Liebe Leserinnen, liebe Leser,

wir freuen uns, Ihnen nach einer längeren, Corona-bedingten Pause eine neue Ausgabe des Forschungsmagazins ‚Blick in die Wissenschaft' in der Ausgabe 44/45 präsentieren zu können.

Die Corona-Pandemie hat auch die Universität Regensburg und alle ihre Mitglieder vor große Herausforderungen gestellt. Dennoch konnten zentrale Zukunftsprojekte weitergeführt und umgesetzt werden. So stellt vor allem die Gründung unserer neuen Fakultät für Informatik und Data Science (FIDS) einen wahren Meilenstein in der Geschichte und Entwicklung der Universität Regensburg dar. Als größtes Strukturprojekt seit der Gründung der Fakultät für Medizin vor 30 Jahren ist unsere Informatikfakultät ein Zukunftsprojekt von weitreichenden Dimensionen. Mit der neuen strategischen Schwerpunktsetzung im Bereich Informatik und Data Science und vor allem auch der Querschnittsorientierung der neuen Fakultät sieht sich die Universität Regensburg sehr gut gerüstet, ihre bisherigen Stärken in diesen Bereichen zu bündeln, weiter auszubauen und zu vertiefen. Schließlich sind *Digital Transformations* als eines der vier Gestaltungsfelder und Zukunftsthemen in unserem *Hochschulentwicklungsplan 2025* fest verankert. Dieses Gestaltungsfeld adressiert die neue Fakultät ebenso wie den Bereich *Integrated Sciences in Life, Health, and Disease* als ein weiteres Schwerpunktgebiet unserer Universität.

Die Grundsatzbeschlüsse in den Gremien der Universität Regensburg im Sommer und Herbst 2019 zur Einrichtung der neuen Fakultät erfolgten nach einer vorhergehenden Phase intensiver Planungen dann letztlich fast zeitgleich mit der Regierungserklärung des Bayerischen Ministerpräsidenten Dr. Markus Söder am 10. Oktober 2019 und der Verkündigung der Hightech Agenda Bayern. Unterstützt und beschleunigt durch die Mittel der Hightech Agenda Bayern konnte der Auf- und Ausbau der Fakultät für Informatik und Data Science zügiger umgesetzt werden, nachdem die neue Fakultät im März 2020 formal gegründet und im Laufe des WS 2021/22 aus sich heraus handlungs- und funktionsfähig wurde. Im Mai 2022 konnten wir gemeinsam mit Ministerpräsident Dr. Markus Söder und Staatsminister für Wissenschaft und Kunst Markus Blume den offiziellen Kickoff für die Fakultät begehen. Dass dieser komplexe Prozess im Kontext der Herausforderungen der Corona-Pandemie vollzogen und abgeschlossen werden konnte, ist ein Zeichen für die Bedeutung dieser gesamtuniversitär-strategischen Maßnahme und für den Rückhalt für das Großprojekt in der universitären Gemeinschaft.

Im Laufe des Gründungsprozesses ist es gelungen, die verschiedenen Informatiknahen und -interessierten Kräfte der Universität an einen Tisch zu bringen und gemeinsam ein zukunftsorientiertes Konzept für die Fakultät zu entwickeln. Ein externes Gutachten mit hochrangiger Expertise skizzierte und evaluierte 2019 wesentliche inhaltliche Schwerpunkte und Strukturierungen für die neue Fakultät, an denen sich in den Jahren 2019-2021 die von Vizepräsident Prof. Dr. Nikolaus Korber geleitete Gründungskommission in der

konkreten Arbeit zum Aufbau der Fakultät orientierte. In insgesamt 15 Berufungsverfahren wurden die ersten neuen Professuren in der Fakultät zügig besetzt – ein Prozess, der in Kürze abgeschlossen sein wird. Im Besetzungsprozess hat sich vor allem auch gezeigt, wie attraktiv die Neugründung einer Fakultät und die Möglichkeiten zur Mitgestaltung und zum Aufbau neuer Strukturen für Wissenschaftlerinnen und Wissenschaftler sind und wie viel Zukunftspotential von unserer neuen Fakultät ausgeht. So konnten wir zum Wintersemester 2023/24 130 Studierende für den B.Sc. Informatik und den B.Sc. Data Science begrüßen.

