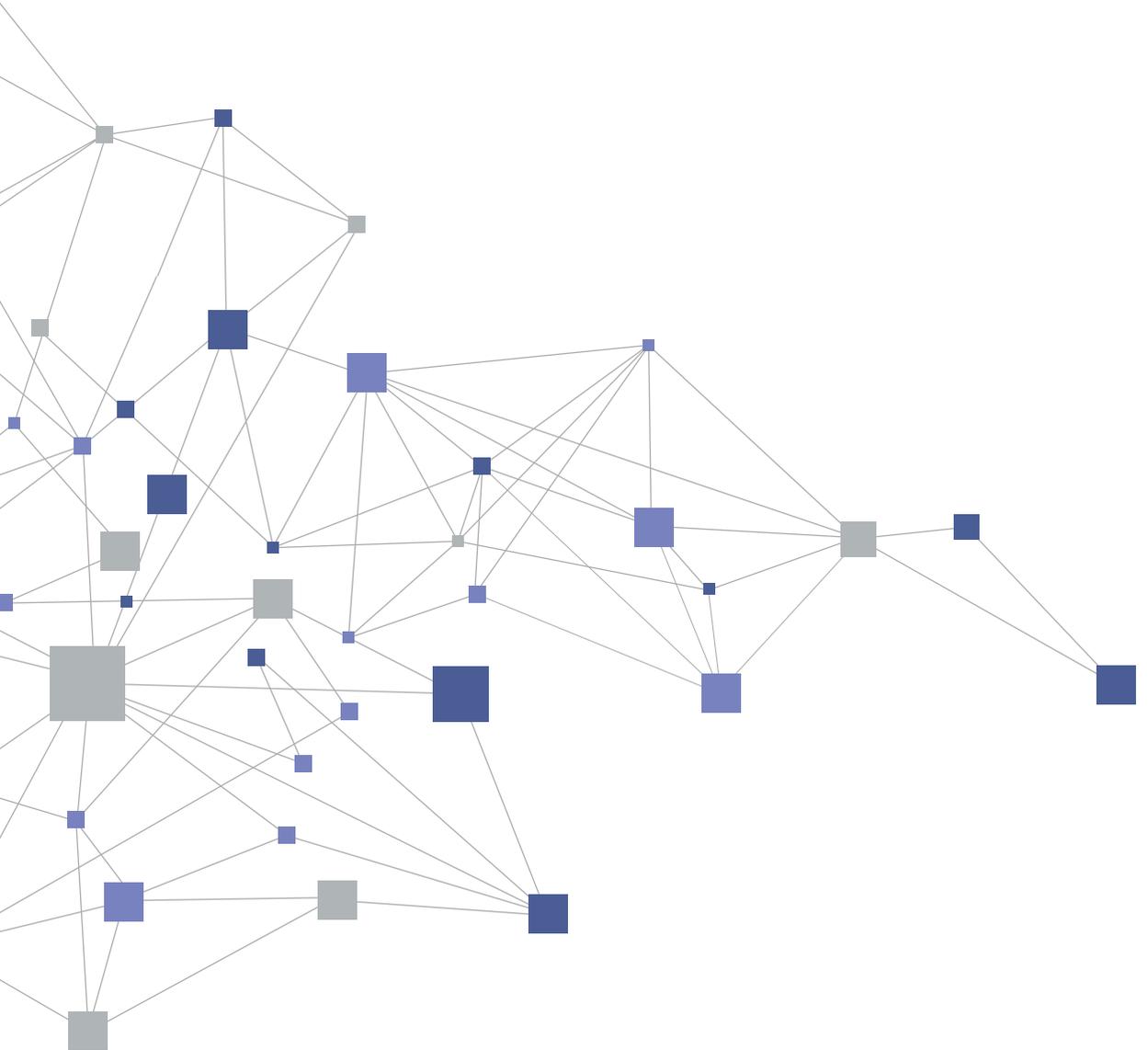


Potsdamer Konferenz für  
**Nationale  
CyberSicherheit  
2024**



## Konferenz-WLAN



Netzwerk: HPI\_Event  
Passwort: plof-BIB-jel

## Konferenz Broschüre / Conference brochure



PDF-Broschüre in Deutsch  
[hpi.de/siko/broschuere\\_de](http://hpi.de/siko/broschuere_de)



PDF brochure in English  
[hpi.de/siko/broschuere\\_en](http://hpi.de/siko/broschuere_en)

# SEHR GEEHRTE TEILNEHMERINNEN UND TEILNEHMER

herzlich willkommen auf der Potsdamer Konferenz für Nationale CyberSicherheit. Wir freuen uns, Sie am Hasso-Plattner-Institut für Digital Engineering begrüßen zu dürfen.

Globale Krisen prägen weiterhin die internationalen Beziehungen - und damit auch die Diskussionen über Cybersicherheit. Konflikte in verschiedenen Krisenherden der Welt werden nicht nur mit Waffen, sondern auch mehr denn je im Cyberraum ausgetragen. Und dies hat direkte Auswirkungen auch auf Deutschland.

Verschiedene Cyberangriffe auf kritische Infrastruktur, Industrie und staatliche Institutionen zeigen uns die Verwundbarkeit unserer digitalisierten Gesellschaft. Die breite Verfügbarkeit generativer künstlicher Intelligenz eröffnet zudem neue Angriffsvektoren und beschleunigt etablierte Methoden. Leider führt uns die Epidemie an Ransomware-Vorfällen in Staat, Wissenschaft und Industrie mit teils langanhaltenden Konsequenzen vor Augen, dass unsere Organisationen und wir als Gesellschaft nicht ausreichend auf diese Herausforderungen vorbereitet sind.

Neben dem Schutz von Systemen geht es in der Cybersicherheit auch immer um den Schutz von Informationen. 2024 ist das globale Superwahljahr - fast die Hälfte der Weltbevölkerung ist zu Wahlen aufgerufen. Mit Desinformation Meinungen zu beeinflussen und damit das Vertrauen in die Demokratie zu zerschlagen - diese Ambition wird mittlerweile im Systemkonflikt offen ausgesprochen und mit intensiven Mitteln verfolgt.

Alle diese großen Konfliktfelder werden auch im Cyberraum ausgetragen und fordern die Widerstandskraft unserer Gesellschaft heraus, worauf Regierungen, Organisationen und die Gesellschaft Antworten finden müssen. In den kommenden zwei Tagen möchten wir mit Ihnen diskutieren, wo wir in Bezug auf Cybersicherheit stehen, wie sich Chancen und Gefahren darstellen und mit welchen Maßnahmen wir diesen Herausforderungen souverän begegnen können.

Wir freuen uns auf den Austausch mit Ihnen.



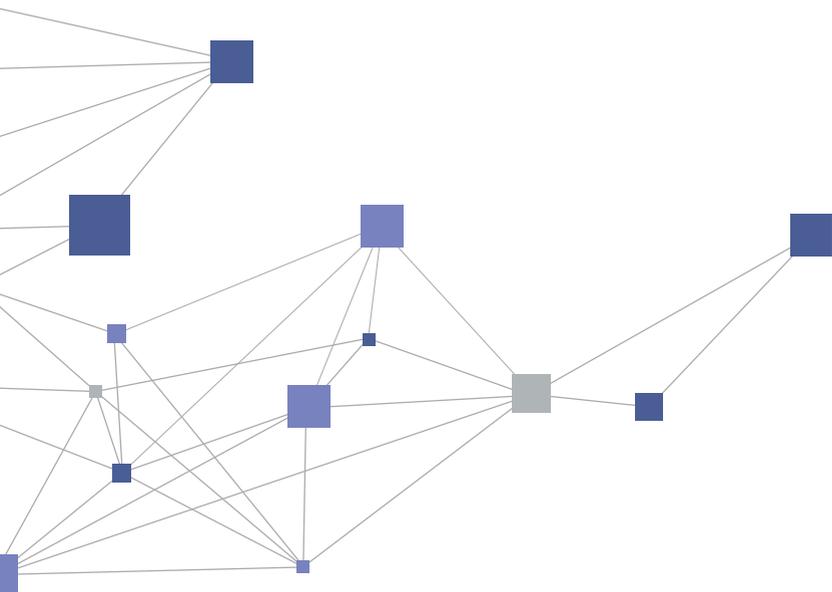
**Prof. Dr. Christian Dörr**  
Vorsitzender der Potsdamer Konferenz  
für Nationale CyberSicherheit

# DAS HASSO-PLATTNER-INSTITUT

Das Hasso-Plattner-Institut (HPI) in Potsdam ist Deutschlands universitäres Exzellenz-Zentrum für Digital Engineering. Mit dem Bachelorstudiengang „IT-Systems Engineering“ bietet die gemeinsame Digital-Engineering-Fakultät des HPI und der Universität Potsdam ein deutschlandweit einmaliges und besonders praxisnahes ingenieurwissenschaftliches Informatikstudium an. Derzeit zählt das HPI mehr als 1000 Studierende.

