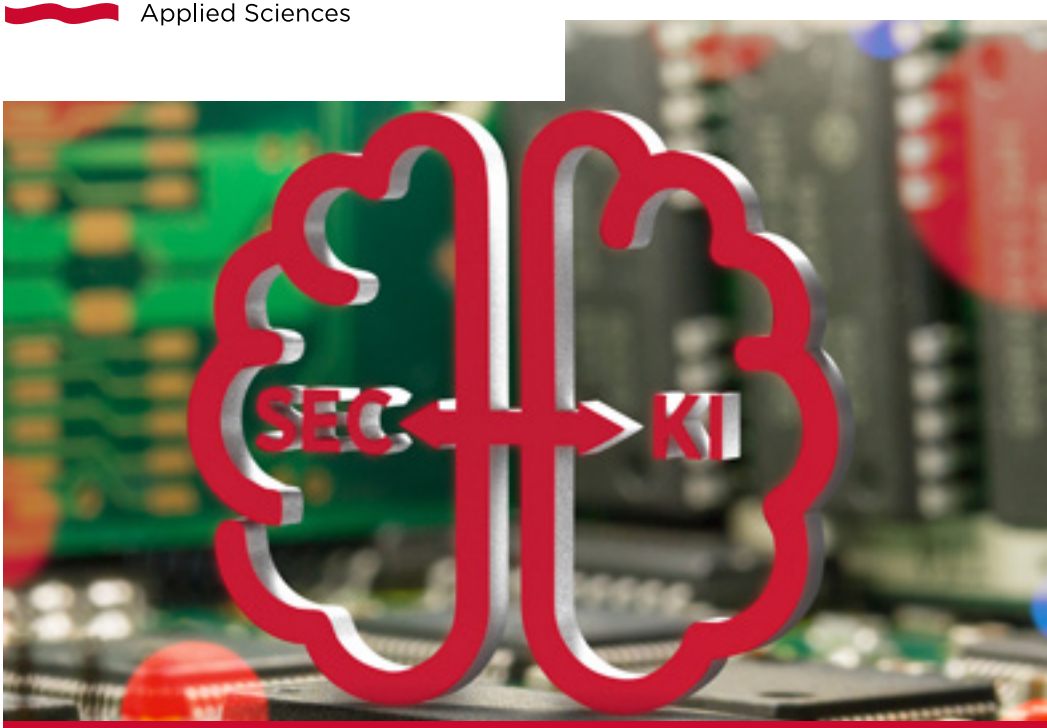
Technische Hochschule
Brandenburg
University of
Applied Sciences



13. Security Forum

17.01.2019

Künstliche Intelligenz und Security

www.th-brandenburg.de

Technische Hochschule Brandenburg

Auf einen Blick

Gegründet 1992 in Brandenburg an der Havel
Drei Fachbereiche

- Informatik und Medien
- Technik
- Wirtschaft

21 Studiengänge und 67 Professorinnen und Professoren
2600 Studierende und 240 Beschäftigte
60 Partnerschaften mit Hochschulen in Europa und Übersee

Sponsoren

Hiermit bedanken wir uns bei unseren Sponsoren.

Inhalt

Willkommen

Sehr geehrte Teilnehmerinnen und Teilnehmer des Security Forums 2019,
Künstliche Intelligenz (KI) ist DAS Thema in Wirtschaft und Politik. Zurzeit überbieten sich die Nationen darin, Investitionen in KI anzukündigen. China erhebt den Anspruch, bis zum Jahr 2030 die globale Führung auf dem Gebiet der Künstlichen Intelligenz zu übernehmen. Allein die Stadt Schanghai plant, 15 Milliarden Dollar in KI-Projekte zu investieren. Unter anderem soll eine volldigitalisierte „Smart City" aufgebaut werden. In diesem Jahr preschte dann Frankreich vor und kündigte Milliardeninvestitionen an. Auch die deutsche Bundesregierung identifiziert KI als Schlüsseltechnologie im internationalen Wettbewerb. In einem Gutachten für das Bundeskanzleramt warnte die Expertenkommission für Forschung und Innovation erst im Frühjahr, dass Deutschland im Kontext von KI nur beim autonomen Fahren konkurrenzfähig sei. Auf anderen Feldern, vor allem den autonomen Systemen in der industriellen Fertigung, beim Smart Home und beim Einsatz von Computern in menschenfeindlichen Umgebungen, liege Deutschland hingegen weit zurück.
Der Hype um die Künstliche Intelligenz ist begründet durch die riesigen Mengen gut qualifizierter Daten, die es ermöglichen, die technischen Ansätze des Deep Learning zu verwenden; durch die Rechenkapazitäten in großen Cloud-Rechenzentren und durch die Hardwareunterstützung durch GPUs, die eine nunmehr effektive Berechnung erlauben.
In den letzten Jahren waren zahlreiche Erfolgsmeldungen rund um KI zu hören. Es scheint immer mehr so, als könne man mit KI einfach jede Problemstellung lösen. KI beschränkt sich dabei nicht nur auf Computer Vision (Bildverarbeitung) oder Natural Language Processing (Sprachverarbeitung), sondern umfasst auch Themen wie Robotik und Lernen. Häufig ist das technische Mittel dahinter Deep Learning: Der Hammer, für den nun jedes Problem wie ein Nagel aussieht. Ob diese Entwicklung hält, was sie verspricht, wird sich noch zeigen und auf dem Security Forum der THB besprochen. Die Verbreitung von KI birgt eben auch Risiken. Einmal kann KI auch für politische Zwecke genutzt werden, wie die Vorfälle um Cambridge Analytics zeigen. Andererseits sind KI-Systeme selbst Ziel von Angriffen neuer Art, zum Beispiel sogenannten Adversarial Attacks, die KI-Modelle destabilisieren.
Die Technische Hochschule Brandenburg engagiert sich zugunsten der Wirtschaftsregion Brandenburg-Berlin auf dem Feld der Digitalisierung ebenso wie der dafür nötigen IT-Sicherheit. Dies zeigt sich unter anderem darin, dass IT-Sicherheit einer der Forschungsschwerpunkte in Brandenburg ist. Den Aktivitäten aus der Forschung stehen viele Aktivitäten des Studiengangs „Security Management" und aus dem Fachbereich Informatik und Medien zur Seite. Im Zusammenhang mit dem Projekt

„Sichere Software-Entwicklung“ gibt es seit 2017 in Berlin ein „Lernlabor Cybersicherheit“ der THB, der Hochschule für Technik und Wirtschaft Berlin und des Fraunhofer-Instituts FOKUS. An der THB selbst konnte das „Labor für Netzwerk und Sicherheit“ technisch runderneuert werden zum „Labor für Cybersicherheit und Schutz kritischer Infrastrukturen“.
Die Hochschule hält somit bei der Ausbildung von Fachkräften für die IT-Sicherheit erfolgreich Schritt mit der hohen Entwicklungsdynamik. Sie ist mit der regionalen Industrie ebenso eng verzahnt wie in der Online-Ausbildung präsent. Digitalisierung bedarf eines Gleichmaßes an Cybersicherheit.
Das diesjährige Security Forum soll erneut eine Plattform bieten für spannende Themen aus der Hochschule. Dazu konnten wir versierte Vertreter aus Wirtschaft, Gesellschaft und Politik gewinnen, um gemeinsam das Thema Künstliche Intelligenz zu diskutieren. Ich bin ganz sicher, dass es viele Denkanstöße geben wird.
Ich wünsche Ihnen spannende und anregende Vorträge und Gespräche.

