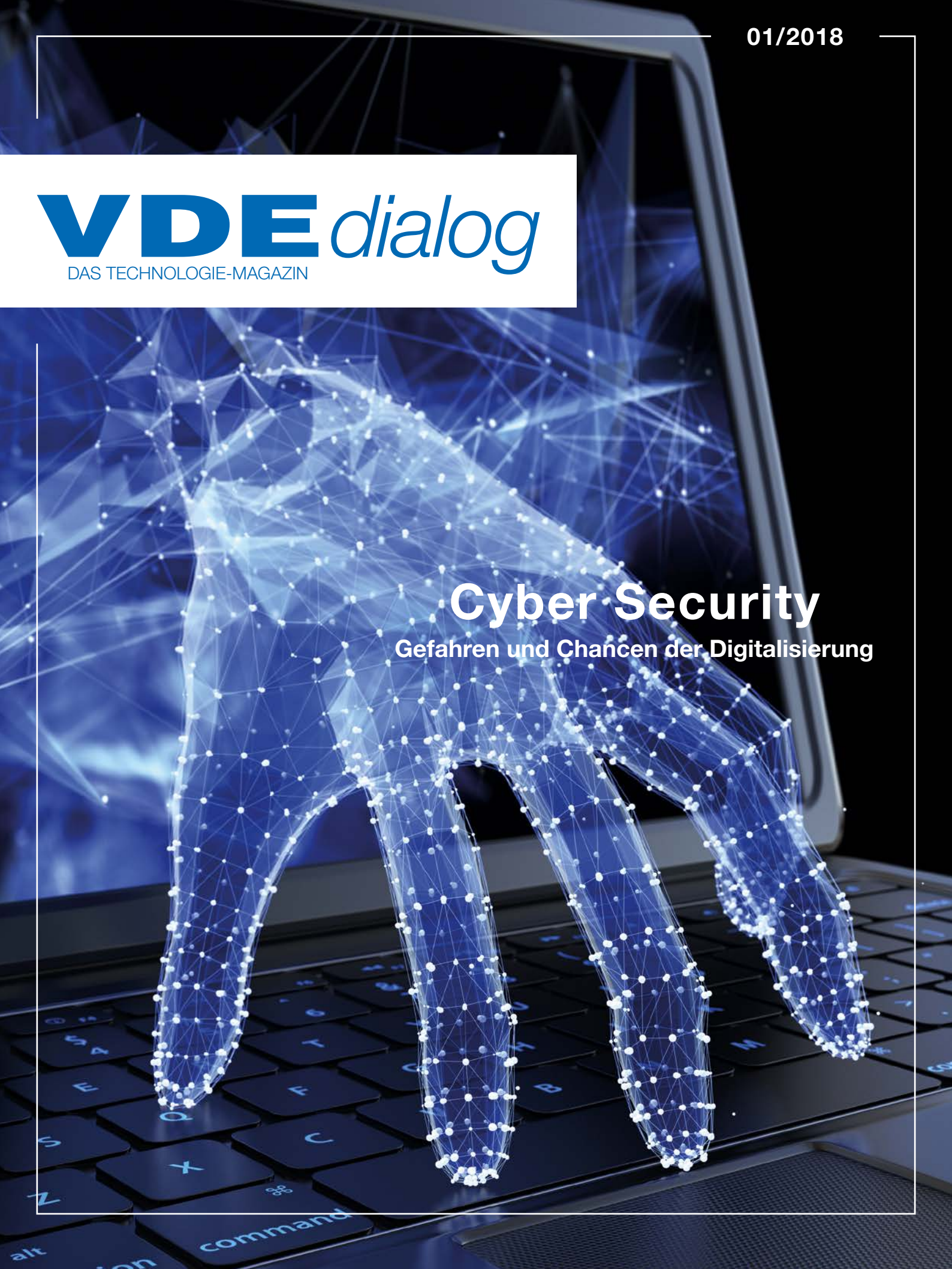
01/2018

VDE dialog

DAS TECHNOLOGIE-MAGAZIN



Cyber Security

Gefahren und Chancen der Digitalisierung

VDE – für eine lebenswerte Zukunft

Der VDE steht seit 125 Jahren für Wissen, Fortschritt und Sicherheit. In einem einzigartigen Netzwerk mit über 36.000 Mitgliedern gestalten wir eine lebenswerte Zukunft: elektrisch, digital, für alle, mit Idealen.

- Wir stehen für Innovation, Sicherheit und Qualität
- Wir sind das Forum für die nächste Generation
- Wir sind regional stark und weltweit vernetzt
- Wir bieten die neutrale Arbeitsplattform
- Wir teilen unser Wissen
- Wir gestalten und verbinden Bildung, Forschung und Anwendung
- Wir fördern und qualifizieren
- Wir erarbeiten gemeinsam Perspektiven
- Wir setzen Standards

www.vde.com

VDE

Ergreifen wir unsere Chance!

Das Bundesamt für Sicherheit in der Informationstechnik kommt in seinem Bericht zur Lage der IT-Sicherheit in Deutschland zu dem Ergebnis, dass die Gefährdungslage weiterhin auf hohem Niveau angespannt ist. Die häufigsten Einfallstore: Schwachstellen bei Soft- und Hardware, laxer Umgang mit Sicherheitslücken, Botnetze aus IoT-Geräten, Ransomeware und last but not least der „Faktor Mensch“. Den Schaden für die deutsche Wirtschaft schätzen Experten auf über 50 Milliarden Euro im Jahr. Keine Frage: Deutschland als führendes Industrieland zählt zu den attraktivsten Targets für Cyberkriminelle.

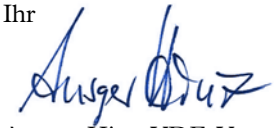
»IT-Sicherheit ist kein Zustand, sondern ein lebendiger Prozess, der auch bewusst gestaltet und vor allem gelebt werden muss.«

VDE-Mitgliedsunternehmen wissen ein Lied davon zu singen. 71 Prozent unserer Unternehmen mit mehr als 5000 Mitarbeitern gaben zu, bereits Opfer von Cyberangriffen geworden zu sein, die Dunkelziffer dürfte weitaus höher sein. Was tun? Abkapseln, Schweigen und Nichtstun sind keine Optionen. Eine neue Kultur der Offenheit ist notwendig, um konzertiert Angriffen vorzubeugen beziehungsweise diese abzuwehren. CERT@VDE ist die erste Plattform zur Koordination von IT-Security-Problemen im Bereich Industrieautomation, die diese Dienstleistung anbietet. Auch einmaliger Aktionismus ist die falsche Reaktion. Investitionen in die IT-Sicherheit ohne strukturierte Analyse, daraus resultierendem Maßnahmenplan und konsequentes Monitoring der Umsetzung sind aus dem Fenster geworfenes Geld. Denn IT-Sicherheit ist kein Zustand, sondern ein lebendiger Prozess, der auch bewusst gestaltet und vor allem gelebt werden muss.

Der VDE hilft dabei. Als Partner der Bundesregierung härten wir mit Expertenteams, Standards, IT-Security Dienstleistungen und umfangreichen Test-Szenarien in unseren Labs kritische Infrastrukturen. Aktuell entwickeln wir international eine Sicherheits-Charta pro IT-Sicherheit für Netze und Systeme und entwerfen Regeln für den sicheren IKT-Einsatz im Stromnetz. Wir fördern die branchenübergreifende Nutzung von Standards, sichern Smart-Home-Anwendungen über eine spezielle Testplattform und setzen uns für Security-by-Design & Co. und die innovationsfreundliche Balance zwischen Usability und IT-Security ein.

Das ist umso wichtiger, als Cyber Security nicht nur – virengleich – eine schnell mutierende Bedrohung darstellt, sondern auch einen boomenden Wachstumsmarkt eröffnet. Deshalb mein guter IT-Wunsch zum neuen Jahr: Nehmen wir IT-Sicherheit ernst, aber nutzen wir auch die damit verbundenen Zukunftschancen. Alles Gute für das neue Jahr und viel Spaß beim Lesen wünscht Ihnen

Ihr



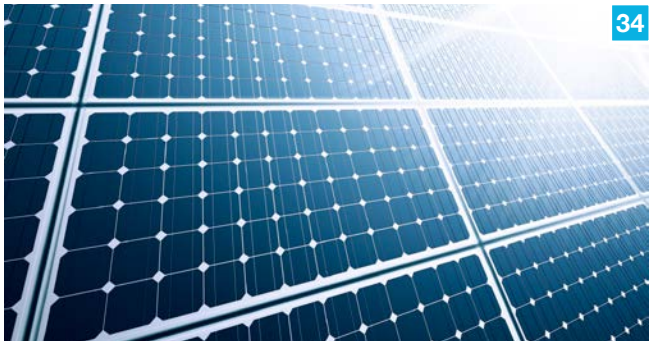
Ansgar Hinz, VDE-Vorstandsvorsitzender

INHALT

Durch die wachsende Vernetzung der Fertigungsanlagen eröffnen sich stetig neue Möglichkeiten für Cyberkriminelle. Um gegen Hackerangriffe gewappnet zu sein und daraus resultierende kostenintensive Ausfallzeiten zu verhindern, benötigen Unternehmen neue Sicherheitssysteme.

SPEKTRUM

TITEL



Der Ausbau erneuerbarer Energien verzeichnet enorme Anstiege. Insbesondere die Photovoltaik-Wachstumsraten übertreffen alle Erwartungen.

Ende Oktober kam die Elektronik- und Mikrosystemtechnikbranche in München und Berlin zusammen, um die Topthemen rund um Mikroelektronik zu diskutieren.

Digitale Bildung ist ein zentrales Anliegen quer durch alle Parteien. Der VDE hat ein Thesenpapier vorgelegt, das die nötigen Definitionen der Inhalte umreißt.

THEMEN

KOMPAKT

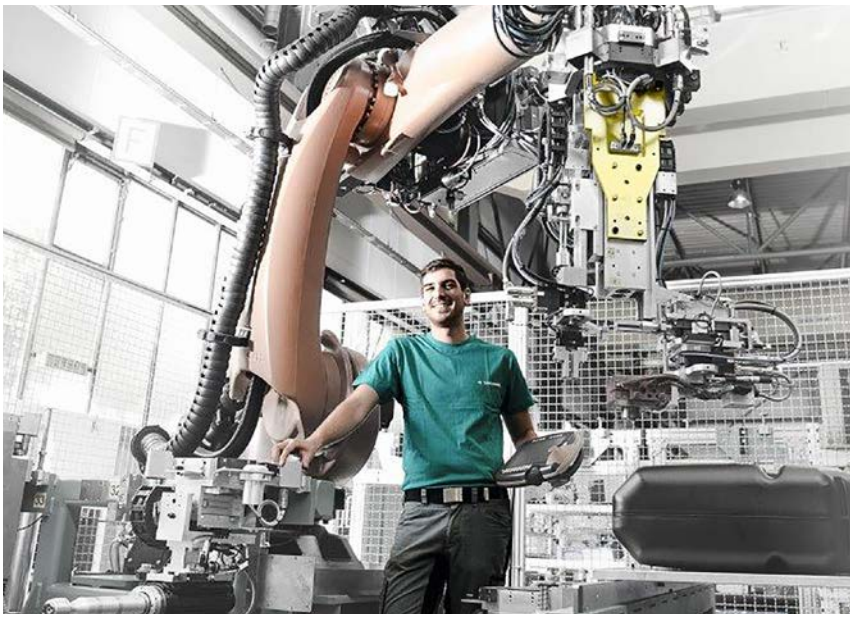
AUTONOMES FAHREN

Smarte Schilder

Sicherheit durch Barcodes: Verkehrsschilder und Fahrbahnmarkierungen sollen mit maschinenlesbaren Daten versehen werden.

Der Technikkonzern 3M will die Sicherheit des autonomen Fahrens auf vernetzten Straßen durch unsichtbare Barcodes, die über Tempolimits und Fahrbahnsperren informieren, erhöhen. Die Technologie ergänzt bereits vorhandene kamera- und GPS-basierte Systeme. Die intelligenten Materialien sollen dem Anbieter zufolge bei Regen, Nebel und Schnee funktionieren, benötigen keinen Strom, keine Elektronik und kein GPS. Derzeit testet das Unternehmen seine Lösung auf verschiedenen Teststrecken – unter anderem in Michigan, USA. Dort werden Baustellen mithilfe der neuen Technologie sicherer gemacht. Selbstfahrende Autos können ihr Tempo frühzeitig reduzieren, um die Baustelle vorsichtig zu passieren. Auch in Deutschland will 3M die Materialien für Teststrecken zur Verfügung stellen.

Der Konzern entwickelt bereits seit Anfang der 1960er-Jahre Produktlösungen für die Verkehrssicherheit und hat nach eigener Aussage die ersten reflektierenden Verkehrsschilder erfunden, die auch bei Nacht sichtbar sind.



ROBOTIK

Auf zu neuen Rekorden!

Die deutsche Robotik und Automation ist weiter auf Wachstumskurs. Für 2017 rechnet der Maschinenbauverband VDMA damit, dass die Rekordmarke von 14 Milliarden Euro Umsatz geknackt wurde. Auch weltweit gibt es eine verstärkte Nachfrage nach den Technologien.

Norbert Stein, Vorsitzender des Vorstands von VDMA Robotik + Automation, konnte zum Jahresende 2017 erfreuliche Zahlen vermelden: Alle drei Segmente der deutschen Robotik und Automation sind auf starkem Wachstumskurs. Sowohl die Auftragseingänge als auch die Umsatzentwicklung für 2017 hätten die Erwartungen deutlich übertroffen. Die industrielle Bildverarbeitung erreicht laut Prognose ein Umsatzplus von 18 Prozent. Das entspricht einem Branchenumsatz von 2,6 Milliarden Euro.