Wer ein Bachelorstudium in IT-Systems Engineering oder ein gleichwertiges Studium erfolgreich absolviert hat, kann sich für verschiedene Masterprogramme am HPI bewerben. Diese bieten die Möglichkeit, sich tiefgehend und forschungsorientiert mit einem Teilgebiet der Informatik zu beschäftigen und eng mit renommierten Wissenschaftlerinnen und Wissenschaftlern sowie externen Partnern zusammenzuarbeiten. Zur Auswahl stehen dafür am HPI drei Masterstudiengänge:

- **IT-Systems Engineering:** Der Studiengang konzentriert sich auf die arbeitsteiligen Prozesse der Entwicklung sowie die Verteilung und Nutzung von komplexen Softwaresystemen.
- **Digital Health:** Der interdisziplinäre, englischsprachige Masterstudiengang richtet sich an Studierende mit einem Informatik- oder Medizinhintergrund, die das Gesundheitssystem durch den gezielten Einsatz neuer IT-Technologien voranbringen wollen.
- **Computer Science:** Das interdisziplinäre, englischsprachige Studium vereint diverse Informatikdisziplinen, um zukunftsweisende Themen unserer Zeit zu adressieren: Von der Digitalisierung in der Medizin bis zur Gestaltung von künstlicher Intelligenz, die inklusiv und verantwortungsbewusst agiert.



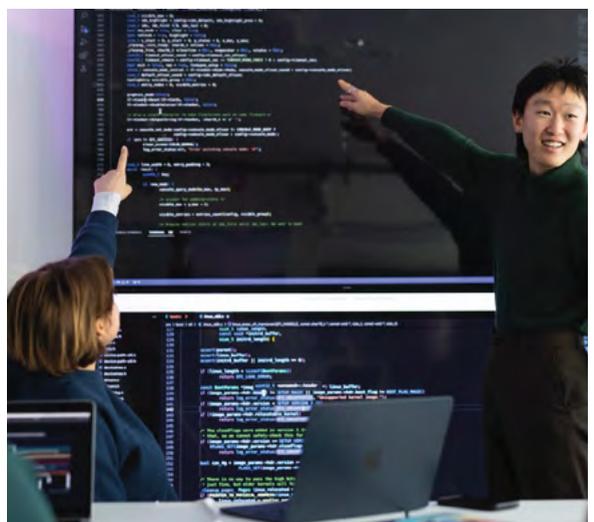
Bei den CHE-Hochschulrankings belegt das HPI stets Spitzenplätze. Die d-school, die HPI School of Design Thinking, ist Europas erste Innovationschule für Studierende nach dem Vorbild der Stanford d.school und bietet jährlich 160 Plätze für ein Zusatzstudium an.

Die HPI School of Entrepreneurship, kurz E-School, unterstützt und motiviert Studierende, das Potenzial unternehmerischen Denkens und Handelns zu erkennen und zu nutzen. Ein starker Fokus liegt auf dem Transfer von Ideen und digitalen Technologien in kunden- und marktzentrierte Produkte und Startups.

Derzeit sind am HPI 22 Professorinnen und Professoren tätig, dazu kommen über 40 weitere Lehrbeauftragte und Dozierende. Das HPI betreibt exzellente universitäre Forschung - in seinen IT-Fachgebieten in Potsdam, aber auch in den HPI Research Schools für Doktoranden mit ihren Forschungsaußenstellen in Kapstadt und Irvine, sowie mit Kooperationspartnern wie dem Massachusetts Institute of Technology (MIT), der Stanford University und dem Hasso Plattner Institute for Digital Health at Mount Sinai (HPI-MS) in New York. Schwerpunkt der HPI-Lehre und -Forschung sind die Grundlagen und Anwendungen großer, hoch komplexer und vernetzter IT-Systeme. Hinzu kommen das Entwickeln und Erforschen nutzerorientierter Innovationen für alle Lebensbereiche.



Weitere Informationen zum HPI unter:  
<https://hpi.de>



# CYBERSECURITY@HPI

Das Thema Cybersicherheit gewinnt mit der fortschreitenden Vernetzung und wachsenden Abhängigkeit der Gesellschaft von digitalen Technologien stetig an Bedeutung. Der Schutz digitaler Systeme wird angesichts wachsender Datenbestände immer wichtiger.

Am HPI bildet Cybersicherheit einen zentralen Fokus von Forschung und Lehre. Schwerpunkte liegen auf der Erforschung und Entwicklung von Sicherheitsstrategien, -methoden und -techniken für die Überwachung und den Schutz komplexer IT-Infrastrukturen. Ob es um die Eigenschaften verschiedener Angreifertypen geht, um kryptographische Algorithmen oder um Datenschutzaspekte - der Bereich Cybersicherheit am HPI befasst sich vor allem mit praktischen Problemen und zeichnet sich durch ingenieurwissenschaftlich geprägte Lösungen von IT- Sicherheitsproblemen aus.

## Security Analytics

Zwar betreiben viele Unternehmen Security Operation Centers (SOCs), doch längst nicht alle nutzen für ihre Aktivitäten, wie beispielsweise die Erkennung von Bedrohungen, State of the Art Data Science/Engineering.

In Zusammenarbeit mit unseren Partnern SAP, Shell, Deutsche Telekom (T-Labs), T-Systems International und Siemens haben wir neue daten- gesteuerte Ansätze für Sicherheitsoperationen erforscht, um das Feld voranzubringen und daran gearbeitet, unbekanntere und fortschrittlichere Bedrohungen zu bekämpfen.

## Alvarium: Frühwarnung und Ablenkung per Mausclick

Welche Angreifer versuchen in meine Organisation einzudringen und wie gehen sie dabei vor? Wenngleich diese Informationen wichtig für eine effektive Verteidigung sind, ist es komplex, sie zu sammeln. Eine Möglichkeit für die Früherkennung von Angriffen bieten Honeypots, die jedoch selten in der Praxis eingesetzt werden - und was, wenn die Angreifenden aus diesem System ausbrechen?

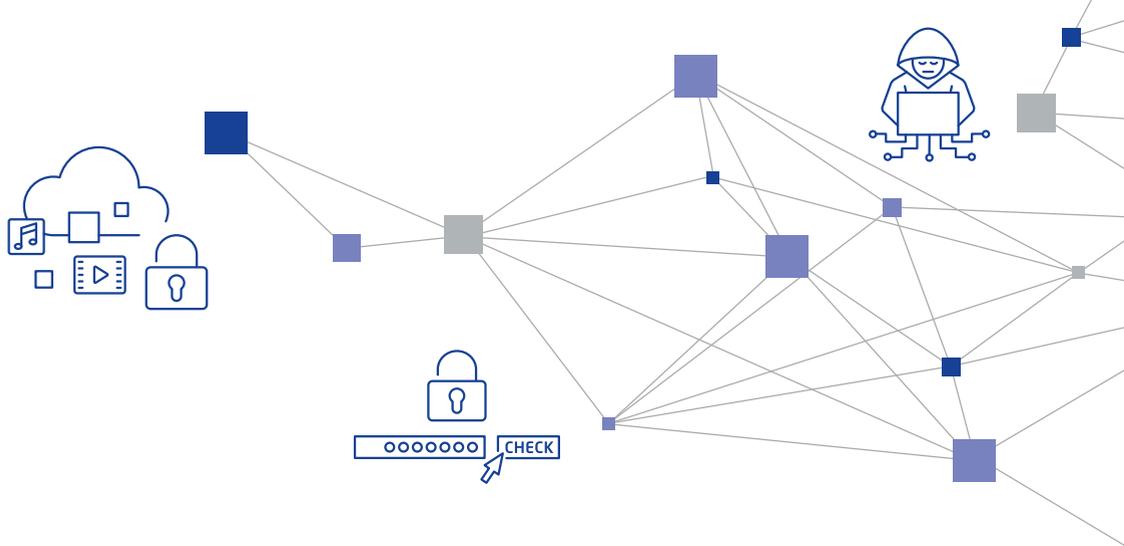
Das Projekt Alvarium des HPIs schafft hier Abhilfe. Mit wenigen Klicks können sich Unternehmen und Privatpersonen ein Schein-System im Webbrowser zusammenstellen. Das Spektrum der Möglichkeiten reicht von einfachen, verwundbaren Systemen bis zur Bereitstellung von echten industriellen Steuerungsanlagen. Während eingehende Angreifer eine Interaktion

mit dem Unternehmen vermuten, werden die Anfragen in eine geschützte Umgebung am HPI umgeleitet und dort ausgewertet. So kann lokal kein Schaden entstehen und Nutzende erhalten durch den Vergleich mit anderen globalen Messpunkten maßgeschneiderte Berichte über die Aktivitäten gegen ihre Organisation. Die Forschungsplattform steht interessierten Firmen sowie Bildungseinrichtungen zur Nutzung offen.

