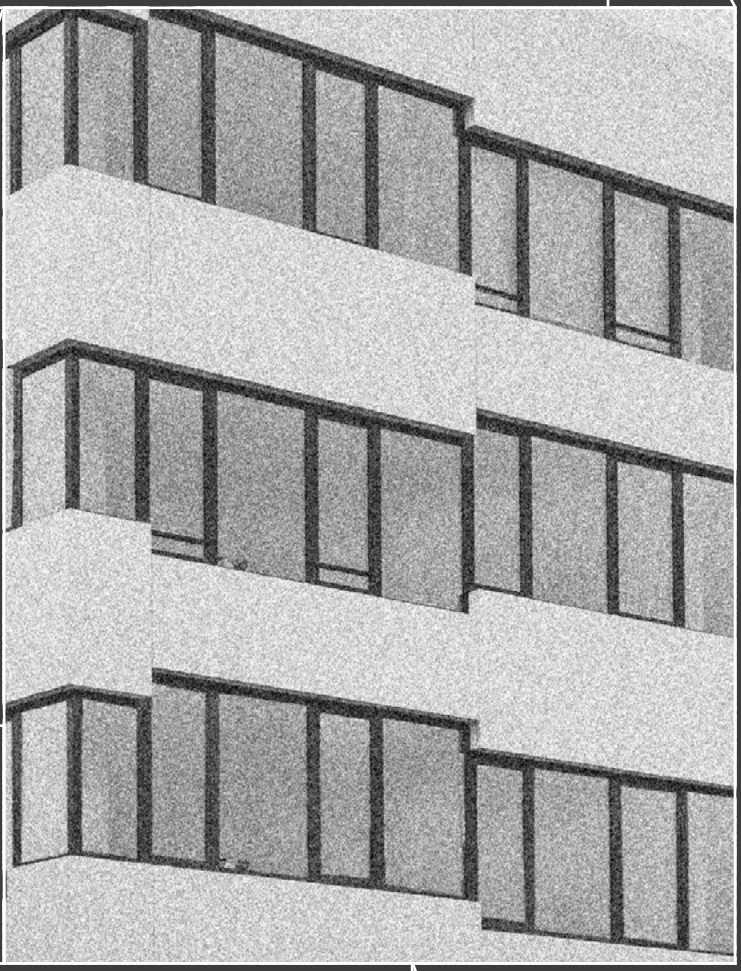
CISPA



CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

ZINE 1

Deutsche Edition

LIEBE LESER:INNEN,

Vor zehn Jahren bestand das heutige *CISPA – Helmholtz-Zentrum für Informationssicherheit* noch aus einer Handvoll Büros und einem Dutzend Menschen. Wie sich das alles entwickeln würde, hätte ich mir damals nicht träumen lassen. Heute forschen und arbeiten hier über 350 Menschen aus der ganzen Welt – Tendenz steigend. Die Zahl unserer leitenden Wissenschaftler:innen ist seit der vollwertigen Aufnahme in die Helmholtz-Gemeinschaft im Jahr 2019 auf 31 angewachsen. Sie alle sind von renommierten Forschungseinrichtungen nach Saarbrücken gekommen. Das zeigt deutlich, welchen Stellenwert unser Forschungsstandort schon heute hat. Inzwischen ist das *CISPA* die Nummer eins der Welt in Cybersicherheit.

Die *CS-Rankings* listen uns vor vielen namenhaften internationalen Forschungseinrichtungen. Mit dieser Spitzenforschung und Projekten wie dem *CISPA Innovation Campus* wollen und werden wir zudem die treibende Kraft des Strukturwandels in der Region und darüber hinaus sein.

Wachstum bedeutet immer auch Veränderung. Leider ist nicht jede Veränderung positiv. So mussten wir uns traurigerweise von unserem ehemaligen administrativen Geschäftsführer Bernd Therre verabschieden, der im September 2021 verstorben ist. Er hat in den ersten Jahren die Entwicklung des Zentrums entscheidend mitgeprägt.