Ebenfalls deutlich dynamischer als erwartet zeigt sich die deutsche Robotik. Die ursprüngliche Wachstumsprognose von acht Prozent wurde auf 15 Prozent angehoben. Der Branchenumsatz wird damit auf 4,2 Milliarden Euro geschätzt. Die größte Teilbranche der deutschen Robotik und Automation bleiben sogenannte Integrated Assembly Solutions – intelligente Montage- und Produktionslösungen. Für 2017 nennt der VDMA ein Umsatzwachstum von sechs Prozent auf den neuen Rekord von 7,4 Milliarden Euro.

Diese Ergebnisse bestätigen den weltweiten Robotik-Boom, wie ihn die Statistik des Weltroboterverbands International Federation of Robotics (IFR) ausweist. Demnach stiegen die weltweiten Installationen von Industrierobotern 2016 um 16 Prozent auf 294.000 Einheiten. Für 2017 geht die IFR von einem Zuwachs der Stückzahlen von 18 Prozent auf 346.000 Einheiten aus. Deutschland ist der fünftgrößte Robotermarkt der Welt.

Besonders gefragt sind auch Serviceroboter. Im Oktober rechnete die IFR bis Ende 2017 mit einem neuen Rekordumsatz von 5,2 Milliarden US-Dollar. Auch die weitere Prognose ist positiv: Im Zeitraum 2018 bis 2020 wird ein durchschnittliches Wachstum von 20 bis 25 Prozent erwartet. „Bei der Umsatzprognose 2018-2020 erwarten wir für das Professional-Service-Segment ein kumuliertes Volumen von rund 27 Milliarden US-Dollar“, sagt Gudrun Litzenberger, Generalsekretärin der IFR. „Roboter für Medizin, Logistik und Field-Services sind dabei die wichtigsten Wachstumstreiber.“

Personalia

+++ Ein großer Moment für Robotikforscher **1 PROF. DR. SAMI HADDADIN** von der Leibniz Universität Hannover: Bundespräsident Frank-Walter Steinmeier hat ihm Ende November in Berlin den Deutschen Zukunftspreis verliehen. Hadaddin erhielt die Auszeichnung gemeinsam mit zwei Forschungskollegen für die Entwicklung eines sensiblen und intuitiv bedienbaren Roboters, der als Basis für viele neue Anwendungen der Automatisierungstechnik dient. Die Auszeichnung gilt als einer der bedeutendsten Wissenschaftspreise in Deutschland und ist mit 250.000 Euro dotiert. **+++ 2 PROF. DR. HANS DIETER SCHOTTEN** vom Deutschen Forschungszentrum für Künstliche Intelligenz in Kaiserslautern (DFKI) ist neuer Vorsitzender der Informationstechnischen Gesellschaft (ITG) im VDE. Der Direktor der Forschungsgruppe Intelligente Netze im DFKI bekleidet das Amt des ITG-Vorsitzenden für drei Jahre. **+++** Der saudische **3 KRONPRINZ MOHAMMED BIN SALMAN** will für mehr als 500 Milliarden Dollar die futuristische Megastadt Neom bauen lassen. Nach den Plänen des Thronfolgers wird es sich dabei um ein Gebiet handeln, das sich über Saudi-Arabien, Ägypten und Jordanien erstreckt. Sowohl Solartechnologie als auch Windkraftanlagen sollen Neom mit Energie versorgen und damit Saudi-Arabien unabhängiger vom Öl machen. Der ehemalige Siemens-Chef **4 DR. KLAUS KLEINFELD** soll das Projekt leiten. **+++ 5 PROF. DR. REINHART POPRAWE,** Leiter des Clusters Photonik in Aachen und des Fraunhofer-Instituts für Lasertechnik ILT, hat den US-„Peter M. Baker Leadership Award" erhalten. Das Laser Institute of America (LIA) zeichnet damit den Wissenschaftler für seinen außerordentlichen Einsatz in der internationalen Laserbranche aus.

PREPAID-SYSTEME

Strom per Guthabenkarte

So einfach wie Telefonieren – ähnlich wie bei Mobiltelefonen könnte sich auch der Bezug von Strom mit Prepaid-Systemen abwickeln lassen.

Die vom Wuppertal Institut erstellte Studie „Guthabenzahlung für Strom" kommt zu einem klaren Ergebnis: Der anstehende Breiteneinsatz von intelligenten Stromzählern ermöglicht dem Verbraucher ganz neue Perspektiven für den Bezug von Strom. Ähnlich wie beim Mobiltelefonieren ließe sich auch hier die Einführung einer Prepaid-Funktion einfach umsetzen. Demnach könnte ein Tarifmodell für Privathaushalte und Unternehmen Realität werden, das sich an dem von Guthaben-Handys orientiert. „Daraus ergibt sich ein enormes Potenzial", sagt Dr. Michael Kopatz, Mitautor der Studie und Projektleiter in der Forschungsgruppe Energie-, Verkehrs- und Klimapolitik am Wuppertal Institut. Prepaid-Zähler könnten einen Beitrag für den Klimaschutz leisten, indem sie dazu führen, dass private Haushalte bewusster mit Strom umgehen, die finanzielle Lage von einkommensarmen Haushalten stabilisieren und die Versorgungsunternehmen im Inkassobereich entlasten.

Das Prinzip von Prepaid-Zählern: Der Nutzer verbraucht nur das, was er vorher bereits eingezahlt hat. Das Guthaben für den Stromverbrauch kann er über ein Display am Zählergerät jederzeit einsehen. So sind die Kosten für den Anwender laut der Studie transparent. Das Wuppertal Institut hat die Studie, die neben Recherche- und Befragungsergebnissen auch Handlungsempfehlungen aufzeigt, im Auftrag des Ministeriums für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen erstellt.

KÜNSTLICHE INTELLIGENZ

Wenn die Black Box entscheidet

Künstliche Intelligenz eröffnet ungeahnte Möglichkeiten. Doch: Was bedeutet es, wenn Technologien kritische Prozesse steuern sollen – etwa die Produktion in Unternehmen oder ein autonomes Fahrzeug?

PROF. DR. THOMAS GABEL, Frankfurt University of Applied Sciences, Fachbereich Informatik und Ingenieurwissenschaften

„Die Forderung nach interpretierbaren oder sich selbst erklärenden Ergebnissen von Algorithmen der Künstlichen Intelligenz (KI) ist nicht neu. Die Kritik am Black-Box-Charakter von Modellen, die mit Verfahren des maschinellen Lernens optimiert worden sind, gab es in ähnlicher Weise schon in den 90er-Jahren und im letzten Jahrzehnt. Im Unterschied zu damals sind diese Verfahren jedoch – dank der Verfügbarkeit großer Datenmengen und gestiegener Rechenleistung – weitaus leistungsfähiger und daher bereits viel stärker in unseren Alltag integriert. Vor diesem Hintergrund kommt der Forschung im Bereich Erklärbarkeit besondere Bedeutung zu."

DR. STEFAN RÜPING, Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme, Geschäftsfeldleiter Big Data Analytics

„In Zukunft werden mit der steigenden Nutzung von Techniken der Künstlichen Intelligenz in immer anspruchsvolleren Anwendungen Transparenz, Erklärbarkeit und Zertifizierbarkeit zentrale Anforderungen sein. KI schafft für die Anwender intelligenter Systeme neue Herausforderungen, die zu Einsatzmöglichkeiten, Hintergründen und Grenzen von KI-Technologien geschult werden müssen. Auch in der Forschung haben wir uns dieser Thematik angenommen und entwickeln Verfahren des sogenannten Informierten Maschinellen Lernens, das KI durch Integration von Anwenderwissen robuster und verlässlicher macht.

DR. WOLFGANG HILDESHEIM, Leiter Watson und AI Innovation, IBM Deutschland, Österreich, Schweiz

„Es darf nicht passieren, dass Systeme Entscheidungen treffen, die für den Menschen nicht (mehr) nachvollziehbar sind. In absehbarer Zeit werden Technologien zeitkritische Prozesse nicht selbstständig steuern können und sollten dies auch nicht. Es geht gegenwärtig und auf absehbare Zeit darum, dass kognitive Systeme uns dabei unterstützen, bessere Entscheidungen zu treffen. Das bedeutet: klar definierte, relativ eng begrenzte Einsatzzwecke. Diese Systeme sollen uns einfache Routineaufgaben abnehmen, uns dabei helfen, Sachverhalte besser einzuschätzen oder uns unterstützen, in möglichst kurzer Zeit die richtigen Antworten zu finden."

PERSONALSCHULUNG

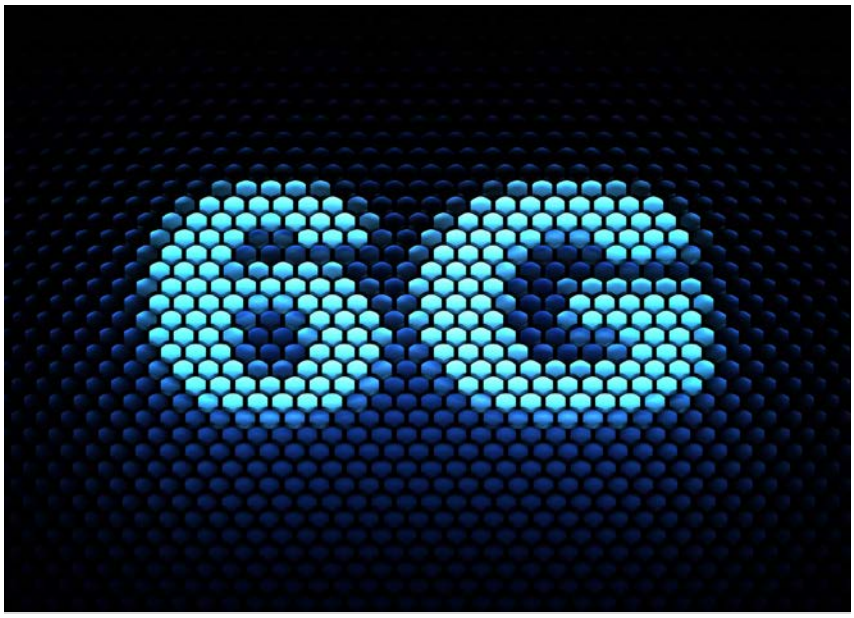
Fit für Industrie 4.0

Nicht selten wird die digitalisierte Fertigung von Ängsten der Mitarbeiter begleitet. Ein spezielles Training soll Abhilfe schaffen.

Auf Initiative des Innovationsnetzwerks „Produktionsarbeit 4.0" und Industriepartnern wie Festo und Siemens entstand das Programm „Akteure 4.0". Es richtet sich an Werker, Mitarbeitende in der Fertigung und angrenzende Berufsgruppen sowie die direkte Führungsebene. Häufig verbreitete Ängste vor Industrie 4.0 sollen damit abgebaut und den Teilnehmenden spielerisch die Grundlagen der Digitalisierung vermittelt werden. Ziel ist es, ein Grundverständnis für die digitalisierte Fertigung zu schaffen.

In drei Modulen mit einem Zeitumfang von zwei Präsenztagen werden Prinzipien, Notwendigkeit und Auswirkungen der Digitalisierungsprozesse in der Industrie vermittelt. In Modul 1 beispielsweise führt ein Planspiel in das Jahr 2030. Darin muss die Existenz einer Fabrik gesichert werden. Durch die Simulation der Zukunft soll ein Verständnis für den digitalen Wandel im eigenen Unternehmen erzeugt und die Veränderungsbereitschaft der Mitarbeitenden gesteigert beziehungsweise überhaupt aktiviert werden. Modul 2 führt den Ideenprozess des ersten Teils fort und fordert die Teilnehmenden auf, ihr eigenes Arbeitsumfeld zu analysieren und Industrie-4.0-Anwendungen zu identifizieren. Im abschließenden dritten Modul werden die erarbeiteten Ideen gemeinsam diskutiert und bewertet. Die ersten Trainings wurden bereits erfolgreich durchgeführt.

Das Programm wurde vom Netzwerk Produktionsarbeit 4.0 ins Leben gerufen, das vom Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO geleitet wird und an dem Partner aus Industrieunternehmen, Verbänden und von Technologieausrüstern beteiligt sind. Das Netzwerk möchte laut Fraunhofer IAO konkrete Industrie-4.0-Anwendungsfälle konzipieren und als Demonstrator umsetzen.



FUNKTECHNOLOGIE

Nach dem Standard ist vor dem Standard

5G ist noch nicht mal Realität – schon arbeiten Wissenschaftler im Rahmen des EU-Projekts Terranova an 6G, dem Mobilfunk der übernächsten Generation. Die Funktechnologie der Zukunft soll Terahertz-Funklösungen in Glasfasernetze mit hohen Datenraten einbetten.

Der kommende Mobilfunkstandard 5G steht gerade erst in den Startlöchern. Er verspricht eine enorme Leistungssteigerung in der drahtlosen Kommunikation – mit bis zu zehn Gigabit pro Sekunde. Doch in Zukunft wird die Nachfrage nach stabiler drahtloser Kommunikation weiter steigen und die vorhandenen Frequenzbänder belasten.

Forscher des Fraunhofer-Instituts für Angewandte Festkörperphysik (IAF) arbeiten daher gemeinsam mit Wissenschaftlern des Fraunhofer-Instituts für Nachrichtentechnik, dem Heinrich-Hertz-Institut (HHI), und weiteren Partnern aus Industrie und Forschung im Rahmen des EU-geförderten Projekts Terranova am übernächsten Mobilfunkstandard. Mit diesem soll eine Netzverbindung im Terahertz-Frequenzbereich möglich werden, die so stabil ist, dass Daten auch drahtlos mit einer Geschwindigkeit von bis zu 400 Gigabit pro Sekunde transportiert werden können. Die Experten arbeiten dabei an einem Transfer von optischer zu drahtloser Datenübertragung. „Wir wollen das Potenzial, das in der Glasfaser liegt, voll ausschöpfen, es aber nicht auf das Kabel beschränken, sondern auch auf die Funkstrecke übertragen“, erklärt Projektleiter Thomas Merkle vom Fraunhofer IAF.