## Tarpitting - ein neuer Ansatz zur Malware-Bekämpfung?

Seit vielen Jahren verbreitet sich Malware innerhalb der ungesicherten Geräte des Internet-of-Things und DDoS-Angriffe waren in der Lage, Ausfälle selbst bei großen Internet-Dienstleistern zu verursachen. Bisherige Versuche der Eindämmung über Awareness-Kampagnen oder die Etablierung von Sicherheitsstandards für Hersteller haben nicht den gewünschten Erfolg erzielt.

Da sich IoT Malware i.d.R. selbst verbreitet, haben HPI-Wissenschaftlerinnen und -Wissenschaftler einen alternativen Ansatz zur Eindämmung dieser Internet-Bedrohung entwickelt, die keine Mitarbeit von Nutzenden oder Herstellern erfordert. Die Tarpits binden die Ausbreitungsversuche von infizierten Geräten an sich, beschäftigen sie und verhindern damit, dass infizierte Geräte andere Opfer im Internet finden und schädigen können. Im Forschungsprojekt konnte nachgewiesen werden, dass bereits ein einziger solcher Tarpit die Ausbrei-



tungsgeschwindigkeit von Schadsoftware wie Mirai um mehr als 20% weltweit senken kann und selbstausbreitende Malware mit Hilfe von einigen tausend Tarbits eingedämmt werden kann, ohne dass es messbare, nachteilige Auswirkungen auf die kompromittierten Router oder das Internet gegeben hätte.

### Verteidigung gegen resiliente Malware

Cyberkriminelle steuern Angriffe und Botnetze zunehmend aus der Blockchain. So auch bei der Malware Pony, die bereits seit 2011 in unterschiedlichen Varianten aktiv ist und weltweit eine der größten Bedrohungen darstellt, wenn es um den Diebstahl persönlicher Daten geht. HPI-Forschenden ist es gelungen, eine Gruppe von Cyberkriminellen über 12 Monate zu beobachten, deren Verhalten und technische Weiterentwicklung in einer Studie detailliert zu dokumentieren und festzuhalten, wie die Gruppe Cyberkrimineller Anpassungen und Verfeinerungen der Bitcoin-Steuerung implementierte. Für einige Wochen gelang ihnen sogar die komplette Übernahme des großen Botnetzes.

### Sicherheit für die Medizintechnik

Vernetzte medizinische Geräte, darunter lebenserhaltende Geräte wie Herzschrittmacher oder Patientenmonitore, haben im Gesundheitswesen eine transformative Rolle gespielt. Gleichzeitig sind sie anfällig für Hackerangriffe und unbefugten Zugriff, was im schlimmsten Fall die Patientensicherheit gefährdet. Im SEPTON Projekt entwickelt das HPI in Zusammenarbeit mit europäischen Partnern Lösungen, um Medizintechnik qua Design besser vor Schwachstellen und Angriffen zu schützen, Angriffe und versuchte Manipulationen von medizinischen Geräten detektierbar, und den digitalen Austausch von medizinischen Daten sicher und selbstbestimmt nutzbar zu machen.

### Autarke, resiliente Krisenkommunikation

In Krisen und Katastrophen ist schnelles Handeln erforderlich. Um Notrufe und Warnungen entgegen zu nehmen, Ressourcen und Helfer:innen effizient zu koordinieren, sind Kommunikationswege nötig, die resilient auch bei Ausfall der Stromversorgung, Verlust bestehender Kommunikationsinfrastruktur oder auch Cyberangriffen funktionieren können. Im BMBF geförderten Projekt KriKom-LK-MEI beteiligt sich das HPI an der Entwicklung eines autarken, resilienten Krisenkommunikationssystems, mit dem staatliche Stellen, Katastrophenschutz, Hilfsdienste und Bevölkerung im Krisenfall verbunden bleiben.



Weitere Informationen dazu unter:  
[www.hpi.de/sicherheitskonferenz/krikom](http://www.hpi.de/sicherheitskonferenz/krikom)

### Cybersicherheit in der Supply Chain

Jedes Unternehmen ist auf Zulieferer und externe Dienstleister angewiesen. Oft haben diese besondere Zugänge zu eigenen Systemen und ein Angriff auf ein Unternehmen kann alle andere Partner in den heutigen Netzwerken von globalen Lieferketten empfindlich treffen. Das Cybersicherheitsmanagement von Lieferketten ist ein komplexes Problem und seit Jahren nehmen Cyberangriffe auf und via der Lieferkette drastisch zu: für das BSI mittlerweile eine der Top-3-Bedrohungen der Wirtschaft. Zusammen mit der MIT Sloan Business School untersucht das HPI Möglichkeiten, mit denen Unternehmen die Cybersicherheit ihrer Lieferketten evaluieren können, sowie Mechanismen und Anreizsysteme, um Zulieferer und Kund:innen auf ein gemeinsames Sicherheitsniveau zu heben.



Weitere Informationen dazu unter:  
[www.hpi.de/sicherheitskonferenz/septon](http://www.hpi.de/sicherheitskonferenz/septon)

Mittwoch, 19. Juni 2024

09:00

---

## Begrüßung und Blick in die HPI-Werkstatt, Teil I

**Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

09:20

---

## Grußwort

**Benjamin Grimm**  
Staatskanzlei des Landes Brandenburg |  
Staatssekretär

09:30

---

## Keynote

**Claudia Plattner**  
Präsidentin des Bundesamtes für Sicher-  
heit in der Informationstechnik

09:45

---

## Cybersicherheitsstrategie Deutschland 2025 - Quo vadis?

**Moderation: Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

**Claudia Plattner**  
Präsidentin des Bundesamtes für Sicher-  
heit in der Informationstechnik

**Dr. Philipp Trinius**  
Deutsche Telekom Security GmbH,  
Cyberdefence & Cloud Security |  
Senior Vice President

**Marian Rachow**  
Rohde & Schwarz Cybersecurity | Chief  
Executive Officer

**Klaus Lensen**  
Cisco Deutschland | Chief Technology  
Officer

10:45

---

## Kaffeepause (Pressekonferenz)

11:30

---

## Keynote

**Holger Münch**  
Präsident des Bundeskriminalamtes

11:45

---

## Cyberlagebild 2024

**Moderation: Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

**Fred-Mario Silberbach**  
BKA Wiesbaden | Stellv. Abteilungsleiter  
Cybercrime

**Mike Hart**  
Google Inc | Head of Mandiant Western  
Europe

**Felix von Leitner**  
Code Blau GmbH | Co-Founder & Blogger

12:30

---

## Mittagspause

13:30

---

## Keynote

**Wilfried Karl**  
Präsident der Zentralen Stelle für  
Informationstechnik im Sicherheitsbereich

# 13:45

---

## Wie verändert Künstliche Intelligenz die Cybersicherheitslandschaft?

**Moderation: Prof. Dr. Sandra Wachter**  
University of Oxford | Professor of Technology and Regulation

**Elmar Geese**  
Greenbone AG | Vorstand

**Dr. Christoph Bausewein**  
CrowdStrike GmbH | Director & Counsel,  
Data Protection & Policy

**Dr. Sven Herpig**  
Stiftung Neue Verantwortung | Leiter  
Cybersicherheitspolitik und Resilienz

**Dr. Kim Nguyen**  
Bundesdruckerei GmbH | Leiter Bereich  
Innovations

# 14:45

---

## Keynote

**Sinan Selen**  
Vizepräsident des Bundesamts für  
Verfassungsschutz

# 15:00

---

## Sicherheit von Kritischen Infrastrukturen und Industrie

**Moderation: Klaus Landefeld**  
Vorstand Infrastruktur und Netze, stellv.  
Vorstandsvorsitzender, eco Verband der  
Internetwirtschaft e.V.

