelbaren Situationen.

Teilnahme bei Accelerator 2022

SpeedUp Secure

30+
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Consulting

Kontakt

Webseite:
trufflepig-forensics
kontakt@trufflepig-forensics.com

BMBF Projektseite:
Phase II

PROJEKTE: QUERYELLA UND APPRISK
QUERYELLA GMBH

2023	ca. 800Tsd.€	ca. 750Tsd.€	Darmstadt
Gründungsjahr	Fördersumme Phase I	Fördersumme Phase II	Standort

Motivation & Beschreibung der Projekte

Bei Queryella stehen IT-Sicherheit und Datenschutz mobiler Apps im Fokus. Unternehmen, Datenschutzbeauftragte und Zertifizierungsstellen sind oft stark ausgelastet und müssen dennoch sicherstellen, dass mobile Apps den hohen Anforderungen an Sicherheit und Datenschutz gerecht werden.
Queryella bietet eine KI-basierte Plattform, die tiefgehende Analysen zur IT-Sicherheit und Datenschutzkonformität aller mobilen Apps ermöglicht. Unabhängig vom Betriebssystem unterstützt die Plattform eine effiziente Risikobewertung, bevor Apps auf Geräten installiert werden.
Diese Lösung hilft dabei, die Lücke zwischen technischen, datenschutzrechtlichen und gesetzlichen Anforderungen zu schließen, sodass mobile Anwendungen sicher und rechtskonform gestaltet werden können, ohne unnötige Ressourcen zu binden.
Queryella verwendet eine eigene Analyseplattform, die verschiedene Code-Scanner integriert, um potenzielle Gefahren in mobilen Apps bereits vor der Installation zu identifizieren und eine umfassende Risikobewertung zu ermöglichen. Diese Plattform wurde entwickelt, um tiefere Analysen von Applikationen und Programmbibliotheken durchzuführen, einschließlich der Erkennung versteckter Sicherheitsprobleme.
Die Ergebnisse werden automatisiert und benutzerfreundlich aufbereitet, um sowohl Endnutzer als auch Unternehmen effektiv zu unterstützen.

Startup-Vorstellung

Queryella GmbH ist ein Spin-Off der TU Darmstadt und wurde im April 2023 gegründet. Die Mehrzahl der Gründer*innen sind Forscher aus der Software Technology Group von Prof. Mira Mezini. Ergänzt wird dieses Know-How durch Gründer*innen, die einen betriebswirtschaftlichen Hintergrund haben und jahrelange Praxiserfahrung einbringen können.

Teilnahme bei Accelerator 2023

8
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0

Kontakt

Webseite:
queryella
leonid.glanz@queryella.de

BMBF Projektseiten:
Phase I & Phase II

PROJEKTE: SANCTUARY I UND II
SANCTUARY SYSTEMS GMBH

SANCTUARY
The Embedded Security Experts

2023	ca. 960 Tsd.€	ca. 720 Tsd.€	Darmstadt
Gründungsjahr	Fördersumme Phase I	Fördersumme Phase II	Standort

Teilnahme bei Accelerator 2023 & Gewinner 1. Platz
SpeedUp Secure

11
aktuelle Teamgröße in 2024

Anwendungs-Branche:

- Raumfahrt

Motivation & Beschreibung der Projekte

Moderne eingebettete Systeme, also Computersysteme, die für Steuerungsfunktionen eingesetzt werden, stehen vor der Herausforderung einer komplexen Software-Lieferkette. Kostendruck und kurze Markteinführungszeiten zwingen die Anbieter, sich auf Drittanbieter-Software zu verlassen, welcher häufig blind vertraut wird. Dieses Problem hat zu folgenschweren Cyberangriffen mit enormen finanziellen Verlusten geführt. Die im SANCTUARY Projekt entwickelte Software-Lösung, kapselt Komponenten von Drittanbietern proaktiv, um Cyberangriffe effektiv einzudämmen. Kombiniert mit sicheren Identitäten pro Komponente wird das blinde Vertrauen in diese durch explizite Vertrauensbeziehungen ersetzt. Ohne die Notwendigkeit, jeder einzelnen Komponente zu vertrauen, schützt die entwickelte Lösung die Software-Lieferkette der eingebetteten Systeme direkt auf dem Gerät.