Eine weitere Herausforderung, die im Rahmen des Projekts angegangen wird, ist der nahtlose Übergang zwischen den verschiedenen Zugangstechnologien. Schon heute wechseln mobile Nutzer je nach Verfügbarkeit zwischen Mobilfunknetz und WLAN. Bei Laptops kommt zusätzlich die Möglichkeit hinzu, sich über Kabelverbindungen ins Internet einzuwählen. Es gibt allerdings derzeit keinen fließenden Übergang zwischen den Zugangsarten, sodass es bei einem Wechsel zu Unterbrechungen kommt.

„Im Rahmen von Terranova soll das Erleben und Erfahren für den Nutzer so gestaltet werden, dass er Übergänge zwischen den Zugangstechnologien gar nicht bemerkt“, sagt Colja Schubert, Gruppenleiter Optische Untersee- und Kernnetze im Fraunhofer HHI.

MESSTECHNIK

Quantenkompetenz

Ehrgeizige Pläne: Ein neues Innovationszentrum in Jena soll Thüringen zu einem Vorreiter der industriellen Messtechnik machen.

Große Hoffnungen sind an das Innovationszentrum für Quantenoptik und Sensorik (InQuoSens) in Jena geknüpft: Es soll „die in Thüringen vorhandenen Kompetenzen auf dem Gebiet der Quantenoptik und der industriellen Sensorik bündeln und für neue Anwendungen nutzbar machen“, so Wolfgang Tiefensee, Wirtschafts- und Wissenschaftsminister des Landes Thüringen. Die Einrichtung wird mit drei Millionen Euro aus EU- und Landesmitteln gefördert. Träger des standortübergreifenden Innovationszentrums sind die Friedrich-Schiller-Universität Jena (FSU) sowie die Technische Universität Ilmenau. Gemeinsam mit dem Fraunhofer-Institut für Angewandte Optik und Feinmechanik wird bereits an aktuellen Fragestellungen gearbeitet – etwa wie sich Quantentechnologien im autonomen Fahren oder der medizinischen Diagnostik anwenden lassen. „Das Innovationszentrum soll nicht zuletzt der Graduiertenausbildung und dem Technologietransfer dienen“, sagt Prof. Dr. Kai-Uwe Sattler, Prorektor Wissenschaft der TU Ilmenau.

JOHANN-PHILIPP-REIS-PREIS

Speed mit Eleganz

Für den innovativen Weg der schnelleren Datenübermittlung wurde ein Ingenieur von der TU München ausgezeichnet.

Dr. Georg Böcherer von der TU München konnte sich über den mit 10.000 Euro dotierten Johann-Philipp-Reis-Preis für seine Arbeit zur „kanalangepassten Signalformung bei der digitalen Nachrichtenübertragung“ (Probabilistic Amplitude Shaping) freuen. Ihm ist es gelungen, bisher nur theoretisch bekanntes Verbesserungspotenzial für die praktische Nutzung zu erschließen – durch eine innovative Umordnung der üblichen Verarbeitungsblöcke bei der Signalaufbereitung. Die Häufigkeit bestimmter Signalamplituden wird dabei an die besonderen Eigenschaften der Übertragungsstrecke angepasst. „Und das alles in besonders eleganter, innovativer Art und Weise, die eine breite Anwendung erst ermöglicht“, so Laudator Prof. Dr. Stephan ten Brink.

Der Johann-Philipp-Reis-Preis richtet sich an Nachwuchswissenschaftler und wird alle zwei Jahre vom VDE gemeinsam mit der Deutschen Telekom sowie den hessischen Städten Friedrichsdorf und Gelnhausen vergeben, in denen der Erfinder Reis lebte.

BLOCKCHAIN

Brooklyn im Allgäu

Direkter Stromhandel zwischen Privatpersonen? Ein New Yorker Energie-Start-up will dies in Kooperation mit dem Allgäuer Überlandwerk künftig ermöglichen. Als technische Basis für solche Transfers dient eine Blockchain.

Mit dem Ziel des Aufbaus einer Handelsplattform, auf der Erzeuger und Verbraucher zusammengebracht werden und untereinander Strom handeln können, hat das Energieversorgungsunternehmen Allgäuer Überlandwerk (AÜW) ein zukunftsweisendes Projekt gestartet. Mithilfe der Blockchain-Technologie sollen bilaterale Handelsgeschäfte dezentral verifiziert und gespeichert werden. So können die Transaktionen ohne Bank oder Zahlungsdienstleister abgewickelt werden. Der Clou daran: Es gibt keinen dazwischengeschalteten Energieversorger.

Das AÜW setzt dafür auf die Unterstützung durch das Start-up LO3 Energy, das in New York bereits das Brooklyn Microgrid umgesetzt hat. Dieses vernetzt Nutzer zu einem virtuellen Stromnetz, in dem überschüssige Energie von regenerativen Erzeugungsanlagen direkt an andere Teilnehmer in der Nachbarschaft verkauft wird. Die Blockchain bildet die Grundlage für die Vertragsabschlüsse und gilt als besonders fälschungssicher. Bei dem Projekt im Allgäu sollen Haushalte nun aus einer Vielzahl verschiedener Lieferanten ihren Strombezug flexibel selbst auswählen können. Außerdem könnte überschüssig produzierter Strom nicht wie bisher über die EEG-Vergütung ins Netz eingespeist, sondern lokal an den nächsten Abnehmer – zum Beispiel den Nachbarn – verkauft werden.

Für den Aufbau der Plattform werden Pilotkunden ausgewählt, die mit einem von LO3 Energy speziell entwickelten Smart Meter ausgestattet werden, der Teil der Blockchain ist. Über eine darauf zugeschnittene App können die Teilnehmer dann mit einer digitalen Währung Strom handeln. Dabei sollen die Pilotkunden Präferenzen angeben können, wie sie ihren Strommix zusammensetzen möchten, der in lokalen Erzeugungsanlagen produziert wird.

Das Vorhaben zwischen AÜW und LO3 Energy ist Teil eines dreijährigen Versuchsprojektes, das im ersten Quartal 2018 starten soll. Die AÜW möchte diese Art des Stromhandels langfristig auf ihr gesamtes Netzgebiet ausweiten.

ELEKTROMOBILITÄT

Raus aus der Abhängigkeit

Die Elektromobilität kommt in Deutschland nur langsam vom Fleck. Prof. Dr. Stefan Bratzel, Direktor des Center of Automotive Management, erklärt, warum wir hierzulande eine Batteriezellenproduktion brauchen und warum Subventionen keine Lösung sind.

PROF. DR. STEFAN BRATZEL,
Direktor des Center of Automotive Management, Bergisch Gladbach

Herr Bratzel, wo stehen die deutschen Autobauer derzeit beim Thema Elektromobilität?
Bei den Plug-in-Hybriden sind sie mittlerweile Technologieführer. Aber bei den reinen Elektroautos befinden sich deutsche Hersteller nur im Mittelfeld – sowohl was die Innovationen als auch die Marktanteile betrifft. Und genau diese Fahrzeuge sind die Zukunft. Man hat die Elektromobilität früher hierzulande nicht ernst genommen und als wirkliche Alternative gesehen. Das ist seit circa zwei Jahren anders. Nun werden auch große Summen in das Thema investiert.

Welche Rolle spielt das Thema Batterie dabei?
Die Batterie ist zu einem großen Teil für die hohen Preise der Elektrofahrzeuge verantwortlich. Daher muss man erreichen, dass die Kosten für die Batteriezellen unter 100 Euro pro Kilowattstunde fallen. Wichtiger ist aber, sich aus der Abhängigkeit von den Produzenten der Batteriezellen zu lösen, die hauptsächlich aus Asien kommen. Es ist entscheidend, dass die deutsche Autoindustrie eine eigene Batteriezellenproduktion aufbaut. Dabei spreche ich von der kommenden Technikgeneration – den Festkörperzellen. Continental und Bosch sind da bereits sehr aktiv. Den Rückstand bei der aktuellen Generation von Batteriezellen wird man dagegen nicht mehr aufholen.

Könnten Subventionen helfen, um die E-Mobilität in Deutschland voranzubringen?
Das Auto hat sich auch nicht gegen das Pferd durchgesetzt, weil man für das Auto Subventionen bekommen hat. Eine Technologie muss von sich aus so gut sein, dass sie sich durchsetzt. Dabei geht es etwa um den Preis. Wenn ein Elektroauto sehr viel teurer ist als eines mit Verbrennungsmotor, dann muss es auch sehr viel besser sein. Und das ist noch nicht der Fall. Wir rechnen aber damit, dass wir Anfang der 2020er-Jahre auf ein Preislevel kommen, das das Elektroauto genauso attraktiv macht wie den Verbrennungsmotor. Außerdem müssen bestimmte Rahmenbedingungen geschaffen werden, etwa eine funktionierende Ladeinfrastruktur. Auch regulative Rahmenbedingungen sind wichtig. Wir haben ja bereits sehr strenge Vorgaben beim Thema CO_2, die die Elektromobilität vorantreiben werden.

Weiterer Knackpunkt ist die Ladeinfrastruktur. Für den schleppenden Ausbau haben sich die Beteiligten gerne gegenseitig die Schuld zugewiesen.
Sich gegenseitig den schwarzen Peter zuzuschieben, war eine Katastrophe. Der Tesla-Chef Elon Musk hat relativ schnell gemerkt, dass Reichweite und Infrastruktur ein zusammenhängendes System sind. Man verkauft Elektroautos nur, wenn man die Infrastruktur schafft. Und wenn es kein anderer macht, dann muss man es eben selbst tun. Aber die deutschen Hersteller haben das jetzt auch verstanden und investieren in Schnellladestationen.

ELEKTROMOBILITÄT

China an der Spitze

Eine Studie zum weltweiten E-Mobilitätsmarkt bestätigt: China bleibt der Leitmarkt für Elektrofahrzeuge. Deutschland kann sich zwar deutlich steigern, hat aber noch viel Luft nach oben.

Auch wenn der Absatz von Elektroautos 2017 hierzulande um 116 Prozent gewachsen ist, muss Deutschland sich anstrengen, um mit den internationalen Konkurrenzmärkten mitzuhalten. Zu diesem Ergebnis kommt eine Studie des Center of Automotive Management (CAM). Demnach wird die globale Elektromobilität weiter durch den Leitmarkt China bestimmt, der ein hohes Wachstum aufweist.

Der Abstand von China zum zweitgrößten Markt USA hat sich deutlich vergrößert. In den ersten drei Quartalen des vergangenen Jahres wurden in China insgesamt 398.000 Elektroautos abgesetzt. Das bedeutet eine Steigerung um 38 Prozent im Vergleich zum Vorjahreszeitraum. In den USA wurden von Januar bis September 2017 140.000 Elektrofahrzeuge verkauft. Die Zahl der Neuzulassungen konnte dort ebenfalls deutlich zulegen und wuchs um 29 Prozent. Spitzenreiter in Europa bleibt Norwegen mit 43.000 verkauften Elektroautos, was einer Steigerung von 33 Prozent entspricht.

Trotz gestiegener Absatzzahlen in Deutschland bleibt weiterhin noch viel Luft nach oben. Zwar wurden von Januar bis September 2017 36.849 Elektrofahrzeuge verkauft, der Marktanteil der elektrisch angetriebenen Autos liegt damit dennoch bundesweit nur bei 1,4 Prozent.


Linie4
99 %
5
****
Login
SMD 4

INDUSTRIE 4.0

INTELLIGENZ STATT MAUERN

Produktionsanlagen sind mittlerweile ähnlich vernetzt wie klassische IT, doch sie lassen sich nicht genauso wirksam schützen. Eine Lösung könnten Systeme bieten, die den Datenfluss in der Fertigung ständig nach Auffälligkeiten analysieren. Auch der regelmäßige Austausch über Sicherheitsprobleme senkt das Bedrohungspotenzial.

VON **MARKUS STREHLITZ**

„Für eine Produktionsanlage ist Verfügbarkeit das höchste Gut“, sagt Thorsten Henkel, zuständig für Industrial Security Solutions beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT). Ein Sensor an einer Maschine sendet pro Sekunde unter Umständen eine große Menge an Daten. „Wenn dabei Datenpakete fehlen oder verfälscht werden, hat das Unternehmen ein Problem. Denn ein anderes System, das diese Daten verarbeitet, kann dann nicht weiterarbeiten.“ Ein Angriff auf die IT im Fertigungsumfeld, das einen Produktionsausfall zur Folge hat, kann daher besonders große Schäden verursachen.

Das Risiko, dass solche Attacken eine Firma tatsächlich treffen, steigt. Durch die wachsende Vernetzung der Fertigungsanlagen eröffnen sich stetig neue Möglichkeiten für Cyberkriminelle. Dass die Gefahr real ist, zeigen Malware-Angriffe wie Stuxnet, der schon etwas länger zurückliegt, oder aktuelle Aktivitäten einer Gruppe namens Dragonfly, die den Energiesektor ins Visier nimmt. IT-Sicherheitsspezialist Trend Micro hat außerdem erst vor Kurzem Sicherheitslücken bei Industrierobotern offengelegt (siehe Kasten).

Das Risiko besteht für große Unternehmen ebenso wie für kleine und mittlere Firmen. Auch diese stellen ein attraktives Ziel für Hacker dar – zum Beispiel deutsche mittelständische Maschinenbauer, die in ihren Bereichen Weltmarktführer sind. Deren Anlagen zu sabotieren, ist ebenso ein verlockendes Ziel für Cyberkriminelle wie auch der Diebstahl ihres intellektuellen Eigentums.

Im Mittelstand fehlen aber häufig sowohl das nötige Personal als auch das Know-how – der Schutz der Fertigungsanlagen stellt somit für alle Unternehmensgrößen eine besondere Herausforderung dar. „Ansätze aus der klassischen IT lassen sich nicht immer einfach auf die Produktions-IT übertragen“, sagt Henkel. Technologien, die dort für Sicherheit sorgen wie Virenscanner oder Firewalls, können nicht ohne Weiteres in der Fertigungsumgebung eingesetzt werden.