Prof. Dr. Dr. h. c. Michael Backes ©Peter Kerkrath

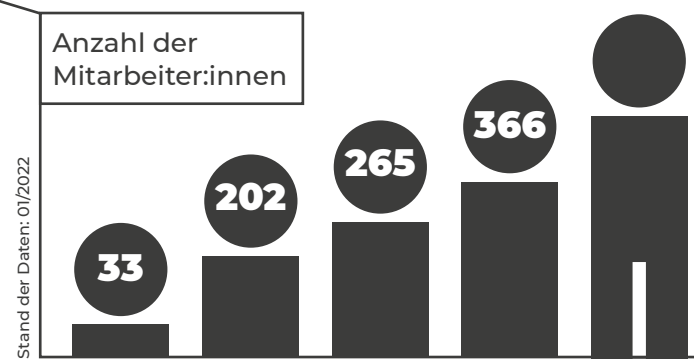
Alles ist im Wandel. Damit dabei sichtbar bleibt, was am *CISPA* alles bewegt wird, gibt es jetzt das *CISPA Zine*. Alle drei Monate berichten wir darin über unsere Cybersicherheits- und KI-Forschung und die Menschen dahinter – von Wissenschaft bis Administration.

Viel Spaß beim Lesen!

Prof. Dr. Dr. h. c. Michael Backes

FACTS ABOUT CISPA

Anzahl der Mitarbeiter:innen



Stand der Daten: 01/2022

38

Nationalitäten am CISPA

Ägypten — Albanien — Bangladesch
Brasilien — Bulgarien — Burkina Faso
China — Deutschland — Frankreich
Gambia — Griechenland — Indien — Irak
Iran — Israel — Italien — Jordanien — Kanada
Kolumbien — Libanon — Malaysia
Nordmazedonien — Niederlande
Österreich — Pakistan — Palästina — Polen
Rumänien — Russland — Schweden
Schweiz — Südkorea — Taiwan — Tunesien
Türkei — Ungarn — Vietnam — Zypern

Altersspanne am CISPA

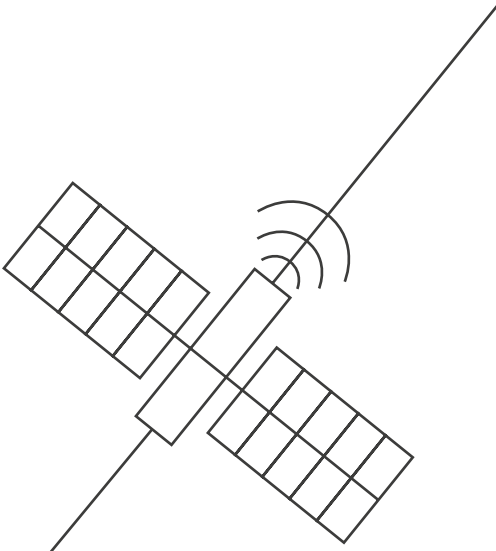
18–57 Jahre

29

Jahre alt sind die Mitarbeiter:innen im Durchschnitt

DAS CISPA WÄCHST:

Das Jahr 2022 ist wie schon seine Vorgänger von der Corona-Pandemie geprägt, die unser Leben einschränkt. Aufhalten lassen wir uns am *CISPA* davon nicht: Unser Zentrum wächst und wächst – mittlerweile nicht mehr nur über die Stadt-, sondern auch über die saarländischen Landesgrenzen hinaus.