Anwendungsgebiete

Die im SANCTUARY Projekt entwickelte Sicherheitsarchitektur kann auf allen eingebetteten Systemen eingesetzt werden, bei denen Software-Komponenten von einer Vielzahl von Herstellern mit Open-Source-Software kombiniert werden. Aktuell werden Teile der Gesamtarchitektur für eine Anwendung auf Satelliten angepasst und erweitert.

Startup-Vorstellung

Die SANCTUARY Systems GmbH entwickelt proaktive Cybersicherheits-Lösungen mit einem Fokus auf eingebetteten Systemen. Das sind Computersysteme, die in den verschiedensten Branchen für Steuerungsfunktionen eingesetzt werden. SANCTUARY Systems bietet seinen Kund*innen einerseits eine durchgängige Unterstützung bei allen Sicherheitsaspekten von Projekten im Embedded-Bereich und andererseits auch fertige Sicherheitslösungen.

Anerkennungen

Gewinn mehrerer ESA-Projektausschreibungen | 1. Platz Pitch-Wettbewerb Booster Accelerator (2021) | 1. Platz Pitch-Wettbewerb SpeedUpSecure Accelerator (2023) | Finale Deutscher Startup-Pokal Cybersecurity (2024) | Finale Innovationstagung der Universität der Bundeswehr (2024)

Kontakt

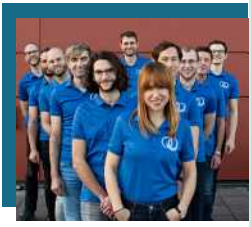
Webseite: www
sanctuary-dev
info@sanctuary.dev

BMBF Projektseiten:
Phase I & Phase II

PROJEKT: Q-SEC-PRO
QUANTUM OPTICS JENA GMBH

2020	ca. 793 Tsd. €	Jena
Gründungsjahr	Fördersumme Phase II	Standort

QUANTUM OPTICS JENA



Motivation & Beschreibung des Projekts

Mit der zunehmenden Digitalisierung in unserer Gesellschaft wächst auch der Bedarf an leistungsfähigen IT-Sicherheitslösungen. Doch viele heute eingesetzte kryptografische Verfahren könnten schon bald von Quantencomputern und Hochleistungsrechnern entschlüsselt werden. Hier kann die Technologie der Quantenkommunikation, insbesondere die Quantenschlüsselverteilung, Abhilfe schaffen. Sie setzt im Gegensatz zu bestehenden Sicherheitslösungen nicht auf der mathematischen, sondern auf der physikalischen Ebene an. Durch Ausnutzung quantenphysikalischer Effekte kann bereits bei der Übertragung von Daten bzw. den dazugehörigen Sicherheitsschlüsseln Abhörsicherheit gewährleistet werden.

Startup-Vorstellung

Die Quantum Optics Jena GmbH ist eine Ausgründung des Fraunhofer-Instituts für Angewandte Optik und Feinmechanik (IOF). Nach der Gründung im Oktober 2020 konnte das junge Unternehmen eine erste Finanzierungsrunde im siebenstelligen Bereich im Januar 2021 sichern. Das Team nutzt quantenphysikalische Effekte, um neue Lösungen im Bereich Informationssicherheit, Bildgebung und Quantenhardware zu entwickeln.

Anerkennungen

IQ Innovationspreis Mitteldeutschland (2022) | Startup Award itsa (2023) | Entwicklung und Aufbau eines Demonstratorsystems

Anwendungsgebiete

Bereitstellung innovativer und kundenspezifischer fortschrittlicher Photonenquellen und quantenoptischer Systeme mit herausragender Leistung für die sichere Kommunikation sowie für die biomedizinische Bildgebung und die Wissenschaft.

Teilnahme bei Accelerator 2022

SpeedUp Secure

1.Platz

UP23@it-sa
ATHENE Startup Award

17
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Forschung
- Elektrotechnik/ Telekommunikation

Kontakt

Webseite:
quantum-optics-jena-gmbh
info@qo-jena.com

BMBF Projektseite:
Phase II

PROJEKT: MITIGANT SCE
MITIGANT GMBH

Mitigant
Be Secure. Be Resilient.