„Die Architekturen der Produktions-IT eignen sich schlecht, um Security-Funktionen auszuführen“, so Henkel. Es fehlt an der nötigen Rechenleistung, den Speicherkapazitäten und den verfügbaren IT-Lösungen. „Und selbst wenn man bestehende Technologien anpassen und installieren würde, dann würde die Maschine so langsam arbeiten, dass sie für die Produktion gar nicht mehr einsetzbar wäre.“ Das gelte besonders für ältere Maschinen, die nur eine grundlegende IT-Anbindung zulassen.

FOTO: SEITE 12: SIEMENS

»Für die Vernetzungsszenarien in Industrie 4.0 benötigen Unternehmen Handlungsanweisungen und Werkzeuge, um die Security-Anforderungen zu meistern.«

Prof. Dr. Claudia Eckert, Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit

»Im Zeitalter von Industrie 4.0 ergeben sich aus der zunehmenden Digitalisierung neue Herausforderungen für die IT-Sicherheit der Industrieautomation.«

ANDREAS HARNER, Leiter VDE Kompetenzzentrum Informationssicherheit und Leiter CERT@VDE

»Ein Monitoring der Netzwerk-Datenflüsse ist klassischen Methoden wie etwa Firewalls überlegen. Burgen zu bauen bringt nichts. Das hat sich schon seit dem Mittelalter erledigt.«

CHRISTIAN NERN, Security Software Sales Leader DACH bei IBM

»Unternehmen müssen – abgesehen von den erforderlichen technischen Maßnahmen – die eigenen Mitarbeiter mit hoher Priorität stärker für das Thema Sicherheit sensibilisieren.«

KAI GRUNWITZ, Senior Vice President EMEA bei NTT Security

Die heterogene Altersstruktur ebenso wie die abweichenden Standards verschiedener Hersteller in der Fertigungslandschaft sind grundlegende Probleme für Industrie 4.0. Und auch dann, wenn es um die IT-Sicherheit geht. Mit OPC UA (Open Platform Communication Unified Architecture) wird daher gerade an einer Lösung gearbeitet, um die Maschinen verschiedener Hersteller miteinander zu vernetzen. Diese enthalte auch bestimmte Security-Funktionen, so Henkel. „OPC UA ist schon jetzt mehr als nur ein Protokollstandard und lässt sich zu einer Middleware ausbauen“, erklärt der Experte. „Es bietet unter anderem Verschlüsselungsschichten und rollenbasierte Zugriffsmodelle.“ Wenn man zwei Maschinen per UPC UA miteinander verbinde, ließe sich damit „zumindest grundlegende IT-Sicherheit in die Produktion einbringen“. Das Problem: Nicht alle Maschinen sprechen bereits OPC UA. Für deren Anbindung müssen noch proprietäre Protokolle verwendet werden, die keine Sicherheitsfunktionen bieten.

Um Produktionsumgebungen zu schützen, braucht es daher andere als die bisher üblichen Konzepte, glauben Experten wie Henkel. Sein Institut arbeitet an einem Ansatz, der allein auf der Auswertung von Daten basiert. Das entsprechende System analysiert die Informationsflüsse aus allen im Fertigungsprozess involvierten Instanzen wie Sensor-, Konstruktions- und Auftragsdaten sowie gegebenenfalls auch personenbezogenen Daten. Ziel ist es, Unregelmäßigkeiten in der Kommunikation der verschiedenen Systeme zu erkennen – zum Beispiel, ob größere Datenmengen in eine bestimmte Richtung abfließen.

Zwar gibt es bereits sogenannte Intrusion-Detection-Systeme, die auf eine ähnliche Weise vorgehen. Aber diese stoßen in der smarten Fabrik an ihre Grenzen. „Eine klassische Intrusion-Detection-Lösung arbeitet mit einem Referenzsystem, das den Normalzustand darstellt. Alles, was davon abweicht, wird als gefährlich klassifiziert“, erklärt Henkel.

Industrie 4.0 ist von Agilität geprägt – der Normalzustand ist kaum definierbar

Ein elementarer Wesenszug von Industrie 4.0 ist jedoch die Agilität. Alle Komponenten arbeiten sehr dynamisch miteinander. „Es ist daher kaum möglich, eine flexible Industrie-4.0-Architektur abschließend zu beschreiben“, so der Wissenschaftler. Es lässt sich also nicht definieren, wie der Normalzustand eines entsprechenden Systems aussieht, weil es sich ständig ändert.

Die Security-Lösung, an der das Fraunhofer SIT arbeitet, nutzt daher Machine-Learning-Methoden, um stets auf dem aktuellen Stand zu bleiben. „Im Grunde muss die Software zwei Dinge können“, so Henkel. „Sie muss kontinuierlich lernen, wie sich die Architektur im laufenden Betrieb immer wieder anpasst. Und sie muss trotzdem in der Lage sein, eine Mustererkennung abzuleiten und zu erkennen, wie sich ein dynamisches System verhalten muss, damit alles in Ordnung ist.“ Henkel geht davon aus, dass ein solches System nicht unbedingt im Unternehmen selbst installiert sein muss. Gerade kleine und mittlere Un-

Um Produktionsumgebungen zu schützen, braucht es andere als die bisher üblichen Sicherheitskonzepte. In den Fokus rücken Protokollereignisse und der Fluss der Datenströme, um möglichst schnell auf Unregelmäßigkeiten aufmerksam zu werden. Dabei hilft unter anderem Künstliche Intelligenz.

ternehmen könnten damit überfordert sein. „Es ist wahrscheinlicher, dass ein Mittelständler seine Daten an das System schickt, das irgendwo in der Cloud sitzt. Dort werden die Informationen analysiert und das Unternehmen erhält dann eine Rückmeldung."

Interessierte Firmen müssen allerdings noch etwas warten, bis sie eine solche selbstlernende Lösung einsetzen können. Das Fraunhofer SIT entwickelt das Verfahren im Rahmen des Projekts IUNO, das vom Bundesministerium für Bildung und Forschung initiiert wurde und bis Mitte 2018 abgeschlossen sein soll.

Auch andere Lösungsansätze arbeiten mit Künstlicher Intelligenz (KI), um Fertigungsanlagen vor Cyberangriffen zu schützen. IBM nutzt seine KI-Allzweckwaffe Watson, um die Sicherheitsverantwortlichen zu unterstützen. Die Technologie ist eine Ergänzung für QRadar – eine sogenannte SIEM-Lösung (Security Information and Event Management). Diese analysiert ebenfalls Protokollereignisse und Datenströme in einem Netzwerk, das Industrie-4.0-Geräte und IT-Anwendungen umfasst.

Monitoring-Systeme schlagen Alarm bei ungewöhnlichen Aktivitäten

Das System erkennt Unregelmäßigkeiten sowie hochentwickelte Sicherheitsbedrohungen und liefert zusätzlich Informationen, wie ein Unternehmen darauf reagieren sollte. Auf einem Dashboard kann der Sicherheitsverantwort-

INFORMATION

ENISA: Ausbau zur EU-weiten Agentur für Cybersicherheit

Die EU will ihre Bemühungen um IT-Sicherheit verstärken. Die bereits bestehende EU-Agentur für Netz- und Informationssicherheit (ENISA) soll zu einer Agentur für Cybersicherheit ausgebaut werden. Diese wird mit einem ständigen Mandat ausgestattet, um die Mitgliedsstaaten dabei zu unterstützen, Cyberangriffen wirksam vorzubeugen und zu begegnen. Durch jährliche europaweite Cybersicherheitsübungen und der Einrichtung von Informationsaustausch- und Analysezentren soll die neue Einrichtung die Reaktionsfähigkeit der EU erhöhen. Daneben wird sie die Umsetzung der Richtlinie zur Sicherheit von Netz- und Informationssystemen unterstützen. Diese sieht vor, dass schwerwiegende Cybersicherheitsvorfälle einer nationalen Behörde gemeldet werden müssen.

Weitere Aufgabe der Agentur ist es, an der Einrichtung und Umsetzung des EU-weiten Zertifizierungssystems mitzuwirken, das laut EU-Kommission dafür sorgen soll, dass Produkte und Dienstleistungen „cybersicher" werden.

FOTOS: SEITE 14: (V.O.N.U.) FRAUNHOFER INSTITUT, VDE, IBM, STEFFEN LEIPRECHT/NTT SECURITY; SEITE 15: SIEMENS

VERSICHERUNGSSCHUTZ

»Der Kunde muss sein Risiko kennen und verstehen«

Carsten Wiesenthal leitet die Firmenhaftpflichtsparte der Allianz Deutschland und ist damit auch für Cyberlösungen für den deutschen Mittelstand verantwortlich. Im Interview erklärt er, wie sich Firmen gegen entsprechende Gefahren versichern können.

CARSTEN WIESENTHAL,
Leiter der Sparte Firmenhaftpflicht der Allianz Deutschland AG

Was bietet die Allianz, um sich gegen Cyberangriffe zu versichern?
Wir haben dafür seit Kurzem ein eigenständiges Produkt auf dem Markt. Dieses besteht aus drei Bausteinen. Der erste deckt Haftpflichtansprüche Dritter ab, die durch Cyberkriminalität entstehen. Daneben bieten wir Leistungen in Zusammenhang mit der kommenden EU-Datenschutzgrundverordnung und der damit verbundenen Informationspflicht von Unternehmen an. Der für Mittelständler fast wichtigste Baustein bezieht sich auf Schäden, die Firmen selbst durch Cyberattacken entstehen. Unternehmen können sich dabei gegen Betriebsunterbrechungen versichern, die sich zum Beispiel durch den Ausfall von Maschinen in der Produktion ergeben. Zusätzlich dazu bieten wir alle wichtigen Services – vor allem auch im Bereich Krisenmanagement – rund um Cyberrisiken.

Wie sehen diese Services aus?
Gerade dem Mittelstand fehlen oft gut ausgebildete Mitarbeiter sowie das Know-how in Sachen IT-Sicherheit. Wenn aber heute ein Unternehmen gehackt wird, dann braucht es sofort Hilfe und auch Krisenspezialisten, die im Notfall die Kommunikation steuern. Dabei bedienen wir uns einer unserer Töchter – der metafinanz. Dort gibt es IT-Spezialisten, an die man sich rund um die Uhr wenden kann. Diese können sich gegebenenfalls auf den Rechner schalten. Oder auch bei besonders komplexen Fällen jemanden ins Haus schicken. Mithilfe der IT-Experten führen wir bei den Kunden außerdem ein Risk-Assessment durch.

Wie sieht ein solches Risk-Assessment aus?
Wir versuchen zunächst, das Risiko eines Kunden zu verstehen. Das läuft über unseren Risikocheck. Wenn wir Sicherheitslücken erkennen, geben wir unserem Kunden eine Lösung an die Hand, um diese zu schließen. Daneben gibt es aber auch sehr exponierte Risiken – zum Beispiel bei Unternehmen, die für kritische Infrastrukturen zuständig sind, wie etwa regionale Energieversorger. Mit diesen gehen Ingenieure aus unserem Haus im Einzelfall auch in einen direkten Dialog.

Was heißt das konkret?
Die Kunden legen ihre Sicherheitsarchitektur auf den Tisch. Und unsere Ingenieure schauen sich das sehr genau an und machen konkrete Vorschläge.

Wenn Sie ein eigenständiges Produkt für Cyberrisiken anbieten, gibt es wohl einen steigenden Bedarf an solchen Versicherungen.
Das ist richtig. Die Allianz fragt regelmäßig Kunden weltweit, wie sie ihre eigenen Risiken einschätzen. Vor zwei Jahren waren Naturkatastrophen und Feuer das Risiko, das sie am meisten fürchteten. In unserem Risk-Barometer 2016 sah das schon anders aus. Da waren Cybervorfälle schon auf Platz 3. Durch Industrie 4.0 ist alles miteinander vernetzt. Und den Firmeninhabern ist bewusst, dass sie auch dadurch angreifbar sind.

Gibt es auch Fälle, in denen Sie Unternehmen keinen Versicherungsschutz geben?
Es kann auch passieren, dass wir einen Kunden ablehnen, weil wir glauben, dass er zu wenig für seine IT-Sicherheit tut. Ein Unternehmen muss einfach sicherstellen, dass zum Beispiel bestimmte Back-ups laufen, Firewalls installiert sind und Ähnliches. Auch die Mitarbeiter müssen sensibilisiert sein. Denn durch bewusste oder auch unbewusste Fehlbedienungen kann extrem viel passieren. Wir verfolgen grundsätzlich einen sehr partnerschaftlichen Ansatz und versuchen, in einem Dialog die richtige Lösung für ein Unternehmen zu erarbeiten.

> »Wenn ein Unternehmen gehackt wird, dann braucht es sofort Hilfe und auch Krisenspezialisten, die die Kommunikation steuern.«

Manche IT-Experten glauben, dass sich Unternehmen, sobald sie versichert sind, weniger um ihre Schutzmaßnahmen kümmern. Wie sehen Sie das?
Ich teile diese Einschätzung der IT-Experten nur bedingt. Aber wir schauen uns das Risiko bei einem Unternehmen genau an. Wir sind darauf angewiesen, dass der Kunde sein Risiko kennt und versteht. Und dass er bereit ist, mitzuarbeiten. Eine Versicherung kann immer nur das Restrisiko abdecken. Aber es wäre fatal, wenn die Verantwortlichen in einem Unternehmen sich nicht um ihre IT-Sicherheit kümmern und stattdessen denken: Wenn es schiefgeht, dann zahlt schon irgendjemand.