Ihre Prof. Dr.-Ing. Burghilde Wieneke-Toutaoui
Präsidentin der Technischen Hochschule Brandenburg

Präsidentin der Technischen Hochschule Brandenburg

Security Forum

Künstliche Intelligenz und Security
Als Anfang der 90er der PC flächendeckend eingezogen war, begann der erste Hype der „Künstlichen Neuronalen Netze“. Man legte ein Netz über die Messpunkte und fand so etwas Ähnliches auch in der Großhirnrinde von Affen. In einem allgemeinen Schöpferrausch wurde alles, was aus Daten eine Entscheidung ableiten konnte, „neuronal“.

Das blieb zwar bis vor kurzem sehr mühsam, denn man brauchte man Zehntausende von Beispielen. Seit einigen Jahren aber können sich Maschinelle Lernverfahren selbst optimieren, und nun zeigt sich die Macht des unbestechlichen Beobachtens: Sind die Kriterien erstmal abstrahiert, lässt sich jedes Optimierungsziel vorgeben.

- Das nach einer sicheren Ankunft mit dem „Datenvernetzer autonomes Fahrzeug“.
- Das nach einer souveränen Durchführung des Geschäftsbetriebs (Security), wofür man die Mitarbeitermotivation, die Korruptionsgefährdung, aber auch die Resilienz der Lieferkette beobachtet.
- Das nach unbeeinträchtigter Aufrechterhaltung einer digitalisierten Infrastruktur, indem man Cyberbedrohungen mitbedenkt und die Identitäten sichert.
- Das nach einer Ausweitung der Datenbasis bei sozialen Netzen, deren Mitglieder zugleich Datenquelle und Ziel für das Target Marketing geworden sind.
- Das nach einem langfristig günstigen politischen Rahmen, indem man, wie Cambridge Analytica vermuten lässt, Wähler psychometrisch modelliert.

Nutzen und Bedrohungen sind leider monopolisiert. Denn obwohl heterogenste Daten verarbeitet werden, haben sich die erfolgreichen Algorithmen und IT-Strukturen vereinheitlicht. Aus europäischer Sicht wirkt sich fatal aus, dass die großen Innovationen der Soft-, dann der Hardware und später der KI erst zögerlich angegangen und später der Marktliberalisierung preisgegeben wurden. So sind technologische Souveräne entstanden, deren KI-Werkzeuge zwar gern genutzt werden, die aber Partikularinteressen nicht forcieren.

Es gilt, diesen mit Sachkenntnis zu begegnen: Wo findet sich heute welche KI und wie dient sie der Security? Warum werden sich welche Prozesse verändern und wie kann ich dies aktiv mitgestalten, ohne auf der anderen Seite meinen künftigen Gestaltungsspielraum schwinden zu sehen? Eine sichere Antwort liegt in einer soliden Ausbildung –
willkommen beim 13. Security Forum der Technischen Hochschule Brandenburg!

Ihr

Prof. Dr. Ivo Keller

Studiengang Security Management (M. Sc.)

Security Management, ein akkreditierter Masterstudiengang, bietet eine Gesamtsicht auf ein integriertes Management für Unternehmens- und Organisationssicherheit sowie IT-/Cyber Security. Dabei steht interdisziplinäres technisches Grundlagenwissen gleichauf mit Methoden- und Managementkompetenzen, insbesondere in den Gebieten der Informationssicherheit, des Secure Software Engineerings, der rechtlich sicheren Unternehmensführung und dem Risiko-, Sicherheits- und Krisenmanagement. Im Rahmen der Wahlpflichtmodule kann dann jeder Studierende seine individuelle Profilierung umsetzen, etwa:

- Informationssicherheit,
- IT-Forensik,
- IT- und Cyber Security;
- Bankensicherheit
- Gebäude-, Anlagen- und Personensicherheit und
- Business Continuity und Krisen-Management,

Studiert wird berufsbegleitend in Blockveranstaltungen (freitags, samstags, montags). Unsere, zumeist aus Unternehmen stammenden Dozenten gestalten die Lehre sehr praxisnah und bereiten die Studierenden auf ihre zukünftigen Tätigkeitsfelder punktgenau vor.
Für weitere Informationen zum Berufsumfeld verweisen wir Sie gern auf https://www.security-management.de/ .

Veranstaltung im Überblick

Uhrzeit	Thema	Referent
09:00	Eröffnung	Moderation: Robert Skuppin Prof. Dr.-Ing. Wieneke-Toutaoui Prof. Dr. Ivo Keller
09:30	Was ist Künstliche Intelligenz?	Prof. Dr.-Ing. Jochen Heinsohn für Wissensbasiertes Systeme/KI-Techniken Prof. Dr.-Ing. Sven Buchholz Angewandte Informatik (insbes. Datenmanagement/Data Mining) Dipl.-Inform. Ingo Boersch Technische Hochschule Brandenburg
10:00	Künstliche Intelligenz in der Mobilität	Dr. Tobias Miethaner Abteilungsleiter „Digitale Gesellschaft" im Bundesministerium für Verkehr und digitale Infrastruktur
10:30	Künstliche Intelligenz und Cybersecurity sind Eckpfeiler der Digitalisierung	Christoph Winterhalter Vorsitzender des Vorstandes des DIN
11:00	Kaffeepause	
11:30	Angriffe auf Maschinelle Lernverfahren - was lernen wir daraus?	Prof. Markus Ullmann Referatsleiter „Technologisches Grundlagen sicherer elektronischer Identitäten, Chipsicherheit" im Bundesamt für Sicherheit in der Informationstechnik (BSI)
12:00	Cyber Security im Lichte der letztjährigen Sicherheitsvorfälle und neuer Regularien - hilft uns KI?	Wihelm Dolle Partner, Cyber Security, KPMP AG Wirtschaftsprüfungsgesellschaft
12:30	Rotes Sofa I mit Referenten und Publikum	Robert Skuppin
13:00	Mittagspause	
14:00	ML und Deep Learning: Gewinn oder Gefahr für die Sicherheit?	David Fuhr Heas of Research HiSolutions
14:30	Künstliche Intelligenz und maschinelles Lernen im Kampf gegen Cyberkriminelle	Udo Schneider Security Evangelist Trend Mircor Deutschland GmbH
15:00	Künstliche Intelligenz - Hackers best friend!	Dr. Andreas Lang Expert Syber Security T-Systems Multimedia Solutions GmbH
15:30	Kaffeepause	
16:00	Begehrlichkeit der KI-Daten von vernetzten, autonomen Fahrzeugen - eine datenschutzrechtliche Betrachtung	Rafael Gatzka Sr. Consultant ISMS, DEKRA Assurance Services GmbH
16:30	Cambridge Analytica und die Europawahl 2019	Hannes Grassegger Journalist
17:00	Künstliche Intelligenz: Chancen nutzen - Freiheitsrechte sichern	Ulf Buermeyer Berliner Richter und Blogger
17:30	Rotes Sofa II mit Referenten und Publikum	Robert Skuppin Ulf Buermeyer, Hannes Grassegger
18:00	Get Together	

Was ist Künstliche Intelligenz

Prof. Dr. Jochen Heinsohn
Prof. Dr. Sven Buchholz
Dipl.-Inform. Ingo Boersch

Technischen Hochschule Brandenburg

Künstliche Intelligenz (KI)

KI ist in aller Munde - aber was verbirgt sich hinter dem Begriff? Man möchte von einer Inflation der KI sprechen, aber meinen alle das Gleiche?

Welche zentralen Konzepte gehören zu diesem Forschungsfeld: was ist neu, was ist alt, was funktioniert, was ist noch weit entfernt (mindestens 2 Jahre)?