2021	ca. 750Tsd.€	Potsdam
Gründungsjahr	Fördersumme Phase II	Standort

Motivation & Beschreibung des Projekts

Viele Unternehmen nutzen heutzutage Cloud-Computing, greifen also über das Internet auf ausgelagerte Rechenressourcen zu. Doch häufig wissen die Nutzenden nicht, wie sich die Dienstleistungen sicher verwenden lassen. Immer wieder führen etwa Fehlkonfigurationen zu kritischen Schwachstellen, was Cyberangriffe möglich macht. Datenverlust sowie andere Sicherheitsvorfälle sind die Konsequenz. Dies führt nicht nur zu finanziellen Schäden, sondern auch zu Image- und Reputationsverlusten. Die Komplexität der Computersysteme erfordert also neue Werkzeuge und Vorgehensweisen zur Absicherung.

Startup-Vorstellung

Die Mitigant GmbH, vormals Resility GmbH, wurde im November 2021 von dem Team gegründet, das den Startschuss für die Entwicklung von Mitigant gab. Mitigant ist eine Cloud-Sicherheitslösung, die darauf abzielt, die Cloud-Infrastruktur von Unternehmen sicher und widerstandsfähig gegen mögliche Cloud-Angriffe zu machen.

Anerkennungen

Im Dezember 2021 erhielt Resility eine siebenstellige Anfangsfinanzierung von drei deutschen Risikokapitalgebern: High-Tech Gründerfonds, Brandenburg Kapital und adesso Ventures. Im Rahmen des Mitigant SCE-Projekts wurde der Security Chaos Engineering-Ansatz erfolgreich entwickelt. Dieser besteht in einer Cloud Attack Emulations-Funktion für Amazon Web Service (kurz AWS), welche in der Lage ist, Cloud-Attacken auf der Grundlage des MITRE ATT&CK-Frameworks zu emulieren. Im Rahmen des Projekts wurden auch die Sicherheitsassessments für Microsoft Azure und Kubernetes vollständig integriert.

Anwendungsgebiete

Die Mitigant-Plattform revolutioniert die Sicherheit für Cloud-Infrastrukturen, indem sie Unternehmen in die Lage versetzt, Cloud-Compliance, Sicherheit und Cyber-Resilienz praktisch und nahtlos in Einklang zu bringen. Mitigant ermöglicht es Unternehmen, Sicherheitslücken in der implementierten Cloud-Sicherheitsstrategie schnell zu identifizieren, um sicherzustellen, dass die Cloud-nativen Infrastrukturen gegen potenzielle Cyberangriffe (z.B. Ransomware) gewappnet sind.

12
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- Cloud Security
- Cyber Resilience

Kontakt

Webseite:
mitigant
contact@mitigant.io

BMBF Projektseite:
Phase II

PROJEKT: KO-SI
SYNOGATE UG

2021
Gründungsjahr

ca. 660 Tsd.€
Fördersumme Phase II

Berlin
Standort

Motivation & Beschreibung des Projekts

DDoS-Angriffe (Distributed Denial of Service) gehören zu den häufigsten Methoden, um Internetdienste – wie beispielsweise Webseiten – lahmzulegen. Dabei wird eine massive Anzahl von Anfragen an den Dienst gesendet, bis dessen Speicher- und Verarbeitungskapazitäten überlastet sind und der Dienst nicht mehr reagiert.

In sicherheitskritischen Umgebungen erfordert eine umfassende, session-basierte Analyse des Datenverkehrs, dass alle Verbindungsanfragen, unabhängig davon, ob sie gut- oder bösartig sind, für einen bestimmten Zeitraum in einem Kontextspeicher vorgehalten werden. Dies bringt bestehende Systeme schnell an ihre Leistungsgrenzen. Traditionell basieren Sicherheitslösungen gegen DDoS-Angriffe darauf, dass viele Systeme parallelgeschaltet werden, um die enorme Datenlast zu bewältigen. Diese Methode ist jedoch äußerst kosten- und energieintensiv, da sie einen erheblichen Hardwareeinsatz erfordert.
Im Rahmen des Projekts „Kostengünstige Kontextspeicher zum großflächigen Schutz bestehender Infrastruktur (Ko-Si)“ schafft Synogate Lösungen, die dank Hardwarebeschleunigung und effizienter Speichernutzung selbst unter extremen Bedingungen nicht überlastet werden können.