Das Interview führte Markus Strehlitz.

liche auch erkennen, wie hoch die Wahrscheinlichkeit einer Bedrohung ist. „Unternehmen müssen mit einer Fülle von sicherheitsrelevanten Daten fertig werden, die sie ohne kognitive Unterstützung gar nicht mehr untersuchen können“, sagt Christian Nern, der bei IBM für den Bereich Security-Software im deutschsprachigen Raum zuständig ist. Entscheidungen müsse letztlich der Mensch treffen, aber Watson könne diesen dabei stark unterstützen – auch mit proaktiven Vorschlägen. „Um einen komplexen Angriff wie etwa durch Dragonfly zu analysieren, braucht Watson gerade mal eine Minute“, so Nern. Ein menschlicher Experte benötige für die Analyse relevanter Sicherheitsvorfälle dagegen mehrere Stunden.

Auch Siemens bietet eine Reihe von Security-Lösungen für Produktionsumgebungen. Dazu zählt ebenfalls ein Monitoring-System, das anhand von Algorithmen Datenströme nach Auffälligkeiten untersucht. Das können beispielsweise große Datenmengen sein, die zu ungewöhnlichen Tageszeiten in Bewegung geraten, oder Befehle, die ohne Grund unzählige Male hintereinander ausgeführt werden. Auch wenn sich Nutzer, die nur tagsüber arbeiten, plötzlich nachts einloggen, könnte dies ein ernst zu nehmender Hinweis auf eine Cyberattacke sein, wie Heiko Patzlaff berichtet, dessen Team die Lösung entwickelt hat. Wenn das Monitoring-System Auffälligkeiten entdeckt hat, benachrichtigt es automatisch das zuständige Sicherheitszentrum. „Dort analysieren IT-Security-Spezialisten den Angriffsversuch und leiten Gegenmaßnahmen ein“, so Patzlaff.

Siemens arbeitet daneben auch an einer Ausweispflicht für Maschinen. Grundlage dafür ist eine Public-Key-Infrastructure (PKI) für industrielle Anlagen, die mittels digitaler Zertifikate die Authentizität von Maschinen, Sensoren oder einem Bauteil nachweisen kann. Wenn ein Kontrollsystem einen Schaltbefehl an die Steuerungseinheit eines Feldgerätes gibt, versichern sich beide anhand des PKI-Zertifikates, ob die Gegenstelle wirklich die ist, die sie zu sein vorgibt.

Sicherheitsrisiken in Industrie 4.0 lassen sich nur gemeinsam lösen

Der VDE hat eine solche – in Deutschland und Europa bislang einmalige – Plattform gegründet, die speziell auf Sicherheitsprobleme in der Industrieautomation bei Mittelständlern ausgerichtet ist. Über CERT@VDE können Hersteller, Integratoren, Maschinenbauer und Betreiber von Produktionsanlagen Informationen über Cybersicherheitsprobleme und potenzielle Schwachstellen austauschen. Entdeckt ein Teilnehmer der Plattform beispielsweise eine Sicherheitslücke in einer bestimmten Steuerungseinheit in einem seiner eigenen Produkte, wird ein koordinierter Prozess zwischen CERT@VDE und dem jeweiligen Teilnehmer ausgelöst, in dessen Verlauf ein Lösungsweg sowie eine entsprechende Veröffentlichung erarbeitet wird. Die Ausarbeitung der Lösungsstrategie geschieht bei Bedarf gemeinsam mit anderen Teilnehmern der Plattform und gegebenenfalls mit anderen CERTs und ähnlichen Organisationen, die dem CERT@VDE als vertrauensvolle Partner zur Verfügung stehen. Am Ende des Prozesses wird gemeinsam eine Warnmeldung („advisory“) veröffentlicht, die über die Schwere der gemeldeten Sicherheitslücke, die potenziellen Gefahren und die betroffenen Produkte informiert. Unter https://cert.vde.com/de-de/advisories sind diese für jedermann einsehbar. Anwender der betroffenen Produkte sind somit gewarnt und können auf Basis dieser Warnmeldungen entsprechende organisatorische beziehungsweise technische Maßnahmen ergreifen, beispielsweise die im Advisory referenzierten Patches installieren.

CERT@VDE ist geprägt von den Prinzipien Vertrauen und Vertraulichkeit. Diese sind in den Leitlinien verankert, die unter anderem den koordinierten Veröffentlichungsmechanismus (coordinated disclosure) festlegen. Weiterhin zählen dazu die sichere Technologie, der Status des VDE als einer Non-Profit-Organisation und die Einbindung von CERT@VDE in übergeordnete Organisationen, die Vertraulichkeit verlangen.

Andreas Harner, Leiter des CERT@VDE, ist überzeugt, dass gerade Mittelständler nur gemeinsam den Sicherheitsrisiken in der smarten Fabrik gewachsen sind. „Wenn kleine und mittlere Unternehmen im Wettbewerb mit den Großen der Branche sicherheitstechnisch mithalten wollen, müssen Mauern fallen, um firmenübergreifend voneinander zu lernen.“ Dann werden sich auch die besonderen Herausforderungen bewältigen lassen, vor denen Unternehmen stehen, wenn sie ihre Produktionsanlagen ähnlich wirksam schützen wollen wie die IT in ihrem Büro.

INFORMATION

Industrieroboter – ein potenzielles Ziel für Angriffe

Industrieroboter werden zunehmend vernetzt und stellen somit ein mögliches Ziel für eine Cyberattacke dar. Wie hoch die Gefährdung ist, haben die Experten des IT-Sicherheitsanbieters Trend Micro anhand eines konkreten Robotermodells untersucht. Dabei entdeckten sie eine Reihe von Sicherheitslücken. Diese reichen von technischen Dokumenten, die auf öffentlich zugänglichen Websites verfügbar sind, über Zertifikate, die über alle Produktinstanzen wiederverwendet werden, veraltete Softwarekomponenten bis hin zu ungenügenden Authentifizierungspraktiken. Hinzu kamen schlechte Transportverschlüsselung sowie leicht zugängliche Firmware-Bausteine.

MARKUS STREHLITZ
schreibt als freier Journalist hauptsächlich über Informationstechnologie.

Gemeinsam für mehr Sicherheit

Die Zahl der Cyberattacken wächst in hohem Tempo. Diese Erfahrung wird auch im VDE geteilt: Der Großteil der Mitgliedsunternehmen wurde bereits Opfer von Hackerangriffen. Hinzu kommt: Digitale Angreifer verbessern laufend ihre Angriffsstrategien – Bedrohungen lauern prinzipiell bei jeder vernetzten, digitalen Technologie. Die VDE-Gruppe kämpft daher auf breiter Front für mehr Cyber Security. Ein Überblick.

VDE CERT

Die IT-Sicherheitsplattform für KMU

Die IT-Sicherheitsplattform für KMU CERT@VDE ist die erste neutrale geschützte IT-Security-Plattform für den Mittelstand in Deutschland. Sie unterstützt bei Bewältigung von Schwachstellen in den Systemen der Industrieautomation – über Organisationsgrenzen hinweg und unter Wahrung der Anonymität und Vertraulichkeit. Der VDE unterstützt mit den Security-Spezialisten seiner Kooperationsplattform Hersteller, Integratoren, Anlagenbauer und Betreiber beim Schließen von Sicherheitslücken und bietet zielgruppenorientierte Schwachstellenanalysen und Lösungsstrategien an. Mehr Infos unter:

www.vde.com/cert-vde

Förderprojekt VeSiKi

IT-Sicherheit für Kritische Infrastrukturen

Der VDE ist Partner des BMBF-Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen (ITS|KRITIS). In der Begleitforschung des Projekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)“ koordiniert der VDE den Austausch zwischen den insgesamt zwölf Forschungsprojekten und den relevanten Normungsgremien. Zudem werden sektorübergreifende Ansätze und Verbesserungsvorschläge erarbeitet. Mehr Infos unter:

www.dke.de/de/themen/projekte/vesiki

IT-Security NAVIGATOR

Recherche-Tool zu Normen und Gesetzen

Der Online-Navigator ermöglicht dem Anwender, relevante Normen, Standards und Richtlinien sowie gesetzliche Vorgaben für den eigenen Anwendungsfall zu finden. Das Tool ist im Rahmen des Projekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen (VeSiKi)“ in Zusammenarbeit mit der Universität Bremen entstanden. Mehr Infos unter:

www.security-standards.de

Normungs-Roadmap

IT-Sicherheitsstrategie, Version 3

Regelmäßig aktualisieren die VDE|DKE Kontaktstelle Informationssicherheit (KSI) und die Koordinierungsstelle IT-Sicherheit im DIN (KITS) die Deutsche Normungs-Roadmap IT-Sicherheit. Die aktuelle Version geht insbesondere auf die neuen gesetzlichen und regulatorischen Entwicklungen auf EU-Ebene ein. Zudem nimmt sie verstärkt kritische Infrastrukturen ins Visier. Sie steht kostenlos im Shop unter www.vde.com/shop als Download zur Verfügung.

Smart-Home-Testplattform

Funktionale Sicherheit und Interoperabilität

Smart-Home-Komponenten bieten ganz neue Einfallstore für Hacker. Deshalb hat das VDE-Institut eine Smart-Home-Testplattform entwickelt, mit der sich Smart-Home-Technologien verschiedener Branchen – Multimedia, Haushaltsgeräte, Gebäudeautomation, Heizung – prüfen und zertifizieren lassen. Dabei werden diese auf ihre einwandfreie Funktion und die Interoperabilität geprüft und somit Verbraucher geschützt. Mehr Infos unter:

www.vde.com/tic-de/dienstleistungen/vernetzung-und-interoperabilitaet

Task Force Trusted Computing

Sichere Geräteidentitäten im Internet der Dinge

Industrie 4.0, Smart Home oder Smart Traffic werden nur funktionieren, wenn jede Maschine, jedes Stück Hardware, jedes Gerät eine eigene, unverwechselbare „Identität“ hat, die gleichzeitig den Anforderungen an den Privatsphärenschutz genügt. Der VDE und das Fraunhofer-Institut SIT haben deshalb die Task Force „Trusted Computing“ gegründet. Mehr Infos unter:

www.vde.com/topics-de/cyber-security/task-force-trusted-computing

Förderprojekt DELTA

Laden und Bezahlen im Umfeld von Elektromobilität

Im Projekt DELTA geht es darum, den Lade- und Bezahlvorgang IT-sicher zu gestalten. Denn während für die Kommunikation zwischen Elektrofahrzeugen und Ladeinfrastruktur Standards definiert sind, sieht es bei Ladevorgängen und Mehrwertdiensten anders aus: Diese Kommunikation ist heute noch nicht standardisiert. Das Projekt DELTA schließt diese Lücke. Mehr Infos unter:

www.dke.de/de/themen/projekte/delta-foerderprojekt

Förderprojekt HARBSAFE

Harmonisierung des Begriffsverständnisses

Häufig ist ein und derselbe Begriff in verschiedenen Anwendungsfällen und über Branchengrenzen hinweg unterschiedlich definiert. Dies kann zu erheblichen Problemen führen. Hier setzt das Verbundprojekt von DKE und TU Braunschweig zur Harmonisierung unterschiedlicher Begriffsverständnisse an. Mehr Infos unter:

www.dke.de/de/themen/projekte/harbsafe

FOTO: J.MEL/FOTOLIA

NETZKRIMINALITÄT

Cybersoldaten gesucht

Cyberangriffe nehmen zu und die Einbrüche in fremde Computer und Systeme dienen nicht nur dem Datenklau – dahinter steckt ein Milliardengeschäft. Was häufig darauf zielt, die IT von Unternehmen großflächig lahmzulegen, gefährdet auch die Bevölkerung. Sie ist betroffen, wenn beispielsweise Krankenhäuser vom Netz gehen. Wer schützt uns?

VON **JONAS JANSEN**

Zu den gefährlichsten Cyberangriffen für die Bevölkerung gehören Attacken auf die sogenannte kritische Infrastruktur, also auf Energienetze, Wasserversorgung, Banken oder Krankenhäuser. Das ist durchaus kein unheilschwangerer Blick in die Zukunft, solche Angriffe gibt es schon jetzt regelmäßig. Zuletzt waren britische Krankenhäuser durch die Ransomware-Attacke WannaCry gelähmt – das bringt die Manager ins Schwitzen und Patienten in Gefahr. Und solche Angriffe nehmen tendenziell zu. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die nationale Cybersicherheitsbehörde, die sich darum kümmert. Sie hat mit MIRT eine Art GSG 9 für die Cyberabwehr geschaffen. MIRT steht für Mobile Incident Response Team, eine mobile Truppe, die bei Vorfällen ausschwärmt. Nachdem das Lukaskrankenhaus in Neuss vor einem Jahr eine Ransomware-Attacke gemeldet hatte, zogen später rund 60 ebenfalls betroffene Krankenhäuser nach. Das MIRT-Team ist relativ häufig draußen unterwegs, trotzdem wird darüber noch wenig geredet. Das liegt daran, dass das BSI von sich aus keine Unter-

nehmen oder Behörden an den Pranger stellt. Und auf der anderen Seite schrecken vor allem kleine und mittelgroße Unternehmen davor zurück, Erpressungen anzuzeigen: Sie treibt die Angst, damit den eigenen Ruf zu ruinieren.

Die Behörde rüstet deshalb auf und gibt Handwerkszeug an die Hand. Da werden Systeme „gehärtet" und die Software mit sogenannten Penetrationstests auf mögliche Lücken untersucht. Das BSI bleibt positiv gestimmt: Zwar steige die Gefahr von Hackerangriffen, doch gebe es auch robuste Systeme und fähige Entwickler in Deutschland. „Wir haben hier eine Kultur, uns schnell schlechtzureden. Dabei gibt es in Deutschland mit die besten Forscher im Feld der Kryptologie", sagt Arne Schönbohm, Chef des BSI. Auf diese Verschlüsselungsexperten sei selbst das Silicon Valley neidisch.

Cybercrime ist ein größeres Geschäft als Drogenkriminalität

Arne Schönbohm hat das BSI verändert, seitdem er Anfang 2016 auf Vorschlag von Bundesinnenminister Thomas de Maizière das Amt in Bonn übernahm. Seine Vorgänger waren Techniker, aber keine Leute für die Öffentlichkeit, die auch den Politikern und Managern in Unternehmen mit einfachen Worten erklären können, warum sie sich in einer digitalisierten Zukunft besser schützen müssen. „Wir haben in der Vergangenheit oft zu wenig darüber geredet, was wir tun", sagt Schönbohm. Früher ähnelte die Behörde eher einem Geheimdienst. Dabei gebe es heute knapp 600 Millionen Schadprogramme, Cybercrime sei ein größeres Geschäft als Drogenkriminalität. Die Zeit des BSI-Schweigens ist vorbei.