**Jan Hoff**  
Dragos | Principal Industrial Incident  
Responder

**Arlene Bühler**  
DB Cargo AG | Chief Information Officer  
und Chief Digital Officer

**Johannes „Jon“ Rundfeldt**  
AG KRITIS | Mit-Gründer und Sprecher

# 15:45

---

## Kaffeepause

# 16:15

---

## Keynote

**Generalmajor Jürgen Setzer**  
Stellvertreter Inspekteur Cyber- und  
Informationsraum und Chief Information  
Security Officer der Bundeswehr

# 16:30

---

## Cyberwar

**Moderation: Dr. Tim H. Stuchtey**  
Direktor Brandenburgisches Institut für  
Gesellschaft und Sicherheit

**Dr. Martin Wolff**  
Leiter des Internationalen Clausewitz-  
Zentrums an der Führungsakademie der  
Bundeswehr

**Generalmajor Jürgen Setzer**  
Stellvertreter Inspekteur Cyber- und  
Informationsraum und Chief Information  
Security Officer der Bundeswehr

**Botschafter Rainer Rudolph**  
Vize-Vorsitzender der Münchner Sicher-  
heitskonferenz

**Hannes Munzinger**  
DER SPIEGEL | Autor

# 17:30

---

## Resümee 1. Konferenztag

# 18:00

---

## Get-together

Donnerstag, 20. Juni 2024

09:00

---

### Begrüßung und Blick in die HPI-Werkstatt, Teil II

**Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

09:15

---

### IT-Sicherheit in Organisationen - Wie macht man es richtig?

**Moderation: Dr. Michael Littger**  
Deutschland sicher im Netz e.V.

**Marc Lindike**  
222 Degree Consulting GmbH |  
Chief Executive Officer

**Sabine Griebisch**  
GovThings | Managing Director

**Dr. Alexander Köppen**  
PwC Deutschland | Head of PwC Risk &  
Regulatory - Public Sector

**Stefan Maith**  
Check Point | Sales Director Public

10:15

---

### Spotlight Talk

**Insights in the Chinese Disinformation  
Campaign during the Taiwanese  
Elections**

**Mary Ma**  
Taiwan Fact Checking Center | Journalistin  
und Fact Checker

10:30

---

### Kaffeepause

11:00

---

### Keynote

**Generalmajor Dag Baehr**  
Vizepräsident des Bundesnachrichten-  
dienstes

11:15

---

### Desinformation im globalen Superwahljahr 2024

**Moderation: Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

**Generalmajor Dag Baehr**  
Vizepräsident des Bundesnachrichten-  
dienstes

**Katja Muñoz**  
Deutsche Gesellschaft für Auswärtige  
Politik e.V. | Research Fellow

**Georg Mascolo**  
Journalist

**Dr. Konstantin von Notz**  
Bündnis 90/Die Grünen

12:15

---

### Keynote

**Dr. Markus Richter**  
Staatssekretär im Bundesministerium des  
Innern und für Heimat sowie Beauftragter  
der Bundesregierung für Informations-  
technik

12:30

---

### Wrap-Up

**Prof. Dr. Christian Dörr**  
HPI | Fachbereich Cybersecurity -  
Enterprise Security

12:45

---

**Mittagspause**

13:45

---

**Workshops**

Workshop 1

**Krisenübung Vorfallsmanagement**

Workshop 2

**Thematische Cybersicherheit**

Workshop 3

**Einführung ins Design Thinking**

Workshop 4

**Herausforderungen beim Sichern von  
Cloud-Infrastrukturen**

17:00

---

**Ende der Veranstaltung**

# WORKSHOPS UND NETWORKING

Am Nachmittag des 2. Konferenztages bieten wir Ihnen als neues Format thematische Workshops zur fachlichen Vertiefung und Gelegenheiten zum weiteren Austausch und Networking an. Im Vorfeld der Konferenz konnten Sie sich für einen der Workshops anmelden, über mögliche Restplätze informieren wir Sie am Workshoptag. Die Workshops beginnen um 13:45 Uhr und finden im HPI Hauptgebäude statt. Die entsprechenden Räume werden am 2. Konferenztag bekannt gegeben.

---

## Workshop 1

### **Krisenübung Vorfallsmanagement**

„Die Frage ist nicht ob, sondern wann ein Cybersicherheitsvorfall passiert“ – so heißt es oft. In diesem Moment stellt sich die drängende Frage, was zu tun ist, um möglichst schnell und gut aus dieser Situation herauszukommen. Wie effektiv dies gelingt und wieviel Schaden ein Cybersicherheitsvorfall verursacht, hängt auch maßgeblich davon ab, wie gut die Organisation vorbereitet ist und den Vorfall behandelt.

In diesem Workshop lernen Sie die Grundlagen des Vorfallsmanagements praktisch im Rahmen einer Krisenübung kennen. Gemeinsam mit den Expert:innen von CrowdStrike gehen Sie durch die Phasen eines typischen Cybersicherheitsvorfalls, diskutieren und evaluieren Handlungsoptionen, damit Sie Ihre eigene Organisation bestmöglich auf den Fall der Fälle vorbereiten können.

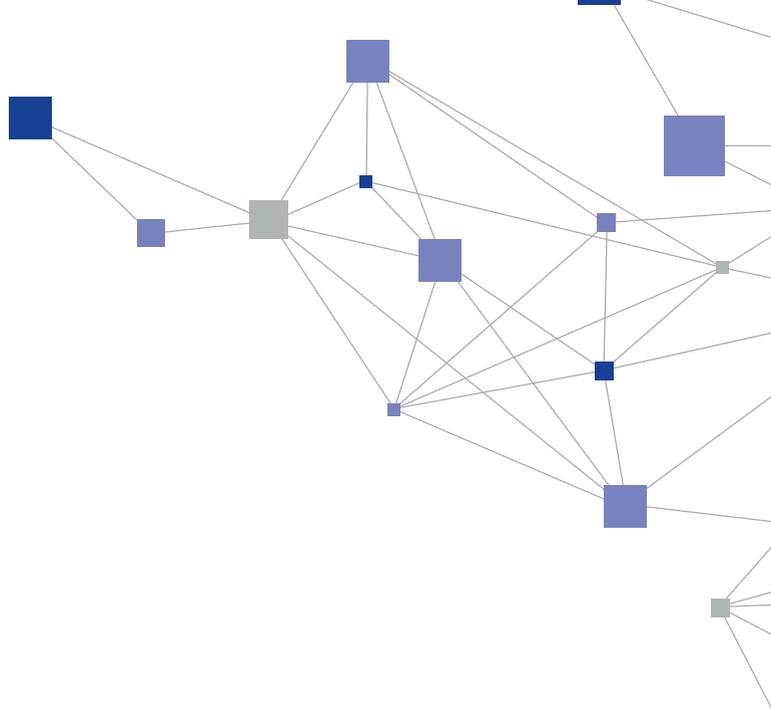
Der Workshop richtet sich an Mitarbeitende in der IT-Sicherheit, CIOs, Referent:innen für Cybersicherheit etc. in Unternehmen und Behörden.

---

## Workshop 2

### **Thematische Cybersicherheit**

Zum Abschluss der Konferenz wollen wir allen Teilnehmenden noch einmal Gelegenheit geben, miteinander über die diesjährigen Themen und Impulse der HPI-Sicherheitskonferenz ins Gespräch zu kommen und diese zu vertiefen. Mit fachkundigen Moderator:innen können Sie an verschiedenen Thementischen unter anderem über Themen wie zum Beispiel KI für Cybersicherheit, Absicherung von kritischen Infrastrukturen sowie über die Implementierung von Cybersicherheit in Unternehmen und anderen Institutionen diskutieren. Die Thementische bieten eine hervorragende Gelegenheit, sich mit den übrigen Teilnehmenden zu vernetzen und eigene neue Einsichten zu entwickeln.



---

### Workshop 3 Einführung ins Design Thinking

Begleitet von den Coaches der HPI d-school erleben die Teilnehmenden einen strukturierten und professionell moderierten Workshop zur Annäherung an die Methoden des Design Thinking. In speziell konzipierten Übungen lernen Sie die Kernelemente des Design-Thinking-Prozesses anhand beispielhafter Problemstellungen kennen.

Beim Design Thinking handelt es sich um eine systematische Herangehensweise an komplexe Problemstellungen aus allen Lebensbereichen. Im Zentrum des Prozesses stehen Nutzerwünsche und -bedürfnisse sowie nutzerorientiertes Erfinden. Design Thinker schauen durch die Brille der Nutzenden auf das Problem und begeben sich dadurch in die Rolle von Anwenderinnen und Anwendern.

Die HPI d-school - Professional Development ist einer der führenden Anbieter für Weiterbildung und Zertifizierung im Bereich Design Thinking, Innovation, digitale Transformation und Tech-Leadership.

An der Schnittstelle von Mensch und Technologie qualifiziert sie Professionals für die Herausforderungen von morgen. Hier können Individuen und Teams Wissen und Know-how erlernen, damit sie innovative Produkte, Dienstleistungen oder Strategien entwickeln können, um Wirkung zu erzielen.

---

### Workshop 4 Herausforderungen beim Sichern von Cloud-Infrastrukturen

Die Skalierbarkeit und Kosteneffizienz von öffentlichen Clouds haben zu einer deutlichen Verlagerung von bisher in herkömmlichen Rechenzentren betriebenen Applikationen und Diensten in die Cloud geführt. Da in Konsequenz Cyberangriffe auf Cloud-native Infrastrukturen in den vergangenen Jahre erheblich zugenommen und sich weiterentwickelt haben, hat sich Mitigant auf diese Herausforderung spezialisiert. Oft sind diese Sicherheitsvorfälle auf einen Mangel an Wissen, Ressourcen und Vorbereitung für das Cloud-Sicherheitsmanagement zurückzuführen.

In diesem Workshop diskutieren wir den aktuellen und zukünftigen Stand der Cloud-Einführung, -Sicherheit und -Resilienz in Deutschland. Darüber hinaus werden die neuesten Trends und die für deutsche Unternehmen geltenden Vorschriften und Best Practices für die Cloud-Sicherheit erörtert, wie z. B. die NIS2-Richtlinie, das DORA-Gesetz und die BSI C5-Richtlinie, sowie Tipps, wie Cloud-native Infrastrukturen sicher, konform und widerstandsfähig gestaltet werden können.

# DER IDENTITY LEAK CHECKER DES HASSO-PLATTNER-INSTITUTS

Ob man selbst Opfer eines Datendiebstahls geworden ist, lässt sich mit dem Identity Leak Checker, einem Online-Sicherheitscheck des HPI, sehr leicht überprüfen. Seit 2014 können Sie kostenlos durch Eingabe Ihrer E-Mail-Adresse prüfen lassen, ob Ihre Identitätsdaten frei im Internet kursieren und missbraucht werden könnten. Hierfür gleichen wir Ihre Informationen mit mittlerweile mehr als 13,4 Milliarden gestohlener und im Internet verfügbarer Identitätsdaten ab. Dabei liegt der Fokus auf Leaks, bei denen deutsche Nutzende betroffen sind.

Insgesamt haben mehr als 18,6 Millionen Nutzerinnen und Nutzer mithilfe des Identity Leak Checkers die Sicherheit ihrer Daten in den letzten fünf Jahren überprüfen lassen. In mehr als 5,1 Millionen Fällen mussten Nutzende darüber informiert werden, dass ihre E-Mail-Adresse in Verbindung mit anderen persönlichen Daten im Internet offen zugänglich war.

## **Spezialangebot für Unternehmen und Organisationen: Identity Leak Checker Desktop Client**

Auch für Unternehmen ist der Diebstahl der Identitätsdaten ihrer Mitarbeitenden ein Problem, im schlimmsten Fall ermöglicht dies Angreifern Zugriff auf die Systeme des Unternehmens. Damit Unternehmen das Risiko besser einschätzen können, bieten wir mit dem Identity Leak Checker Desktop Client ein kostenpflichtiges Angebot für Unternehmen und Organisationen an, das sie bei der kontinuierlichen Überwachung der eigenen Domäne unterstützt. Werden neue Datenlecks entdeckt und in den ILC importiert, prüft der Desktop Client automatisch, ob E-Mail-Adressen des Unternehmens betroffen sind. Die betroffenen E-Mail-Adressen können dann sofort gewarnt werden.



Weitere Informationen zum Angebot  
unter: [www.ilc.hpi.de](http://www.ilc.hpi.de)

„Die Sicherheit eines Passworts steigt mit der Länge exponentiell an: Bei 15 Zeichen würde eine Maschine, die eine Milliarde Passwörter pro Sekunde rät, mehr als sieben Millionen Jahre brauchen. Das lohnt sich für Angreifer nicht mehr.“



**Prof. Dr. Christian Dörr**  
Vorsitzender der Potsdamer Konferenz  
für Nationale Cybersicherheit und Leiter  
Fachbereich Cybersecurity - Enterprise  
Security

# DAS KI-SERVICEZENTRUM BERLIN-BRANDENBURG AM HPI

Das KI-Servicezentrum Berlin-Brandenburg ist ein vom Bundesministerium für Bildung und Forschung gefördertes Projekt am Hasso-Plattner-Institut. Ziel ist es, den allgemeinen Zugang zur Schlüsseltechnologie „Künstliche Intelligenz“ zu erleichtern und die Barrieren für den Einsatz von KI in Wirtschaft und Gesellschaft zu senken.

Das KI-Servicezentrum unterstützt Start-ups, Unternehmen, öffentliche Einrichtungen, Studierende und die Forschung dabei, KI-Anwendungen zu entwickeln, zu betreiben und einzusetzen. Seit seiner offiziellen Eröffnung im Oktober 2023 konnte das KI-Servicezentrum in über 25 Workshops bereits über 120 Teilnehmende zählen und rund 40 Organisationen bei KI-Anwendungsfällen beraten. Die Einsatzbereiche reichen dabei von der Öffentlichen Verwaltung, über Finanzen, bis hin zu Pflege und Medizin.

Die KI-Infrastruktur des Servicezentrums bietet Plattformen für Training, Inferenz und Systemintegration. Damit schafft das KI-Servicezentrum ein Fundament für die Entwicklung und den Transfer von KI-Anwendungen. Die KI-Infrastruktur baut auf bestehenden Rechenressourcen und Betriebskonzepten des HPIs wie dem Future SOC Lab auf.

Alle angebotenen KI-Services, angefangen bei der Bereitstellung von Rechenressourcen bis hin zur Beratung bei der Auswahl und Anwendung von KI-Methoden, vortrainierten KI-Modellen oder der richtigen Hardware, stehen KI-Anwender:innen in ganz Deutschland kostenlos zur Verfügung und können über die öffentlich zugängliche Plattform des KI-Servicezentrums abgerufen werden.



Weitere Informationen zum Angebot  
unter: <https://hpi.de/kisz/home.html>

**KI Service  
Zentrum**  
by Hasso-Plattner-Institut



GEFÖRDERT VOM



Bundesministerium  
für Bildung  
und Forschung

# HPI CONNECT - UNSER KARRIERESERVICE FÜR UNTERNEHMEN UND STUDIERENDE

Im Rahmen des Karriereservices HPI Connect organisiert das HPI jedes Semester vielfältige Karriereevents in enger Zusammenarbeit mit Partnern aus der Wirtschaft oder Bundesinstitutionen. Unternehmen stellen bei Veranstaltungen der „HPI meets ...“- und „HPI inside ...“-Reihe in Vorträgen die Arbeitsbereiche und IT-Fragestellungen in ihren Firmen vor Ort sowie am HPI den Studierenden vor, um sich als Arbeitgeber zu präsentieren.

Die HPI Connect Messe ist das Networking-Event für Unternehmen und Studierende des Hasso-Plattner-Instituts. Als Unternehmen oder Institution haben Sie die Möglichkeit, bei dieser HPI Connect Messe die hochtalentierten IT-Studierenden und Alumni persönlich kennenzulernen und Karrieremöglichkeiten in Ihrem Unternehmen zu präsentieren.

In einem „Speed-Dating-Verfahren“ stellen sich die Aussteller allen teilnehmenden Studierenden und Alumni vor und informieren zu Karriereperspektiven, konkreten Jobs, Praktika und Trainee-Programmen in ihren Unternehmen

Wenn Sie an der Messe oder an einer Vortragsveranstaltung interessiert sind, senden Sie uns gerne eine Mail an [connect@hpi.de](mailto:connect@hpi.de).



Weitere Informationen zum Angebot  
unter: [www.hpi.de/connect](http://www.hpi.de/connect)



# HPI WISSENSPODCAST NEULAND

Der HPI Wissenspodcast Neuland feiert dieses Jahr sein fünfjähriges Bestehen. In den mittlerweile rund 80 Folgen sprechen Expertinnen und Experten des HPI einmal im Monat verständlich über digitale Entwicklungen und Trends, über Chancen und Risiken der Digitalisierung. Jede Folge widmet sich einem gesellschaftlich relevanten Thema - mal geht es um die Bedeutung und die Risiken künstlicher Intelligenz, mal um Cybersicherheit und Sicherheitsmaßnahmen, eine energieeffizientere Digitalisierung oder digitale Bildung.

**„Ethik und Künstliche Intelligenz (KI)“**

**„Die Zukunft von Digital Global Public Health“**



**„Quantencomputing einfach erklärt“**

**„Kann ein KI-Modell fehlerfrei trainiert werden?“**

**„Cybersicherheit: Wie gut ist Deutschland geschützt?“**

**„Wie lassen sich Geheimnisse in geschlossener Software aufdecken?“**



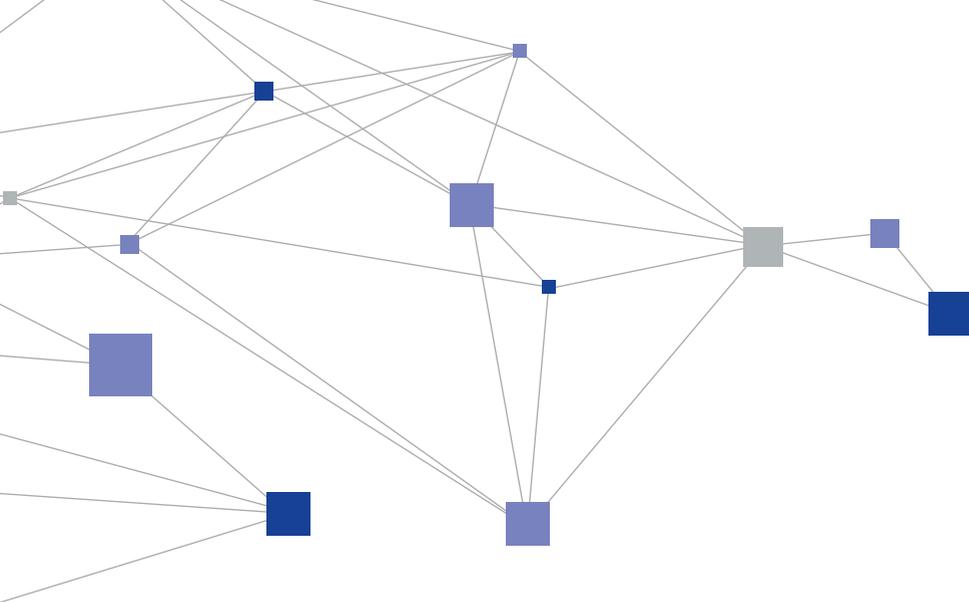
Alle Podcastfolgen von Neuland finden Sie unter: <https://podcast.hpi.de>

„Mit unserem Podcast machen wir den neuesten Stand der Forschung am HPI hörbar. Von Themen der Cybersicherheit über künstliche Intelligenz, Digital Health bis hin zu Design Thinking. Der Podcast bietet die Möglichkeit, sich jederzeit und ganz einfach über neue digitale Entwicklungen zu informieren. Seit 5 Jahren bieten wir dieses Angebot und uns gehen die Themen nicht aus. Deshalb freuen wir uns auch in der Zukunft auf weitere spannende Folgen.“



**Leon Stebe**

„Neuland“-Moderator und Head of Communications and Content am HPI



## PARTNER



Bechtle ist mit über 100 IT-Systemhäusern nah bei den Kunden und zählt mit IT-E-Commerce-Gesellschaften in 14 Ländern zu den führenden IT-Unternehmen in Europa. Bechtle verfügt zudem über ein weltweites Netzwerk an Partnern, das die Anforderungen global agierender Kunden erfüllt. Gegründet 1983, beschäftigt die Bechtle Gruppe mit Hauptsitz in Neckarsulm derzeit über 15.000 Mitarbeitende.

Die mehr als 70.000 Kunden aus Industrie und Handel, dem Public Sector sowie dem Finanzmarkt begleiten wir bei ihrer digitalen Transformation und bieten herstellerübergreifend ein lückenloses Angebot rund um IT-Infrastruktur und IT-Betrieb. Bechtle ist im MDAX und im TecDAX notiert. 2023 lag der Umsatz bei 6,42 Mrd. €. Mehr unter: [bechtle.com](https://www.bechtle.com)

## bundesdruckerei.

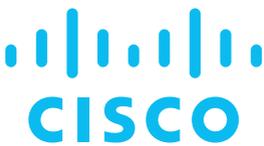
Die Bundesdruckerei GmbH samt ihrer Tochtergesellschaft Maurer Electronics GmbH ist ein führendes deutsches Hightech-Sicherheitsunternehmen mit Hauptsitz in Berlin. Mit innovativen Lösungen, Produkten und Technologien „Made in Germany“ schützt sie Identitäten und Daten. So schafft sie Vertrauen und Rechtssicherheit in der digitalen Gesellschaft – und ermöglicht das souveräne Handeln von Staaten, Unternehmen und Bürgern in der analogen und der digitalen Welt. Als Unternehmen der BundesdruckereiGruppe und mit der

Erfahrung von über 250 Jahren ebnet das Unternehmen den Weg in eine sichere digitale Zukunft. Die Bundesdruckerei GmbH besitzt aktuell über 4.500 nationale und internationale Patente, beschäftigt rund 2.350 Mitarbeiter und hat 2019 einen Umsatz von 549,5 Millionen Euro erzielt. Weitere Informationen unter [www.bundesdruckerei-gmbh.de](https://www.bundesdruckerei-gmbh.de)



Check Point Software Technologies Ltd. (<https://www.checkpoint.com/de/>) ist ein führender Anbieter einer KI-gestützten, in der Cloud bereitgestellten Cybersicherheitsplattform, die über 100.000 Organisationen weltweit schützt. Check Point nutzt die Kraft der KI überall, um die Effizienz und Genauigkeit der Cybersicherheit durch seine Infinity-Plattform zu verbessern, mit branchenführenden Erkennungsraten, die eine proaktive Antizipa-

tion von Bedrohungen und intelligentere, schnellere Reaktionszeiten ermöglichen. Die umfassende Plattform umfasst Cloud-Technologien, bestehend aus Check Point Harmony zur Absicherung des Arbeitsplatzes, Check Point CloudGuard zur Absicherung der Cloud, Check Point Quantum zur Absicherung des Netzwerks und Check Point Infinity Core Services für kollaborative Sicherheitsabläufe und -dienste.



Die Digitalisierung von Behörden, Ministerien und Verwaltungen ist ein Großprojekt. Cisco weiß, dass Angebote für staatliche Zusammenarbeit auf Sicherheit und Vertrauen beruhen, um die informationelle Selbstbestimmung zu gewährleisten. Diese Unabhängigkeit, die digitale Souveränität, wollen wir weiterentwickeln. Dabei bedeutet digitale Souveränität nicht, alles selbst zu entwickeln, sondern zur Verfügung stehende Technologien zu verstehen, um diese sicher und souverän einzusetzen. Dazu entwickelt Cisco Produkte und Lösungen

rund um das Netzwerk, Netzwerkinfrastrukturen, Cybersicherheit, Rechenzentrumsausrüstung, Videokommunikations- und Kollaborationslösungen, Cloud/Software und Services. Unsere Technologien werden regelmäßig durch das BSI zertifiziert. In unserem Technology Verification Service Lab in Berlin lassen sich die Sicherheit und der Betrieb von Netzwerktechnologien unter realen Bedingungen testen. Zudem steht unser Security and Trust Office für Fragen zur Verfügung.



CrowdStrike, ein global führendes Unternehmen im Bereich der Cybersicherheit, definiert mit der weltweit fortschrittlichsten Cloud-nativen Plattform zum Schutz von Workloads, Endgeräten, Identitäten und Daten moderne Sicherheit. Dank der CrowdStrike Security Cloud und erstklassiger künstlicher Intelligenz verarbeitet die CrowdStrike Falcon®-Plattform in Echtzeit Angriffsindikatoren, Bedrohungsdaten, sich ständig weiterentwickelnde Methoden der Gegner sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen und ermög-

licht hochpräzise Erkennungen, automatisierte Schutz- und Abhilfemaßnahmen, hervorragendes Threat Hunting und eine nach Prioritäten geordnete Beobachtung von Schwachstellen. Die funktionsorientierte Single-Agent Cloud Architektur der Falcon Plattform bietet eine schnelle und skalierbare Anwendung, ausgezeichnete Sicherheit und Leistung, weniger Komplexität und sofortige Wertschöpfung.

# DELLOS CLOUD

Delos Cloud stellt eine souveräne und sichere Cloud-Plattform für die Digitalisierung des Öffentlichen Diensts in Deutschland bereit. Sie ist hersteller- und lösungsneutral sowie anwendungsoffen. Damit ist sie ein wesentlicher Baustein für die Umsetzung der Deutschen Verwaltungs-Cloud-Strategie (DVS) unter Einhaltung aller relevanten Sicherheits- und

Geheimhaltungsvorgaben des BSI. Delos Cloud versteht sich als vertrauensvoller Partner der IT-Dienstleister von Bund, Ländern und Kommunen und ergänzt deren Leistungsportfolio. Für weitere Informationen besuchen Sie: [www.deloscloud.de](http://www.deloscloud.de)



## Deutschland sicher im Netz

Die gemeinnützige Organisation wurde 2006 im Rahmen des Nationalen IT-Gipfels der Bundesregierung (heute: Digital-Gipfel) gegründet. Durch vielfältige Projekte und Partnerschaften unterstützt DsiN Menschen im privaten und beruflichen Umfeld sowie Unternehmen im sicheren Umgang mit digitalen Diensten und Technologien. Zu seinen Initiativen zählen

DsiN-Digitalführerschein, SiBa-App sowie reichweitenstarke Transferangebote für ausgewählte Zielgruppen (Politiker: innen, Berufsschulen, Schulen, Senior: innen, Vereine). DsiN steht unter Schirmherrschaft der Bundesministerin des Innern und für Heimat. Mehr Infos unter [www.sicher-im-netz.de](http://www.sicher-im-netz.de)

# DRAGO

Dragos hat es sich zum Ziel gesetzt, die Gesellschaft vor denjenigen zu schützen, die versuchen, die industrielle Infrastruktur zu stören, auf die wir tagtäglich angewiesen sind. Basierend auf leistungsstarker industrieller Cybersicherheitstechnologie, branchenführender OT Threat Intelligence und der Expertise des Dragos Services Teams, bietet die Dragos Plattform den Kunden vollständige Transparenz über ihre ICS/OT Assets, Schwachstellen, Bedrohungen und Handlungsoptionen. Dragos Ansatz ermöglicht Kunden den Zugang zur größten Industrial-Cybersecurity-Community

und sorgt so für ein Höchstmaß an Transparenz. Dragos Lösungen schützen Unternehmen in einer Vielzahl von Branchen, z. B. in der Strom-, Öl- und Gasindustrie, im verarbeitenden Gewerbe, in der Gebäudeautomatisierung, in der chemischen Industrie, im öffentlichen Sektor, in der Wasserwirtschaft, in der Lebensmittel- und Getränkeindustrie, im Bergbau, im Transportwesen und in der pharmazeutischen Industrie.



Mit rund 1.000 Mitgliedsunternehmen ist eco der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und

in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.

## GESELLSCHAFT FÜR INFORMATIK



Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähl-

gen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Die GI hat sich Ethische Leitlinien gegeben, die ihren Mitgliedern als Orientierung dienen. Weitere Informationen finden Sie unter: [www.gi.de](http://www.gi.de)



Google hat es sich zur Aufgabe gemacht, die Informationen der Welt zu organisieren und sie allgemein zugänglich und nutzbar zu machen. Dazu gehört es auch, künstliche Intelligenz ambitioniert, verantwortungsvoll und im Austausch mit anderen weiterzuentwickeln, so dass alle davon profitieren können. Mit Produkten wie der Google Suche, Maps, Gmail, Chrome, Gemini, den Pixel Smartphones und Watches oder Plattformen wie YouTube spielt Google eine wichtige Rolle im täglichen Leben von Milliarden von Menschen. In Deutschland ist Google seit 2001 vertreten und beschäftigt mittlerweile mehr als 2.500 Mitarbeitende an den vier Standorten Hamburg, Berlin, München und Frankfurt. Gemeinsam mit lokalen Partnern

arbeitet Google Deutschland an zahlreichen Digitalisierungsprojekten, etwa im Bereich Bildung, Handel, Infrastruktur, Klima- oder Datenschutz. Im Google Safety Engineering Center (GSEC) in München entwickelt Google Datenschutz-Anwendungen für die ganze Welt. Und mit Kommunikationslösungen, einem Cloud-Rechenzentrum in der Nähe von Frankfurt und zwei Cloud-Regionen mit Fokus auf erhöhter Effizienz und Nachhaltigkeit unterstützt Google Unternehmen in Deutschland bei ihrer digitalen Transformation. Google ist eine Tochtergesellschaft von Alphabet Inc.



## Greenbone

Greenbone gilt weltweit als führender Anbieter von Open-Source Schwachstellenmanagement-Lösungen. Unsere Expertise liegt in der Entwicklung von hochentwickelten Algorithmen und Programmen, die Schwachstellen in den IT-Systemen unserer Kunden frühzeitig aufspüren, bevor potenzielle Angreifer sie ausnutzen können.

Gegründet wurde Greenbone im Jahr 2008 und seit 2023 agieren wir als Aktiengesellschaft. Wir schützen die digitalen Vermögenswerte von mehr als 1.000 Kunden durch über 50.000 Installationen weltweit, die sämtliche Bereiche der IT abdecken. Unsere umfangreiche Datenbank enthält mehr als hunderttausend

Sicherheitsmeldungen sowie weitere relevante Informationen, die eine präzise Risikobewertung der IT-Systeme ermöglichen. Unsere Kunden profitieren von automatisierten Sicherheitstests und täglichen Updates im Rahmen unseres Abonnementmodells.

Qualität, Sicherheit und Nachhaltigkeit stehen bei uns an erster Stelle. Daher sind wir seit 2001 nach ISO 9001 und ISO 27001 zertifiziert und seit 2024 auch nach ISO 14001.

Für die neuesten Informationen zu Greenbone, unserem Produktportfolio sowie zu aktuellen Schwachstellen und Tipps zur Absicherung Ihrer IT-Infrastruktur besuchen Sie unseren Blog: <https://www.greenbone.net/blog>



## Microsoft

Die Microsoft Deutschland GmbH, im Jahr 1983 als Niederlassung der Microsoft Corporation (Redmond, U.S.A.) gegründet, beschäftigt in Deutschland über 3.000 Mitarbeiter:innen an den sieben Standorten Berlin, Frankfurt, Hamburg, Köln, München, Stuttgart und Walldorf. Gemeinsam mit unseren 30.000 Partnern in Deutschland unterstützen wir Unternehmen durch innovative Lösungen für die intelligente Cloud und das Intelligent Edge, damit sie erfolgreich für die digitale Transformation und das KI-Zeitalter aufgestellt sind. Daneben ist Microsoft ein weltweit führender

Anbieter in Bereichen wie produktive Softwarelösungen, IT-Sicherheit, innovative Hardware und Entwicklungsplattformen, die auch auf der Open-Source-Technologie basieren. Microsoft investiert in den Ausbau von KI-Infrastrukturen und Cloud-Kapazitäten sowie in die Qualifizierung von Fachkräften in Deutschland. Gemeinsam mit Politik, Wirtschaft und Wissenschaft beteiligen wir uns an vielfältigen Initiativen und Projekten, damit alle Menschen am Fortschritt der digitalen Gesellschaft teilhaben können.



## MYRA

Neue digitale Sicherheit

Myra Security ist ein deutsches Cybersicherheitsunternehmen und Anbieter einer Security-as-a-Service-Plattform. Die von Myra entwickelte Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Sie überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Myra erfüllt alle 37 Kriterien des BSI für qualifizierte DDoS-Mitigation-

Dienstleister. Ministerien und Behörden sowie Unternehmen aus dem Finanz-, Versicherungs- und Gesundheitswesen vertrauen für den Schutz kritischer Infrastrukturen auf Myra. Dazu gehört die Abwehr von DDoS-Attacks, Bot-Netzen und Angriffen auf Datenbanken. Zu den Kunden zählen unter anderem das Bundesministerium für Gesundheit, die Sparkasse und die Münchner Sicherheitskonferenz.



Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch,

Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 151 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen. PwC Deutschland. Mehr als 14.000 engagierte Menschen an 20 Standorten. Rund 2,93 Mrd. € Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

**ROHDE & SCHWARZ**  
Make ideas real



Rohde & Schwarz Cybersecurity ist ein führendes IT-Sicherheitsunternehmen, das hoheitlichen und privatwirtschaftlichen Kunden mit besonderen Sicherheits- und Zulassungsanforderungen Schutz vor den sich stetig ändernden Cyberbedrohungen bietet. Der Pionier hochsicherer Verschlüsselungstechnologien liefert Hochgeschwindigkeits-Netzwerkverschlüsselung und Zero-Trust-basierte Endpoint-Sicherheit. Die meisten dieser

Produkte sind vom BSI für die Absicherung VS-NfD-eingestufter Daten zugelassen. Diese vertrauenswürdigen Sicherheitslösungen unterstützen die Anwender auf dem Weg in eine sichere und digitalisierte Welt und leisten damit einen wesentlichen Beitrag zur digitalen Souveränität. Weitere Informationen unter [www.rohde-schwarz.com/cybersecurity](http://www.rohde-schwarz.com/cybersecurity).



### **SAP-Unternehmensinformationen und Strategie**

Als Marktführer für Unternehmenssoftware unterstützen wir Unternehmen jeder Größe und Branche dabei, ihre Abläufe zu verbessern, indem wir ERP neu definieren und Netzwerke mit intelligenten Unternehmen aufbauen, die für Transparenz, Resilienz und Nachhaltigkeit in allen Lieferketten sorgen. Unsere End-to-End-Suite mit Anwendungen und Services ermöglicht es unseren Kunden, rentabel zu arbeiten, sich kontinuierlich anzupassen und sich weltweit vom Wettbewerb abzuheben. Wir setzen auf Geschäftliche Agilität, Supply Chain Resilienz und Nachhaltige Ergebnisse.

### **Unsere Werte**

Zielsetzung und Nachhaltigkeit  
Vielfalt und Inklusion  
Corporate Social Responsibility

### **Innovationen bei SAP**

Für uns bedeutet Innovation Entwicklung bahnbrechender Technologien, die in der IT und im Business neue Maßstäbe setzen.

### **Weltweites Sponsoring**

Partnerschaften mit Teams, Ligen und Sportstätten ermöglichen uns die Entwicklung von Technologie-Lösungen mit cloudbasierten Analysen in Echtzeit.



## secusmart®

Secusmart ist der führende Anbieter von sicheren mobilen Kommunikationslösungen im IT-Sicherheitsmarkt und Hersteller von drei Produktlinien: SecuSUITE für Samsung Knox und SecuSUITE für iOS ist eine hochsichere mobile Plattform für mobile Daten und Sprache auf Samsung- und Apple-Smartphones und -Tablets und hat die Freigabeempfehlung bis zur Geheimhaltungsstufe VS-NfD („Classified Information-For Official Use Only“). Secusmart bietet daneben auch SecuSUITE an, eine Softwarelösung zur Sprachverschlüsselung auf Apple iOS und Google Android

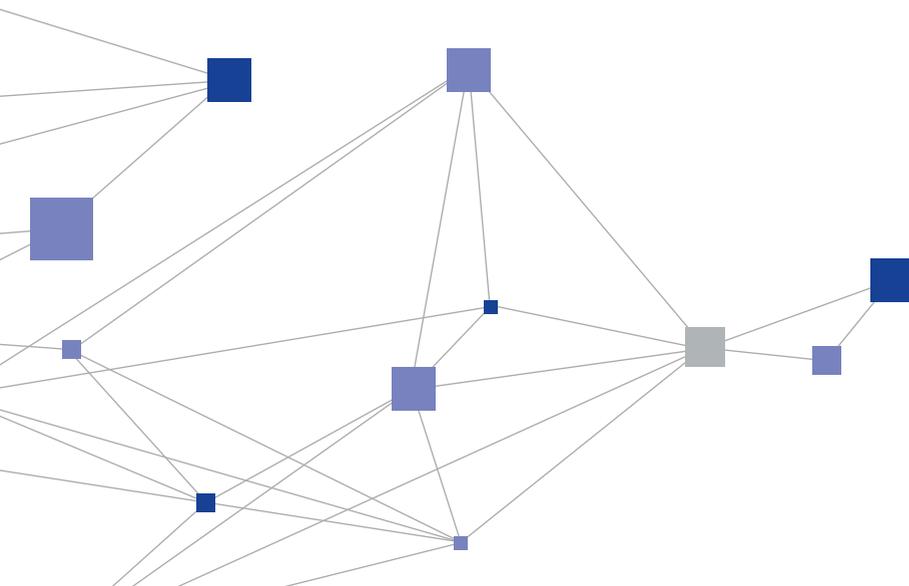
Smartphones. Im Jahr 2022 hat die NATO Communications and Information Agency (NCIA) der SecuSUITE von BlackBerry die Sicherheitsakkreditierung für den weltweiten Einsatz in der offiziellen sicheren NATO-Kommunikation erteilt.

Zu den wichtigsten Kundenorganisationen von Secusmart gehören deutsche Bundesbehörden. Darüber hinaus wird die SecuSUITE-Softwarelösung an Regierungen und Unternehmen weltweit verkauft.

## T SECURITY

**Telekom Security: Mit Sicherheit zum Erfolg.** Wir glauben an eine sichere digitale Zukunft mit maximalen Möglichkeiten und minimalem Risiko. Eine Welt der digitalen Teilhabe, in der jeder uneingeschränkt erleben kann, was verbindet. In dieser Welt gestalten wir passgenaue und ganzheitliche digitale Sicherheit für den Konzern und unsere Kund:innen. Mit rund 1.700 Spezialist:innen und über 25 Jahren Erfahrung erkennen wir Gefahren frühzeitig und bieten umfassende Beratung, technologische Lösungen sowie Managed Services - von der Identifizierung, Einordnung und Abwehr der Gefährdung bis hin zur Wiederherstellung im Ernstfall.

Kernstück der Überwachung ist das integrierte Cyber Defense & Security Operations Center (SOC). Mit mehr als 240 Security-Spezialisten und 24/7 Verfügbarkeit haben wir jederzeit einen umfassenden Blick auf die sich ständig verändernde Bedrohungslandschaft. Somit können wir Angriffe nahezu in Echtzeit erkennen, abwehren und analysieren. Ob im Telekom Konzern weltweit oder für unsere externen Kund:innen: wir schützen, was bewegt.





Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst.

Durch die breit gefächerte Mitgliedschaft und die Partnerorganisationen verkörpert TeleTrust den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa.



Bei Trend Micro ist es unser Ziel, die Welt für den Austausch digitaler Informationen sicherer zu machen. Wir sind davon überzeugt, dass Cyberrisiken gleichzeitig Geschäftsrisiken darstellen. Deshalb ermöglichen wir Unternehmen vollständige Transparenz und Kontrolle ihrer digitalen Assets. So verstehen sie, wie gut sie geschützt sind und welche Investitionen wichtig sind, um das Risiko zu senken.

Mit uns wird die Welt sicherer, da wir schon früh erkennen, wie sich moderne Infrastrukturen, Nutzerverhalten, Applikationsentwicklung und damit auch Cyberbedrohungen verändern und darauf reagieren.

Wirtschaftsförderung  
Brandenburg | **WFBB**



Die Wirtschaftsförderung Land Brandenburg GmbH (WFBB) ist zentraler Ansprechpartner für Investoren, ansässige Unternehmer und technologieorientierte Existenzgründungen. Ziel des Clustermanagements innerhalb der WFBB ist es, Wirtschaft und Wissenschaft so zu vernetzen, dass insbesondere die Innovationskraft und damit die Wettbewerbsfähigkeit der Unter-

nehmen gestärkt werden. Gemeinsam mit den anderen Akteuren im Cluster treiben sie die strategische Weiterentwicklung in den Themen Digitale Transformation, Green Deal, Verkehrs- und Energiewende sowie eHealth und innovative Versorgungskonzepte voran.

**Hasso-Plattner-Institut  
für Digital Engineering gGmbH**

Prof.-Dr.-Helmert-Str. 2-3  
14482 Potsdam  
T +49 (0)331 5509-0  
F +49 (0)331 5509-129  
[www.hpi.de](http://www.hpi.de) | [hpi-info@hpi.de](mailto:hpi-info@hpi.de)

**Geschäftsführer:**

Prof. Dr. Tobias Friedrich, Prof. Dr. Ralf Herbrich, Dr. Marcus Kölling

**Registergericht:** Amtsgericht Potsdam

**Registernummer:** HRB 12184

**Konzeption, Text und Redaktion:**

Dr. Maxim Asjoma, Joana Bußmann, Prof. Dr. Christian Dörr, Marc Skupch,  
Leon Stebe, Nora Trübestein / HPI Presse und Öffentlichkeitsarbeit

**Photos:** Kay Herschelmann, Nicole Krüger

**Design:** Polygraph Design, Berlin

Juni 2024

**Folgen Sie uns auf:**

[www.hpi.de/linkedin](http://www.hpi.de/linkedin)

[www.hpi.de/twitter](http://www.hpi.de/twitter)

[hpi.social/@Hasso\\_Plattner\\_Institute](https://www.instagram.com/Hasso_Plattner_Institute)

[www.hpi.de/youtube](http://www.hpi.de/youtube)

[www.hpi.de/facebook](http://www.hpi.de/facebook)

[www.hpi.de/instagram](http://www.hpi.de/instagram)



