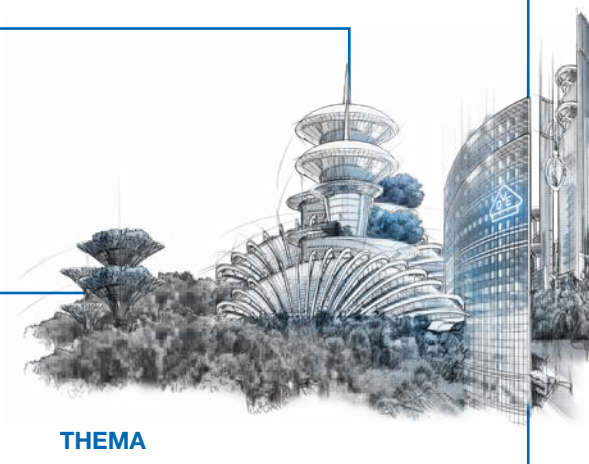
VDE
Rhein-Main *info*



EDITORIAL

Liebe Leserinnen und Leser,

wer online ist, ist angreifbar. Jede Organisation, aber auch jeder private Nutzer kann von Cyberkriminellen angegriffen werden – und wird das auch immer häufiger. Die Anzahl erfasster Cyberstraftaten steigt weiter an, so das Bundeskriminalamt in einem aktuellen Lagebericht. Denn je komplexer die Strukturen in einer globalisierten, digitalisierten Welt sind, desto verletzlicher sind sie. Chancen und Risiken bleiben in der digitalen Welt zwei Seiten der gleichen Medaille. Die Cybersicherheitsforschung arbeitet weiter unter Hochdruck daran, die Risiken zu verringern, um die Chancen besser nutzen zu können. So wie die Experten unter dem Dach des europaweit größten Forschungszentrums für angewandte Cybersicherheitsforschung ATHENE, das Lösungen für mehr digitale Sicherheit entwickelt – ein Projekt, das wir Ihnen in unserem Schwerpunkt Cybersicherheit vorstellen.
Nicht zu unterschätzen bei IT-Sicherheitsproblemen und Cyberangriffen bleibt der „Faktor Mensch". Neugierde, Sorglosigkeit und Naivität sind bei den allermeisten Angriffen das Einfallstor. Eine Gefahr, die zum Beispiel mit der wachsenden Beliebtheit der sozialen Medien oder dem Trend zum Homeoffice bestimmt nicht kleiner geworden ist. Wie technische Vorsorge und Aufklärung als Schutz vor Datenklau dabei zusammenspielen, erklärt Prof. Dr. Bernhard Geib von der Hochschule RheinMain im Interview unserer Serie „Professoren aus der Region".

Achten Sie auf sich und bleiben Sie gesund!
Ihr

Rolf Bergbauer

THEMA

Cybersicherheit

Ebenso dynamisch wie sich die Digitalisierung entwickelt, werden Cyberkriminelle gewiefter und deren Angriffe zahlreicher. Nicht nur die Bewältigung im Schadenfall, auch das frühzeitige Erkennen von Bedrohungen wird daher immer wichtiger, um eine stabile und sichere Informations- und Kommunikationstechnologie zu gewährleisten. Das gilt für den privaten Bereich genauso wie für mittelständische Betriebe und kritische Infrastrukturen wie Krankenhäuser, Flughäfen und die Strom- und Wasserversorgung.

Weder auf eine Disziplin beschränkt, noch regional eingegrenzt lassen sich wirksame Methoden gegen Cyberkriminalität entwickeln. Wir haben uns daher in hessischen Forschungseinrichtungen, in den Abteilungen der Landesregierungen, aber auch bei Polizei und Bundeskriminalamt umgeschaut, wie den vielfältigen Angriffen aus dem Netz begegnet wird. Dass ein wirksamer Schutz gegen Cyberkriminalität nur im Schulterschluss von Polizei, Verfassungsschutz, Wissenschaft und Forschung funktioniert, lesen Sie ab Seite 2.

CYBERSICHERHEIT

Schritt halten

Cyberkriminelle sind schnell, professionell und weltweit per Mausklick unterwegs. Forschungseinrichtungen in Hessen, aber auch Abteilungen der Landesregierung, der Staatsanwaltschaft und des Bundeskriminalamts halten dagegen und zeigen, wie die digitale Welt sicherer gemacht werden kann.

Die Digitalisierung eröffnet Chancen, birgt aber auch Risiken, denn einen umfassenden Schutz vor Angriffen gibt es nicht. Ein Restrisiko bleibt. Cybersicherheit, also Maßnahmen, um Computer, Server, Mobilgeräte, elektronische Systeme, Netzwerke und Daten vor böswilligen Angreifern zu schützen, wird deshalb immer wichtiger. Und noch etwas kommt hinzu: Digitalisierung ist dynamisch und steht niemals still. Neue Gefahren müssen deshalb frühzeitig erkannt, innovative Lösungen erforscht und erarbeitet werden. Dabei hat sich gezeigt, dass auch staatliche Institutionen zur Cybersicherheit zunehmend vernetzt vorgehen müssen. Innere und äußere Sicherheit im Cyberraum sind nicht mehr trennscharf voneinander abzugrenzen. Die Cybersicherheit zu bewahren und sich gegen Angriffe zu verteidigen ist eine gesamtstaatliche, gemeinsame Aufgabe. Vernetzung, Kooperation und Zusammenarbeit sind deshalb zentrale Voraussetzungen, um Cybercrime wirkungsvoll zu bekämpfen.

ATHENE in Darmstadt

Hessen, genauer: Darmstadt, ist heute bereits einer der führenden Standorte für Cybersicherheitsforschung. 2020 haben sich dort im Nationalen Forschungszentrum für angewandte Cybersicherheit, ATHENE, die TU Darmstadt, die Hochschule Darmstadt sowie das Fraunhofer-Institut für Sichere Informationstechnologie SIT und das Fraunhofer-Institut für Graphische Datenverarbeitung IGD zusammengeschlossen. Dies ist nicht nur die europaweit größte Allianz von Forschungseinrichtungen im Bereich Cybersicherheit, sondern auch ein einzigartiges Kooperationsmodell von universitärer und außeruniversitärer Forschung. Das Aufgabenfeld ist groß: ATHENE entwickelt Sicherheitslösungen, berät regelmäßig Wirtschaft und öffentliche Verwaltung und unterstützt Firmengründer und Start-ups. Dabei fließen die aus der Grundlagenforschung der Hochschulen gewonnenen Erkenntnisse in die weitere anwendungsorientierte Forschung ein. Mit seinen Forschungs- und Entwick-

lungsarbeiten deckt ATHENE ein sehr großes Spektrum von Expertisen ab, die für verschiedene Technologien und Anwendungsbereiche relevant sind, wie die Sicherheit von Systemen, Software, Anwendungen, Prozessen, Hardware, Daten oder der Internet-Infrastrukturen. Das Forschungszentrum arbeitet agil und effizient und kann so auch kurzfristig auf neue Herausforderungen und veränderte Bedrohungslagen reagieren.

Beispielhafte Unterstützung

Das Zentrum wird von Bund und Land gemeinsam gefördert. In der Regel, so der Direktor Prof. Dr. Michael Waidner bei der Eröffnung von ATHENE, können 80 Prozent der Cyberattacken abgewehrt werden. In der Forschung liege das Potenzial, mit den verbleibenden 20 Prozent fertig zu werden. Ein Beispiel? ATHENE startete Ende 2020 ein Projekt, um die im Bundestag vertretenen Parteien gegen Cyberangriffe zu unterstützen. Aus der Analyse von Hackern, die sich auf politische Akteure spezialisiert haben, ergaben sich bestimmte Muster und bevorzugte Angriffsmethoden. Das Team untersuchte dann die über das Internet zugängliche IT-Landschaft der Parteien auf Schwachstellen, die professionelle Angreifer ausnutzen können. Nach Abschluss der ersten Analysen im März 2021 wurden die im Bundestag vertretenen Parteien sowie die Präsidenten des Bundestages und des Bundesamts für Sicherheit in der Informationstechnik (BSI) informiert. Anschließend fanden Gespräche mit einzelnen Parteien statt, meist auf der Ebene der Bundesgeschäftsführungen und der IT-Verantwortlichen auf Bundesebene. Die Diskussionen zeigten, dass die Parteien sich der Risiken durchaus bewusst sind.