Professor Dr. Sascha Fahl baut in Hannover in Zusammenarbeit mit der *Leibniz Universität* und dem Land Niedersachsen den ersten *CISPA-Satelliten* auf. In den kommenden Jahren werden dort Wissenschaftler:innen zu Industriesicherheit und anwenderorientierter Cybersicherheit forschen. Der neue *CISPA*-Faculty macht mit seiner Forschungsgruppe den Anfang. Perspektivisch soll der *CISPA-Satellit* – wie nicht nur Fahl die unselbständige Betriebsstätte in Niedersachsen nennt – noch um ein Vielfaches anwachsen.

Die letzte Hiring Season war sehr erfolgreich. Neben Sascha Fahl konnten neun weitere exzellente Wissenschaftler:innen von Top-Einrichtungen wie der *University of Maryland*, der *Harvard University* und der *ETH Zürich* gewonnen werden, um in Saarbrücken ihre Forschung voranzutreiben und unsere Forschungsbereiche zu erweitern. Der Personalzuwachs beschränkt sich aber bei Weitem nicht auf die wissenschaftlichen Spitzenkräfte. Jeden Monat kommen neue Mitarbeiter:innen zu uns und bereichern das Zentrum im wissenschaftlichen und im administrativen Bereich.

CISPA-Hauptgebäude in Saarbrücken © Stephanie Bremerich

Das Mutterhaus ist längst zu klein für die mittlerweile 366 Mitarbeiter:innen geworden. Büros am Beckertum in St. Ingbert und im alten Sinn-Gebäude in der Innenstadt sollen unser Platzproblem vorerst beheben. Auf der *Alten Schmelz* St. Ingbert entsteht außerdem mit dem Innovation Campus ein einzigartiger Raum für Gründer:innen. Nicht der einzige: Rund um das Haupthaus in Saarbrücken wird ein eigener Campus entstehen. Im Ideenwettbewerb überzeugte der Entwurf des Teams *raumwerk* mit *ST raum a. Landschaftsarchitekten* aus Berlin. In der Verbindung von Urbanität und Natur soll ein einzigartiges und nachhaltiges Forschungsumfeld entstehen. Bis aus dieser Vision Wirklichkeit wird, werden allerdings noch einige Jahre vergehen.

Wo derzeit neben dem *CISPA*-Hauptgebäude noch eine riesige Baugrube eher zum Sandburgenbauen als zum Arbeiten einlädt, sollen im Frühjahr 2023 die ersten Räume bezogen werden können. Die Entstehung des Campus voranzutreiben, steht auf der Agenda des neuen administrativen Geschäftsführers (COO) Dr. Kevin Streit ganz weit oben. Kevin ist ein *CISPA*-Urgestein und war lange unser Verwaltungsleiter. Er folgt auf den ersten COO, Bernd Therre, der traurigerweise kurz nach dem Eintritt in seinen Ruhestand verstarb. Wird sich jetzt alles ändern, Kevin? „Selbstverständlich wird sich alles ändern – aber nicht wegen mir. Wir haben 2019 einen Aufwuchsplan über acht Jahre vorgezeichnet und sind gerade erst in Jahr drei. Da kommen also noch fünf weitere und noch viele Veränderungen. Es ist schade, dass ich Bernd nicht mehr nach seiner Meinung fragen kann.“ Auf die neuen Herausforderungen freut sich der 37-Jährige – und das Tempo, mit dem das *CISPA* wächst, verheißt noch einiges.

Dr. Kevin Streit © Tobias Ebelshäuser

„ICH HABE MICH FÜR DIE WISSENSCHAFT ENTSCHIEDEN — WEGEN DER FREIHEIT“

Prof. Dr. Thorsten Holz hat im Oktober 2021 seine Arbeit am CISPA *aufgenommen. Der neue Tenured Faculty wechselte zu uns von der* Ruhr-Universität *Bochum, wo er in den vergangenen 11,5 Jahren geforscht und gelehrt hat. Seine alte Wirkungsstätte zu verlassen, ist dem 40-Jährigen sicher nicht leichtgefallen. Im Interview verrät er uns, warum er den Sprung dennoch gewagt hat, und wie seine Karriere ihren Anfang nahm.*

Prof. Dr. Thorsten Holz ©Tobias Ebelshäuser

In Saarbrücken eilt dir der Ruf eines exzellenten Forschers auf seinem Gebiet voraus. Was hat dich an der Forschung im Bereich IT-Sicherheit gereizt?