Im vorliegenden Heft von ‚Blick in die Wissenschaft' möchten wir Ihnen nunmehr vor allem die Forschungsaktivitäten der Fakultät für Informatik und Data Science näher vorstellen. Dabei beglückwünsche ich die Fakultät, dass sie bereits eineinhalb Jahre nach ihrer vollständigen Handlungs- und Funktionsfähigkeit und während der weiteren Planungen zum Aufbau und der Ausarbeitung ihrer Studiengänge insbesondere im Master-Bereich ein so vielfältiges Themenheft zu ihren aktuellen Forschungsarbeiten vorlegen konnte.

Das facettenreiche und vielfältige Themenspektrum dieses Sonderhefts illustriert, wie die Fakultät für Informatik und Data Science die an der Universität Regensburg bisher vorhandenen IT-Kompetenzen erfolgreich bündelt und in die Zukunft gerichtet erweitert. Sie ermöglicht die essentielle interdisziplinäre Vernetzung mit der gesamten Universität, von den Geistes- und Sozialwissenschaften bis zu den Natur- und Lebenswissenschaften. Die Beiträge verdeutlichen, wie interdisziplinäre Forschung das Fundament starker methodischer und fachlicher Grundlagen weiterentwickelt und wie die bisherigen Informatik-Schwerpunkte der Universität Regensburg (Computational Science, Informationswissenschaft, Medieninformatik, Wirtschaftsinformatik) erfolgreich in die neue Fakultät überführt werden konnten und die Querschnittsorientierung unterstützen.

Das vorliegende Heft mit seinem Schwerpunkt auf aktuellen Forschungsarbeiten begleitet den im Wintersemester 2023/24 erfolgten Start der beiden grundständigen Bachelor-Studiengänge Informatik und Data Science. Ein kurzer Überblicksbeitrag zur Lehre in der neuen Fakultät zeigt anschaulich die bereits gewachsene Vielfalt der Informatikstudiengänge und die intensive und gelebte Verbindung von Forschung und Lehre auch an dieser neuen Fakultät.

Unsere neue Fakultät leistet hervorragende Arbeit und ich bin sicher, dass Ihnen die nachfolgenden Seiten einen spannenden Einblick in die verschiedenen Facetten der FIDS geben werden. Ein ganz besonderes Dankeschön möchte ich an dieser Stelle an das gesamte Dekanat der Fakultät für Informatik und Data Science und insbesondere an Forschungsdekanin Prof. in Dr. Meike Klettke richten, die für diese Sonderausgabe die Koordinationsarbeit der vorliegenden Ausgabe federführend übernommen hat.

Prof. Dr. Udo Hebel
Präsident der Universität Regensburg

Blick in die Wissenschaft
Forschungsmagazin
der Universität Regensburg
ISSN 0942-928-X
Heft 44/45
31. Jahrgang

Herausgeber
Prof. Dr. Udo Hebel
Präsident der Universität Regensburg

Redaktionsleitung für diese Ausgabe
Prof.in Dr. Meike Klettke / Fakultät für Informatik und Data Science

Redaktionsbeirat
Prof. Dr. jur. Christoph Althammer
Prof. Dr. rer. nat. Ferdinand Evers
Prof. Dr. rer. nat. Stefan Friedl
Prof. Dr. rer. nat. Mark W. Greenlee
Prof. Dr. theol. Andreas Merkt
Prof. Dr. phil. Omar W. Nasim
Prof. Dr. rer. nat. Klaus Richter
Prof. Dr. rer. pol. Daniel Rösch
Prof. Dr. med. Ernst Tamm
Prof. Dr. paed. Oliver Tepner
Prof. Dr. phil. Christiane Heibach

Universität Regensburg
93040 Regensburg
Telefon +49 941 9432300
Telefax +49 941 9433310

Verlag
Universitätsverlag Regensburg GmbH
Leibnizstraße 13, 93055 Regensburg

Telefon +49 941 78785-0
Telefax +49 941 78785-16

info@univerlag-regensburg.de
www.univerlag-regensburg.de
Geschäftsführer: Dr. Albrecht Weiland, Felix Weiland M.A.