4
aktuelle Teamgröße in 2024

Startup-Vorstellung

Synogate entwickelt digitale Schaltkreisentwürfe für Chips, mit Fokus auf Hochgeschwindigkeitsnetzwerken und KI. Sie arbeiten mit Gatery, ihrem open-source Hardware Construction Library für produktiveres, zugänglicheres Schaltkreisdesign. Dies ermöglicht es ihnen, schnell und iterativ zu entwickeln sowie ihre Expertise in Softwareentwicklung und Kenntnisse in Bereichen wie Algorithmen, Datenstrukturen, Netzwerkprotokollen, Cybersecurity und Machine Learning in den Hardwaredesignprozess einzubringen.

Anerkennungen

Synogate haben die schnellste single-device Stateful Firewall der Welt entwickelt (DDoS-resilient mit 240M neuen Verbindungen pro Sekunde und 200 GbE Stateful Durchsatz).

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Consulting
- Forschung
- Elektrotechnik/ Telekommunikation
- Marketing/Medien
- Marketing/Medien Soziales/Gesundheit
- Netzwerk-Appliances
- Cybersicherheit
- LLM-Beschleuniger
- Halbleiterentwicklung

Kontakt

Webseite:
synogate
mail@synogate.com

BMBF Projektseite:
Phase II

PROJEKT: MLPOLICY

2024	ca. 500 Tsd. €	Köln
Gründungsjahr	Fördersumme Phase I	Standort

Motivation & Beschreibung des Projekts

Managementsysteme für Informationssicherheit (engl. Information Security Management Systems, ISMS) und zugehörige Zertifizierungen dienen dazu, die Informationssicherheit in Unternehmen zu verbessern und Haftungsrisiken zu minimieren. Grundlegendes Fundament ist die Erstellung einer harmonisierten und unternehmensspezifischen Informationssicherheitsrichtlinie (Information Security Policy). Allerdings ist es für Unternehmen aufwändig und kostenintensiv, ein ISMS aufzusetzen und sich zertifizieren zu lassen. Zusätzlich wird oftmals ein hohes Maß an Expertise benötigt, die sich Mitarbeitende der Unternehmen erst aneignen müssen oder die extern von spezialisierten Anbietern eingekauft werden muss. Die hohen Kosten und der Arbeitsaufwand schrecken viele mittelständische Unternehmen davon ab, ein ISMS zu etablieren und sich entsprechend zertifizieren zu lassen.

Startup-Vorstellung

MLPolicy unterstützt Organisationen beim Aufbau einer unternehmensspezifischen Informationssicherheitsrichtlinie durch Künstliche Intelligenz. Die Förderphase II von StartUpSecure wird angestrebt.

Anwendungsgebiete

Die Lösung MLPolicy soll Unternehmen in die Lage versetzen, mit verringertem Aufwand ein Informationssicherheitsmanagementsystem (ISMS) zu erstellen und zu nutzen. Die geplante SaaS-Anwendung soll insbesondere die Erstellung von Informationssicherheitsrichtlinien vereinfachen.