Da kommt wohl ein bisschen der Spieltrieb in mir durch. Als Forscher:in versucht man ja meist, an irgendwelchen Schutzmechanismen vorbeizukommen und so Zugriff auf Dinge zu bekommen, auf die man eigentlich keinen Zugriff haben sollte. Das hat mich schon in der Jugend gereizt. Weil ich das alles spannend fand, habe ich dann auch Informatik als Studienfach gewählt. Während meines Studiums in Aachen bin ich in Kontakt mit dem *Chaos Computer Club* in Köln gekommen und habe dort viel Zeit verbracht. Zusammen mit Freunden habe ich dann angefangen, mich mit der Sicherheit von Funknetzen zu beschäftigen. Dann wurden Honeypots mein Thema – das sind Computersysteme, mit denen Angreifer:innen angelockt werden sollen – und ich habe dazu meine Diplomarbeit geschrieben. Im Laufe der Zeit habe ich mich mehr und mehr auf IT-Sicherheit spezialisiert.

Hast du heute noch Spaß an dem, was du tust?

Ja, absolut! Nach der Promotion hatte ich auch interessante Angebote aus der Wirtschaft. Aber ich habe mich dann doch für die Wissenschaft entschieden, vor allem wegen der Freiheit, die man in der Forschung hat. Und die IT-Sicherheit ist einfach ein spannendes und vielfältiges Thema. Was ich vor fünf Jahren gemacht habe, ist etwas ganz anderes als das, was ich heute mache oder was es in 10 Jahren sein wird. Forschung in diesem Bereich ist nicht monoton, sondern sie entwickelt sich immer weiter.

Woran forschst du gerade?

Wir beschäftigen uns derzeit vor allem mit Themen aus drei Bereichen. Der erste ist Software-Sicherheit. Da befassen wir uns vor allem mit dem sogenannten *Fuzzing*, also dem automatischen Aufspüren von Schwachstellen, und entsprechenden Schutzmechanismen, um Softwaresysteme robuster gegen Angriffe zu machen. Ein wichtiger Aspekt dabei ist *Reverse Engineering*. Diese Technik wird genutzt, wenn man keinen Zugriff auf den *Source Code* hat – also auf das, was ein Programmierer implementiert hat –, sondern nur den *Binärcode* anschauen kann – also das, was die Maschine letztlich ausführt. Der zweite Bereich ist die Schnittstelle von IT-Sicherheit und Maschinellem Lernen. Wir haben zum Beispiel sogenannte *Adversarial Examples* untersucht, die die *ML-Algorithmen* zur Spracherkennung austricksen können. Dazu haben wir Smart Speaker wie *Siri* oder *Alexa* studiert und wollten herausfinden, ob und wie oft sie „aufwachen" und mithören, obwohl ihre Nutzer:innen sie gar nicht angesprochen haben. Der dritte Bereich ist die Sicherheit von Mobilfunksystemen, insbesondere *LTE*. In diesem Bereich haben wir verschiedene Arten von Sicherheitslücken gefunden und praktisch demonstriert.

Warum hast du dich für den Wechsel ans *CISPA* entschieden und bei welchen Themen siehst du Anknüpfungspunkte zu den Forscher:innen hier?