Abonnementservice
bestellung@univerlag-regensburg.de

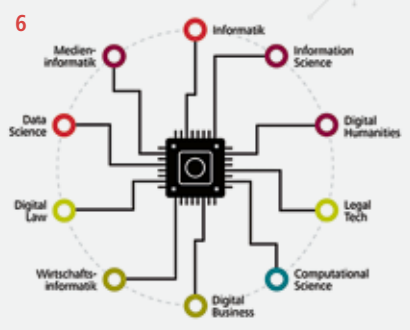
Anzeigenleitung
Larissa Nevecny
MME-Marquardt
info@mme-marquardt.de

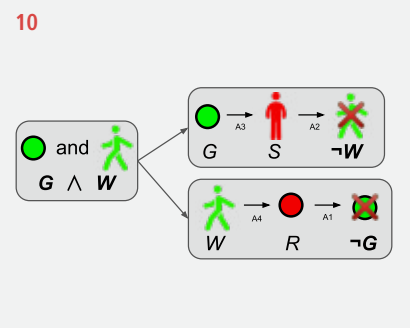
Herstellung
Universitätsverlag Regensburg GmbH
info@univerlag-regensburg.de

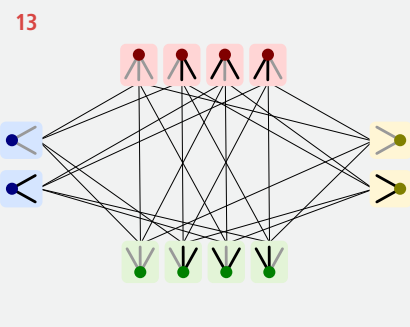
Einzelpreis € 7,00
Doppelheft € 14,00

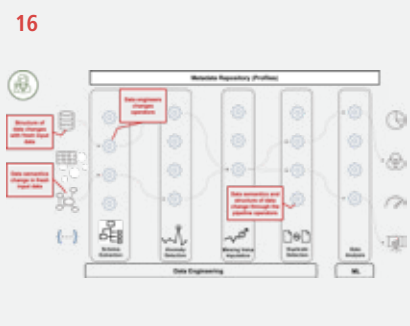
Jahresabonnement
bei zwei Ausgaben pro Jahr
€ 10,00 / ermäßigt € 9,00
Für Schüler, Studierende und Akademiker/innen im Vorbereitungsdienst (inkl. 7 % MwSt.) zzgl. Versandkostenpauschale € 1,64 je Ausgabe. Bestellung beim Verlag. Für **Mitglieder des Vereins der Ehemaligen Studierenden der Universität Regensburg e.V.**, des **Vereins der Freunde der Universität Regensburg e.V.** und des **Vereins ehemaliger Zahnmedizinstudenten Regensburg e.V.** ist der Bezug des Forschungsmagazins im Mitgliedsbeitrag enthalten.

Inhalt









Einleitung 5
Florian Erhard, Bernd Heinrich, Meike Klettke, Christian Wolff

Lehre an der Fakultät für Informatik und Data Science 6
Florian Erhard, Udo Kruschwitz, Bernd Heinrich, Christian Wolff

Automatisches Beweisen: Methoden und Anwendungen 10
Julie Cailler, Philipp Rümmer

Algorithmen und Komplexitätstheorie 13
Radu Curticapean

Evolution in Datenbanken und Data Engineering Workflows 16
Meike Klettke

IoT-basiertes Prozessmanagement – Mobile Benutzerführung in der digitalen Fabrik 19
Stefan Schönig

Cyber Threat Intelligence: Gemeinschaftliche IT-Sicherheit durch den Austausch von Informationen 23
Johannes Grill, Daniel Schlette, Günther Pernul

Kann man den Entscheidungen Künstlicher Intelligenz trauen? Zu den Auswirkungen unsicherer Daten auf die Entscheidungen Neuronaler Netze 26
Thomas Krapf, Bernd Heinrich

Mensch vs. Maschine: Wettbewerb und Kooperation mit künstlicher Intelligenz in digitalen Märkten 30
Andreas Schauer, Daniel Schnurr

Notfallpläne für den Ernstfall testen 34
Maria Leitner

Maschinelles Lernen mit Anwendungen in den Naturwissenschaften 37
Merle Behr, Markus Schmitt

Automatisierte, KI-basierte Analyse von Bilddaten: Der Lehrstuhl für Bildverarbeitung 40
Dorit Merhoff

Die Genome des Menschen – Forschungsschwerpunkte der Arbeitsgruppe für Algorithmische Bioinformatik 43
Birte Kehr