5

aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0

Kontakt

stefan@xpolicy.de

BMBF Projektseite: Phase I

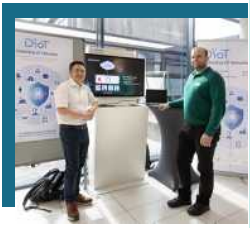
PROJEKT: DÏOT

(vorraus.) 2024
Gründungsjahr

ca. 700Tsd.€
Fördersumme Phase I

Darmstadt
Standort

Motivation & Beschreibung des Projekts



Geräte für das Internet der Dinge (engl. Internet of Things, IoT) werden zunehmend in Haushalten, Fabriken und Smart-City-Infrastrukturen eingesetzt. Schätzungen gehen davon aus, dass die Zahl der IoT-Geräte im Jahr 2025 auf mehr als 30 Milliarden ansteigen wird. Allerdings sind viele dieser Geräte anfällig für Cyberangriffe, was zu Geräteausfällen, Netzwerkunterbrechungen und Datenlecks führen kann. Die bestehenden Abwehrmaßnahmen gegen Cyberangriffe reichen für IoT nicht aus, denn die meisten dieser Maßnahmen basieren auf bekannten Angriffsmustern. So sind sie gegenüber neuen, sogenannten Zero-Day-Angriffen, wirkungslos, weil sie diese nicht erkennen können. Auch auf Anomalieerkennung basierende Lösungen stehen vor Herausforderungen, da die Komplexität und Heterogenität von IoT-Systemen die Erstellung genauer Detektionsprofile erschwert und zu hohen Fehlalarmraten führt.

Startup-Vorstellung

Um die Herausforderung zu meistern, bietet DÏoT eine einzigartige KI-gesteuerte Lösung zur Erkennung von Cyberangriffen im Internet der Dinge (IoT). Im Gegensatz zu kommerziell erhältlichen Lösungen arbeitet DÏoT autonom, erfordert keine langwierige manuelle Einrichtungsphase und kann neue und unbekannte Angriffe (Zero-Day-Angriffe) erkennen. Darüber hinaus bietet DÏoT eine herstellerunabhängige Sicherheitslösung zum Schutz von Geräten und Netzwerken in verschiedenen Anwendungsszenarien, in denen IoT-Geräte zunehmend eingesetzt werden, wie z.B. in Smart Homes, Smart Factories und Smart Cities. Die Förderphase II von StartUpSecure wird angestrebt.

Anerkennungen

Teilnahme als Finalist des Startup Competition des AI Startup Rising Programms von hessian.ai (2024)

Teilnahme bei Accelerator 2024

SpeedUp Secure

7
aktuelle Teamgröße in 2024

Anwendungs-Branchen:

- IT/Internet/Web 2.0
- Cybersicherheit/IoT/AI

Kontakt

Webseite:
diot-iot
info@diot.dev

BMBF Projektseite: Phase I

WEITERE GEFÖRDERTE PROJEKTE

SEIN

Ziel des Projekts Seln ist es, die Identifizierung von natürlichen und juristischen Personen im digitalen EU-Binnenmarkt zu vereinfachen, zu beschleunigen und günstiger zu machen. Es sollen die technischen und rechtlichen Grundlagen für eine neue Art des sicheren und vertrauenswürdigen Online-Identitätsnachweises geschaffen werden. Dieser soll das mittlere Vertrauensniveau „substanziell" nach der Verordnung der EU zur elektronischen Identifizierung (eIDAS) erreichen, für das sich bisher noch kein zugeschnittenes Identifizierungsmittel durchsetzen konnte. Dazu wird im Projekt die aktuelle Zahlungsrichtlinie im Online-Banking PSD2 genutzt, nach der Banken auch Programmierschnittstellen für Drittparteien anbieten müssen. Das Vorhaben setzt also auf bereits vorhandenen Strukturen beim Online-Banking auf und nutzt sie für eine neue Identifikationslösung. […]

➡ weitere Informationen, siehe hier: BMBF

TRUSTDBLE

Ziel des Projektvorhabens „The Trusted Database" (TrustDBle, ausgesprochen: trustable) ist es, eine neue Plattform für ein vertrauenswürdiges Datenmanagement zu entwickeln und bereitzustellen, um Anwendungsfälle für eine gemeinsame Nutzung von Daten besser und schneller umzusetzen. Durch eine standardisierte Schnittstelle, basierend auf der weitverbreiteten Abfragesprache SQL, soll TrustDBle ermöglichen, sogenannte verifizierbare Datenbankprozeduren (Data Contracts) zu definieren. Hierdurch können verbindliche Umsetzungen von individuellen Nutzungsvereinbarungen oder gesetzlichen Vorgaben beim Zugriff auf gemeinsame Daten garantiert werden. Die Entwicklung dieser Plattform soll Blockchains als Speichermedium für gemeinsam genutzte Daten verwenden und mit etablierten Datenbanktechnologien kombinieren. […]