Digitalisierung, Vernetzung, Automatisierung und Robotik, Datensammlungen, Elektromobilität, Smartphones und soziale Medien verändern spürbar die Gesellschaft - und das bereits ohne künstliche Intelligenz. Gleichzeitig werden im Bereich der Wissensverarbeitung, des maschinellen Lernens und der Sprachverarbeitung Erfolge erzielt, die vor einigen Jahren utopisch erschienen: Kann ein Roboter lernen, ohne dass ein Mensch ihn programmiert oder ihm beibringt, was er zu tun hat? Sogar ohne, dass es einen Menschen gibt, der ihm die Fähigkeit hätte erklären können. Und können wir Vertrauen in intelligente, autonome Systeme aufbauen, wenn sie sich jeden Tag verändern und wir nicht verstehen, wie?

Wir werden uns diesen Aspekten im Vortrag zuwenden und natürlich geht es auch kurz um Deep Learning.

Jochen Heinsohn ist seit 1994 Professor für Angewandte Informatik/Wissensbasierte Systeme/wKI-Techniken an der TH Brandenburg. Nach seinem Studium der Informatik an der TU Braunschweig arbeitete er ab 1986 als wissenschaftlicher Assistent im Philips GmbH Forschungslabor Hamburg, Abteilung Informationssysteme sowie von 1990 bis 1994 beim DFKI - Deutsches Forschungszentrum für Künstliche Intelligenz in Saarbrücken. Am DFKI promovierte er mit einer Arbeit zum „Soft Computing“.

Sven Buchholz, Jahrgang 1971, studierte Informatik an der Universität Kiel. Ebenfalls dort wurde er mit einer Arbeit über Neuronale Netze promoviert. Nach der Promotion forschte er in Kiel auf den Gebieten des Maschinellen Lernens und der allgemeinen Datenanalyse mit mehrmonatigen Gastaufenthalten an der Universität Nagoya und am INP Grenoble. Dr. Buchholz verfügt über umfangreiche Erfahrung als Data Mining Consultant. Er ist Mitgründer eines Berliner Start-Up für die wissenschaftliche und technologische Entwicklung und Vermarktung neuro-kognitiver Messverfahren.
Seit August 2014 ist Dr. Buchholz Professor für Angewandte Informatik, insbesondere Datenmanagement und Data Mining an der Technischen Hochschule Brandenburg. Er ist der wissenschaftliche Leiter des Weiterbildungsangebotes „Machine Learning mit Python“.

Ingo Boersch ist Diplom-Informatiker und wissenschaftlicher Mitarbeiter im Studiengang Informatik der Technischen Hochschule Brandenburg. Auf dem Gebiet der „Intelligenten Systeme“ befasst er sich mit wissensbasierten Systemen, insbesondere Data Mining im medizinischen und technischen Umfeld. Beim internationalen studentischen Data Mining Cup erreichten von Boersch betreute Teams in den vergangenen Jahren mehrfach Plätze unter den Top 10 bei jeweils mehr als 100 teilnehmenden Gruppen.
Er ist Mitglied im Programmkomitee des Workshops “Air Quality and Open Data” der WorldCIST 2019.

Fachbuch:
Boersch I., Heinsohn J., Socher R.: Wissensverarbeitung - Eine Einführung in die Künstliche Intelligenz für Informatiker und Ingenieure, Spektrum/Elsevier, 2007

Künstliche Intelligenz in der Mobilität

Dr. Tobias Miethaner
Abteilungsleiter Digitale Gesellschaft im Bundesministerium für Verkehr und digitale Infrastruktur

Dr. Tobias Miethaner ist seit August 2014 Leiter der Abteilung Digitale Gesellschaft im Bundesministerium für Verkehr und digitale Infrastruktur. Dort ist er etwa zuständig für den Breitbandausbau, das automatisierte und vernetzte Verfahren sowie die Datenpolitik. Zuvor war er bei der CSU-Landesleitung unter anderem als Leiter der Abteilung Politik tätig.
Dr. Miethaner absolvierte seine juristische Ausbildung in Regensburg, wo er auch promovierte, und in Aberdeen.

Künstliche Intelligenz und Cybersecurity sind Eckpfeiler der Digitalisierung

Christoph Winterhalter

Vorsitzender des Vorstandes von Deutsches Institut für Normung

Der Vortrag zeigt, weshalb Künstliche Intelligenz und Cybersecurity zu den Eckpfeilern der Digitalisierung gehören. Es gibt so gut wie keine Branche und so gut wie keinen Bereich der Gesellschaft, der nicht von der Digitalisierung betroffen ist. Überall fallen Daten an und werden Daten ausgewertet. Das geht nicht ohne Cybersecurity und Datenschutz. Die Auswertung der Daten ist längst mehr als ein reines Auflisten von Zahlen und Fakten. Jeder der Google oder andere Suchmaschinen nutzt, trägt zum Thema der intelligenten Auswertung von Daten und damit zu Künstlicher Intelligenz bei. Für eine nachhaltige und durchdringende Digitalisierung von Wirtschaft und Gesellschaft sind Normung und Standardisierung vor allem bei diesen Punkten eine Grundvoraussetzung ist. Vor allem die deutsche mittelstandsgeprägte Wirtschaft benötigt internationale Standards, um erfolgreich zu sein. Es ist wichtig, dass die deutsche Wirtschaft in der internationalen Normung und Standardisierung auch auf den Gebieten Cybersecurity und Künstlicher Intelligenz eine impulsgebende und führende Rolle spielt.

Angriffe auf Maschinelle Lernverfahren - was lernen wir daraus?

Prof. Markus Ullmann

Referatsleiter „Technologie Grundlagen sicherer elektronischer Identiäten, Chipsicherheit“ im Bundesamt für Sicherheit in der Informationstechnik (BSI)

In dem Vortrag werden zunächst exemplarische Anwendungsfälle maschineller Lernverfahren dargestellt, wie z.B. zur Identifikation von Personen mit Hilfe der Gesichtsbiometrie. Anschließend werden ausgewählte Angriffe präsentiert, die eine spezifische Angreifbarkeit entsprechender Systeme darlegen. Dabei beschränken wir uns nicht nur auf biometrische Systeme. Der Vortrag endet mit offenen Fragen zur (IT)-Sicherheit und Zuverlässigkeit maschineller Lernverfahren.

Cyber Security im Lichte der letztjährigen Sicherheitsvorfälle und neuer Regularien - hilft uns KI?

Wilhelm Dolle

Partner, Cyber Security, KPMG AG Wirtschaftsprüfungsgesellschaft

Wilhelm Dolle arbeitet als Partner der KPMG AG Wirtschaftsprüfungsgesellschaft im Bereich Cyber Security und ist Geschäftsführer der KPMG CERT GmbH. Er verfügt über mehr als 20 Jahre Berufserfahrung und ist Experte sowohl für technische als auch organisatorische Aspekte der Informationssicherheit. Dazu gehören etwa Risiko- und Sicherheitsanalysen, der Aufbau von Informationssicherheitsmanagementsystemen bis zur Zertifizierungsreife, aber auch Themen wie Penetrationstests und Sicherheit von Industrieanlagen. Wilhelm Dolle beschäftigt sich ebenfalls intensiv mit regulatorischen Anforderungen an die Informationssicherheit und das IT-Risikomanagement. Er hat einige Studien zum IT-Sicherheitsgesetz und zur Sicherheit in kritischen Infrastrukturen verfasst, ist Autor eines Buches, zahlreicher Artikel in Fachzeitschriften und hat Lehraufträge an verschiedenen Hochschulen inne.

ML und Deep Learning: Gewinn oder Gefahr für die Sicherheit?

David Fuhr

Head of Research
HiSolutions

In den letzten Jahren hat dank des Durchbruchs von Deep Learning-Methoden in bestimmten Anwendungsbereichen das Oberthema KI einen Boom erlebt, der Befürchtungen und Heilsversprechen quer durch alle Gebiete auslöst, die mit IT auch nur entfernt in Berührung stehen. In der Security werden aus Marketinggründen häufig vor allem die Vorteile betont, die Künstliche Intelligenz bei der Verteidigung bringen kann. Der Vortrag versucht die Kräfteverschiebungen systematisch darzustellen, die sich durch die neuen Techniken im Feld zwischen Offense und Defense ergeben. Dabei werden Elemente einer Theorie der „KI-Security" entwickelt, welche auch KI-Safety umfasst.