Überzeugt hat mich letztlich, dass das *CISPA* ein sehr großes Zentrum werden soll, das IT-Sicherheit ganzheitlich mit vielen Facetten sieht. Aber natürlich freue ich mich auch auf das andere Umfeld und die neuen Kolleg:innen. Es gibt in meiner Forschung ja auch einige Überschneidungen mit anderen *CISPA*-Forscher:innen. So beschäftigt sich zum Beispiel Andreas Zeller mit Softwaretests, viele Personen arbeiten im Bereich Systemsicherheit, und Mario Fritz ist wie ich im Bereich Machine Learning aktiv. Aber auch in den Bereichen *Usable Security* und *Web Security* gibt es sicher Anknüpfungspunkte mit Katharina Krombholz oder Ben Stock.

DAS FEIERN WIR!

Wir kümmern uns nicht mehr nur um den wissenschaftlichen Nachwuchs, sondern bilden auch in der Verwaltung aus. Am 1. September 2021 hat Sara Starck als erste Auszubildende des *CISPA* ihren Dienst als angehende Kauffrau für Büromanagement angetreten und wird in den kommenden zwei Jahren alle Abteilungen kennenlernen.

Sara Starck
© Tobias Ebelshäuser

Prof. Dr. Andreas Zeller
© Stephanie Bremerich

Den sechsten *Most Influential Paper Award* hat *CISPA*-Faculty Prof. Dr. Andreas Zeller 2021 abgeräumt. Damit gehört er zu den einflussreichsten Forscher:innen der Welt und ist höchst wahrscheinlich Rekordhalter. „Ein *Most Influential Paper Award* zeigt eindrucksvoll, dass die eigene Forschung nicht nur für den Moment Begeisterung hervorrufen konnte, sondern dass die wissenschaftliche Community die Arbeit selbst nach vielen Jahren noch als wegweisend ansieht", sagt *CISPA*-Direktor Prof. Dr. Dr. h. c. Michael Backes.

Insgesamt 108 Paper von *CISPA*-Forscher:innen wurden 2021 auf IT-Konferenzen angenommen, davon 35 auf den Top-4-Konferenzen im Bereich Cybersicherheit und den Top-2 im Bereich Kryptografie. Das wirkt sich auf die *CS-Rankings* aus, in denen wir weiterhin im Bereich Computer Security den ersten Platz belegen und uns im weltweiten Vergleich vor den renommiertesten Einrichtungen platzieren können. Auf diesen Lorbeeren ausruhen werden sich unsere Forscher:innen natürlich nicht, denn die ersten Deadlines laufen schon. Übrigens: Bei der sehr wichtigen IT-Sicherheitskonferenz *CCS* ist *CISPA*-Faculty Cas Cremers gemeinsam mit Elaine Shi in diesem Jahr der verantwortliche Leiter der Programmkommission.

Prof. Dr. Cas Cremers
© Tobias Ebelshäuser

© Tobias Ebelshäuser

Unser erster CISPA-Podcast ist online. In *TL;DR* (kurz für *too long didn't read*) sprechen wir jeden Monat – mal auf Deutsch mal auf Englisch – mit Forscher:innen über ihre Arbeiten zu Cybersicherheitsthemen und Künstlicher Intelligenz. Den Podcast gibt es auf allen gängigen Plattformen.

Herausgeber:
CISPA – Helmholtz-Zentrum
für Informationssicherheit gGmbH
Stuhlsatzenhaus 5
66123 Saarbrücken, Deutschland

Verantwortliche
Redaktion:
Sebastian Klöckner

Redaktion:
Annabelle Theobald

Design:
Lea Mosbach,
Janine Wichmann-Paulus

Stand des Impressums:
Januar 2022

Fotografie:
Stephanie Bremerich,
Tobias Ebelshäuser, Peter Kerkrath

Kontakt
Unternehmenskommunikation:
T: +49 681 87083 2867
M: pr@cispa.de
W: https://cispa.de/

NEUE FACULTY →→→→ 2021

Sebastian Stich

Sebastian Stich kam von der *EPFL Lausanne* zu uns und forscht zu Methoden für verteiltes Maschinelles Lernen. Ihm gelang es, innerhalb von zwei Jahren 15 Paper auf den Top ML-Konferenzen zu präsentieren. Seine hochwertigen Veröffentlichungen werden sehr häufig zitiert, was zu einer beeindruckenden Zitationsstatistik führt.

Rebekka Burkholz

Mit Rebekka Burkholz, zuvor Postdoc an der *Harvard University*, konnte eine ausgebildete Mathematikerin für die Bereiche KI und Maschinelles Lernen, insbesondere die Anwendung auf medizinische Daten, gewonnen werden. Für ihre Promotion erhielt sie den Dissertationspreis der *ETH Zürich*.

Thorsten Holz

Thorsten Holz kommt von der *Ruhr-Universität Bochum* zu uns. Er forscht zu Systemsicherheit, unter anderem zum automatisierten Finden von Software-Schwachstellen und zur Sicherheit von Mobilfunksystemen. Ein weiteres Thema ist die Schnittstelle zwischen IT-Sicherheit und Maschinellem Lernen. Er ist *Heinz Maier-Leibnitz*-Preisträger und erhielt 2014 einen *ERC Starting Grant*.

Aleksandar Bojchevski

Aleksandar Bojchevski promovierte an der *TU München*. Er arbeitet an Forschungsfragen zu vertrauenswürdigem Maschinellen Lernen, beweisbaren Garantien, Interpretierbarkeit, Maschinellem Lernen unter Wahrung der Privatsphäre sowie Maschinellem Lernen auf Graphdaten.

Mridula Singh

Mridula Singh promovierte an der *ETH Zürich* zur Sicherheit von drahtlosen Netzwerken und autonomen Systemen sowie zur Sicherheit der Verwertung von Positionsinformationen. Neben ihren zahlreichen Papern ist ihr Engagement als Co-Leiterin der „CSNOW – Network of Women in Computer Science Initiative“ hervorzuheben.

Christoph Lenzen

Christoph Lenzen kam im Juli vom *Max-Planck-Institut für Informatik* zu uns. Seine Forschung umfasst Theorie und Sicherheit von verteilten Systemen, darunter Clock Synchronization, Fehlertoleranz und verlässliche Hardware. Neben diversen Preisen erhielt er 2017 einen *ERC Starting Grant* sowie 2020 einen *ERC Proof of Concept Grant*.

Julian Loss

Julian Loss kam nach seiner Zeit als Postdoc von der U*niversity of Maryland* ans *CISPA*. Für seine Arbeit erhielt er bereits einen Best Paper Award auf der wissenschaftlichen Konferenz *EUROCRYPT* 2021. Am *CISPA* beschäftigt er sich mit Forschungsfragen zu kryptographischen Protokollen und verteilten Algorithmen.

Sebastian Brandt

Sebastian Brandt war als Postdoc an der *ETH Zürich* und forscht zu sicheren dezentralen Systemen und diskreten und verteilten Algorithmen. Für seine Arbeiten erhielt er mehrere *Best Paper Awards*. Alleine in den Jahren 2019 und 2020 wurden 10 hochwertige Publikationen veröffentlicht.

Karl Wüst

Karl Wüst promovierte an der *ETH Zürich* und konzentriert sich auf Sicherheit und Zuverlässigkeit von Blockchain-Technologie. Sechs seiner Paper wurden auf den Top-4-Security-Konferenzen angenommen. Beeindruckend ist der Impact seiner Arbeiten: Eines seiner Paper wurde bereits mehr als 1000 Mal zitiert.

Sascha Fahl

Sascha Fahl ist Professor an der *Leibniz Universität Hannover*. In Niedersachsen baut er den ersten *CISPA-Satelliten* auf. Sein Forschungsschwerpunkt liegt auf verhaltens- und anwender:innenorientierter Cybersicherheit. Neben zahlreichen Auszeichnungen erhielt Fahl auch den *Heinz Maier-Leibnitz-Preis* der *DFG*.