➡ weitere Informationen, siehe hier: BMBF

VUSC

Diesen Herausforderungen wird im Vorhaben VUSC mit einem „App-Scanner für eine sichere IT-Landschaft" begegnet. Der Scanner soll es Unternehmen erlauben, ihre Apps inklusive aller Fremdbestandteile während der Entwicklungsphase auf Schwachstellen zu prüfen. Wichtig für den effektiven und effizienten Einsatz des App-Scanners ist die verlässliche und genaue Erkennung von Gefahren im Softwarecode. Dafür muss an den Erkennungsverfahren geforscht werden. Darüber hinaus werden im Vorhaben Konzepte erarbeitet, wie sich die automatisierte Code-Überprüfung sinnvoll in Unternehmensprozesse integrieren lässt. Die Frage der Selektion und Aufbereitung von relevanten Informationen für die entscheidenden Stellen in den Unternehmen ist dabei zentral. […]

➡ weitere Informationen, siehe hier: BMBF

STATEMENTS ZUR STARTUPSECURE-INITIATIVE AUS DEM GRÜNDER*INNEN-NETZWERK

"Wir haben deutlich wahrgenommen, dass es als Deep-Tech-Unternehmen in Deutschland extrem schwierig ist, Kapital zu beschaffen. Daher war das StartUpSecure-Förderprogramm eine wertvolle Unterstützung."

„Als Team zeichnet uns aus, dass wir – vielleicht auch im Vergleich zu anderen Startups – sehr vielfältig aufgestellt sind […]. Wir haben viele Wissenschaftler und Forscher von der TU Darmstadt, die die gesamte Technologie entwickelt haben. Deshalb freuen wir uns besonders so nah an der Initiative zu sein."

„Die Beratung während der Antragstellung war sehr gut und extrem hilfreich."

„Im Deep-Tech-Bereich sind vor allem Erfahrungen mit der Technologie entscheidend, nicht unbedingt frühere Gründungserfahrung. Innerhalb des StartUpSecure Netzwerkes haben wir von den Erfahrungen viel lernen können."

„Im Accelerator-Programm konnten wir wirklich individuell unsere Probleme, wie den Markteintritt und andere Themen, besprechen. Das war unglaublich wertvoll. Die Gründungskultur wurde dort stark gefördert, und die Kompetenzen wurden auf eine Weise aufgebaut, wie es durch theoretische Vorlesungen allein nicht möglich ist."

„Das Förderformat – ich würde das jederzeit unterschreiben – ist eines der besten, das ich bisher gesehen habe, besonders für Startups. Es ist wirklich für Startups konzipiert und sollte meiner Meinung nach unbedingt fortgeführt werden. Wenige Programme waren für uns als Unternehmen so hilfreich wie StartUpSecure."

"Es ist eindeutig ein Aushängeschild von dem Bundesministerium für Bildung und Forschung (BMBF) gefördert zu sein."

WO SEHEN SICH DIE GRÜNDUNGSPROJEKTE IN 5 JAHREN?

"National etabliert mit Stammkund*innen und stabilem Cashflow, der es ermöglicht, Internationalisierung auf Basis der Innovationsführerschaft anzustoßen."

"[...] als wachsendes Startup."

"Als Marktführer in Europa."

"[...] profitabel und auf Wachstumskurs."

DANKESCHÖN

"Nach knapp über fünf Jahren Gründungsinkubator wird dieser nach BMBF-Förderende im ATHENE-Forschungszentrum verstetigt. Die Zusammenarbeit mit den anderen Inkubatoren, Partnern, Forschungseinrichtungen und Startup-Projekten im StartUpSecure-Umfeld hat uns stets viel Freude bereitet. Wir sind begeistert, dass unsere Aktivitäten in den letzten Jahren die Sichtbarkeit des Standorts Darmstadt erheblich gesteigert haben und wir gemeinsam viele Erfolge erzielen konnten. Auf weitere erfolgreiche Jahre!"

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung