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

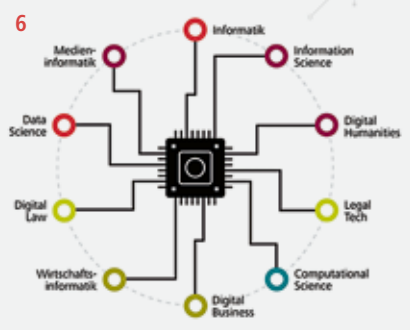
Anzeigenleitung
Larissa Nevecny
MME-Marquardt
info@mme-marquardt.de

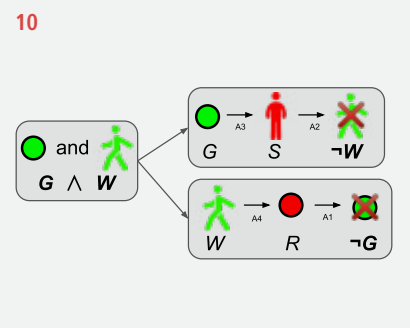
Herstellung
Universitätsverlag Regensburg GmbH
info@univerlag-regensburg.de

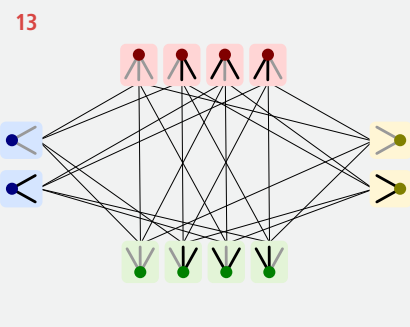
Einzelpreis € 7,00
Doppelheft € 14,00

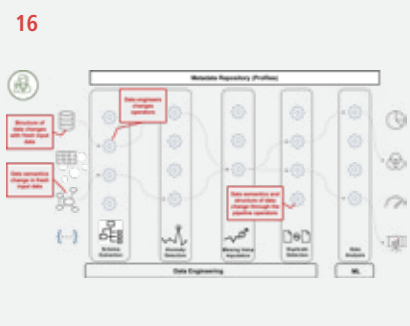
Jahresabonnement
bei zwei Ausgaben pro Jahr
€ 10,00 / ermäßigt € 9,00
Für Schüler, Studierende und Akademiker/innen im Vorbereitungsdienst (inkl. 7 % MwSt.) zzgl. Versandkostenpauschale € 1,64 je Ausgabe. Bestellung beim Verlag. Für **Mitglieder des Vereins der Ehemaligen Studierenden der Universität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

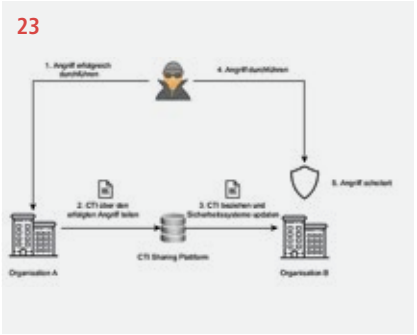
Inhalt

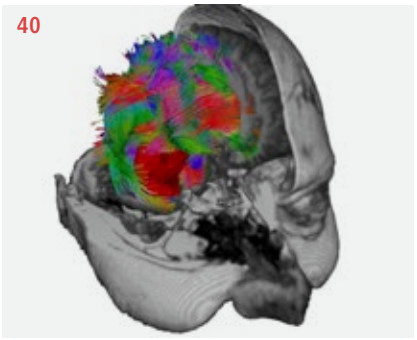


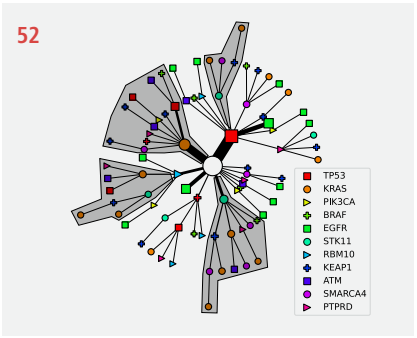












Cyber Threat Intelligence

Gemeinschaftliche IT-Sicherheit durch den Austausch von Informationen

Johannes Grill, Dr. Daniel Schlette, Prof. Dr. Günther Pernul

Cybersecurity ist ein Thema von gesellschaftlicher Relevanz

Die tägliche Verwendung von Informationssystemen und Daten im privaten und beruflichen Kontext ist elementarer Bestandteil unserer Gesellschaft. Dadurch hat die Sicherheit dieser Systeme und der Schutz persönlicher Daten sowohl für Unternehmen als auch für gesellschaftliche Institutionen und Privatpersonen eine hohe Relevanz. In den letzten Jahren haben erfolgreiche Angriffe in immer größerem Ausmaß gezeigt, dass Cyberkriminelle zum Beispiel mittels Phishing E-Mails oder Ransomware vorhandene Schwachstellen zu ihrem Vorteil ausnutzen. Neben Spionage und Datendiebstahl hat sich ein profitables, arbeitsteiliges Ökosystem um die Verschlüsselung von Daten und die Lösegelderpressung entwickelt (Verizon. Data Breach Investigations Report 2023). Ins Visier sind dabei auch kritische Netzwerke wie Industrieanlagen und staatliche Behörden gerückt. Aktuelle Zahlen belegen, dass weltweit mehr als jedes zweite Unternehmen Opfer eines Angriffes mit erheblichen Schäden wurde (Hiscox. Cyber Readiness Report 2023). Auch viele kleinere Unternehmen verwenden Anwendungen (z. B. E-Mail, Dateitransfer-Dienste, oder Webanwendungen), die ein Eintrittstor für Cyberkriminelle darstellen können. Das weltweite Phänomen lässt sich leider auch in Deutschland beobachten und hat durch geopolitische Konflikte an Bedeutung gewonnen (BSI. Die Lage der IT-Sicherheit in Deutschland 2022). Dabei finden vermehrt auch Angriffe statt, die darauf abzielen, Systeme und Dienste lahmzulegen (Denial of Service) und erst in einem zweiten Schritt auf die Kompromittierung aus sind.

Um diesen Bedrohungen in einer vernetzten Welt entgegenzutreten, wird unter den Begriffen Cybersecurity, IT-Sicherheit, oder Informationssicherheit das Wissen rund um die Gewährleistung von Vertraulichkeit, Integrität, und Verfügbarkeit der Systeme (bestehend aus Hardware und Software) und Daten zusammengefasst. Da heutzutage Industrieanlagen (bezeichnet als Operation Technology, OT) und klassische Informationssysteme (IT) zunehmend vernetzt sind, existieren Sicherheitsinformationen über heterogene Systeme und vielfältige Arten von Bedrohungen. Trotz verstärkter Bemühungen im Bereich der Cybersecurity nimmt jedoch die Anzahl der erfolgreichen Angriffe weiter zu. Aus diesem Grund rücken nun vermehrt kollaborative Ansätze basierend auf Sicherheitsinformationen in den Fokus.

Cyber Threat Intelligence beschreibt vielfältige Sicherheitsinformationen

Daten-basierte Ansätze sind in der IT allgegenwärtig und dienen der Optimierung von Systemen, darauf aufbauenden Anwendungsfällen und der Gewinnung von neuen Erkenntnissen. Auch im Bereich Cybersecurity besteht durch die Gesetzgebung sowie die konstante Gefahrenlage die Notwendigkeit sicherheitsrelevante Daten und Informationen zu erfassen, auszutauschen und einzusetzen. Sicherheitsinformationen über aktuell vorhandene sowie neu auftretende Gefahren werden unter den Begriff *Cyber Threat Intelligence (CTI)* zusammengefasst. Dabei kann CTI hinsichtlich ihrer Verwendung unterteilt werden (Tounsi and Rais 2018). Eine grundlegende Form stellt die *Technical CTI* dar. Diese beschreibt Informationen, welche direkt in den Sicherheitssystemen (z. B. als Blocklist der Firewall) einer Organisation verarbeitet werden. Bekannte Beispiele hierfür sind IP-Adressen von bösartigen Servern oder Signaturen von Malware, welche auch Indicators of Compromise (IoCs) genannt werden. Ein Sicherheitssystem kann diese IoCs nutzen, um Verbindungen zu bösartigen Servern zu blockieren oder anhand einer Malware-Signatur einen Download von Schadsoftware zu erkennen. Die *Tactical CTI* hingegen beschreibt Methoden und wiederkehrende Taktiken, welche Angreifer verwenden, um Systeme erfolgreich zu infiltrieren. Damit sind umfangreichere Modellierungen von komplexen Angriffen und Gegenmaßnahmen möglich. Eine umfassende und strukturierte Beschreibung von Angriffsverhalten und Indikatoren sowie Informationen über angegriffene Systeme wird auch als *Threat Report* bezeichnet. Diese Threat Reports werden von Analysten genutzt, um geeignete Abwehrmaßnahmen auszuwählen und auf das aktuelle Verhalten der Angreifer auszurichten. Threat Reports ähneln in gewisser Weise Dossiers, welche zum Austausch von relevanten Informationen verwendet werden. Zuletzt stellt *Strategic CTI* Sicherheitsinformationen auf hoher Abstraktionsebene dar, wie beispielsweise finanzielle Schäden durch bestimmte Cyberangriffe und Vorhersagen über zukünftige Entwicklungen. Diese Informationen rich-

CTI-Beispiele für die MOVEit Schwachstelle (CVE-2023-34362)

Technical CTI (IP-Adresse und Malware Hashwert): 91[.]222[.]174[.]95 und 0b3220b11698b1436d1d866ac07cc90018e59884e91a8cb71ef8924309f1e0e9 (SHA256)

Tactical CTI (Angriffsverhalten nach MITRE ATT&CK): Exploit Public-Facing Application (SQL Injection), Server Software Component: Web Shell

Strategic CTI (Angriffskampagne): CL0P Ransomware Gang, Januar/Februar und Mai/Juni Angriffswelle 2023, vermuteter Schaden 75–100 Mio USD

ten sich an Personen mit Leitungsfunktion und Führungsverantwortung, welche auf dieser Grundlage langfristige Entscheidungen bezüglich der Ausrichtung der organisationseigenen IT-Sicherheit treffen können. Zusammengefasst lässt sich über die verschiedenen Arten von Sicherheitsinformationen sagen, dass Technical CTI gerade für kurzfristige Zeiträume wertvoll ist, wohingegen Tactical CTI und Strategic CTI auch auf längere Sicht einen Mehrwert für die Wahrung der IT-Sicherheit bieten. Dies liegt daran, dass Angreifer sehr leicht die bösartige IP-Adresse ihres Malware-Servers umstellen können, eine Änderung von grundlegenden Angriffsmustern und Methoden aber wesentlich aufwändiger ist (Bianco. The Pyramid of Pain. 2014).

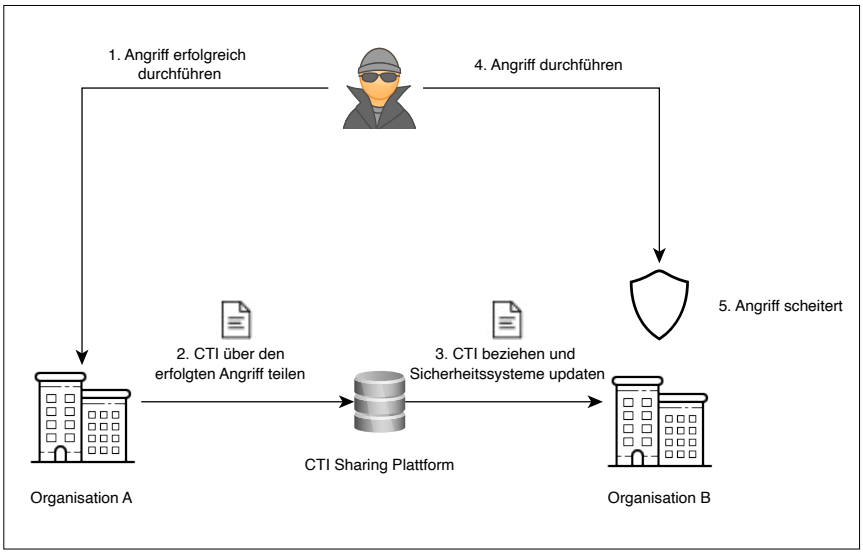
Der Austausch von Sicherheitsinformationen spielt eine wesentliche Rolle bei der Verteidigung

Für reibungslose und effiziente Prozesse setzen Organisationen eine Vielzahl an digitalen Informationssystemen ein. Alle diese Systeme müssen jedoch auch ausreichend gegen Cyberangriffe geschützt werden. Dabei ist es nötig, sämtliche Schwachstellen und Angriffsvektoren der Systeme zu kennen und bewältigen zu können, was im Allgemeinen einen großen Aufwand darstellt. Dahingegen reicht den Angreifern oftmals eine einzige Schwachstelle, um einen erfolgreichen Angriff gegen eine Organisation durchzuführen. Dieser grundlegende Nachteil gegenüber den Angreifern verschlimmert sich dahingehend, dass diese untereinander sehr gut vernetzt sind und arbeitsteilig agieren. In bestimmten Bereichen des Darknets können Cyberkriminelle aktuelle und hochspezialisierte Schadsoftware wie Ransomware gegen Bezahlung erwerben.

Vor diesem Hintergrund ist die Idee der kollaborativen Sicherheit vielversprechend. Die Cyberabwehr wird dafür nicht mehr ausschließlich siloartig (ausschließlich im Kontext einer Organisation), sondern gemeinschaftlich gedacht und durchgeführt. Kollaborative Cybersecurity beschreibt im Wesentlichen das Zusammenwirken von mehreren Akteuren (Unternehmen, Organisationen, Privatpersonen) mit dem gemeinsamen Ziel, die Sicherheit von Informationssystemen und Daten zu verbessern. Ein konkreter und vielversprechender Ansatz dafür ist der Austausch von CTI unter den verschiedenen Akteuren. Damit besteht die Möglichkeit, von vergangenen Erfahrungen und Erkenntnissen anderer zu lernen und seine eigene IT-Sicherheit anzupassen und zu verbessern. Neben einer rein internen Perspektive, bei der eine Organisation ihre internen Systeme und Abläufe kennt, wird somit eine zweite externe Perspektive im Rahmen der Cybersecurity hinzugenommen.

Für einen Austausch solcher Sicherheitsinformationen werden in der Praxis/Industrie verschiedene Kommunikationskanäle genutzt. Zum einen wird CTI informell in persönlichem Kontakt oder über E-Mail ausgetauscht. Ein vielversprechenderer Ansatz hingegen ist der systematische Austausch über dedizierte Plattformen. CTI sollte hierbei strukturiert erfasst und aufbereitet werden, um den Empfänger:innen der Sicherheitsinformationen einen wirklichen Mehrwert zu liefern. Dafür werden geeignete Datenformate bzw. Standards wie Structured Threat Information Expression (STIX) genutzt. Die Funktionsweise des Austausches über eine CTI-Plattform ist in der folgenden Abbildung beschrieben:

Ein bösartiger Akteur greift zunächst Organisation A an und nutzt beispielsweise ein fehlerhaft konfiguriertes System in der IT-Architektur von Organisation A aus. Organisation A muss nun den Angriff unter Kontrolle bringen und den Angreifer aus den internen Netzwerken der Organisation entfernen. Im Rahmen dieser Vorfallsbewältigung (Incident Response) wird auch analysiert, wie der Angreifer sich Zugriff auf die Infrastruktur verschaffen konnte. Die Erkenntnisse bereitet Organisation A als strukturierte CTI im STIX-Format auf und lädt die Daten anschließend auf einer Austauschplattform für CTI hoch. Organisation B, welche auch Teilnehmerin an dieser Plattform ist, bemerkt den neuen Eintrag. Da Organisation B eine ähnliche IT-Architektur wie Organisation A hat, kann der dokumentierte Angriff durch den bösartigen Akteur auch für Organisation B eine Gefahr darstellen. Daher bezieht Organisation B die CTI aus der Plattform und updatet seine Systeme entsprechend, um die bisherige Schwachstelle in der Konfiguration und somit den Angriffsvektor zu beseitigen. Startet der bösartige Akteur nun einen Angriff auf Organisation B, so scheitert dieser wegen der Anpassung basierend auf der zuvor bezogenen CTI.



Bildnachweis: Wirtschaftsinformatik I

1 Der systematische Austausch von CTI über Sharing Plattformen ermöglicht kollaborative Sicherheit und kann Angriffe verhindern.

Der Umgang mit Herausforderungen beschäftigt Forschung und Industrie.

Der Austausch von CTI mittels CTI Sharing Plattformen bietet Vorteile. Sowohl präventiv als auch reaktiv kann CTI zu einer Verbesserung der Cybersecurity einzelner Organisationen beitragen. Nichtsdestotrotz bestehen Herausforderungen im Austausch von CTI. Dem Austausch vorgelagert ist die Erfassung und Strukturierung von CTI. Auf Seite der teilenden Organisation sind dafür Ressourcen in Form von Personal und Zeit nötig. Ohne strukturierte CTI jedoch ist ein Austausch zwischen verschiedenen Akteuren schlicht nicht möglich oder liefert nur begrenzten Mehrwert wegen deutlicher Auswirkungen auf die Datenqualität. Es lässt sich bereits vermehrt feststellen, dass Organisationen bereit sind personelle Ressourcen für CTI zu Verfügung zu stellen. Auf kleine und mittlere Unternehmen trifft dies jedoch nur bedingt zu. Auch die Thematik der Datenqualität von CTI ist ein Thema der aktuellen Forschung und wurde teilweise in CTI Sharing Plattformen integriert. So können basierend auf semi-strukturierten Daten verschiedene Datenqualitätsmetriken angewendet werden und damit eine Einordnung der zugrundeliegenden CTI liefern. Die Thematik der Datenqualität ist Bestandteil eines aktuellen Forschungsprojekts am Lehrstuhl. Genauer entsteht im Rahmen des DEVISE Projekts ein Reifegradmodell zur Messung und Verbesserung der Datenqualität von CTI.

Es stellen sich noch weitere organisatorische Fragen hinsichtlich des Austausches, dem Zusammenwirken und der Verwendung von CTI. Hierzu zählen: Welcher Akteur ist vertrauenswürdig? Welche Informationen sind relevant? Wie können Informationen in einem anderen Kontext verwendet werden? Neben der Ressourcenproblematik ist dabei der Reputationsverlust eine Herausforderung beim Austausch von CTI, da das Teilen der CTI einen (erfolgreichen) Angriff impliziert. Mittels Pseudonymisierung/Anonymisierung lässt sich hier nur teilweise Abhilfe schaffen, da Kontextinformationen häufig den Mehrwert von CTI deutlich verbessern. Erkenntnisse über die ideale Konstellation von Sharing Communities liegen außerdem nur begrenzt vor. Auch im Hinblick auf neuartige Technologien (insbesondere Blockchain zum Austausch und generative KI zur Strukturierung von CTI) ergeben sich weitere Forschungsfragen, deren Beantwortung den Austausch von CTI in der Praxis unterstützen kann.

Aktuelle Forschung am Lehrstuhl adressiert den Austausch von CTI mittels Blockchain. Im Rahmen eines weiteren Forschungsprojekts (BMBF DEFENSIVE) wird um die Technologie herum ein Sharing System entwickelt. Dabei werden wesentliche Anforderungen von Teilnehmer:innen erfasst. Auch dienen Erkenntnisse aus langjährigen Industriekooperationen dazu, relevante Ergebnisse für aktuelle Herausforderungen zu erzielen.

Kollaborative Cybersecurity basierend auf dem Austausch von CTI verspricht einen schnelleren und treffsicheren Umgang mit Bedrohungen. Die Entwicklungen der letzten Jahre machen deutlich, dass dieser Ansatz vielversprechend ist und die Bereitschaft zum Austausch besteht. Mittels aktueller Forschung können bestehende Herausforderungen adressiert und die nächsten Schritte hin zu mehr Cybersecurity unternommen werden.

Quellen

Verizon. Data Breach Investigations Report (DBIR) (2023).

Hiscox. Cyber Readiness Report (2023).

BSI. Die Lage der IT-Sicherheit in Deutschland (2022).

Tounsi, W., and Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Comput. Secur. 72 (2018), 212–233.

Bianco, D. The Pyramid of Pain (2014).

Foto © Johannes Grill

Johannes Grill, M. Sc.,
studierte Wirtschaftsinformatik an der Universität Regensburg. Seit 2023 promoviert er am Lehrstuhl Wirtschaftsinformatik I (Prof. Dr. Pernul) und ist an dem BMBF-Forschungsprojekt DEFENSIVE beteiligt. Zu seinen Forschungsschwerpunkten zählen Cyber Threat Intelligence (CTI) sowie Datentreuhändersysteme, über die CTI Daten zur Beschreibung von Sicherheitsvorfällen vertrauenswürdig ausgetauscht werden können.

Foto © Daniel Schlette

Dr. Daniel Schlette
hat seinen Bachelor und Master in Wirtschaftsinformatik an der Universität Regensburg im Rahmen der Honors Elitestudiengänge des Elitenetzwerks Bayern erlangt. In seiner Promotion am Lehrstuhl Wirtschaftsinformatik I (Prof. Dr. Pernul) beschäftigte er sich mit Cyber Threat Intelligence und Incident Response. Er war an Forschungsprojekten mit Siemens und dem BMBF-Projekt DEVISE beteiligt.

Foto © Günther Pernul

Prof. Dr. Günther Pernul
studierte Betriebs- und Wirtschaftinformatik an der Universität Wien/TU Wien und schloss daran seine Promotion und Habilitation für Informatik an. Neben längeren Forschungsaufenthalten an der University of Florida und am Georgia Institute of Technology, USA war er Lehrstuhlinhaber an der Universität Duisburg-Essen. Seit 2002 hat er den Lehrstuhl für Wirtschaftsinformatik I an der Universität Regensburg und forscht schwerpunktmäßig im Bereich IT-Sicherheit.