BKA, Abteilung Cybercrime

Von der Security-Hochburg Darmstadt in die hessische Landeshauptstadt Wiesbaden. Zwei neue Einrichtungen arbeiten hier daran, die digitale Welt sicherer zu machen: die Abteilung Cybercrime (CC) des Bundeskriminalamts und das Cyber Competence Center (3C) der hessischen Landesregierung. Die Abteilung CC des Bundeskriminalamts hat am 1. April 2020 ihre Arbeit aufgenommen. Ein wichtiger Schritt, um Kompetenzen zu bündeln und die Spezialisierung der Mitarbeiterinnen und Mitarbeiter voranzutreiben. Das BKA blickt bei der Bekämpfung von Cyberkriminalität auf eine lange Erfahrung zurück: vom Arbeitsbereich „Informations- und Kommunikationskriminalität“ des Referates für Wirtschaftskriminalität Mitte der 1990er Jahre bis zur Gruppe „Cybercrime in der Abteilung Schwere und Organisierte Kriminalität (SO)“. Eine Gruppe, die den Grundstein der neuen Abteilung mit bis zu 280 Mitarbeitern bildet. Kriminalbeamte, Analysten und IT-Experten mit verschiedenen Spezialisierungen arbeiten hier Hand in Hand.

»Die Abhängigkeit unserer Gesellschaft von einer funktionsfähigen technischen Infrastruktur nimmt stetig zu.

Zeitgleich haben es Straftäter relativ einfach, sich im Netz kriminelle Kompetenz einzukaufen, um etwa die Webpräsenz ganzer Unternehmen zu blockieren.«

Holger Münch
Präsident des Bundeskriminalamts

Weiterentwicklung von Kompetenzen

Die neue Abteilung erweitert die klassischen Aufgaben wie die Koordinierung des internationalen Informationsaustausches um die Analysekompetenz des BKA, etwa bei neuen Cybercrime-Phänomenen und digitalen Angriffsmustern. Aber auch gegen kriminelle Akteure, Netzwerke und Strukturen wird hier verstärkt ermittelt. Die nationale und internationale Vernetzung spielt dabei eine ebenso wichtige Rolle wie die Kooperation mit verschiedenen Akteuren aus anderen Behörden und der Wirtschaft. Holger Münch, Präsident des Bundeskriminalamts, betonte bei der Arbeitsaufnahme der Abteilung CC: „Die Abhängigkeit unserer Gesellschaft von einer funktionsfähigen technischen Infrastruktur nimmt stetig zu. Zugleich haben Straftäter es noch immer vergleichsweise einfach, sich im Netz kriminelle Kompetenz einzukaufen, um ohne umfängliche technische Kenntnisse etwa die Webpräsenzen ganzer Unternehmen zu blockieren oder die Informationstechnik in Krankenhäusern und Verwaltungen anzugreifen. Hier gilt es für uns, mit diesen Entwicklungen Schritt zu halten und unsere Kompetenzen stetig fortzuentwickeln, um Straftaten im digitalen Raum schnell analysieren, wirkungsvoll bekämpfen und die Täter ihrer realen Verantwortung zuführen zu können.“

Umfängliche Kooperation

Die in der Abteilung CC angesiedelte Nationale Kooperationsstelle Cybercrime (NKC) ist für die Zusammenarbeit mit Behörden und Unternehmen der Privatwirtschaft zuständig. Darüber hinaus bestellt dieser Arbeitsbereich den Koordinator und den Verbindungsbeamten der Abteilung CC in das Nationale Cyber-Abwehrzentrum (Cyber-AZ). Das schon 2011 gegründete Cyber-AZ mit Sitz in Bonn ist keine eigenständige Behörde, sondern eine behörden- und institutionenübergreifende Plattform. Hier geht es vor allem darum, relevante Informationen zwischen den beteiligten Behörden und Partnern schnell auszutauschen und Schutzmaßnahmen zur Cybersicherheit in Deutschland zu koordinieren. In diesem Kreis werden also sicherheitsrelevante Cybervorfälle gesammelt und gemeinsam bewertet. Zu den Vertretern im Nationalen Cyber-Abwehrzentrum gehören neben dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundesamt für Verfassungsschutz (BfV), dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), der Bundespolizei (BPOL), der Bundeswehr (BW), dem Militärischen Abschirmdienst (MAD) und dem Zollkriminalamt (ZKA) auch die Abteilung Polizeilicher Staatsschutz (Abteilung ST) des BKA.

Um gegen Angriffe von Cyberkriminellen gewappnet zu sein, muss die Expertise von Polizei und Verfassungsschutz mit der Kompetenz von Wissenschaft und Forschung verknüpft werden.

Hessen Cyber Competence Center

Auf Vernetzung und Zusammenarbeit setzt auch das Hessen Cyber Competence Center (Hessen3C), das im Frühjahr 2019 seine Arbeit aufnahm. IT-Experten aus der Verwaltung, der Polizei sowie des Verfassungsschutzes arbeiten hier Seite an Seite, um das Landesnetz vor Cyberangriffen zu schützen. Die Spezialisten unterstützen auch hessische Städte und Gemeinden, sind zentrale Ansprechpartner für Unternehmen der kritischen Infrastrukturen (zum Beispiel Stromversorger, Wasserwerke oder Krankenhäuser) und bieten darüber hinaus auch kleinen und mittleren Betrieben ihr Know-how an. „In einer immer stärker vernetzten virtuellen Welt sind wir auf smarte Behörden angewiesen, die frühzeitig Bedrohungen erkennen und unsere Daten vor Manipulation oder Spionage schützen“, betonte der Hessische Innenminister Peter Beuth bei der Eröffnung von Hessen3C. „Oberstes Ziel unserer IT-Spezialisten ist es, Cyberangriffe zu verhindern. Dafür können unsere Fachleute genauso auf die Expertise von Polizei und Verfassungsschutz setzen wie auch auf den Austausch mit Wissenschaft und Forschung in Hessen.“

Schutz kritischer Infrastrukturen

Hessen3C bietet eine Plattform und einen Rahmen für die strukturierte Zusammenarbeit kompetenter Cyber-

»In einer immer stärker vernetzten Welt sind wir auf smarte Behörden angewiesen, die frühzeitig Bedrohungen erkennen.«

Peter Beuth
Hessischer Minister des Innern und für Sport

sicherheitsspezialisten aus den Bereichen Cybercrime, Cybersecurity und Cyberintelligence. Sie arbeiten zusammen in einer Organisationseinheit und beziehen dabei die fachlich oder örtlich zuständigen Stellen gezielt mit ein. Die Mitarbeiter setzen sich zusammen aus Fachleuten des Computer Emergency Response Teams (CERT-Hessen), der hessischen Polizei und des Landesamts für Verfassungsschutz. Täglich erstellen die IT-Spezialisten ein behördenübergreifendes Cybersicherheitslagebild. Soweit Bedrohungen akut sein sollten, werden die Partner aus der Landes- und Kommunalverwaltung umgehend mittels eines Warn- und Informationsdienstes unterrichtet. Ein besonderes Augenmerk der IT-Spezialisten liegt auf dem Schutz der sogenannten kritischen Infrastrukturen. „Strom, Wasser oder die ärztliche Versorgung muss jederzeit gewährleistet sein. Als zentrale Ansprechstelle steht Hessen3C Unternehmen der kritischen Infrastrukturen, aber auch der Wirtschaft jederzeit rund um die Uhr zur Verfügung. Mit unserem neuen Mobile Incident Response Team (MIRT) unterstützen wir im Falle eines Cyberangriffes auch landesweit vor Ort. Unsere Spezialisten helfen bei der Analyse und Schadensbegrenzung und führen digitalforensische Datensicherungen durch“, so der Innenminister. Das Kompetenzzentrum steht Unternehmen 24 Stunden am Tag und sieben Tage die Woche zur Verfügung, um konkrete Vorfälle zu melden. Auch bei konzeptionellen Fragen unterstützen die Experten. Die Beratung ist immer streng vertraulich, ergebnisoffen und produktneutral.

Kampf gegen Internetkriminalität

Von Wiesbaden in die hessische Finanzmetropole Frankfurt. Neben Forschungseinrichtungen, Landesregierung und Bundeskriminalamt arbeiten auch die Staatsanwaltschaften in Hessen mit neuen, spezialisierten Einrichtungen intensiv daran, die Cyberkriminalität zu bekämpfen. So wurde schon Anfang 2010 die Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) als Außenstelle der Generalstaatsanwaltschaft Frankfurt am Main mit Sitz in Gießen errichtet. Seit Juli 2019 hat die Zentralstelle ihren Sitz in Frankfurt am Main. Sie verfügt über 22 Stellen im staatsanwaltlichen Bereich. Die ZIT ist erster Ansprechpartner des Bundeskriminalamtes für Internetstraftaten bei noch ungeklärter örtlicher Zuständigkeit in Deutschland oder bei Massenverfahren gegen eine Vielzahl von Tatverdächtigen bundesweit. Als operative Zentralstelle bearbeitet die ZIT besonders aufwendige und umfangreiche Ermittlungsverfahren aus den Bereichen Kinderpornografie und sexueller Missbrauch von Kindern, Darknet-Kriminalität, Cyberkriminalität wie Hackerangriffe, Datendiebstahl und Computerbetrug sowie Hasskriminalität (Hate Speech). Sie ist darüber hinaus für Aus- und Fortbildung von Richtern, Staatsanwälten und Polizeibeamten zuständig. Die ZIT ist zudem Gründungsmitglied im Judicial Cybercrime Network, einem europäischen Netzwerk der Justizbehörden zur Bekämpfung der Internetkriminalität. Zuletzt waren der ZIT beachtliche Ermittlungserfolge gegen die Malware „Emotet“ und die Kinderpornografieplattform „Boystown“ gelungen.

Trotz einzelner Erfolge steht aber fest: Die Cyberkriminalität nimmt weiter zu. Die Anzahl der erfassten Straftaten ist in den vergangenen Jahren kontinuierlich angestiegen, so das Bundeskriminalamt. 2020 wurden bundesweit rund 108.000 Delikte registriert, eine erneute Steigerung von rund acht Prozent im Vergleich zu den 2019 erfassten Fällen. Nur rund ein Drittel der Fälle konnte aufgeklärt werden. Das zeigt die enorme Dimension der Bedrohungen, denen sich IT-Sicherheitsforschung und Cybercrime-Bekämpfung heutzutage widmen müssen. Die Zahlen müssen runter! Eine Aufgabe, der sich auch die Einrichtungen und Organisationen in Hessen weiter mit Hochdruck stellen werden. *(thb)*

Mehr Informationen zu den vorgestellten Einrichtungen und Organisationen unter:

↗ *https://www.athene-center.de*

↗ *https://innen.hessen.de/sicherheit/hessen3c*

↗ *https://bit.ly/3mxlnuy*

Mehr zur Arbeit der Abteilung Cybercrime des BKA sowie das BKA-Lagebild Cybercrime 2020 finden Sie hier:

↗ *https://bit.ly/3zncMy6*

↗ *https://bit.ly/3jledaN*

An dieser Stelle lassen wir in unregelmäßigen Abständen Professoren aus der Region des VDE Rhein-Main zu ihren Fachgebieten und aktuellen Themen zu Wort kommen. 2021 wurden vorgestellt:

Ausgabe 1: Prof. Dr. Manfred Stoll, Hochschule Geisenheim University
Ausgabe 2: Prof. Dr. Matthias Hollick, TU Darmstadt
Ausgabe 3: Prof. Dr. Christian Reuter, TU Darmstadt

CYBERSICHERHEIT

»Ein Restrisiko bleibt«

Für eine sichere, zuverlässige und verfügbare Informations- und Kommunikationstechnik (IKT), so Prof. Dr. Bernhard Geib aus dem Studienbereich Informatik der Hochschule RheinMain, gelte es nicht nur Risiken zu minimieren, sondern auch Vertrauenswürdigkeit und Qualität sicherzustellen.

Herr Professor Geib: Was beschäftigt Sie gerade besonders? Worüber forschen Sie aktuell?
Gegenwärtig beschäftige ich mich mit der modellbasierten Analyse bei Vorliegen von dynamisch-strukturellen Redundanzkonzepten. Hohe Zuverlässigkeit und Verfügbarkeit erreicht man nur durch geplante und bereitgestellte Reserveeinheiten. Die angestellten Betrachtungen sind im Kontext der fortschreitenden Annäherung (Konvergenz) von Security und Safety zu sehen.

Warum ist das wichtig? Was versprechen Sie sich davon?
Die größte Herausforderung in punkto Sicherheit, Zuverlässigkeit und hoher Verfügbarkeit besteht neben der intendierten Risikominimierung an sich auch in der Notwendigkeit, durch die Prüfung und Bewertung der eingesetzten IKT-Systeme den Nachweis der „Vertrauenswürdigkeit" zu erbringen oder eine bestimmte Qualitätsstufe nachzuweisen. Weil sich menschliche und technische Fehler grundsätzlich nicht vermeiden lassen, kann es in einer frühen Entwicklungsphase sinnvoll und zielführend sein, mittels formaler Methoden und Analysen neben einer Korrektheits- und Vollständigkeitsprüfung auch die Beurteilung der dynamischen Sicherheitseigenschaften vorzunehmen. Daher verspreche ich mir von meinen Aktivitäten eine Erhöhung der Nachfrage, was insbesondere simulative Testverfahren bei hochzuverlässigen Systemauslegungen anbelangt.

In welchen Bereichen sehen Sie für die Computersicherheit derzeit das größte Potenzial?
Trotz geeigneter Schutzvorkehrungen können nicht alle Angriffe abgewehrt und auch nicht alle Widrigkeiten vorhergesagt werden. Es bleibt ein Restrisiko, auf das wir uns alle einstellen müssen, dem wir aber geeignet begegnen können. Angesichts der wachsenden Bedrohungslage im Cyber-Umfeld müssen wir uns zukünftig von der ausschließlichen Betrachtung der klassischen IT-Sicherheit ein Stück weit wegbewegen und einen Zustand der sogenannten „Sustainable Cyber Resilience" anstreben. Dies meint und erfordert neuartige Strategien und Konzeptionen dahingehend, bei einem eingetretenen Sicherheitsvorfall einerseits schnell zu reagieren und andererseits den Geschäfts- und Nutzbetrieb auch im Falle eines erfolgten Angriffs – wenn auch möglicherweise eingeschränkt – aufrechterhalten zu können. Oberstes Ziel ist es, die Angriffsfläche für eine Cyberattacke und deren Auswirkungen gering zu halten.

Und wo sehen Sie die größten Hindernisse auf dem Weg dahin?
Momentan vor allem bei den Rechtsunsicherheiten sowie dem Fehlen von wirksamen Durchsetzungsmechanismen für global agierende Unternehmen und Organisationen. Zwar wurden mit dem IT-Sicherheitsgesetz und gemäß der EU-DSGVO Regulierungen und Handlungsfelder adressiert beziehungsweise aufgezeigt, deren faktische Umsetzung in der Realität aber zu keiner nennenswerten Verbesserung von IT-Sicherheit in der Fläche

geführt hat. Große Anstrengungen werden nötig sein, um die möglichen Wechselwirkungen in globalen Wertschöpfungsnetzwerken managen zu können. Bei diesen und insbesondere die Cybersicherheit betreffenden Fragestellungen stehen wir erst am Anfang.

Wie groß ist der Faktor Mensch bei IT-Sicherheitsproblemen und Cyberangriffen?
Sehr groß! Laut seriösen Schätzungen beträgt der Anteil der Cyberangriffe, die ganz bewusst den Menschen als Schwachstelle ausnutzen, rund 99 Prozent. Dabei werden vor allem die Neugier, Naivität und Auskunftsfreudigkeit des Menschen ausgenutzt. In sozialen Netzwerken zum Beispiel werden viele private Informationen immer noch leichtfertig preisgegeben. Jedes neue Gerät und jede Unwissenheit des Menschen kann vom Hacker genutzt werden, um Angriffe zu initiieren. Das Sensibilisieren der Benutzer ist daher so notwendig wie eh und je.

Wie könnte ein Best Practice Ansatz gegen Cybergefährdungen und Computer-Kriminalität aussehen, der auch wirklich umgesetzt wird?
Ausgangspunkt ist, den innerhalb einer IT-Infrastruktur als schutzwürdig erachteten Datenbestand zu ermitteln sowie eine darauf abzielende Bedrohungsanalyse. Bei den ausgewählten Schutzmaßnahmen und Abwehrlinien sind die Sensibilisierung der Benutzer und eine eingeschränkte Rechtevergabe ein essenzieller Schritt. Eine aktuelle Antivirussoftware und Firewall sollten standardmäßig installiert sein und eine kontinuierliche Datensicherung, die regelmäßige Aktualisierung von Software und IT-System sowie die Verwendung einer Zwei-Faktor-Authentifizierung sind sehr zu empfehlen. Verschiedene Passwörter sind ebenfalls ein probates Mittel, das Schadensausmaß einzuschränken.

Warum gilt Erpressersoftware, sogenannte „Ransomware", die den Zugriff auf Daten und Systeme einschränkt oder unterbindet, als derzeit größte Bedrohung?

Schock-Bilanz: Cyberangriffe im Homeoffice haben im vergangenen Jahr einen Schaden von mehr als 52 Milliarden Euro verursacht, teilt das Institut der deutschen Wirtschaft in einer aktuellen Berechnung mit. Weitere Infos dazu unter: ↗*www.iwkoeln.de/studien.html*

Weil das Vorgehen der Täter zu den fortschrittlichsten Angriffen überhaupt zählt. In vielen Fällen erfolgt der Angriff stufenweise und mit immer neueren, oft automatisierten Schadfunktionen. Cyberangriffe mit Erpressungsabsicht sind heutzutage ein boomendes und lukratives Geschäftsmodell, da für die Angreifer das Entdeckungsrisiko und die mögliche Strafverfolgung äußerst gering sind. Der Bezahlvorgang ist völlig anonym und erfolgt durchweg durch nicht rückverfolgbare Zahlungsmethoden. Von Ransomware geht ein sehr hohes Bedrohungspotential aus, da durch sie nicht nur einzelne lokale Datenbestände, sondern auch ganze Unternehmensnetzwerke einschließlich der installierten Backup-Server betroffen sein können. Das erhöht den Leidensdruck und die Zahlungsbereitschaft Betroffener zusätzlich.

Wie können sich Unternehmen dagegen am besten schützen?
Künstliche Intelligenz und Machine Learning helfen vor allem bei der Erkennung von Mustern, der Bewertung und Priorisierung von Risiken und der Automatisierung von Analyse- und Abwehrmaßnahmen. In jedem Fall sollten Unternehmen präventive Maßnahmen vorsehen, um so die Angriffsfläche zu verringern und die Ausnutzbarkeit von bekannt gewordenen Schwachstellen zeitnah einzuschränken. Eine Netzwerksegmentierung, die Absicherung von Remote-Zugängen und vor allem die Sensibilisierung von Benutzern sind allesamt empfehlenswerte Maßnahmen, um dem Einschleusen von Schadprogrammen zu begegnen. Als professionelle Schutzvorkehrungen sind regelmäßige Schwachstellenscans und Penetrationstests anzusehen, da diese den Absicherungs- und Härtegrad aktuell unter die Lupe nehmen.

Ist das Homeoffice ein großes Einfallstor für Betrüger und Cyberkriminelle?
Beliebt als Einfallstore sind bei Cyberkriminellen neben der IT des Homeoffice vor allem Fern- und Wartungszugänge von Zugangsroutern, mobile Access-Endpunkte in Etagenwohnungen und USB-Ports von Smarthome- sowie internetfähigen IoT-Gerätschaften. Begünstigt wird das Eindringen in die Homeoffice-IT, weil in diesem Sektor noch oftmals auf ein Segmentieren und Separieren des Heimnetzes aus Gründen des Komforts verzichtet wird. Die in Firmennetzen vorzufindenden Sicherheitsstandards, wie das Einrichten eines Sicherheitstunnels oder das gezielte Deaktivieren von speziellen Funktionalitäten, sind im Homebereich eher die Ausnahme. Daher denke ich, dass Office-IT-Systeme weit weniger geschützt sind als Unternehmensnetze und vorrangig auch dazu benutzt werden, um sich hierüber zielgerichtet auch auf andere, durchaus sensiblere Bereiche auszudehnen. (*thb)*

Prof. Dr. Bernhard Geib leitet seit Oktober 2000 das Fachgebiet Kommunikationssysteme und Computersicherheit im Studienbereich Informatik der Hochschule RheinMain. Er ist Mitglied verschiedener Arbeitsgruppen von VDE und DKE und beschäftigt sich vor allem mit der Modellierung und Simulation zeit- und sicherheitskritischer Systeme.

Kontakt: *bernhard.geib@hs-rm.de*

FOTOS: SEITE 6: SASUN BUGHDARYAN / STOCK.ADOBE.COM; SEITE 7: REBECCA DERNBACH FOTODESIGN

Der Hessische Rundfunk (hr) bietet als öffentlich-rechtliche Landesrundfunkanstalt der ARD Programm aus und für Hessen: mit sechs Radiowellen (hr1, hr2-kultur, hr3, hr4, hr-iNFO, YOU FM), im hr-Fernsehen und für Das Erste, Arte, 3sat, Kika, phoenix und funk sowie im hr-text und online auf digitalen Plattformen, in hr-Apps und auf Social-Media-Kanälen. Dazu gibt es Konzerte vom hr-Sinfonieorchester und der hr-Bigband sowie zahlreiche Bildungsangebote, Schul- und Education-Projekte.

Kontakt: Nicole Kohse-Stumpf,
↗ *Nicole.Kohse-Stumpf@hr.de*

↗ *www.hr.de*

NACHHALTIGE FILMPRODUKTION

Grüner drehen

Klimaschutz am Filmset: Das Drama „Die Luft, die wir atmen“, zu sehen am 24. November in der ARD, ist der erste nachhaltig produzierte Spielfilm des Hessischen Rundfunks. Die Ideen des grünen hr-Drehs münden in ein Regelwerk für nachhaltige Kino- und TV-Produktionen in Deutschland: mit umweltschonendem Drehbuch, Bio-Filmschminke und Special Effects mit Regenwasser vom Landwirt.

Einen Spielfilm klimaschonend zu drehen – geht das überhaupt? Erst war es eine Idee, dann eine Herausforderung für die Filmschaffenden des Hessischen Rundfunks, bald Ansporn. Der Spielfilm „Die Luft, die wir atmen“ sollte die erste grüne hr-Produktion sein – die erste von vielen weiteren und ein Startschuss fürs „Green Shooting“ im Hessischen Rundfunk. Doch bevor im Frühjahr 2020 am Set im Taunus die erste Klappe fiel, stürzten täglich neue Fragen auf Produktionsleiter Dominik Diers und sein Team ein: Ist das Hotel für die Schauspiel-Crew umweltzertifiziert? Woher bekommt die Maske Bio-Kosmetik, die vor Spielfilmkameras besteht? Sind die Bügel beim Kostüm aus Plastik, Draht oder Holz? Bietet das Catering regionale und vegetarische Kost an? Kann man am Filmset einen Anschluss für grünen Strom legen lassen? Dann recherchierten sie Öko-Labels und Inhaltsstoffe, Herstellungsarten und Energieverbräuche und klickten sich rein in den CO_2-Rechner.

Auf dem Weg zum nachhaltigen Dreh

Denn Diers wusste: Spielfilmdrehs sind energiefressende Produktionen. Noch immer landen am Set oft Tausende Plastikbecher im Müll, während Dieselgeneratoren, Auto- und Flugreisen Hunderte Tonnen CO_2 in die Luft schleudern. Der hr will gegensteuern, so Diers: „Wir Filmschaffenden beim hr sehen uns in der Verantwortung für mehr Nachhaltigkeit. Wir müssen und wollen uns mit unserem Handeln dem Klimawandel entgegenstellen. Da lautet die Frage nicht mehr ob, sondern wie.“

Gut ein Jahr später: Der Film wurde fertig geschnitten und vertont. Der Sendetermin steht: 24. November 2021 in der ARD. Und da lag sie endlich auf dem Tisch – nur digital auf dem Desktop, nicht ausgedruckt: die Bilanz des ersten grünen Spielfilmdrehs des hr. Strich drunter unter die Zahlenreihen mit CO_2-Verbräuchen von Technik, Kulissenbau, Requisite, Kostüm, Catering und Co., summa summarum und … geschafft! „Die Luft, die wir atmen“ hatte als einer der ersten Filme erfolgreich die Kriterien des „Arbeitskreises Green Shooting“ erfüllt, einer Nachhaltigkeitsinitiative vieler Filmproduktionsunternehmen, die sich in einem Pilotprojekt zu „100 grünen Produktionen“ in 2020/21 verpflichtet hatten. Die grünen Ideen des hr-Filmteams mündeten in ein zukünftig verpflichtendes Regelwerk für nachhaltige Kino- und TV-Produktionen in Deutschland.

Unterm Strich wurden bei dieser Produktion 58.625,46 kg CO_2 emittiert. Gegenüber der unter normalen, „umweltsündigen“ Produktionsbedingungen für diesen Film veranschlagten Menge hat man 7,52 Prozent CO_2 eingespart. Klingt nicht so viel? „Sie müssen wissen“, sagt Fabian Linder, externer Green Consultant für den Film, „dass ein durchschnittlicher ‚Tatort‘ beispielsweise 100.000 bis 120.000 kg CO_2 emittiert. Bei Blockbustern sind es auch mal 500.000 kg CO_2.“ Dagegen sei der CO_2-Verbrauch dieses ARD-Mittwochsfilms sehr gering, etwa so wenig wie bei einer Folge einer Vorabendserie. „Bei diesem Spielfilm hat der hr den größten Beitrag zum Klimaschutz bereits vor der ersten Klappe erarbeitet – mit einem nachhaltigen Drehbuch: wenige Drehorte, somit weniger Auf- und Umbauten, möglichst lang zusammenhängende Einsätze der Schauspieler*innen, somit weniger Reisen.“

Motivaufnahmeleiter Robert Hertel, während des Drehs zum zweiten Green Consultant ausgebildet, ergänzt: „Man muss früher beginnen, nachhaltig zu handeln, und viel Zeit in die Motivsuche investieren.“ So hat er ihn gefunden, den idealen Drehort: Die Jugendherberge Oberreifenberg im Taunus passte zur Geschichte des Films und bot genügend Räume, sodass man anders als sonst keine Wohnmobile für Maske, Garderobe und Schauspieler*innen ans Set transportieren musste. Hertel kann Anekdoten erzählen, wie kompliziert es sein kann, anderthalb Kilometer Starkstromkabel zu zwei Ökostrom-Verteilerkästen zu verlegen. Doch das Ergebnis zählt: Der Diesel-Lkw, der sonst ein tonnenschweres Diesel-Stromaggregat vom Funkhaus in den Taunus hätte schleppen müssen, blieb ungenutzt – und emissionsfrei – stehen.

Recycling und Upcycling

Schauspieler*innen, die länger als zwei Tage vor Ort waren, übernachteten in Ferienwohnungen statt in verbrauchsintensiveren Hotels und reisten mit der Bahn statt mit dem Flieger. Szenenbildner*innen verwendeten umweltfreundliche Stoffe, recycelten Baumaterialien und Kulissen aus früheren Produktionen. Kostümleute nutzten Second-Hand-Kleidung und reinigten mit ökologischem Waschmittel. Maskenbildner*innen schminkten mit umweltschonend und natürlich hergestellten Make-Ups, mit Pinseln aus recyceltem Material und Bambus-Wattestäbchen. Drehbücher gab’s digital auf Laptops, nicht ausgedruckt. Statt Plastikbechern nutzte die Crew Kaffeetassen und wiederverwendbare Flaschen.

Die Aufnahmeleitung tauschte Batterien gegen Akkus aus. Die Lichttechnik leuchtete mit LED-Scheinwerfern aus, was deren Stromverbrauch um 40 Prozent reduzierte. Ohnehin versuchte man, viel Tageslicht zu nutzen. Die Fahrbereitschaft organisierte Hybridfahrzeuge. Nur Hybrid-Lkw konnte sie nicht organisieren. Da war die TV-Produktion schneller als der Mietwagenmarkt, der diese noch nicht anbot.

Zwischendrin kam ein Traktor herangetuckert: Für den Kunstschnee, der laut Drehbuch herabrieselt, wandte sich Robert Hertel an einen Landwirt, der einen 9000-Liter-Tankwagen mit aufgefangenem Regenwasser herankarrte. Kein Tropfen Frischwasser wurde für den Schnee verbraucht. „Grünes Drehen bringt auch einen Zugewinn an Kreativität“, hat Green Consultant Fabian Linder oft erfahren. „Da passiert etwas mit den Leuten, das wirkt sich bis ins Privatleben aus.“

Ziel erreicht, trotz Corona

Doch dann kam Corona. Teammitglieder mussten einzeln in Autos anreisen, das Catering durfte nur separat verpackte Essen zubereiten, alles und alle fanden sich hinter Plastik abgeschirmt wieder. Ausstattung, Catering, Personentransport schlugen höher als kalkuliert zu Buche. „Das hat unsere Zielmarke stark gedrückt“, räumt Dominik Diers ein. „Doch wir hatten vor der Unterbrechung schon solche Mengen an CO_2 eingespart, dass es trotz Corona-Bedingungen für eine grüne Bilanz gereicht hat.“ Stück für Stück weitet der hr die Anzahl „grüner Filme“ aus – in diesem Jahr wird bereits die Hälfte der Produktionen grün gedreht. *(Nicole Kohse-Stumpf, hr)*

Hier finden Sie den ersten ARD-Nachhaltigkeitsbericht:
↗ *www.ard.de/nachhaltigkeit*

Was „Green Shooting“ bedeutet, veranschaulicht dieses Making-of-Video:
↗ *www.hr.de/green-shooting,video-116714.html*

„Die Luft, die wir atmen“ ist nach der Ausstrahlung (ARD, 24.11.2021, 20.15 Uhr) in der ARD-Mediathek abrufbar:
↗ *www.ard-mediathek.de*

Zwischenresümee

Im Herbst letzten Jahres startete unsere Beitragsserie zur Energiewende in Rhein-Main. Infraserv hat uns von der Umsetzung des Kohleausstiegs berichtet. Die TU Darmstadt zeigte, dass die Energiewende zentrales Forschungsthema ist und die OVAG-Gruppe veranschaulichte die Wichtigkeit von Wind- und Solarenergie für unsere Energieversorgung. Die Fraport AG hob hervor, dass die Energiewende auch in der Luftfahrtbranche trotz höchsten Sicherheitsanforderungen eine wichtige Rolle spielt. Neben Forschung und Lehre, Industrie, Energie- und Mobilitätsinfrastruktur befassen sich auch andere Branchen mit dem Thema und finden ihre eigenen Antworten. Ein schönes Beispiel ist die heute vorgestellte nachhaltige TV-Produktion des Hessischen Rundfunks.

Christian Anhaus ist Ansprechpartner der Arbeitsgruppe Energiewende im VDE Rhein-Main und Initiator der Beitragsserie „Energiewende in Rhein-Main“.

Kontakt:
christian.anhaus@vde-online.de

FOTOS: SEITE 8: © HR, FABIAN LINDER/RESSOURCENREGIE; SEITE 9: FOTOGRAFIE ANNE BAD SODEN AM TAUNUS

BARRACUDA NETWORKS AG

Schützen und unterstützen

Mit der Vision, eine sichere Welt für alle Unternehmen an jedem Ort zu bieten, hat sich Barracuda Networks als ein führender Anbieter von Lösungen für Sicherheit, Applikationsbereitstellung und Datensicherheit etabliert.

Über 225.000 Kunden weltweit vertrauen Barracuda den Schutz ihrer Daten und Anwendungen vor einer Vielzahl von Bedrohungen an. Der Cloud-Security-Spezialist bietet einfache, umfassende und kostengünstige Lösungen für E-Mail-Schutz, Anwendungs- und Cloud-Sicherheit, Netzwerksicherheit und Datenschutz. Dabei kommen die Vorteile von Hardware, Cloud-Diensten und virtuellen Technologien voll zum Einsatz. Eine einfache Implementierung, ein bequemes Management sowie ein flexibles Reporting zeichnen die Produkte aus. Sämtliche Barracuda-Produkte verfügen über ein intuitives Web-Interface. Unterstützt von Barracuda Central, bieten die Produkte „Zero-Hour Schutz" – damit lassen sich rund um die Uhr aktuelle Bedrohungen aus dem Internet aufspüren und automatisch blockieren.

Die Pandemie hat die Nutzung der Cloud vorangetrieben. Dies wiederum hat verstärkt Cyberkriminelle auf den Plan gerufen, die immer wieder neue Möglichkeiten der Angriffsmethodik entwickeln. Die Anzahl der Attacken ist massiv gestiegen, Tendenz weiter steigend.

Sicherheitskonzepte müssen individuell angepasst werden

Dies fordert Unternehmen heraus, ihre Abwehrmaßnahmen entsprechend anzupassen und damit ihre Resilienz zu verbessern. Denn Daten, Geschäftsprozesse, Systeme und Netzwerkinfrastrukturen sind die „Kronjuwelen" jedes Unternehmens. Es muss klar sein: Mit nur einer Lösung ist eine umfassende Absicherung dieser Werte nicht durchführbar. Ein Cybersecurity-Konzept, das die für jedes einzelne Unternehmen optimal passende Lösung bietet, ist zwingend erforderlich. Barracuda arbeitet kontinuierlich daran, innovative und die aktuellste Sicherheitstechnologie, die auch morgen noch gilt, bereitzustellen. Nicht zuletzt stehen ein guter Teamspirit und motivierte Mitarbeiterinnen und Mitarbeiter für einen ausgezeichneten Kundenservice – auch dafür ist Barracuda bekannt. *(thb)*

Gründung: 2003
Branche: IT-Sicherheit
Mitarbeiter/-innen: 1600
Website: de.barracuda.com

Drei Fragen an Stefan Schachinger

Stefan Schachinger, Product Manager Network Security

Was zeichnet Ihr Unternehmen aus?

Als international agierendes IT-Security-Unternehmen heben wir uns vor allem technologisch durch ein umfangreiches Produktportfolio mit einer Vielzahl verschiedener Lösungen für IT- und OT-Sicherheit ab. Die Bandbreite reicht hier von E-Mail-Security, über Absicherung von Webapplikationen, Benutzer-Awareness-Trainings, Backup und Archivierung bis hin zur netzwerkseitigen Anbindung und Absicherung von Industrieanlagen und Maschinen aller Art. Gerade im deutschsprachigen Raum sind wir neben einem Vertriebsteam auch mit Standorten zur Forschung und Entwicklung im Bereich Netzwerksicherheit vertreten und pflegen daher einen sehr guten und engen Kontakt zu unseren lokalen Kunden und Verbänden wie dem VDE.

Warum sind Sie VDE Mitglied?

Mit dem VDE haben wir einen Partner gefunden, der maßgeblich an der technologischen Weiterentwicklung in Deutschland und in ganz Europa beteiligt ist und zukunftsweisende Themen wie Digitalisierung und Industrie 4.0 vorantreibt. Als Hersteller können wir unsere Expertise im Bereich IT- und OT-Sicherheit einbringen und andere Verbandsmitglieder dahingehend unterstützen und beraten. Durch die Arbeit im Netzwerk erfahren wir aber auch aus erster Hand, wie sich die Sicherheitsanforderungen in verschiedenen Branchen entwickeln, sodass wir diese Erkenntnisse direkt in die Produktentwicklung einfließen lassen können.