Schönbohm geht es vor allem darum, bei Unternehmen ein Bewusstsein dafür zu schaffen, dass Cybersicherheit zwar viel Geld kostet, sich aber lohnt. „Auf der Entscheiderebene muss das Thema Informationssicherheit mitgedacht werden", sagt Schönbohm. Denn wenn die Unternehmen sich schützen, ist die Gefahr für ihre Kunden geringer. Und auch Krankenhaus-Patienten sind am Ende in vielen Kliniken nichts anderes als Kunden. Der Schutz der Bevölkerung klappt deshalb vor allem darüber, durch den Schutz der Unternehmen den Kriminellen den Geldhahn zuzudrehen.

Denn Cyberkriminalität ist ein Milliardengeschäft, allein mit Ransomware, also Schadprogrammen, die Computer blockieren und zu Geiseln machen, wird Schätzungen zufolge jedes Jahr eine Milliarde Dollar erpresst. Nach Daten des Technologieunternehmens IBM haben 70 Prozent der Unternehmenslenker, die von Ransomware betroffen waren, das Lösegeld bezahlt. Die Hälfte von ihnen bezahlte mehr als 10.000 Dollar, ein Fünftel sogar mehr als 40.000. Im Darknet gibt es die Waffen für den ungleichen Kampf leicht zu kaufen, der digitale Bankraub ist längst leichter als der analoge. In den seltensten Fällen werden einzelne Privatpersonen attackiert, sie sind allerdings in der Folge oft Opfer von Angriffen, wenn Unternehmen schlecht geschützt sind.

Zuständige Behörden und Wirtschaftsverbände versuchen deshalb, die Sensibilität für das brisante Thema in den Unternehmen zu schärfen und unter dem Druck ständiger Cyberattacken gemeinsame Strategien zu entwerfen. Der Verfassungsschutz hat zusammen mit dem BSI, dem Bundeskriminalamt und dem Bundesnachrichtendienst sowie einigen Wirtschaftsverbänden die „Initiative Wirtschaftsschutz" gegründet. Auf einer Internetseite werden Unternehmen Ratschläge gegeben, wie sie sich vor Angriffen schützen und an wen sie sich im Notfall wenden können. In einem passwortgeschützten Bereich erhalten Nutzer auch aktuelle Lageinformationen.

Seit Kurzem gibt es in Deutschland allerdings eine weitere Behörde, die uns vor Gefahren von außen schützen soll. Und zwar indem sie selbst in den Angriffsmodus geht. Die „Zentrale Stelle für Informationstechnik im Sicherheitsbereich" (ZITiS) versucht, Verschlüsselungen zu knacken. Während das BSI in Bonn dafür zuständig ist, sie zu stärken, soll im Münchener Büro daran gearbeitet werden, verschlüsselte Messenger-Dienste wie WhatsApp, Signal oder Threema abzuhören. Ihre Kunden sind andere staatliche Organisationen. Genauso wie das BSI untersteht ZITiS dem Innenministerium. Allerdings bewegen sich die staatlichen Hacker in einem gefährlichen Feld. Wie sollen sie damit umgehen, wenn sie Schwachstellen finden? Der amerikanische Geheimdienst NSA wusste lange von der WannaCry-Schwachstelle, Kriminelle stahlen dieses Wissen und richteten rund um die Welt Millionenschäden an.

Stark gefragt: Hacker mit Hang zur Landesverteidigung

Deshalb ist die Zusammenarbeit der Behörden immens wichtig. Eine der aktivsten Aufklärungsbehörden neben dem BKA in Deutschland ist die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, eine bei der Staatsanwaltschaft Köln angesiedelte Einheit zur Bekämpfung von Wirtschaftskriminalität im Internet. Sie steckte hinter der Aufklärung der Botnetz-Attacke auf die Telekom Ende November 2016. In einem Botnetz werden internetfähige Geräte ohne Wissen der Besitzer zusammengeschaltet, um ihre Rechenleistung für illegale Zwecke wie etwa den Versand von Spam-Mails zu missbrauchen. Damals hatte ein Krimineller in verschiedenen Ländern gezielt Router mit der Schadsoftware „Mirai" infiziert. Im gesamten Rheinland funktionierten die Internet- und Telefonverbindungen von mehr als 1,2 Millionen Telekomkunden nicht mehr. Betroffen waren nicht nur Privathaushalte, sondern auch kommunale Unternehmen wie etwa die Entwässerungsbetriebe der Stadt Köln. Nach Angaben des Konzerns wurde man darauf am gleichen Tag aufmerksam und konnte Gegenmaßnahmen einleiten. Es dauerte trotzdem mehrere Tage, bis alle Störungen behoben waren. Laut Anklage gegen den Angreifer entstand der Telekom ein Schaden von mehr als zwei Millionen Euro. Die Bevölkerung hätte es auch stärker treffen können als nur mit ausgefallenen Internetanschlüssen. Die Behörden sind sensibilisiert und rüsten auf. Doch sie haben auch ein Problem, das im Cyberkrieg essenziell werden könnte. Sie finden kaum Leute für den Kampf gegen die Cyberkriminellen. Auch die Bundeswehr sucht händeringend nach

WHITE-HAT-HACKER

Honeypot auf Steroiden

Nicht immer sind Hacker auf der „dunklen Seite“ und verfolgen kriminelle Absichten. Sogenannte White-Hat-Hacker spüren ihre kriminellen Kollegen auf und locken sie in die Falle. Avi Kravitz, Gründer und CTO des Cyber-Security-Unternehmens CyberTrap erläutert im Interview seine sehr spezielle Methode, die schon viele Unternehmen vor Angriffen geschützt hat.

AVI KRAVITZ, Gründer und CTO von CyberTrap

Als White-Hat-Hacker nutzen Sie ihre Fähigkeiten, um IT-Systeme zu verbessern. Wann haben Sie mit dem Hacken angefangen?
Ich würde sagen, als ich zehn war. Das ist mehr als 20 Jahre her. Und zwar mit dem ersten Rechner, der meiner Schwester gehört hat. Als Jüngster durfte ich den Rechner natürlich nicht nutzen, der war passwortgeschützt und so hat das Ganze begonnen.

Heute locken Sie mittels sogenannter Honeypots, also Honigtöpfen, Kriminelle auf die falsche Fährte. Wie funktioniert das?
Es geht darum, jemanden zu erkennen, der bis dahin „unter dem Radar“ geflogen ist. Honeypots gibt es zwar schon lange, wir haben die Technologie 2012 aber neu erfunden. Quasi einen Honeypot auf Steroiden. Der Hauptunterschied liegt dabei am Entfaltungsspielraum, den wir dem Angreifer geben. Dabei legen wir Fallen in der Infrastruktur aus, also Fragmente, die für Angreifer interessant sind, wenn sie durch das Netzwerk stöbern.

Was passiert dann?
Sobald der erste Rechner kompromittiert ist, entscheidet der Angreifer, was sein nächster Schritt ist. Vereinfacht gesagt gibt es vier Richtungen: rauf, runter, rechts oder links. Sobald er unseren Köder schluckt, landet er in einer Parallelwelt. Er befindet sich dann in einer „echten“ falschen Umgebung.

Wie verhindern Sie, dass der Angreifer das Spiel durchschaut?
Nehmen wir an, wir schützen ein Pharmaunternehmen. Dann würde unsere Technologie alle Informationen über das Pharmaunternehmen zusammensuchen, die sie im Internet findet. Damit füttern wir die Parallelwelt. Da steckt also valide Information drin, die aber keinen weiteren Wert hat, weil sie schon offen im Internet ist. Außerdem markiert unsere Technologie jede Datei. Wenn solche gestohlen und geöffnet werden, sendet sie ein Signal zu einem unserer Sensoren und liefert dabei wertvolle Information über den Angreifer. Wir können also auch im Betrugsfall helfen und herausfinden: Wer sitzt auf der anderen Seite?

Sie können die Bad Guys ausfindig machen?
Der Auftraggeber ist in der Regel nicht selbst der Hacker. Wenn der also Informationen stiehlt, kann er sie oft nicht validieren und gibt sie an den Auftraggeber weiter. So hatten wir schon Fälle, in denen wir die gesamte Befehlskette aufgedeckt haben. Sobald ein Angreifer unsere Täuschungswelt betritt, ist es für uns, wie in eine Glaskugel zu schauen. Man sieht und verfolgt die Angreifer oder kann sie sogar mit falschen Informationen versorgen.

Was braucht ein robustes IT-System?
Bei zielgerichteten Angriffen geht es um Anomalie-Erkennung. Dazu muss man wissen, wie sich die Umgebung im Normalfall verhält, damit man Ausreißer und somit Anomalien erkennt. Unternehmen brauchen aber auch kompetentes Personal, das dem nachgeht. Wenn die Menschen nicht ausreichend sensibilisiert werden, dann bringt auch die teuerste Lösung nichts. Ich finde es höchst bedenklich, dass viele Hersteller hergehen und sagen: „Unsere Lösung löst alle eure Probleme!“ Wenn jemand so etwas sagt, sollte man hellhörig werden.

> »Unser Ziel ist: Angreifer rasch erkennen, sie demaskieren und nachhaltig draußen halten.«

Was können Sie tun, um Unternehmen nachhaltig zu schützen?
Wir sind die Feuerwehr, das letzte Fangnetz. In der Regel verbringen Angreifer zwischen fünf Tagen und sechs Wochen in unserer Deception-Infrastruktur. In dieser Zeit sammeln wir Fingerabdrücke, die sogenannte Threat Intelligence. Diese Information war vorher nicht bekannt, sonst wäre die Verteidigung ja nicht durchbrochen worden. Also sind unsere Informationen dann Gold wert. Sie werden dem Kunden zurückgespielt in seine Infrastruktur, um die Effizienz bestehender Produkte zu erhöhen. Damit können betroffene Organisationen die Angreifer auch nachhaltig draußen halten. Alle unsere Kunden werden Nutznießer dieser Threat Intelligence. Unser Ziel ist zusammengefasst: Angreifer rasch erkennen, die Motivation des Angreifers und sämtliche Threat Intelligence zu sammeln, die Angreifer zu demaskieren und sie nachhaltig draußen zu halten.
Das Interview führte Jonas Jansen

Cybersoldaten, die sie im Kampf im Netz unterstützen. Allein in den ersten Monaten des vergangenen Jahres habe es mehr als 284.000 Angriffe auf das Bundeswehrnetz gegeben. Zeit, etwas dagegen zu unternehmen. Zwar drängen Informatiker auf einen Arbeitsmarkt, der nach IT-Fachkräften lechzt – doch im Vergleich zum marktüblichen Gehalt für Universitätsabsolventen in der IT zahlt die Bundeswehr schlecht. Deshalb verspricht sie eine Sicherheit namens Verbeamtung und eine langfristige Beschäftigung in einem Markt, der sich schnell verändert. Wer zur Bundeswehr kommt, wird nicht schnell wieder rausgeworfen, lautet die Botschaft. Nur klingt eine jahrelange Verpflichtung längst nicht für jeden potenziellen Rekruten attraktiv.

Die Bundeswehr spielt deshalb die Patriotismus-Karte: Wer für sie arbeitet, hilft dem Land und trägt damit zu einer funktionierenden Gesellschaft bei. Doch selbst mit diesem Argument steht die Bundeswehr in Konkurrenz: Der Bundesnachrichtendienst und der Verfassungsschutz suchen ebenfalls Spione für den Staatsdienst, Hacker mit Hang zur Landesverteidigung. Die nicht so sehr aufs Geld schauen, sondern Teil eines großen Ganzen sein wollen. Was für manche verlockend klingt, schreckt andere ab. Mit patriotischen Idealen können sich Informatiker häufig nicht anfreunden, vor allem in der Hackerszene gibt es Widerstand. Die Skepsis vor dem Staat ist dort ausgeprägter als anderswo. Wer versteht, was technisch alles möglich ist in der Überwachung, distanziert sich mitunter davon. Hinzu kommen für viele Informatik-Studenten ganz praktische Gründe: Die Aufstiegschancen in einer Behörde sind begrenzt, befördert wird häufig noch nach starren Altersregelungen. Auch wenn die Truppe gerade versucht, das Bild der unflexiblen und langsamen Organisation zu verändern, steckt es noch in den Köpfen vieler junger Talente.

Die Digitalisierung verändert die Personalgewinnung rasant. Wer nicht schnell reagiert, wird abgehängt. Natürlich kann sich die Bundeswehr nicht so schnell anpassen wie ein Start-up oder ein digitalisierter Konzern. Am 1. April letzten Jahres wurde das Kommando Cyber- und Informationsraum, kurz CIR, vorgestellt. In absehbarer Zeit sollen 14.000 Soldaten und zivile Mitarbeiter in diesem Kommando tätig sein und Deutschland fit machen für die Verteidigung im Netz. Momentan sind es rund 260 Mitarbeiter, die neben dem Heer, der Marine und der Luftwaffe einen vierten, eigenständigen Bereich der Bundeswehr ausmachen. „Deutschlands Freiheit wird auch im Cyberraum verteidigt“, wirbt die Bundeswehr für ihre neue Initiative. Das ehemalige Zentrum für Informationstechnik in Euskirchen wurde Anfang April umbenannt in das „Zentrum für Cyber-Sicherheit der Bundeswehr“. Rund 100 Millionen Euro will sie in den Standort investieren, aus 200 Angestellten dort sollen alsbald 600 werden, welche die IT-Systeme der Bundeswehr schützen. Der jährliche Bedarf der Bundeswehr liegt schon jetzt bei 800 IT-Administratoren und 700 IT-Soldaten.

Der Personalplan ist mindestens ambitioniert, einige, die sich damit auskennen, halten ihn für praktisch unmöglich. Schon ohne Fokus auf die Cybersicherheitseinheit stöhnten die Personalverantwortlichen unter der Last, fähiges Personal für die Informationstechnologie zu finden. „Entwickeln Sie mit uns die Bundeswehr der Zukunft“ steht auf dem Werbeprospekt für den „Admin (m/w)“ und „Jetzt auf eine von 700 Stellen bewerben“. Für „Offiziere und IT-Studenten“ gibt es 200 Stellen und für den „Admin im zivilen Bereich“ 200 Bachelor-Studienplätze. Der gesamte öffentliche Dienst konkurriert mit allen anderen um Fachkräfte.

Das sind heute längst nicht mehr nur Unternehmen wie Google oder Facebook, sondern auch Dax-Konzerne und Mittelständler: Alle sind auf der Suche nach Informatikern, Data Scientists und ethischen Hackern. Der gute Arbeitsmarkt erschwert es Behörden zusätzlich und der demografische Wandel verknappt das Angebot zudem. Bewerber kommen in einen für sie komfortablen Markt. Die größten Konkurrenten auf der Suche nach fähigen Hackern sind für die Bundeswehr die Sicherheitsunternehmen, die selbst ständig gegen die Angreifer aus dem Netz kämpfen. Die Cybersicherheitseinheit des Elektronikkonzerns Rohde & Schwarz zählt allein in Bochum 90 offene Stellen. Vorstandschef Ammar Alkassar sagt, Unternehmen wie seine zahlten schon 30 Prozent mehr als die Behörden und suchten trotzdem ständig Mitarbeiter. „Das wird echt schwierig für die Behörden. Sie brauchen schließlich auch gute Leute und nicht nur die, die am Ende übrig bleiben.“

Andere Länder investieren mehr in den Kampf gegen Cyberkriminelle

Die CIA zahlt einem „Cybersecurity Officer“ zwischen 62.000 und 145.000 Dollar im Jahr. Das ist zwar auch nicht das höchste Gehalt im Markt, aber deutlich mehr, als man von deutschen Behörden erwarten kann. Der Geheimdienst steckt jedes Jahr Hunderte Millionen Dollar in Cybersicherheit. Nun haben die Amerikaner allerdings 2016 auch 611 Milliarden Dollar für Rüstung ausgegeben, mehr als das 15-Fache von Deutschland. Doch es liegt nicht nur am Geld. Zum Vergleich: Israel hat im gleichen Jahr knapp 17 Milliarden Dollar für Rüstung ausgegeben, weniger als die Hälfte von Deutschland. Doch in Israel leistet jeder Mann drei Jahre Wehrdienst und jede Frau zwei Jahre. Schon vor mehr als 60 Jahren wurde dort die Unit 8200 gegründet, die größte Unterorganisation der Israelischen Verteidigungsstreitkräfte, IDF genannt. Mehrere Tausend Mitarbeiter zählt sie, die sich darum kümmern, Codes zu knacken und zu entschlüsseln, und im Cyberkrieg mit zu den bestbewaffneten Kämpfern gehören. Die Einheit ist vergleichbar mit der NSA in den Vereinigten Staaten. Palo Alto Networks und Check Point, zwei der bekanntesten IT-Sicherheitsunternehmen der Welt, sind von Absolventen der Unit 8200 gegründet worden. Israel ist rund um die Welt bekannt für seine Start-ups und für sein Militär, in der Unit 8200 kombiniert es beides.

Von dieser Ausstattung können andere Länder nur träumen.

JONAS JANSEN
ist Redakteur im Wirtschaftsressort der F.A.Z.

SMART HOME

Die Cloud lauscht mit

Das intelligente Heim lockt mit großen Verheißungen – das Leben wird um vieles komfortabler und günstiger, da effizienter, lässt sich freier und vielfältiger gestalten. Doch der Markt für Smart-Home-Geräte ist noch sehr jung und wie bei so vielen Entwicklungen bleibt in den ersten Produktgenerationen so manches auf der Strecke. Hier die IT-Sicherheit und der Datenschutz.

VON **STEFAN MUTSCHLER**

Dank schnellem Internet und vielen neuen Produkten kommt das Smart Home so langsam in Fahrt. Im letzten Jahr wurden rund 80 Millionen Smart-Home-Devices an den Mann gebracht, das entspricht einem Wachstum von 65 Prozent gegenüber dem Vorjahr. Die intelligente Steuerung von Thermostaten, Leuchten und Klimaanlagen via Smartphone-App steht hoch im Kurs, vernetzte Sensoren bestellen im Kühlschrank füllstandabhängig Nachschub, mahnen in der Waage und im Fitness-Band zu mehr Bewegung, spielen im intelligenten Lautsprecher auf Zuruf den gewünschten Musiktitel und vieles mehr. Häufig werden bei solchen Aktionen sehr sensible personenbezogene Daten verarbeitet. Dennoch machen sich nur wenige bewusst, dass der High-Speed-Anschluss an die Welt auch eine Kehrseite hat: Theoretisch könnte bei jedem Ding, das mit einer IP-Adresse im Internet der Dinge (IoT für Englisch: Internet of Things) unterwegs ist, der ganze Globus live dabei sein – als Beobachter oder Angreifer.

Wo liegen die Risiken bei der Nutzung der intelligenten kleinen Helfer? Im Datenschutz und der IT-Sicherheit!

Aus der Forschung kommen regelmäßig beunruhigende Nachrichten über die Verletzlichkeit von IoT-Geräten. So warnten beispielsweise Ende August 2017 Forscher der Universitäten Erlangen-Nürnberg und Mannheim vor Sicherheitslücken bei IoT-Geräten mit der Funktechnologie ZigBee. Ihnen sei gelungen, die damit ausgestatteten Lampen über Stunden hinweg zum Blinken zu bringen und zu verhindern, dass der legitime Nutzer sie steuern konnte. Die betreffende ZigBee-Funktion, über die normalerweise neue Geräte zu einem Netzwerk hinzugefügt werden können, ist auch in vielen anderen IoT-Geräten implementiert, laut Schätzungen bei weltweit rund 100 Millionen Devices. „Mit unserer Forschung möchten wir Hersteller auf die Sicherheitsprobleme im Zusammenhang mit dieser ZigBee-Funktion aufmerksam machen, um zu verhindern, dass zukünftige Smart-Home-Produkte die gleichen Schwachstellen aufweisen“, so Philipp Morgner, IT-Sicherheitsforscher an der Universität Erlangen-Nürnberg. „Während aktuell nur vernetzte Beleuchtungssysteme betroffen sind, könnten es in Zukunft auch Heizungsanlagen, Türschlösser und Alarmanlagen sein.“

Anders als etwa bei PCs und Smartphones, die in der Regel durch Firewall und Antimalware-Programme geschützt sind, ist es für Angreifer im Smart Home vergleichsweise einfach, die Geräte zu missbrauchen. Auf jedem Gerät läuft Software. Schwachstellen gibt es in jeder Software, die Frage ist nur, wie leicht sie zu finden und wie hoch der Anreiz für eine Ausnutzung ist. PC-Software erhält deswegen meist regelmäßige (Sicherheits-) Updates. Im IoT ist diese Praxis noch längst nicht überall üblich. Manche Geräte erhalten nur sehr selten ein Firmware-Update, bei einigen hat der Hersteller keinen Update-Prozess vorgesehen. Das macht sie zur leichten Beute und im Kontext eines Smart Homes zu begehrten Hackerzielen, um sie beispielsweise als Einfallstor für das heimische Computernetzwerk zu missbrauchen.

Das WLAN selbst mag gut geschützt sein – die IoT-Geräte sind es oft nicht

Das heimische WLAN mag IT-seitig gut vor Angriffen von außen geschützt sein, gelangen Hacker aber etwa über ein Heizungsthermostat hinein, sind Schutzmechanismen weitgehend ausgehebelt. So könnten Kriminelle über den Umweg über das smarte Gerät vertrauliche Informationen von den Datenspeichern der IT-Geräte abziehen. Ebenso könnten sie Malware-Programme auf die Rechner einschleusen, über die sich weitere Angriffe starten lassen. Das Gerät selbst kann aber auch gekapert oder ferngesteuert werden. Im Falle der Lichtsteuerung war der Angriff eher psychologischer Natur: Wenn nachts die Lampen unkontrolliert an- und ausgehen, können sich die Betroffenen im eigenen Heim nicht mehr sicher und als Herr der Lage fühlen. Bei Geräten mit Mikrofonen oder Kameras ist dieser Effekt nach der Entdeckung sicher noch um einiges größer – bis dahin können sie für umfangreiche Lauschangriffe genutzt werden. In wieder anderen Fällen sind sicherheitsrelevante Funktionen wie etwa Türschlösser betroffen. Und schlussendlich kann das Gerät selbst oder andere im gleichen Netz arbeitende Devices in ein Botnetz eingebunden werden. Bei Botnetzen handelt es sich gleich um eine ganze Gruppe automatisierter Schadprogramme. Diese brauchen in erster Linie Rechenpower, um beispielsweise massive DDoS-Angriffe auf die Web-Applikationen eines lukrativen Opfers fahren zu können. Locker umschrieben ist ein DDoS-Angriff eine ferngesteuerte „Dienstverweigerung“ des Internets. Über eine entsprechende Malware nehmen die Botnetzbetreiber gerne alles in Beschlag, was starke Prozessoren hat, am liebsten PCs oder Server, sehr gerne aber auch beispielsweise einen WLAN-Router, der obendrein auch noch ständig angeschaltet ist. Der legitime Nutzer merkt

FOTO: SEITE 24: MACROVECTOR / ISTOCK

nur, dass alles irgendwie langsamer wird. Ein Großteil der IoT-Geräte bietet noch nicht einmal theoretisch die Möglichkeit, eine Endpoint-Security-Software darauf zu installieren. Bei zentralen Steuergeräten bestünde diese Möglichkeit zwar meistens, aber wie die Praxis zeigt, fehlt sie meist auch hier. Ein gutes Beispiel für zentrale Steuergeräte, die zumindest in manchen Fällen auch für die Steuerung unterschiedlicher IoT-Endgeräte geeignet sind, sind die sprachgesteuerten Heimassistenten, die in Form einer WLAN-Lautsprecherbox gerade Hochkonjunktur haben. Apple mit Siri, Microsoft mit Cortana und Google mit Assistant haben die Sache mit dem intelligenten Auskunftsservice im Smartphone vorgemacht – Amazon schuf mit der Integration seiner Alexa in eine Box eine neue Spezies von Heimassistenten.

Ein Grund für die hohe Popularität von Alexa liegt darin, dass Amazon seine Software mit offenen Programmierschnittstellen ausgestattet hat, über die sich Smart-Home-Geräte von anderen Herstellern in die Alexa-Steuerung integrieren lassen. Der Markt boomt. Täglich kommen neue Geräte hinzu, die mit ihrem Anschluss an die Alexa-Welt werben – vom elektronischen Thermostat über die Beleuchtung bis hin zu Staubsaugerrobotern und Rasenbewässerungsanlagen.

Smarte Heimassistenten: Ein Desaster in Sachen Datenschutz?

Hinter den sprachgesteuerten Assistenten steht immer ein Cloud-Service des jeweiligen Anbieters. Im Klartext heißt das: Alles, was die sensiblen und stets betriebsbereiten Mikrofone der Sprachsteuerungssysteme empfangen, könnte prinzipiell via Internetverbindung auf den Servern des Cloud-Dienstes landen. Offiziell lauschen die Mikrofone nur „passiv". Das heißt, die Sprache werde lediglich an den Mikroprozessor im Gerät übermittelt, damit dieser erkennen kann, ob das Gerät angesprochen wird. Erst wenn das jeweilige Schlüsselwort fällt, im Falle von Echo eben standardmäßig „Alexa", werde das Gesagte zur Interpretation an den Cloud-Service geschickt. Nach der Antwort liefe sofort wieder nur die Schlagworterkennung.

Datenschützer warnen eindringlich davor, sich die Lauschboxen ins Haus zu holen, Whistleblower Edward Snowdon hält sie gar in Sachen Datenschutz für ein „Desaster". Was den Einsatz dieser Boxen unter Datenschutzgesichtspunkten so katastrophal macht, sind mindestens drei Dinge. Erstens die Sprache – also sowohl die Stimme als biometrisches Merkmal als auch die Worte und damit der Inhalt des Gesagten, werden zur Auswertung in die Rechenzentren der Anbieter übertragen. Aus Letzterem lassen sich leicht sehr genaue Interessenprofile gewinnen, die eigene Stimme gerät für unbestimmte Nutzung in den Besitz einer fremden Organisation. Zweitens ist es zum Teil nicht transparent nachvollziehbar, wo die Server des Anbieters stehen und was genau dort mit den übertragenen Informationen passiert. Und drittens besitzen die Geräte oft keinen oder unzureichenden Schutz vor Missbrauch. Hacker könnten die Geräte kapern und nach ihren Absichten etwa als hochwertige Abhöranlage umfunktionieren. Zumindest die Punkte zwei und drei gelten prinzipiell für alle smarten Heimanwendungen, die über einen Cloud-Service betrieben werden, umso mehr, wenn der Anbieter außerhalb Europas sitzt. Dazu gehören beispielsweise auch viele Fitnessbänder, Smart Watches, intelligente Waagen, Online-Abnehm-Coaches, E-Zahnbürsten und so weiter. Die Experten von Security-Anbietern beobachten im Zusammenhang mit solchen Fällen einen Trend: „Je mehr smarte Geräte wir in unserem Zuhause einsetzen, desto stärker fokussieren sich die Angreifer auf die Verwaltungsprogramme", so Oded Vanunu, Head of Products Vulnerability Research bei Check Point. „Durch Apps haben die Cyberkriminellen wesentlich mehr Möglichkeiten, Nutzer zu attackieren und persönliche Daten abzufangen." Hersteller von IoT-Geräten seien in der Pflicht, bereits während der Entwicklung der Geräte und der Software wirksame Schutzmechanismen zu integrieren. Hersteller von Smart-Living-Produkten wie beispielsweise eQ-3 ziehen hier etwa die Expertise des VDE-Instituts zurate. Der europäische Marktführer im Bereich umfassender Smart-Home-Lösungen erhielt auf der IFA 2017 das VDE-Zertifikat „Smart Home – Informationssicherheit geprüft" (siehe umseitigen Kasten). „Gerade im Smart-Home-Bereich ist es wichtig, dass die Bürger der Technologie vertrauen. Die Angst ist groß, dass sich Kriminelle Zugang in die eigenen vier Wände per Knopfdruck verschaffen. Mit dem VDE-Zertifikat schaffen wir Vertrauen", erklärt Wolfgang Niedziella, Geschäftsführer des VDE-Instituts.