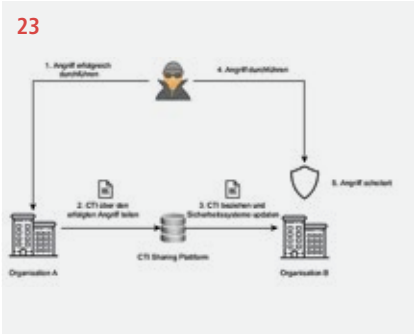
Algorithmen zum Entschlüsseln der Genregulation 46
Francisca Rojas Ringeling, Stefan Canzar

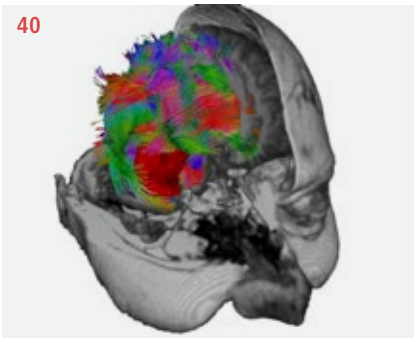
Mit Hilfe von Daten Immunprozesse entschlüsseln: Der Lehrstuhl Computational Immunology 49
Florian Erhard

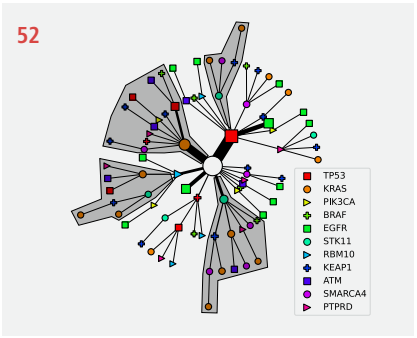
Maschinelles Lernen enthüllt den verborgenen Prozess der Tumorentstehung 52
Linda Hu, Andreas Lösch, Rainer Spang

Allgegenwärtige Mensch-Maschine-Interaktion: Entwicklung, Forschung und Infrastruktur der Medieninformatik 54
Raphael Wimmer, Johanna Bogon, Niels Henze, Christian Wolff

Wissen aus dem Internet – Genug, genau, geprüft und geeignet? Informationswissenschaft in Regensburg 60
Udo Kruschwitz, Bernd Ludwig, David Elsweiler







Notfallpläne für den Ernstfall testen

Prof. Dr. Maria Leitner

Die fortschreitende Digitalisierung und die Leistungssteigerung der digitalen Infrastrukturen der letzten Jahre hat die Informationssicherheit als entscheidendes Thema der Resilienz immer mehr in den Mittelpunkt aller digitalen Systeme, Anwendungen und in Organisationen gerückt. Eine Vielzahl an öffentlichen Beispielen von Cyberangriffen (z. B. Erpressungsversuche bei großen Verkehrsunternehmen, Fahrzeugherstellern, Stadtverwaltungen oder auch Universitäten) zeigt, dass diese im Alltag von allen Organisationen gleich ob in Wirtschaft, Wissenschaft oder auch in der Verwaltung angekommen sind.

Die immer stärkere Nutzung von digitalen Anwendungen in der Gesellschaft (z. B. mit personenbezogenen Daten) benötigt die Umsetzung höherer Schutzniveaus. Diese Anwendungen eröffnen oftmals potenziellen Angreifern eine größere Angriffsfläche, da sie lohnende Ziele für diese darstellen. Beispielsweise gab es noch vor zwanzig Jahren sehr wenige Geräte im Haushalt (Stichwort *Smart Home*), die mit dem Internet verbunden waren. Mittlerweile gibt es eine Vielzahl an Anwendungen und Geräten (z. B. das Handy, der Kühlschrank oder die Hausklingel mit Video), die konstant mit dem Internet verbunden sind. Die Digitalisierung hat ebenso die Industrie maßgeblich verändert. Ehemals isolierte Systeme haben nun oftmals Verbindungen in lokale Netze oder das Internet. Eine derartige Verbindung könnte zum Beispiel auch von Angeifenden ausgenutzt werden. Auch wenn die kontinuierliche Weiterentwicklung und Automatisierung von Technologien der Gesellschaft sehr viel Nutzen gebracht hat, so ist es jedoch auch wichtig, zusätzlich zu den technologischen Entwicklungen, die Sicherheit und Privatsphäre kontinuierlich bei diesen Transformationsprozessen mitzubetrachten.

Denn gleichzeitig haben sich auch die Angreifer weiterentwickelt und nutzen die Automatisierung immer öfter zu ihren Zwecken. Heutzutage ist es einfach, mit nur wenigen Klicks und vorgefertigten Anwendungen, gezielt eine Vielzahl von Computersystemen gleichzeitig anzugreifen. Durch dieses sich kontinuierlich weiterentwickelnde Angreiferfeld, ist es essenziell auch Techniken und Technologien weiterzuentwickeln, um rechtzeitig und systematisch Angriffe zu erkennen und das schadhafte Verhalten schnellstmöglich einzudämmen.

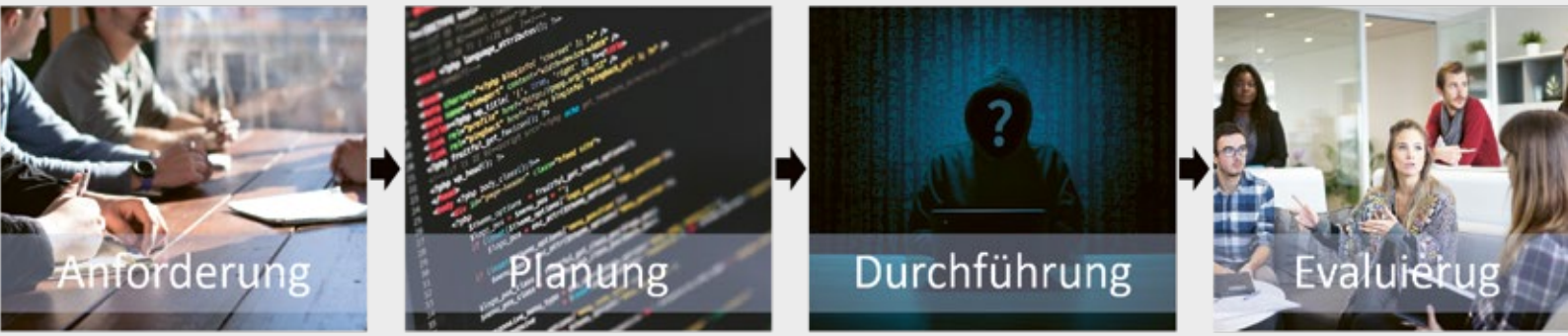
Eine zielführende Möglichkeit sich auf Cyberangriffe vorzubereiten sind Cybersicherheitsübungen. Übungen werden bereits seit Jahrzehnten in verschiedensten Bereichen zur nachhaltigen Vorbereitung genutzt. Beispielsweise werden bei der Feuerwehr oder Rettung regelmäßige Brand- oder Rettungsübungen durchgeführt. Übungen können auch im Bereich der Cybersicherheit zur Anwendung gebracht und zur Vorbereitung genutzt werden. In herausfordernden Übungssituationen (zum Beispiel bei einer simulierten Erpressung oder einem Datenklau) werden die Notfallpläne (engl. *Incident response plans*) einem Stress- und Realitätstest unterzogen. Dadurch können sich Organisationen spielerisch auf den Ernstfall vorbereiten und schneller reagieren.

In der Forschung beschäftigen wir uns daher nicht nur damit wie konkrete zukunftsweisende Übungsumgebungen (z. B. welche Technologien) simuliert und umgesetzt werden können, sondern auch welche Angriffe und Techniken im Cybersicherheitsbereich wichtig sind [1]. Die Vorbereitung einer Übung kann in mehrere Phasen eingeteilt werden [2]. Beispielhafte Ansätze werden bereits von der ENISA (siehe Abbildung 1), der Agentur der Europäischen Union für Cybersicherheit [3], spezifiziert.

Cybersicherheitsübungen – die Methodik

Ausgangsbasis ist eine Idee, konkrete Anforderungen und Ziele der Übung in einer ersten Phase der Anforderungsanalyse zu definieren. Es gibt heutzutage sehr viele verschiedene Cybersicherheitsübungen, die von diskussionsorientierten Ansätzen bis hin zu sehr technisch und hybrid-realisierten Ansätzen reichen. Sie alle verfolgen unterschiedliche Ziele und Resultate [4]. Die Wahl der Übung legt daher auch die weiteren Inhalte und Möglichkeiten insbesondere für Teilnehmende fest, sich im Rahmen einer solchen Übung einzubringen. Beispielsweise kann in einer diskussionsorientierten Übung sehr wenig auf technische Details eingegangen werden, da oftmals nur Papier und Stift verwendet werden können. In einer technischen Übung wird allerdings oftmals die Suche in den technischen Infrastrukturen ermöglicht und auch ein entsprechendes technisches Knowhow bei den Teilnehmenden vorausgesetzt.

In der zweiten Phase, der Übungsplanung, wird ein Drehbuch erstellt, dass einzelne Geschichten und Szenarien definiert. Diese Szenarien helfen den Übungsverlauf erfolgreich zu planen. Die Herausforderung liegt darin, ein Szenario fesselnd, interaktiv, informativ, anonym, nachvollziehbar und sicherheitsfokussiert zu gestalten [2]. Ein Szenario kann zum Beispiel der Ausfall wichtiger technischer Infrastrukturen oder



1 Häufige Phasen einer Cybersicherheitsübung (basierend auf [2,3])

die Erpressung mit *Ransomware* sein. Ransomware ist eine Software, die besitzende Personen von ihren Geräten oder Teilen aussperrt, um dann eine Lösegeldforderung (engl. *Ransom*) zu stellen. Dabei wird häufig die Festplatte ganz oder teilweise verschlüsselt. Ausgehend von diesem Szenario werden dann beide Seiten der Übung geplant. Dabei wird berücksichtigt wie z. B. herausfordernde Situationen durch Einspielungen herbeigeführt werden können und wie sie im Sinne des Übungsziels gestaltet sein sollten. Einspielungen dienen dann dazu diesen Übungsverlauf zu realisieren und können dabei unter anderem auf Mittel wie Emails aber auch technische Informationen zu Angriffen (engl. *Cyber Threat Intelligence*) zurückgreifen. Auf der anderen Seite werden die zu erwarteten Rückmeldungen durch die Teilnehmenden analysiert, um auf Eventualitäten vorbereitet zu sein und um die Ziele der Übung zu unterstützen.

In technischen Übungen werden in der Übungsplanung auch Anforderungen für die Simulationsumgebungen definiert, die dann in weiterer Folge implementiert werden. Oftmals werden Cybersicherheitsübungen in virtuellen Umgebungen, sogenannten *Cyber Ranges* (z. B. [1, 5]) aufgebaut. Diese ermöglichen eine vielfältige und variable Softwareumgebung, wie zum Beispiel eine exemplarische IT-Landschaft eines kleinen- und mittleren Unternehmens. Es werden auch Angriffe auf die exemplarische Infrastruktur in der Cyber Range vorbereitet. Ein Probedurchlauf vor der eigentlichen Durchführung ist sehr empfehlenswert.

In der weiteren Phase der Durchführung steigt die Spannung, da das vorbereitete Szenario dann gestartet wird und die Teilnehmenden mit neuen Situationen konfrontiert werden. Die Einspielungen führen dazu, dass die Übungssituation zur Realität wird und spielerisch der Ernstfall erprobt werden kann. Es werden Cyberangriffe simuliert und dadurch die Notfallpläne der Organisationen und die Reaktionen der Teilnehmenden getestet. Zudem lernen die Teilnehmenden mit neuen und herausfordernden Situationen umzugehen.

In der Phase der Evaluierung, werden die wichtigsten Eckpunkte der Übung reflektiert und das Feedback der Teilnehmenden aufgenommen. Das ist insbesondere wichtig, um den Teilnehmenden die wichtigsten Erkenntnisse mit in die Praxis zu geben.

Neue Herausforderungen der künstlichen Intelligenz in Cybersicherheitsübungen meistern

Cybersicherheitsübungen sind eine ideale Testumgebung für neue Technologien. Neue Werkzeuge und Technologien der künstlichen Intelligenz (KI) können im Rahmen von Cybersicherheitsübungen eingesetzt und getestet werden. Auf Seite der Organisationen und Teilnehmenden kann in Übungen das Potenzial für KI-basierte Cyberangriffe durch Übungen besser verstanden und Notfallpläne adaptiert werden. Neu ist der Einsatz von KI in diesem Bereich keineswegs, denn bereits seit vielen Jahren werden beispielsweise Verfahren zur Mustererkennung dazu genutzt, um Cyberangriffe zu erkennen. Heute gilt es, unter diesen angepassten technologischen Vorzeichen, neue Konzepte zur Erkennung und Minimierung der Auswirkungen zu entwickeln und diese durch Übungen in einem geschützten Rahmen zu erproben. Mit der Forschung können neue Grundlagen und Verfahren entwickelt werden, die eine schnellere Entdeckung und Bearbeitung von Angriffen sowie den dazu notwendigen Informationsaustausch unterstützen.

Über den Lehrstuhl

Der Lehrstuhl von Prof. Dr. Maria Leitner befasst sich mit zentralen Fragestellungen im Bereich Cybersicherheit, Automatisierung und KI. Es geht darum neue Herausforderungen in der Cybersicherheit mit Konzepten, Algorithmen und Anwendungen grundlagennahe zu erforschen und auch praxisorientierte Resultate zu erzielen. In langjährigen Kooperationen mit Wissenschaft, Behörden, Wirtschaft und Industrie werden neue Ideen gemeinsam erarbeitet und Ergebnisse evaluiert.

Literatur

[1] M. Leitner *u. a.*, »Enabling exercises, education and research with a comprehensive cyber range.«, *J Wirel Mob Netw. Ubiquitous Comput Dependable Appl*, Bd. 12, Nr. 4, S. 37–61, 2021.

[2] M. Leitner, »A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned«, in *Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22–24, 2023*, P. Mori, G. Lenzini, und S. Furnell, Hrsg., SciTePress, 2023, S. 634–642

[3] A. Ogee, R. Gavrila, P. Trimintzios, V. Stavropoulos, und A. Zacharis, »The 2015 report on national and international cyber security exercises: Survey, analysis and recommendations«. ENISA, 2015. [Online]. Verfügbar unter: https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises?v2=1

[4] S. Kucek und M. Leitner, »An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments«, *J. Netw. Comput. Appl.*, Bd. 151, Feb. 2020

[5] M. M. Yamin, B. Katt, und V. Gkioulos, »Cyber ranges and security testbeds: Scenarios, functions, tools and architecture«, *Comput. Secur.*, Bd. 88, Jan. 2020

DREI FRAGEN ...

Was ist Ihre größte fachliche Herausforderung?

Durch die alltäglichere Nutzung von Software in allen Lebensbereichen wird es immer mehr Daten geben, die Aktivitäten aller Art beschreiben. Sicherheit und Privatsphäre sind daher zentrale Fragestellungen für unser digitales Leben. Eine der vielen Fragestellungen ist dabei, wie wir Daten noch effizienter interpretieren können, um rascher Cyberangriffe zu entdecken.

Wie verändert KI Ihr Fachgebiet?

KI ist schon lange in der Cybersicherheit verankert. KI wird beispielsweise bei der Filterung von unerwünschten Emails (engl. *Spam*) schon lange angewendet bzw. auch bei der Analyse von Netzwerkdaten, um Cyberangriffe zu erkennen. Der leichte Zugang zu KI verändert jedoch auch die Möglichkeiten der Angreifenden zum Beispiel im Bereich der Desinformation. Es ist jetzt noch leichter geworden Falschinformationen automatisiert zu generieren. Dies gilt auch für die Nachbildung von Stimmen oder Videos. Es ist daher wichtig künftig auch Maßnahmen und Techniken zu entwickeln, die mögliche KI-generierte Inhalte erkennen können und auch die Menschen auf diese Möglichkeiten hinzuweisen, um effektive Schutzmaßnahmen zu treffen.

Welche Entwicklung in der Informatik wünschen Sie sich für die nächsten 5 Jahre?

Ich würde mir wünschen, dass das Wissen und die Denkweisen der Informatik und insbesondere der Informationssicherheit noch stärker an verschiedene Zielgruppen allen Alters vermittelt werden und damit langfristig zur digitalen Resilienz unserer Gesellschaft beitragen.

Fotograf: SIMshot

Prof. Dr. Maria Leitner ist Professorin für KI in der IT-Sicherheit und forscht an den Schnittstellen von KI, Cybersicherheit und Automatisierung. Davor war Sie Gastprofessorin für Informatik an der Universität Wien und Scientist am AIT Austrian Institute of Technology. Am AIT hat sie bis 2021 die AIT Cyber Range geleitet. Unter anderem hat Sie Cybersicherheitsübungen für insgesamt mehr als 350 Personen konzipiert, umgesetzt und angeleitet, wie beispielsweise eine nationale Cybersicherheitsübung. Prof. Dr. Maria Leitner hat zwei Bücher herausgegeben und über 50 von Fachleuten begutachtete wissenschaftliche Publikationen verfasst.