David Fuhr ist Principal Berater bei der HiSolutions AG in Berlin. Spezialisiert auf Kryptographie und die Sicherheit von kritischen Infrastrukturen, untersucht er als Forschungsleiter neue Ansätze für aktuelle und emergente Security-Herausforderungen in Bereichen wie ICS, Quantum Computing und Machine Learning. Er hat Mathematik studiert und ist CISSP, CISA und ISO 27001 Lead Auditor sowie Autor nationaler und Branchenstandards. David Fuhr publiziert und lehrt europaweit und ist als Gestalt-Trainer und Organisationsberater aktiv.

Künstliche Intelligenz und maschinelles Lernen im Kampf gegen Cyber-kriminelle

Udo Schneider

Security Evangelist
Trend Mirco Deutschland GmbH

Udo Schneider kennt sich aus mit den Gefahren, die im Internet lauern, und weiß, wie man sich vor ihnen schützen kann. Bevor er bei Trend Micro seine jetzige Position als Security Evangelist (Germany) antrat, beschäftigte er sich als Solution Architect (EMEA) mehrere Jahre lang mit der Entwicklung geeigneter Maßnahmen gegen diese Gefahren. Er konzentrierte sich dabei auf Themen wie Cloud-Computing, Virtualisierung, Verschlüsselung und Netzwerksicherheit. Davor war er beim japanischen IT-Sicherheitsanbieter als Product Marketing Manager und als Channel Development Manager tätig.
Schneider greift auf eine langjährige Erfahrung zurück, die er bei führenden Anbietern des IT-Sicherheitsmarktes erworben hat: So war er unter anderem in seinen knapp fünf Jahren bei Check Point Technologies als Systems Engineer, als Senior Consultant, als Security Analyst sowie als Trainer tätig und hatte bei Perimetrix Systems den Rang eines Technical Director inne.

Künstliche Intelligenz - Hackers best friend!

Dr. Andreas Lang

Expert Cypber Security
T-Systems Mulitmedia Solutions GmbH

Durch CEO-Fraud wurden in der Vergangenheit mehrere Unternehmen gezielt durch Angreifer um Millionenbeträge erleichtert. Dabei spielt Social Engineering eine wesentliche Rolle für den Erfolg eines derartigen Angriffs. Die Angreifer fälschen dabei Emails oder Briefpost und bewegen unter falschen Vorwand und mit falscher Identität Angestellte dazu größere Geldbeträge zu überweisen.
Bei aktuellen CEO-Fraud Angriffen erfolgt die Kontaktaufnahme und die Kommunikation zwischen Angreifern und Opfern immer schriftlich.
In diesem Vortrag wird die Angriffsform des CEO-Fraud's durch die Verwendung von Künstlicher Intelligenz derart verbessert und optimiert, dass die Wahrscheinlichkeit für den Erfolg der Angriffes extrem steigt. Hierbei wird neben dem bereits genutztem schriftlichen Kommunikationskanal auch die telefonische Kontaktaufnahme zum Opfer verwendet. Künstliche Intelligenz hilft dabei das Opfer zu Überzeugen und die Überweisung zu tätigen. Dabei wird aufgezeigt welchen Gefahren die Unternehmen ausgesetzt sind und wie sich CEO-Fraud Angriffe weiterentwickeln.

Dr. Andreas Lang ist seit über 25 Jahren im Bereich der IT- und Cyber-Sicherheit tätig. Bei der T-Systems Multimediasolutions ist Herr Lang seit über 10 Jahren in den Rollen als IT-Security Auditor, IT-Security Officer und als Trainer bei einer Vielzahl von Kunden national als auch international unterwegs.

Begehrlichkeit der KI Daten von vernetzten, autonomen Fahrzeugen - Eine datenschutzrechtliche Betrachtung

Rafael Gatzka
Sr. Consultant | ISMS,
DEKRA Assurance Services GmbH

Die Datenverarbeitung von Fahrzeugen mit smart Services schafft Begehrlichkeiten, die dort anfallenden Daten nutzen zu wollen. Die Speicherung, KI-Verknüpfungen und Auswertungen der Daten der Nutzer/-in gefährden den Einzelnen in seinen Persönlichkeits- und Freiheitsrechten. Datenschutz-Probleme drohen vor allem dann, wenn Unternehmen vernetzte Fahrzeuge einsetzten, den in der DS-GVO verankerten Prinzipen für einen effektiven Datenschutz ist auch bei vernetzten Autos Genüge zu leisten. Darüber hinaus werden nicht nur die Hersteller, sondern auch verschiedenste Akteure zu Diensteanbietern und damit Verantwortliche im datenschutzrechtlichen Sinne. Neben der Kernfrage der Rechtmäßigkeit der Verarbeitung haben datenverarbeitende Unternehmen weitere technisch-organisatorische Pflichten zu beachten.

Rafael Gatzka, ISMS Senior Berater der DEKRA, berät weltweit Kunde im Rahmen der Lieferantenqualifizierung. An der Schnittstelle zwischen Security, Safety und Quality Excellence steht er auch in Umsetzungsverantwortung.

Cambridge Analytica und die Europawahl 2019

Hannes Grassegger

Journalist

Hannes Grassegger (1980) ist Ökonom und Autor. Er arbeitet als investigativer Reporter für Das Magazin (Zürich). Seine Texte behandeln Fragen der Autonomie des Individuums im Digitalen Zeitalter. Weltweit bekannt wurden seine Enthüllungen zu Cambridge Analytica (2016, mit Mikael Krogerus) und Facebooks Zensurapparat (2017, mit Till Krause & Julia Angwin). Grasseggers Digitalisierungsreportagen erscheinen u.a. im SZ-Magazin, Guardian, Reportagen, Internazionale und Pro Publica. 2018 war Grassegger der Swiss Fellow am Wilson Center Think-Tank in Washington DC. Sein Studium der Volks- und Betriebswitschaft absolvierte er in Berlin und Zürich.

Künstliche Intelligenz: Chancen nutzen - Freiheitsrechte sichern

Ulf Buermeyer

Berliner Richter und Blogger

Die Fortschritte der Informationstechnik in den letzten Jahren machen Computer möglich, die erstmals nicht nur schneller „denken“ als Menschen, sondern scheinbar auch intelligenter sind: Rechnersysteme werten unvorstellbare Datenmengen aus und kommen mittels „künstlicher Intelligenz“ (KI) zu faszinierenden Ergebnissen. Doch welche Risiken für unsere Freiheitsrechte birgt KI, und welche Herausforderungen stellen sich an die Rechtsordnung?

Moderation

Robert Skuppin

Robert Skuppin wurde 1964 in Cham, in Bayern, geboren und studierte in Berlin Publizistik, Politologie und Geschichte. 1988 begann er als Nachrichtenredakteur bei Radio 100. Es folgten Stationen als freier Mitarbeiter und Redakteur bei Radio 4U (SFB) und Radio Fritz (ORB/ rbb). Gemeinsam mit Helmut Lehnert entwickelte Skuppin das Programm radioeins, das am 29. August 1997 auf Sendung ging.

Mit Volker Wieprecht konzipierte er die Sendung „Der schöne Morgen“ und moderiert mit ihm seit mehr als zehn Jahren die Sendungen „Der Tag“ und „Die schöne Woche“. Skuppin lehrte an der Bauhaus-Universität Weimar und ist Autor mehrerer Bücher.

Seit 1. Juni 2011 leitet Robert Skuppin als Programmchef radioeins vom Rundfunk Berlin-Brandenburg (rbb).

HiSolutions AG

Die HiSolutions AG ist seit über 25 Jahren eines der renommiertesten Sicherheitsberatungsunternehmen im deutschsprachigen Raum. Zu den rund 700 Klienten der HiSolutions AG aus unterschiedlichsten Branchen und Unternehmensgrößen gehören u. a. gut die Hälfte der DAX30-Unternehmen und 75 % der deutschen Top 20-Banken. Aus der seit 20 Jahren andauernden Tätigkeit für das BSI resultieren u. a eine Vielzahl von Grundschutzbausteinen und Standards wie 100-4.
Zuletzt hat HiSolutions für das BSI die Neugestaltung des IT-Grundschutzes vorgenommen. HiSolutions beschäftigt eines der größten Teams von akkreditierten IT-Grundschutzauditoren und betreibt im Auftrag des BSI eines von zwei Zertifizierungslabors für die Abnahme von IT-Grundschutz-Zertifizierungen.
Die HiSolutions AG zeichnet ein außergewöhnlich breites Kompetenzprofil aus. Hierzu gehören:

- Technische Audits und Sicherheitskonzepte
- Aufbau und Zertifizierung von ISMS
- eines der größten deutschen Forensik-/Cyber Response-Teams
- eine über IT-Aspekte weit hin ausgehende Betrachtung des Themas Business Continuity
- Aufbau von Krisenmanagement-Organisationen und Durchführung von Krisenstabsübungen
- nicht-technischer Wirtschaftsschutz
- Sicherheitsstrategie-Beratung

HiSolutions arbeitet in Forschung und Lehre eng mit Hochschulen wie der THB, der FH Campus Wien, der TU Berlin, der Frankfurt School of Finance und Management, der Uni Bonn oder der Uni Potsdam zusammen. Ein Ergebnis dieser umfassenden Betrachtung des Themas Sicherheit und der begleitenden Forschung ist die Erstellung des Wirtschaftsgrundschutzes, herausgegeben von BfV, BSI und dem ASW Bundesverband, der den IT-Grundschutz um nicht-IT-spezifische Sicherheitsaspekte ergänzt. HiSolutions engagiert sich darüber hinaus in der Erforschung und Entwicklung neuer Security-relevanter Thematiken wie Machine Learning und Data Science.

Kontakt
HiSolutions AG
David Fuhr
Head of Research
Bouchéstraße 12
12435 Berlin
T +49 30 533 289 0
fuhr@hisolutions.com

HISOLUTIONS

Institute for Security and Safety (ISS)

Das ISS betreibt nationale und internationale Sicherheitsforschung. Im Fokus steht hierbei die Umsetzung von international ausgerichteten Aus-, Weiterbildungs- und Trainingskonzepten in den Bereichen Cyber und Nuclear Security sowie Security Management.

Als An-Institut der Technischen Hochschule Brandenburg (THB) sieht das ISS zudem seinen Auftrag darin, Praxiskenntnisse in Forschungsprojekte einzubringen.

Das ISS ist seit 2016 als NGO beim Economic and Social Council of the United Nations (ECOSOC) akkreditiert. Es ist außerdem Mitglied des International Nuclear Security Education Network (INSEN).

Für die THB hat das ISS die neue Profilrichtung Nuclear Security des Masterstudiengangs Security Management entwickelt. Dies wurde durch die International Atomic Energy Agency (IAEA) unterstützt.
Jüngste internationale Projekt-Aktivitäten des ISS wurden darüber hinaus von der OSZE, der Nuclear Threat Initiative (NTI) sowie dem Science for Peace and Security (SPS) gefördert.

Kontakt
Institute for Security and Safety (ISS)
Prof. Dr. Ivo Keller
David-Gilly-Str. 1
14469 Potsdam
T +49 331-58148330
info@uniss.org
www.uniss.org

Technische Hochschule Brandenburg
University of Applied Sciences
Institute for Security and Safety

T-Systems

Die T-Systems Multimedia Solutions ist die Nummer 1– der größte Digitaldienstleister Deutschlands und damit auch der größte IT-Arbeitgeber in Dresden.
Wir begleiten Großkonzerne und mittelständische Unternehmen bei der digitalen Transformation. Als Marktführer mit einem Jahresumsatz von 173 Mio. Euro im Jahr 2017 zeigen wir mit unserer Beratungs- und Technikkompetenz neue Wege und Geschäftsmodelle in den Bereichen Industrie 4.0, Customer Journey, Arbeitsplatz der Zukunft sowie digitale Zuverlässigkeit. Mit rund 1900 Mitarbeitern an sieben Standorten bietet die T-Systems Multimedia Solutions ein dynamisches Web- und Applikation-Management und sorgt mit dem ersten zertifizierten Prüflabor der Internet- und Multimediabranche für höchste Softwarequalität, Barrierefreiheit und IT-Sicherheit.
Ausgezeichnet wurde T-Systems Multimedia Solutions mehrfach mit dem Social Business Leader Award der Experton Group sowie dem iF Design Award und gehört 2017 zu den Gewinnern des Outstanding Security Performance Awards. Zudem wurden wir mehrmals als einer von Deutschlands besten Arbeitgebern mit dem Great Place to Work Award gekürt sowie als Bester Berater 2018 vom Wirtschaftsmagazin brand eins ausgezeichnet.

Werden Sie ein Teil des Teams, denn wir suchen Sie für die Umsetzung der Digitalisierungsvorhaben unserer Kunden. Gestalten Sie gemeinsam mit dem größten Digitaldienstleister Deutschlands und unseren Kunden in einem stetig wachsenden Markt die digitale Welt.
Weitere Informationen:
www.t-systems-mms.com

Kontakt
T-Systems Multimedia Solutions
Dr. Andreas Lang
Riesaer Straße 5
01129 Dresden
frage@t-systems-mms.com
www.t-systems-mms.com

DEKRA

Ein starker Partner.

Seit der Gründung im Jahr 1925 hat sich die DEKRA Gruppe von einem reinen Fahrzeugprüfer zu einer weltweit führenden Expertenorganisation für Sicherheit, Qualität und Gesundheit entwickelt. Die Zahl unserer Unternehmen, mit denen wir als Partner für zahlreiche Branchen aktiv sind, wächst dabei ständig. Auch die internationale DEKRA Business Assurance Group ist ein Teil unserer weltweiten Organisation. In mehr als 50 Ländern bietet DEKRA mittlerweile Fahrzeugprüfungen, Gutachten, Industrieprüfungen und Personaldienstleistungen an. Unser Geschäftsumfang und unser Leistungsangebot vergrößern sich dabei stetig, wobei Prüf- und Zertifizierungsdienstleistungen die wohl wichtigsten Säulen unseres weltweiten Erfolgs bilden. Vor allem durch internationale Neugründungen und Zukäufe erschließt sich die DEKRA Gruppe neue, zukunftsträchtige Bereiche wie Energie und Nachhaltigkeit und schafft dadurch Jahr für Jahr neue Arbeitsplätze.
DEKRA. Alles im grünen Bereich.

Kontakt
DEKRA Certification GmbH
Michael Spuling
Key Account Manager Cyber Security
T +49 151 18877806
michael.spuling@dekra.com

Cluster IKT, Medien und Kreativwirtschaft

CLUSTER
IKT, MEDIEN UND KREATIVWIRTSCHAFT
BERLIN BRANDENBURG

Das Cluster IKT, Medien und Kreativwirtschaft ist das Cluster der Digitalen Wirtschaft. Innerhalb der gemeinsamen Innovationsstrategie der Länder Berlin und Brandenburg (innoBB) haben sich eine Vielzahl von Clusterakteuren zusammengefunden, die Digitale Transformation voranzutreiben. Diese vereinten Netzwerke, Hochschulen, Unternehmen und Verbände machen das Cluster aus. Sie stehen für Innovation und Kreativität, Intelligente Vernetzung und neue Technologien. Sie arbeiten zusammen in einer Vielzahl von Projekten, ermöglichen Erneuerung, Entwicklung und Fortschritt in unserer Region. Herausragende Forschungseinrichtungen, Startups und etablierte Unternehmen erzielen überregionale und internationale Aufmerksamkeit und tragen zur Steigerung der Wettbewerbsfähigkeit und Wertschöpfung bei. Das Wesen der Digitalen Wirtschaft ist ihr übergreifender und verbindender Ansatz. Die Vernetzung umfasst immer mehr Lebens- und Arbeitsbereiche, verknüpft Technologie und Alltag, öffentlich und privat. Cross-Cluster-Ansätze werden somit immer wichtiger. Das Clustermanagement ist bei der Wirtschaftsförderung Land Brandenburg GmbH (WFBB) angesiedelt.

Kontakt
Clustermanager IKT, Medien und Kreativwirtschaft
Till Meyer
till.meyer@wfbb.de

Yvonne Gruchmann
Projektmanagerin Cluster IKT, Medien und Kreativwirtschaft
yvonne.gruchmann@wfbb.de

www.digital-bb.de
www.wfbb.de

EUROPÄISCHE UNION
Europäischer Fonds für Regionale Entwicklung

Die Cluster werden unterstützt von

Wirtschaftsförderung Brandenburg | WFBB

DAkkS

Die DAkkS ist die nationale Akkreditierungsstelle der Bundesrepublik Deutschland. Sie handelt hoheitlich und nicht gewinnorientiert gemäß der Verordnung (EG) Nr. 765/2008 und dem Akkreditierungsstellengesetz (AkkStelleG) im öffentlichen Interesse. Gesellschafter der GmbH sind zu jeweils einem Drittel die Bundesrepublik Deutschland, die Bundesländer und die durch den Bundesverband der Deutschen Industrie e. V. (BDI) vertretene Wirtschaft.
Um ihre hoheitlichen Akkreditierungsaufgaben erfüllen zu können, wurde die DAkkS GmbH vom Bund beliehen. Als beliehene Stelle untersteht die DAkkS der Aufsicht des Bundes. Bei ihrer hoheitlichen Akkreditierungstätigkeit wendet die DAkkS im Inland das deutsche Verwaltungsrecht an. Die DAkkS ist aber auch weltweit außerhalb des EWR als Akkreditierungsstelle tätig um die Produktsicherheit und die Laborkompetenz zu erhöhen und Handelshemmnisse abzubauen.

Welche Aufgabe hat die DAkkS?
Die Akkreditierung von Konformitätsbewertungsstellen (Laboratorien, Inspektions- und Zertifizierungsstellen) ist der gesetzliche Auftrag der DAkkS. In rund 4.300 Akkreditierungsverfahren begutachtet, bestätigt und überwacht die DAkkS als unabhängige staatliche Einrichtung die fachliche Kompetenz dieser Stellen, deren Dienstleistungen in nahezu allen Bereichen der Wirtschaft und und der Gefahrenabwehr benötigt werden. Das Spektrum der Kunden reicht von kleinen medizinischen Laboratorien bis hin zu multinationalen Prüfunternehmen.
Mit einer Akkreditierung bestätigt die DAkkS, dass das Labor oder die Konformitätsbewertungsstelle diese ihre Aufgaben fachkundig und Unparteilich erfüllt.
Kurz: Die DAkkS prüft die Prüfer.

Kontakt
Deutsche Akkreditierungsstelle GmbH
Dr. Raoul Kirmes M.Sc.
Spittelmarkt 10
10117 Berlin
T +49 (0)30 67 05 91-17
raoul.kirmes@dakks.de
www.dakks.de

DAkkS Deutsche Akkreditierungsstelle

KPMG

KPMG macht den Unterschied | KPMG ist ein Firmennetzwerk mit mehr als 174.000 Mitarbeitern in 155 Ländern. Auch in Deutschland gehört KPMG zu den führenden Wirtschaftsprüfungs- und Beratungsunternehmen. Unser Anspruch: Seite an Seite mit unseren Kunden neue und innovative Wege gehen. Unser Ziel: Schon heute wertvolle Lösungen für morgen liefern. Unser Handwerkszeug: Qualität, Leidenschaft und voller Einsatz. Das fundierte Fach- und Branchenwissen unserer Experten gibt unseren Kunden Sicherheit und Orientierung. Und es ermutigt sie, notwendige Dinge entschlossen anzupacken. Denn wir zeigen Unternehmen nicht nur geschäftliche Chancen auf. Wir unterstützen sie auch dabei, Entwicklungen mitzubestimmen und ihre Wachstumsziele zu erreichen.

Kontakt
KPMG AG
Wirtschaftsprüfungsgesellschaft
Wilhelm Dolle
Partner, Consulting – Cyber Security
Klingelhöferstr. 18
10785 Berlin

T+49(0)30 20682323
M +49(0)174 3049537
wdolle@kpmg.com
www.kpmg.de/cybersecurity

ANNA – Das vernetzte Leben (iRights e.V.)

Anna ist 35 und erlebt einen zunehmend digitalisierten Alltag: Nach einem langen Arbeitstag sucht sie gerne Ablenkung im Internet, scrollt durch ihre Social Media-Feeds oder bestellt online ein Buch. Was sich dabei auf ihrem Bildschirm abspielt, kann sie sehen. Doch im Hintergrund arbeiten intelligente Systeme, die aus Annas Datenspuren lernen. Manchmal ist das ziemlich nützlich. Und manchmal hat das verblüffende Konsequenzen …
Im Projekt **ANNA – Das vernetzte Leben** geht es um die Bedeutung von Algorithmen und Künstlicher Intelligenz im Alltag. Ausgangspunkt sind Technologien, die bereits existieren und in Bereichen wie Gesundheit, Wohnen, Einkaufen oder im sozialen Leben genutzt werden. Mit einer Mischung aus unterhaltsamen Geschichten aus Annas Leben und Sachinformationen unterstützt das Projekt die Verbraucherinnen und Verbraucher beim informierten Umgang mit diesen Technologien.
Alle Inhalte auf annasleben.de stehen unter creative commons-Lizenzen und eignen sich für die Jugend- und Erwachsenenbildung. ANNA – Das vernetzte Leben wird von iRights e.V. umgesetzt; gefördert wird das Projekt durch das Bundesministerium der Justiz und für Verbraucherschutz (BMJV).

Über iRights e.V.
Wir sind ein gemeinnütziger Verein, der Informationen zu Themen wie Urheberrecht, Datenschutz, Computersicherheit und Digitalisierung bereitstellt. Der Verein betreibt die Informationsplattform iRights.info, Webangebote wie annasleben.de und veröffentlicht Publikationen. Wir wollen dazu beitragen, dass Nutzerinnen und Nutzer die Veränderungen, die die Digitalisierung mit sich bringt, besser verstehen und an der Entwicklung teilnehmen können.

Kontakt
iRights e.V.
Projekt: ANNA – Das vernetzte Leben
Almstadtstraße 9/11, 10119 Berlin
T +49(0)30 89 37 19 60
kontakt@annasleben.de
annasleben.de

ANNA
Das vernetzte Leben

BlockAxs - Smart Access Protocol

Die BlockAxs GmbH, ein Berliner Blockchain Start-up, wurde im Juli 2018 gegründet. Seit mehreren Jahren ist die Digitalisierung ein branchenübergreifender Begriff. Die Blockchain-Technologie ist ein Teil dieser und gewinnt in letzter Zeit immer mehr an Bedeutung. Wir nutzen diese neue Technologie und bieten unseren Kunden die bestmöglichen Lösungen an.Zugriffsmanagement muss schnell, sicher und automatisiert ablaufen! Wir als junges, hochqualifiziertes und motiviertes Team der BlockAxs GmbH entwickeln ein plattformübergreifendes Zugriffsmanagementsystem unter Zuhilfenahme der Blockchain-Technologie. Unsere Lösung zeichnet sich durch höchste Sicherheit in den Bereichen des Informationsmanagements und Compliance aus, sowie durch Prozessoptimierung und Anwendung neuer Technologien. Die schnell wachsende Digitalisierung bringt Normen, Standards, Pflichten, aber auch ein erhöhtes Angriffspotential mit sich und erfordert somit eine dynamische und flexible Systemlandschaft. Diese und weitere Aspekte bilden die Hauptsäulen der BlockAxs GmbH, um stetig und schnellstmöglich auf neue Gegebenheiten reagieren zu können und alle Anforderungen der Kunden abzudecken.
Ein weiterer Bereich der BlockAxs GmbH ist die Emission eines „Security Tokens“. Dieser ist eine digitale „tokenisierte“ Aktie und stellt ein neues Finanzinstrument dar.

Kontakt
BlockAxs GmbH
Fabian Pohl
Scharnhorststr. 24
10115 Berlin
T +49 17631732010
mail@blockaxs.com
www.blockaxs.com

Smart Kid Security

Wir entwickeln ein sicheres Ökosystem für Kinder, in dem diese einen verantwortungsvollen Umgang mit dem Internet und den Wert ihrer privaten Daten erlernen können. Wir geben Kindern die richtigen Werkzeuge an die Hand, um sich online zu schützen. Durch unseren spielerischen Lernansatz schaffen wir Sicherheit durch Bildung. Als Teil einer globalen Kid-Security-Community können sie Technologie und das Internet zu ihrem Vorteil nutzen. Im Rahmen dessen bieten wir offline Workshops für Kinder und Eltern als auch Schulungen für
Erzieher, die anschließend die Inhalte und Experimente im Alltag mit den Kindern umsetzen und leben können.
Unser Curriculum umfasst drei große Blöcke:

- Digital Wellbeing
- Digital Literacy
- Digital Skills.

Die Inhalte werden in spielerischen Experimenten vermittelt. Dabei nutzen wir Design Thinking und Gamification, um Kinder in die Problemlösung einzubeziehen und nutzen dabei den natürlichen Wunsch des Kindes nach Sozialisierung, Lernen und der Befriedigung, etwas eigenständig geleistet zu haben. Dazu wollen wir unter anderem Abzeichen einführen, die die Kinder nach Abschluss der einzelnen Einheit erhalten werden.
Die Seminare und Workshops für Pädagogen geben ihnen die Werkzeuge und Methoden an die Hand, die notwendig sind, um die Grundlagen der digitalen Sicherheit in KiTa und Schule zu vermitteln und zu leben. Dabei reichen die Inhalte von der Vermittlung von Grundlagenwissen zu Technologie, Internet und Sicherheitskonzepten bis hin zu konkreten Spiel- und Experimentanleitungen zu den einzelnen Themengebieten.

Kontakt
Smart Kid Security
Anamarija Thomae
Geschäftsführerin
Gartenstraße 47
13355 Berlin
www. smartkidsecurity.com

Zentrum für Gründung und Transfer (ZGT)

Das Zentrum für Gründung und Transfer (ZGT) der Technischen Hochschule Brandenburg (THB) ist die Schnittstelle zwischen Wissenschaft und Wirtschaft. Wir vermitteln und bewerben intensiv alle Formen der Zusammenarbeit
zwischen der Hochschule und Unternehmen der Region. Dabei fokussieren wir uns auf den Technologie- und Wissenstransfer, auf Unternehmensgründungen und -nachfolgen sowie den gesellschaftlichen Transfer. Dafür haben wir mit der Präsenzstelle Prignitz an den Standorten Neuruppin, Pritzwalk und Wittenberge drei Anlaufstellen im Nordwesten des Landes Brandenburgs etabliert.

Unsere Aufgabe ist es, dass Know-how der Hochschule für die Region zugänglich zu machen. Besonders in unserem Fokus steht die regionale Wirtschaft, die durch die Zusammenarbeit in ihrer Innovations- sowie Wettbewerbsfähigkeiten gestärkt werden soll. Dafür organisieren wir den Dialog zwischen den Partnern.
Für die Zusammenarbeit stehen viele Kooperationsmöglichkeiten zur Auswahl. Ob Beratung, gemeinsame Forschungsprojekte, die Nutzung der THB-Infrastruktur oder die Verwertung von Patenten: Gemeinsam mit den Beteiligten wird individuell entschieden, welcher Weg eingeschlagen werden soll. Dafür steht ein kompetentes Team mit langjähriger und spezifischer Berufs- und Projekterfahrung zur Verfügung, um die Anbahnung und Projektrealisierung erfolgreich zu gestalten.

Kontakt
Zentrum für Grundung und Transfer
Diana Rosenthal
Leiterin
T+49 3381 355 517
zgt@th-brandenburg.de
zgt.th-brandenburg.de

VDI/VDE Arbeitskreis Sicherheit (AKSi)

Der AKSi wurde 2013 in der VDI-Geschäftsstelle Berlin-Brandenburg gegründet und hat sich dem Leitgedanken „Sicherheits- und Lernkultur als Herausforderung und Qualitätsmerkmal“ Er widmet sich den dringenden Fragen zu Chancen und Risiken der Technik mit Bezug zu den Wechselwirkungen von technischen und gesellschaftlichen Entwicklungen unserer Zeit und den konkreten Auswirkungen auf die Grundlagen unseres Miteinanders in der Zukunft vor dem Hintergrund des Innovationsklimas in Deutschland und Europa. Als Erforscher, Initiator und Wächter befasst er sich interdisziplinär mit Sicherheitsbelangen, wobei Sicherheit, Sicherung und Schutz, Zuverlässigkeit und Verlässlichkeit fachgebietsübergreifend betrachtet, bewertet und kommentiert werden. Die Gremienarbeit widmet sich aktuell dem Thema „interdisziplinäre Sicherheitsprinzipien“ (z.B. Rückfallebenen, fail-safe / fail-operational).

Schwerpunkt-Themenbereiche:
„Technik und Akzeptanz“ – Chancen und Risiken der Technikanwendung im sozialen Kontext „Technik und Wissen“ – Diskurse zu Innovationen und neuen Technologien als Treiber der Wertschöpfung in einer wissensbasierten Gesellschaft „Technik und Zukunft“ – Aufzeigen von nachhaltigen Entwicklungspfaden im Spannungsfeld unkritischer Fortschrittsglauben vs. fundamentaler Fortschrittsverweigerung „Technik und Kultur“ – Aufgreifen von Impulsen für die Technikanwendung aus anderen Bereichen mit Fokus auf dem sogenannten Faktor Mensch, wie z.B. HFE (human factor engineering)

Kontakt
VDI/VDE-AK Sicherheit
Ltr. Dipl.-Ing. Dirk C. Pinnow, VDI
c/o PINNOW & Partner GmbH
Helmholtzstr. 2-9, Aufg. D, 4. OG
10587 Berlin
T +49 30 39 74 86 21 - 0
dirk@pinnow.com

VDI Bezirksverein Berlin-Brandenburg

Das Lernlabor Cybersicherheit - Kompetenzaufbau zu IT-Sicherheit

Mit dem Weiterbildungsprogramm Lernlabor Cybersicherheit bringen die Technische Hochschule Brandenburg (THB) und Fraunhofer neueste Erkenntnisse aus der IT-Forschung praxisnah und anwendungsorientiert in die Unternehmen. Kompakte Veranstaltungsformate erlauben eine berufsbegleitende Qualifikation im Bereich Cybersicherheit für Fach-und Führungskräfte aus Industrie und öffentlicher Verwaltung.
Die THB bietet im Lernlabor Cybersicherheit zurzeit zwei Schulungen an:

- Sichere Softwareplanung: Softwareentwicklung -ab Beginn
- Software-Härtung: Software gegen Schwachstellen sichern

Sicherheitsanforderungen werden gegenüber den Anforderungen in Software gern vernachlässigt. Die Schulungen des Lernlabors Cybersicherheit zeigen eine systematische Herangehensweise, mit der sich Sicherheit frühzeitig und effizient im Entwicklungsprozess implementieren lässt. Nach der ersten Schulung können die Teilnehmer in einem systematischen Prozess Bedrohungen erkennen, modellieren und Gegenmaßnahmen ableiten. In der zweiten Schulung werden Schwachstellen in einer bestehenden Software-Architektur bestimmt Sicherheitsanforderungen in den Code integriert, geeignete Secure Design Pattern angewendet und Code-spezifische Fallen umgangen..
Das Lernlabor Cybersicherheit ist ein Weiterbildungsprogramm von Fraunhofer und Hochschulen. In der Arbeitsgruppe „Softwarequalität und Produktzertifizierung“ bieten Fraunhofer FOKUS, THBrandenburg und die HTW Berlin zusammen Schulungen zu IT-Sicherheit, Datenschutz, sicherer Softwareentwicklung, Security-Testing und Produktzertifizierung an.

Mehr Informationen unter
www.academy.fraunhofer.de/cybersicherheit
http://s.fhg.de/sichere-softwareplanung
http://s.fhg.de/sichere-softwarehaertung

Kontakt
Prof. Dr. Winfried Pfister
Technische Hochschule Brandenburg
Fachbereich Wirtschaft
Tel. 03381 355 289
winfried.pfister@th-brandenburg.de

Fraunhofer FOKUS | Akademie


Technische Hochschule
Brandenburg
University of
Applied Sciences

Sponsoren und Partner

Wir bedanken uns herzlichen bei allen Sponsoren und Partner für Ihre Unterstützung und das Sie mit uns über die Perspektiven der Security für Künstlichen Intelligenz und der Künstliche Intelligenz für Security und Sicherheit auf dem 13. Security Forum in der Technischen Hochschule Brandenburg diskutieren.

Sponsoren

Hi-Solutions
DEKRA
TrendMicro
WFBB
DAkkS
T-Systems
Frauenhofer Institut

Partner

Deutsches Institut für Normung
Zentrum für Gründung und Transfer
ANNA - ein digitales Leben
VDI/VDE - Arbeitskreis Security
Smart Security Kid
BlockAxs
Bundeskriminalamt

Kontaktliste

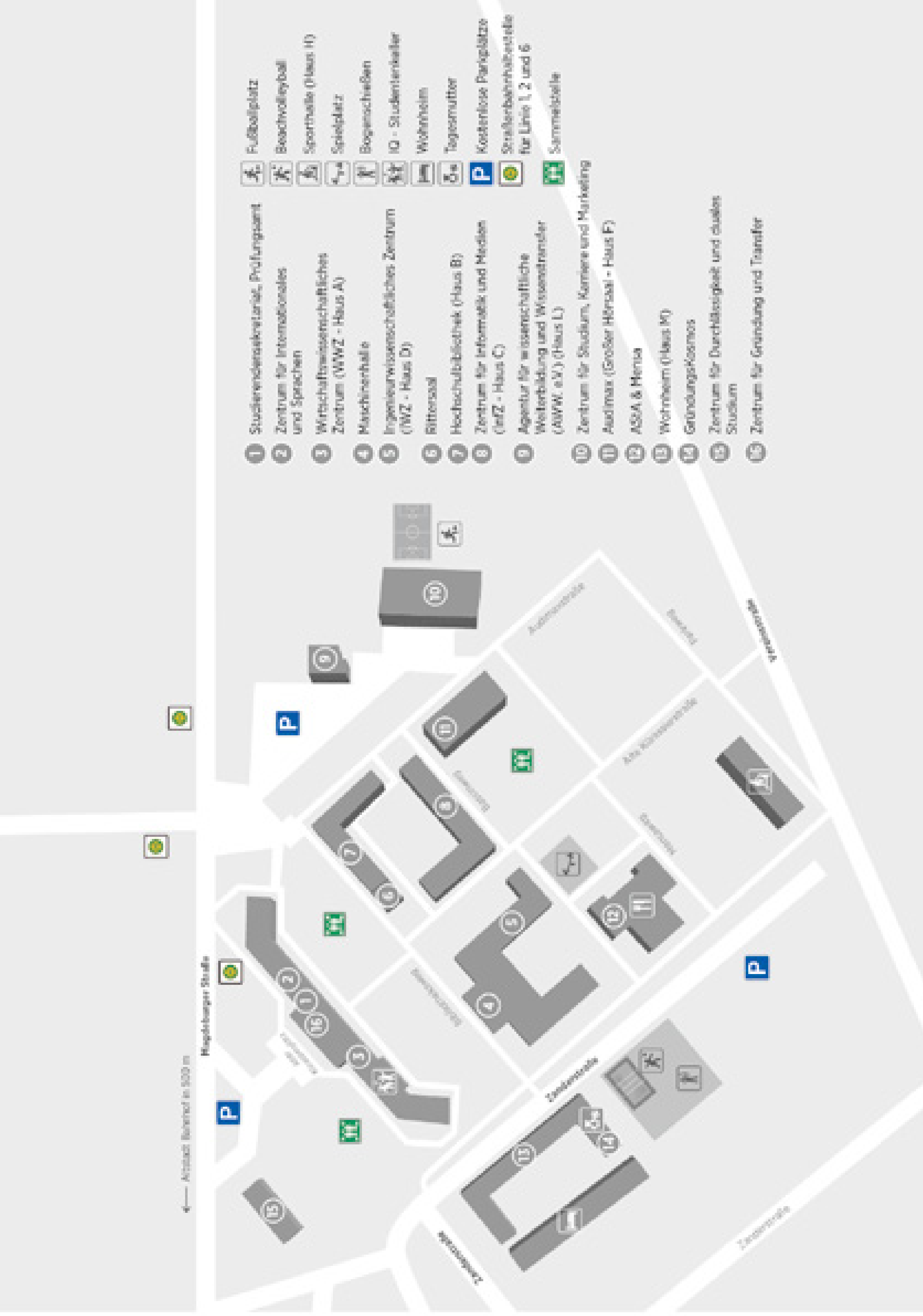
Ansprechpartner

Studiendekan Security Management
Prof. Dr. Ivo Keller
T +49 3381 355-278
ivo.keller@th-brandenburg.de

Studienkoordinatorin
Security Management
Annegrit Seyerlein-Klug
T +49 3381 355-290
seyerlein@th-brandenburg.de

Kontakt

Technische Hochschule Brandenburg
University of Applied Sciences
Magdeburger Straße 50
14770 Brandenburg an der Havel
T +49 3381 355-0
secman@th-brandenburg.de
www.th-brandenburg.de



Impressum

Herausgeberin Die Präsidentin der Technischen Hochschule Brandenburg
Prof. Dr.-Ing. Burghilde Wieneke-Toutaoui

Redaktion und v.i.S.d.P. Prof. Dr. Ivo Keller
Mitarbeit Annegrit Seyerlein-Klug, Jana Liefeldt
Layout Jana Liefeldt
Bilder Technische Hochschule Brandenburg

Technische Hochschule Brandenburg
University of Applied Sciences
Magdeburger Str. 50
14770 Brandenburg an der Havel
T +49 3381 355 - 0
F +49 3381 355 - 199
secman@th-brandenburg.de
www.th-brandenburg.de

Stand Januar 2019