Was wünschen Sie dem VDE Rhein-Main für die Zukunft?

Dem VDE Rhein-Main und den dort ansässigen Verbandsmitgliedern wünschen wir in der Zukunft ganz viele spannende Herausforderungen im Bereich der IT- und OT-Security, aber hoffentlich ohne größere Zwischenfälle.

Gründung: 2020
Branche: Elektrotechnik, Softwareentwicklung für Elektro- und Photovoltaikanlagen
Mitarbeiter/-innen: 40
Website: www.trace-software.com/de

TRACE SOFTWARE GMBH

Software für die Netzberechnung

Lösungen für Bau- und Energiefachleute: Die Trace Software GmbH mit Sitz in Frankfurt am Main setzt den Fokus auf Software zur Berechnung und Planung von Elektro- und Photovoltaikanlagen.

Die Trace Groupe ist eine Familienunternehmensgruppe in Frankreich, die sich auf die Softwareentwicklung für die Industrie-, Bau- und Energiebranche konzentriert. Zur Gruppe gehören unter anderem TraceParts, einer der führenden Akteure für 3D-Digitalisierung von Herstellerkatalogen, und Trace Software International mit über 30-jähriger Erfahrung in der Entwicklung von Softwarelösungen und Dienstleistungen für die Elektro- und Industrietechnik. Trace Software verfügt über ein einzigartiges Fachwissen in der Elektroplanung sowie Netzberechnung und gehört zu den weltweit führenden Anbietern.

Innovation und Weiterentwicklung

Die 2020 gegründete Trace Software GmbH ist das neueste Tochterunternehmen der französischen Unternehmensgruppe und setzt auf ein dauerhaftes Engagement. „Wie wir es für TraceParts gemacht haben, wird Trace Software langfristig in Deutschland dank disruptiver Lösungen investieren“, sagt Geschäftsführer Étienne Mullie. Der Schwerpunkt des Unternehmens liegt deshalb auf Produktneutralität und Normenkonformität. „Trace Software misst der Beziehung mit den Herstellern elektrischer Bauteile sowie der Integration internationaler Normen viel Bedeutung bei, um eine optimale Sicherheit der Menschen und Anlagen zu gewährleisten“, so Étienne Mullie. Die Firma setzt auf technische Weiterentwicklung und legt daher großen Wert auf die Qualität der Produkte und deren Funktionen. Zu diesen Produkten gehören zum Beispiel elec calc™ zur Netzberechnung und Elektroplanung, elec calc™ BIM (Building Infomation Modelling, deutsch: Bauwerksdatenmodellierung) zur Integration der Planung in einen Open BIM-Prozess oder archelios™ PRO zur Photovoltaik-Planung. Für die Maschennetze wiederum wird bald eine neue Lösung verfügbar sein: elec calc™ GRID. Die Software integriert einen Algorithmus zur Lastflussberechnung, um alle Arten von Smart Grids (intelligente Stromnetze) simulieren und auf Normenkonformität prüfen zu können. Es sind auch diese Innovationen, die das Know-how von Trace Software unterstreichen, um Fachleute aus der Elektrotechnik-Branche konsequent zu unterstützen. *(thb)*

Drei Fragen an Étienne Mullie

Étienne Mullie, Geschäftsführer Trace Software GmbH

Was zeichnet Ihr Unternehmen aus?
Als Experte für Elektrotechnik seit mehr als 30 Jahren bieten wir weltweit Softwarelösungen zur Elektro- und Photovoltaikplanung. Wir entwickeln qualitativ hochwertige Lösungen zur Auslegung und Berechnung elektrischer Anlagen, die internationale Normen und herstellerübergreifende Bauteilkataloge integrieren.

Warum sind Sie VDE Mitglied?
Weil wir uns systematisch den Standardisierungsorganisationen nähern und proaktiv zur Normentwicklung beitragen wollen. Aktuell machen wir das bereits, was die französische NF- sowie die IEC-Norm angeht. Nicht zuletzt freuen wir uns als VDE-Mitglied über den permanenten Austausch in einem großen Fachnetzwerk.

Was wünschen Sie dem VDE Rhein-Main für die Zukunft?
Vor allem, dass er seine Konvergenz- und Harmonisierungsarbeit der Normen zur Vereinfachung ihrer Anwendung durch Integration der Best Practices intensiviert, insbesondere bei internationalen Projekten.

FRIEDRICH-DESSAUER-PREIS

Cheers, wenn auch nur digital

Bereits zum 8. Mal hat der VDE Rhein-Main an der TH Aschaffenburg den Friedrich-Dessauer-Preis verliehen. Geehrt wurden dort zwei Masterabsolventen. Eine weitere Friedrich-Dessauer-Preisverleihung gab es an der Staatlichen Technikakademie Weilburg, dort ging der Preis an drei Technik-Abschlussprojekte, die jeweils in Gruppenarbeit entstanden.

Zumindest hybrid konnte sie stattfinden, die Friedrich-Dessauer-Preisverleihung an der TH Aschaffenburg: Schon zum achten Mal wurde dort der begehrte Preis des VDE Rhein-Main verliehen. Die prämierten Master-Absolventen fanden sich Mitte Juni vor Ort ein und präsentierten ihre ausgezeichneten Arbeiten in Anwesenheit des stellvertretenden VDE Rhein-Main-Vorsitzenden, Prof. Dr. Ingo Jeromin, den betreuenden Professoren Prof. Dr. Ralf Hellmann und Prof. Dr. Johannes Teigelkötter sowie des Dekans der Fakultät Ingenieurwissenschaften, Prof. Dr. Konrad Mußenbrock. Als erster Preisträger wurde Daniel Franz geehrt, der seine Masterarbeit für ein Konzept zum Hochgeschwindigkeits-Lasermikrobohren vorstellte, das eine noch effizientere Bearbeitung von elektronischen Leiterplatten ermöglicht.

Ultrakurzpuls für Präzision

Da elektrische Bauelemente immer kompakter werden und die Verdrahtungen immer dichter aneinander liegen, müssen auf einer Leiterplatte mehrere tausend Sacklochbohrungen (sogenannte Mikrovias) hergestellt werden. Zur Realisierung kleinstmöglicher Durchmesser der Mikrovias von weniger als 50 Mikrometern hat sich die Herstellung mittels Ultrakurzpuls (UKP)-Lasern mit einer zeitlichen Pulsdauer in einem Bereich von Billionstel- und Billardstel-Sekunden bewährt. Die Zielsetzung von Daniel Franz' Masterarbeit war, ein schnelles Laserstrahlablenkungskonzept für die Elektronikfertigung mit UKP-Lasern und akusto-optischen Deflektoren zu entwickeln und zu evaluieren.

Hochdynamische Alternative

Die Masterarbeit von Kai Kuhlmann galt der Entwicklung einer hochdynamischen Regelung für einen leistungsfähigen Traktions-Stromrichter mit unterschiedlichen Energiespeichern. Im vorherrschenden Wandel moderner Antriebsstrukturen ist die Kombination eines klassischen Verbrennungs-

Preispräsentation vor dem Gebäude der TH Aschaffenburg (v.l.n.r.): Prof. Dr. Ralf Hellmann, Daniel Franz, Prof. Dr. Ingo Jeromin (stellvertretender Vorsitzender VDE Rhein-Main), Prof. Dr. Johannes Teigelkötter, Kai Kuhlmann, Prof. Dr. Konrad Mußenbrock (Dekan Fakultät Ingenieurwissenschaften).

motors mit einer elektrischen Antriebsmaschine nicht die einzige Möglichkeit, Antriebssysteme zu hybridisieren – Anlass für Kai Kuhlmann, in seiner Masterarbeit Alternativen aufzuzeigen.

Ausgezeichnete Projektgruppen

Im Schwerpunkt Energietechnik und Prozessautomatisierung, Automatisierungstechnik sowie Systemtechnik haben drei Projektgruppen der Staatlichen Technikakademie Weilburg den Friedrich-Dessauer-Preis erhalten. Das Team von Marcel Weber, Lucas Adam und Tom Brasching wurde für die Entwicklung eines Tripod-Roboters für Pick & Place-Anwendungen ausgezeichnet, der nun in der Praxis zeigen soll, welche Folgekosten diese Plattform mit sich bringt.

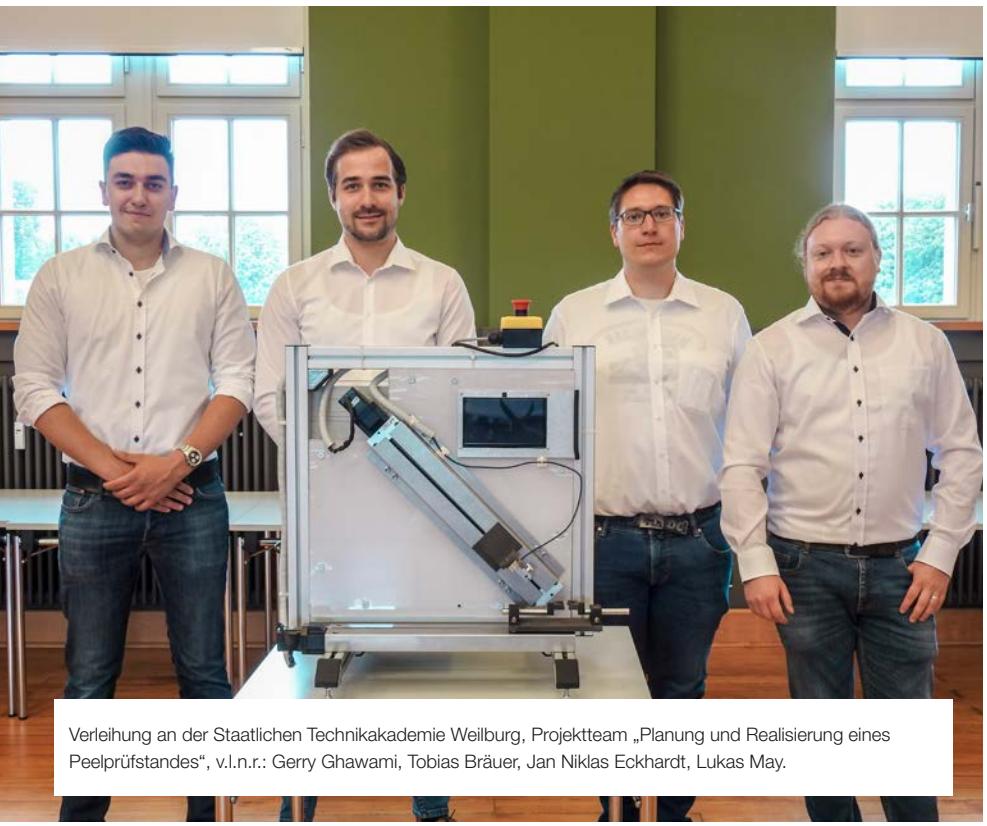
Moritz Hedrich, Simon Römer und Sebastian Wichmann entwickelten ein Qualitätssicherungsverfahren für Röntgenröhren mithilfe von zwei Platinen, die zur Frequenzüberwachung/-auswertung und Sicherheitsabfrage benötigt werden. Über die Messung der Frequenz zogen die drei Forscher Rückschlüsse, ob der Röntgengenerator korrekt arbeitet.

Zu viert arbeiteten Tobias Bräuer, Gerry Ghawami, Jan Niklas Eckhardt und Lukas May an der Realisierung eines Prüfstandes der Siegelnahtfestigkeit (auch Peel genannt) in der Verpackungsindustrie. Bislang wird die Siegelnahtfestigkeit qualitativ noch händisch beurteilt, mit dem Peel-Prüfstand soll dies künftig automatisiert erfolgen.

Sekt und Salzbrezeln

Worauf man in Weilburg verzichten musste, konnte in Aschaffenburg zumindest digital erfolgen: Dort wurde auf die Vergabe des Friedrich-Dessauer-Preises angestoßen, wenn auch nur am Bildschirm gemeinsam mit den zugeschalteten Gästen der Preisverleihung. Unter den Gratulanten war auch die Hochschulpräsidentin der TH Aschaffenburg, Prof. Dr. Eva-Maria Beck-Meuth, die vorab wie die restlichen „digitalen“ Teilnehmer und Teilnehmerinnen ein Preisverleihungskit mit Salzbrezeln und einer Flasche Piccolo zugeschickt bekam. *(sm)*

FOTOS: SEITE 12: TH ASCHAFFENBURG; SEITE 13: LINA HARTWIG



Verleihung an der Staatlichen Technikakademie Weilburg, Projektteam „Planung und Realisierung eines Peelprüfstandes“, v.l.n.r.: Gerry Ghawami, Tobias Bräuer, Jan Niklas Eckhardt, Lukas May.

Preisträger und Themen

Technische Hochschule Aschaffenburg

Daniel Franz, Master
Betreuer: Prof. Dr. Ralf Hellmann
Hochgeschwindigkeits-Lasermikrobohren von Elektronischen Leiterplatten mit Ultrakurzpulslaser und akusto-optischen Deflektoren

Kai Kuhlmann, Master
Betreuer: Prof. Dr.-Ing. Johannes Teigelkötter
Entwicklung eines Stromrichterkonzeptes für Traktionsantriebe mit unterschiedlichen Energiespeichern

Staatliche Technikakademie Weilburg

Lucas Adam, Tom Brasching, Marcel Weber
Betreuer: Dr.-Ing. Stefan Schurig, Wolfgang Kaiser
Realisierung eines marktfähigen Tripod-Roboters für Pick & Place-Anwendungen (HW-Elektrotechnik GmbH)

Moritz Hedrich, Simon Römer, Sebastian Wichmann
Betreuer: Dipl.-Ing. Stefan Fischer, Herr Faist
Qualitätssicherung von Röntgenröhren durch Frequenzüberwachung (Heuft Systemtechnik GmbH)

Tobias Bräuer, Jan Niklas Eckhardt, Gerry Ghawami, Lukas May
Betreuer: Stefan Fischer, Wolfgang Schmidt
Planung und Realisierung eines Peel-Prüfstandes (Hassia Verpackungsmaschinen GmbH)

JAHRESMITGLIEDERVERSAMMLUNG 2021

Wahl und Ehrungen

Die Jahresmitgliederversammlung (JMV) des VDE Rhein-Main Anfang Juli war ursprünglich als Hybrid-Veranstaltung geplant, konnte dann aber wegen der Corona-Auflagen doch nur digital stattfinden. Einer der Tagesordnungspunkte: die Wahl des neuen Vorstands für die Amtsperiode 2021 bis 2023. Wie jedes Jahr wurden auch 2021 im Rahmen der JMV die Jubilare für 25, 40, 50 oder 60 Jahre VDE Rhein-Main-Mitgliedschaft geehrt. Anders als ursprünglich angekündigt, wurde der Festvortrag „Digitale Transformation mit Verantwortung“ kurzfristig von Jens Mühlner, Vorstandsvorsitzender Verein Charta digitale Vernetzung e. V., gehalten.

Ehrungen für langjährige Mitgliedschaft 2021

(Abdruck mit schriftlicher Erlaubnis der Jubilare)

25 Jahre

El.-Meister Peter Blumenstock
Breimer-Roth GmbH Transformatorenwerk
Dr.-Ing. Stefan Brück
Roland Dorn
Dipl.-Ing. (FH) Stephan Escher
Dipl.-Ing. G.H. Werner Faßbinder
Dipl.-Ing. Jens Gotta
HAHN GmbH & Co. KG
Dipl.-Ing. (FH) Edgar Heep
Ing. (grad.) Andreas Hoffmann
Dipl.-Ing. Dipl.-Kfm. Wilfried Jäger
Dipl.-Ing. (FH) Jörg Müller
Dipl.-Ing. (FH) Olaf Christian Müller
Dr.-Ing. Bernhard Müller-Hagen
Dipl.-Ing. (FH) Alexander Olk
Dipl.-Ing. Michael Pfuhl
Dr. Dipl.-Chem. Gerd Sandstede
Ing. (grad) Karl Streb
Dipl.-Ing. Stefan Techau

40 Jahre

Prof. Dr.-Ing. Stephan Breide
Dipl.-Wirtsch.-Ing. Armin Domnick
Dipl.-Ing. Michael Henninger
Prof. Dr.-Ing. Karim Khakzar
Dipl.-Ing. Alfred Kraus
Dipl.-Ing. Rudolf K.J. Kunert
Dipl.-Ing. Andreas Walter Maria Müller
Dr.-Ing. Dieter Pfannstiel
RhönEnergie Fulda GmbH
Dipl.-Ing. Rainer Schaubach
Dipl.-Ing. Klaus Weber

50 Jahre

Dipl.-Ing. Peter Berking
Dipl.-Ing. Gerhard Brauer
Dipl.-Ing. Dieter Busch
Dr.-Ing. Gerhard Dreger
Prof. Dr.-Ing. Wolfgang Popp
Prof. Dr.-Ing. Jürgen Stenzel
Dipl.-Ing. Jürgen Wegner

60 Jahre

Ing. (grad.) Hans Eisenhauer
Dipl.-Ing. Friedhelm Fohrmann
Dipl.-Ing. Karl Großmann
Ing. (grad) Heinz Hellbarth
Dipl.-Ing. Friedrich-Wilhelm Henkemeier
Dipl.-Ing. (FH) Horst Hesmert
Dipl.-Ing. Eike Hoffmann
Prof. Dr.-Ing. Hans-Jürgen Hoffmann
Ing. (grad.) Hans-Heinrich Homeier
Prof. Dipl.-Ing. Gustav Komarek
Ing. (grad) Heinz Krapp
Dipl.-Ing. Horst Kretzschmar
Dipl.-Ing. Ernst Herbert Lehl
Ob.-Ing. (grad.) Hans Radgen
Ing. (grad) Helmut Ries
Ing. Wolfgang Sans
Dipl.-Ing. Gerd Schindewolf
Dipl.-Ing. Rudolf Sucrow
Ing. (grad) Rolf Teske
Dipl.-Ing. Horst Willenberg

Neuer Vorstand gewählt – Stark in der Region, stark für die Region

Auf der JMV 2021 bestätigten die stimmberechtigten Mitglieder des VDE Rhein-Main den Vorschlag zur Zusammensetzung des Vorstands. Die Wahl erfolgte online und anonym.

Neuer Vorsitzender des VDE Rhein-Main-Vorstands ist Thomas Beiderwieden, sein Stellvertreter Prof. Dr. Ingo Jeromin. In der Region ist der VDE Rhein-Main neben den jeweiligen Leitern für Mitte, Nord, West, Süd und Ost mit den Stützpunktleitern für Aschaffenburg, Lich, Marburg, Wetzlar und Weilburg stark vertreten. Die Fokusthemen Automatisierungstechnik, Energiewende und IKT, mit dem neuen Leiter Dr. Christian Groß, bilden weiterhin thematische Schwerpunkte. In den Referaten kümmern sich die Verantwortlichen unter anderem um den Austausch mit der Landesregierung, Themen von Studierenden und Young Professionals und um das Thema Öffentlichkeitsarbeit. Bei Fragen oder Anregungen können Sie sich jederzeit an die Geschäftsstelle des VDE Rhein-Main wenden: vde-rhein-main@vde-online.de

Geschäftsführender Vorstand

Vorsitzender
Thomas Beiderwieden

Stellv. Vorsitzender
Prof. Dr. Ingo Jeromin

Geschäftsführer
Prof. Rolf Bergbauer

Schatzmeister
Dipl.-Ing. Franz Beitz

Rechnungsprüfer
Dipl.-Ing. Christian Lambrecht
Ing. Dieter Rohrbach

Büro der Geschäftsstelle
Christine Rauwald

Regionen

Mitte (Frankfurt)
Prof. Rolf Bergbauer

Nord (Gießen/Wetzlar)
Dirk Peter M.Sc.

West (Mainz/Wiesbaden)
Tommy Mesfin

Süd (Darmstadt)
Ingo Hoyer B.Sc.

Ost (Fulda/Hanau)
Dipl.-Ing.(FH)
Matthias Hahner

Stützpunkte

Aschaffenburg
Prof. Johannes Teigelkötter

Lich
Dipl.-Ing. (FH) Dierk Keil

Marburg
Dirk Peter M.Sc.

Wetzlar
Dr. Bernhard Schild

Weilburg
Andre Bullmann

Referate

Landesvertretung
Prof. Ingo Jeromin

Öffentlichkeitsarbeit
Tommy Mesfin

Korp. MGL & Vorsitz Beirat
Prof. Jutta Hanson

Hochschulkontakte
Dr. Roland Steck

Forschungsexkursionen
Dipl.-Ing. Franz Beitz

Young Professionals/ Young Net
Dipl.-Wirtsch.-Ing. (FH)
Lukas Glotzbach M.Sc.

Vom ETV e.V. entsendet
1. Vorsitzende: zurzeit Mai Bach
2. Vorsitzender: zurzeit Daniel Birnstengel

Fokusthemen

Automatisierungstechnik
Dipl.-Ing. Sven Müller M.A.,M.Sc.

IKT-Forum
Dr. Christian Groß

Energiewende
Dipl.-Ing. Christian Anhaus M.Sc.

VDE Region Südwest

08.10.2021, 10:00–12:00 Uhr
Mannheim & online
Von IT zu OT – Sicherheit in der industriellen Kommunikation
Beim Datenaustausch zwischen Operational Technology (OT) und Information Technology (IT) spielt die Sicherheit der industriellen Kommunikation eine wichtige Rolle. Insbesondere die IT-Sicherheit ist heute funktional und strategisch einer der wichtigsten Aspekte der Governance von produzierenden Unternehmen.
Das Webinar richtet sich an Entscheider, Betreiber, Techniker und anwendungsorientierte Wissenschaftler – insbesondere aber an KMU und Start-ups.

13.10.2021, 17:15–18:15 Uhr
Online-Vortrag
Mathe, Mikroelektronik, Maschinensprache – woher kommt die Digitalisierung?
Die Digitalisierung ruht auf zwei Pfeilern, der Mathematik und der Mikroelektronik. Die Informationstechnik und die Informatik verbinden beide zu einem weltumspannenden Werkzeug – dem Internet. Ausgehend von der Schulmathematik erklärt Prof. Dr. Friedrich Jondral, VDE Mittelbaden, mithilfe des Bits als Informationsquant die Digitalisierung, das heißt die Überführung analoger Größen in diskrete Werte am Beispiel des maschinellen Lesens.

Infos und Anmeldung unter Veranstaltungen auf:
↗*www.vde.com/suedwest*

Fokusthema IKT

06.10.2021, 08:30 – 15:00 Uhr
NTT Global Data Centers EMEA GmbH
(Live-Webseminar aus Berlin)
25.11.2021, 08:30 – 15:00 Uhr
INNIO Jenbacher GmbH & Co OG
(Live-Webseminar aus Gelsenkirchen)
Datacenter Experience 2021
Online-Foren in Kooperation mit dem ETV Berlin
Das Thema Nachhaltigkeit und die damit im Zusammenhang stehenden Anforderungen zur Reduzierung von Emissionen und mehr Klimaschutz stehen im Mittelpunkt des Datacenter Experience. Experten der Elektro- und Informationstechnik erklären, wie Betreiber von Rechenzentren aktiv Emissionen wie CO_2, Geräusche, Licht oder Wärme in ihren Datacentern reduzieren und damit zum Klimaschutz beitragen können. Je nach Corona-Lage finden die Foren zusätzlich als Präsenzveranstaltung statt.
Mehr Infos unter ↗ *www.datacenter-experience.com*

03.11.2021, 16:00–18:00 Uhr
Online-Veranstaltung
VDE IKT-Forum: Digitalisierung als Nachhaltigkeitsmotor oder Nebelkerze
Im Mittelpunkt stehen die besonderen Herausforderungen der Digitalisierung unter folgenden Aspekten: die Frage nach der Wechselwirkung von Digitalisierung und Nachhaltigkeit, die technischen Möglichkeiten und ihre Bedeutung für die Innovationsförderung von Unternehmen und Institutionen.
Mehr Infos unter:
↗*www.vde-rhein-main.de/de/veranstaltungen*

Fokusthema Automatisierungstechnik

Online-Vortragsreihe Automatisierung – Im Wandel der Technik

17.01.2022, 17:30–19 Uhr
Grundlagen der Energieversorgung für Automatisierungstechnik und Prozessleittechnik

24.01.2022, 17:30–19 Uhr
Energieversorgung für die Automatisierungstechnik (Versorgungssicherheit) – Totally Integrität Power

31.01.2022, 17:30–19 Uhr
IT-Sicherheit in der Energiekommunikation /SCADA

07.02.2022, 17:30–19 Uhr
Cybersecurity für kritische Infrastrukturen – Anwendungsbeispiel

Die Referenten und genauen Vortragstitel finden Sie zu einem späteren Zeitpunkt auf unserer Homepage:
↗*www.vde-rhein-main.de*

Infos

Alle aktuellen Veranstaltungen des VDE Rhein-Main, des ETV oder der VDE Region Südwest finden Sie online hier:
↗*www.vde-rhein-main.de/de/veranstaltungen*

www.vde-rhein-main.de/de/veranstaltungen **www.twitter.de/vderheinmain**

Impressum
VDE Rhein-Main e. V.
Stresemannallee 15, 60596 Frankfurt/Main
Tel.: 069 6308-271
Fax: 069 6308-9271
vde-rhein-main@vde-online.de
www.vde-rhein-main.de
Geschäftszeiten: Montag bis Donnerstag
9:00 bis 14:00 Uhr

Redaktion: Tommy Mesfin (V.i.S.d.P.)
Redaktion und Text: Susanne Margraf (sm)
Christine Rauwald (cr), Thomas Beckmann (thb)
Gestaltung: Martin Wolczyk
Druck: H. Heenemann GmbH & Co. KG, Berlin
Erscheinungsweise: vierteljährlich
Nächste Ausgabe: Anfang Januar 2022

Ausblick auf Ausgabe 1/2022

Künstliche Intelligenz (KI)
Hessen will an die Spitze: In Darmstadt entsteht ein neues KI-Zentrum, das von 13 hessischen Hochschulen gemeinsam getragen wird. 38 Millionen Euro stellt die Landesregierung für die fünfjährige Aufbauphase bereit.