Wer sichergehen will, achtet auf das VDE-Zertifikat

Für den Nutzer gibt es eine Reihe von Empfehlungen. Grundsätzlich gilt es strikt zu vermeiden, dass IoT-Geräte mit PCs, Laptops oder Speichersystemen gemeinsam im Heimnetzwerk betrieben werden. Das funktioniert etwa über moderne Home-WLAN-Router oder Switches mit Funktionen zur Segmentierung von Netzen. Noch sicherer ist es, für beide Bereiche eigene WLANs aufzubauen. Am einfachsten gelingt das etwa durch den Einsatz einer Home-Firewall. Wie klassische IT-Geräte, sollten auch IoT-Geräte nicht zuletzt aus Sicherheitsgründen softwaretechnisch immer auf dem neuesten Stand gehalten und Updates möglichst rasch nach Veröffentlichung aufgespielt werden. Und wenn es um den Fernzugriff auf Smart-Home-Geräte via Smartphone geht, empfiehlt sich eine sichere VPN-Verbindung.

Zumindest in Sachen Sicherheit lässt sich mit diesen Maßnahmen ein wirksamer Schutz aufbauen. Was die Geräte aber im Rahmen ihrer normalen Nutzung treiben und an Rechten und privaten Informationen einfordern, bleibt auch damit nur bedingt eingrenzbar. Wer ganz sichergehen will, achtet auf das VDE-Zertifikat für den Nachweis der Informationssicherheit.

STEFAN MUTSCHLER
ist freier Journalist mit dem Fachgebiet IT und arbeitet unter anderem für die Publikationen IT-Sicherheit und LANline.

FOTO: SEITE 27: LUMINA IMAGES / FOTOLIA

DIGITALE BILDUNG

Schule 2.0

Einigkeit allerorten: Deutsche Schulen sollen endlich im digitalen Zeitalter ankommen, um Schülerinnen und Schüler auf die Arbeitswelten der Zukunft vorzubereiten. Doch der VDE-Ausschuss „Studium, Beruf und Gesellschaft“ mahnt in sechs Thesen zur Entwicklung von Lehrinhalten in Schulen und Hochschulen, dass es mit einer neuen IT-Ausstattung allein nicht getan ist.

VON **MARTIN SCHMITZ-KUHL**

Dass die Jamaika-Sondierungen im vergangenen November am Ende geplatzt sind, hat an einer Vielzahl von Themen gelegen. An einem aber sicherlich nicht: dem Thema Digitale Bildung. Ähnlich verhält es sich nun bei den GroKo-Gesprächen. Selbst wenn bei Redaktionsschluss das Ergebnis noch nicht feststand, so ist dennoch klar, dass auch diese nicht an der Digitalen Bildung scheitern würden. Denn eines machten alle Parteien von links nach rechts bereits vor der Bundestagswahl deutlich: In Deutschlands Schulen besteht dringend Handlungsbedarf, eine technische Modernisierung hat oberste Priorität. Es sei wichtig, sowohl in die Hard- und Software der Bildungseinrichtungen als auch in deren Internetanbindung zu investieren, wurde unisono gefordert. Und natürlich müsste man auch die Lehrkräfte entsprechend qualifizieren. Was man eben so sagt, vor einer Wahl.

Und nach der Wahl? Um die Parteien an ihre Versprechen zu erinnern, platzierte die Bertelsmann Stiftung bereits im November eine Studie zur IT-Ausstattung an Schulen. „Rund 2,8 Milliarden Euro würden jährlich anfallen, wenn alle Grund- und weiterführenden Schulen mit lernförder-

licher Computertechnik ausgestattet werden“, schreibt die Stiftung. Hinzu kämen die Kosten für die Anbindung der Schulen an die Versorgung mit schnellem Internet und die Weiterbildung der Lehrer. „Die Digitalisierung der Schulen braucht jetzt einen Kraftakt. Bund, Länder und Kommunen müssen sich in der neuen Legislaturperiode zügig darauf verständigen, Schulen beim Lernen mit digitalen Medien dauerhaft und auskömmlich zu unterstützen“, so Dr. Jörg Dräger, Vorstand der Bertelsmann Stiftung.

Zumindest bei den Jamaika-Sondierern waren die Worte auf fruchtbaren Boden gefallen. Schnell hatte man sich darauf geeinigt, bis 2025 mehr als zehn Prozent des Bruttoinlandsprodukts für Bildung aufwenden zu wollen. Weitere 3,5 Prozent sollten in Forschung und Entwicklung investiert werden. So viel zu dem geplatzten Traum. Doch auch wenn zu Redaktionsschluss noch nicht feststand, mit welchen Prozentzahlen die neue Regierung operieren würde, spricht einiges dafür, dass auch diese es sich zur Aufgabe machen wird, „das Land zur führenden Bildungsnation“ machen zu wollen, wie es überall vollmundig heißt.

Sechs gehaltvolle Thesen statt hohler Plattitüden

So oder so ist es Zeit, sich Gedanken zu machen, was das denn konkret heißen könnte. Der VDE-Ausschuss „Studium, Beruf und Gesellschaft“ hat sich mit dieser Frage auseinandergesetzt und hierzu gerade sechs Thesen zur Entwicklung von Lehrinhalten in Schulen und Hochschulen veröffentlicht. Auffällig dabei und für einen Technologieverband vielleicht auch ein wenig ungewöhnlich: Den Mitgliedern ging es explizit um eben diese Lerninhalte. Auf eine allgemeine Forderung nach einer besseren IT-Ausstattung wurde ganz bewusst verzichtet. Nicht, weil man sich dagegen aussprechen würde, sondern weil man sich mit solchen „Plattheiten ohne Neuigkeitswert“, so der Ausschussvorsitzende Prof. Dr. Michael Berger von der Fachhochschule Westküste, gar nicht aufhalten wollte. Auch wollte sich der VDE-Ausschuss ausdrücklich nicht an der allgemeinen Digitalisierungs-Hysterie beteiligen. Die Entwicklung sei weder gänzlich neu, noch – historisch betrachtet – ungewöhnlich dramatisch, heißt es in dem Thesenpapier. Natürlich würden sich die Arbeitswelten der Zukunft ändern. Doch das taten sie schließlich schon in den 1970er-Jahren mit der Markteinführung des Mikroprozessors und des Personal Computers. Und die damit verbundenen Veränderungen – genannt seien hier nur die Einführung von Scanner-Kassen, Automobilelektronik, CNC-Fertigungsmaschinen, Textverarbeitung, und E-Mail in den 1980er-Jahren – würden heute als völlig normal wahrgenommen werden.

»Die Digitale Bildungsrevolution hat bereits begonnen. Wilhelm von Humboldt hätte großen Gefallen an ihr gefunden.«

Dr. Jörg Dräger,
Vorstand der Bertelsmann Stiftung

Um Schüler und Studenten auf die Veränderungen in der Zukunft vorzubereiten, sind dennoch nach Ansicht der Ausschussmitglieder einige Maßnahmen zu ergreifen. Dabei geht es jedoch weniger um Digitale Bildung, sondern um etwas viel Grundsätzlicheres: „Wesentliche Voraussetzungen zum Gelingen der weiteren Digitalisierung der Arbeitswelt in Europa sind Bildung, Demokratie, Stabilität, Rechtsstaatlichkeit und Weltoffenheit“, heißt es im ersten Punkt des VDE-Thesenpapiers. Denn die Gesellschaft von morgen sei auf die nun anstehenden Veränderungen vorzubereiten. Das gelänge nicht, indem man sie nur lehrt, die Maschinen zu bedienen, die sie vielleicht irgendwann ersetzen. Vielmehr sollte man sie in die Lage versetzen, Vorgänge richtig einzuschätzen und zu bewerten. Und es ginge auch darum, den Transformationsprozess seitens der Gesellschaft aktiv mitzugestalten, Regeln durchzusetzen, Härten abzufangen und den sozialen Frieden zu bewahren.

These zwei des Papiers lautet: „Keiner darf zurückbleiben und Leistungsstarke müssen gefördert werden. Unsere Bildungsanstrengungen in den Schulen müssen sich aber vor allem auf das Mittelfeld der Schülerinnen und Schüler konzentrieren, um dort Bildungschancen zu wahren.“ An diesem Punkt, erläutert Prof. Berger, habe es im Ausschuss die meisten Diskussionen gegeben, weil die geforderte Fokussierung auf das Mittelfeld noch nicht genügend wissenschaftlich belegt sei. Aber zum einen sollte das Papier ja auch ausdrücklich nur eine Diskussionsgrundlage sein und wichtige Fragen überhaupt erst einmal anstoßen, und zum anderen sei es dem Ausschuss vor allem wichtig gewesen, darauf hinzuweisen, dass Digitalisierung nicht zu einer sozialen Selektion führen dürfe, zum Beispiel wegen mangelnder Verfügbarkeit von Geräten und Zugängen.

Heißt das, dass der Staat dafür sorgen muss, dass alle Schülerinnen und Schüler ab der ersten Klasse zum

Beispiel mit Tablets ausgestattet werden müssen oder zumindest ein interaktives Whiteboard anstatt einer klassischen Tafel im Klassenraum hängen muss? Nicht unbedingt. So lautet These 3: „Sowohl Computer als auch Werkbänke müssen als Elemente der Arbeits- und Lebenswirklichkeit in den Schulunterricht integriert werden. Sie dienen bei den jüngeren Kindern als Lernangebot, in der Pubertät zur Lernmotivation und bei den jungen Erwachsenen bereits als selbstverständliches Arbeitsmittel.“ Übersetzt heißt das, dass die Digitalisierung selbstverständlich nicht vor der Schule haltmachen kann, das Heranführen an die damit verbundene Technik aber bei Jugendlichen sicherlich drängender ist als bei Grundschülern. Natürlich muss ein Schulabgänger in der Lage sein, mit einem Computer und den gängigen Programmen umzugehen. Ein Schulanfänger dagegen sollte vielleicht erst einmal Rechnen und Schreiben lernen – und mit Smartphone und Co nur Bekanntschaft machen können, aber eben nicht müssen.

Anders dagegen die Studenten. „Alle, die das tertiäre Bildungssystem durchlaufen haben, müssen über Grundkompetenzen der Digitalisierung verfügen und sich selbstständig fortlaufend weiterbilden“, heißt es in Punkt 4 des Thesenpapiers. Von Akademikern darf die Gesellschaft erwarten, dass diese hier eine Vorbildfunktion übernehmen, so die Begründung des Ausschusses. Das heißt auch, dass sie die digitalen Medien und Werkzeuge zu nutzen wissen sollten, unabhängig davon, was ihnen in den Hochschulen vermittelt oder eben noch nicht vermittelt wurde.

Doch ohnehin seien die Inhalte viel wichtiger als das Gerät, mit dem diese vermittelt werden. Dahin zielt auch These 5: „Der angemessene Umgang mit einer Flut zweifelhafter Informationen, mit komplexen Sachzusammenhängen und mit persönlichen Daten muss in einer weiter vernetzten Welt gelebter Bestandteil des Schulalltags werden.“ Denn das Internet bietet hier vor der Digitalisierung nicht gekannte Möglichkeiten, aber auch eben Risiken bis hin zur völligen Desinformation. Und was mit aus Wikipedia zusammenkopierten, aber inhaltlich völlig wirren Hausarbeiten anfängt, kann bei dem Glauben an Fake News und Verschwörungstheorien aufhören. „Es geht darum, Dinge selbstständig erarbeiten, vergleichen und einschätzen zu können“, erklärt der Ausschussvorsitzende Prof. Berger. Und das habe vor allem mit einer guten Allgemeinbildung und entsprechender Medienkompetenz zu tun und weniger mit einer Digitalen Bildung.

»Eine gute Allgemeinbildung ist wichtiger als eine ›Digitale Bildung‹. Auf die Inhalte kommt es an.«

Prof. Dr. Michael Berger,
Vorsitzender des VDE-Ausschusses „Studium, Beruf und Gesellschaft“

(Digitale) Bildung ist eine Lebensaufgabe

Damit zum letzten und sechsten Punkt des Thesenpapiers, der weit über den Fokus „Schule“ hinausgeht. „Auch die Berufstätigen müssen den Wandel meistern können“, heißt es dort. Und weiter: „Dabei ist die kontinuierliche persönliche Weiterentwicklung eine der Säulen einer erfolgreichen Digitalisierung. Berufsbildungseinrichtungen, Akademien und Hochschulen müssen die berufliche Weiterbildung endlich als vollwertige gesellschaftliche Aufgabe übertragen und damit auch finanziert bekommen.“ Die demografische Entwicklung in Europa wird nämlich voraussichtlich dazu führen, dass die Phase der Berufsausbildung und die Phase der Berufsausübung stärker miteinander verschmelzen und Menschen auch mit 60 Jahren noch einmal neu dazulernen müssen, heißt es in der Begründung des Ausschusses. Das hieße aber auch, dass Weiterbildung nicht mehr nur die Privatangelegenheit jedes Einzelnen sein dürfe.

Aber wenn die neue Regierung – wie auch immer sie sich zusammensetzen und wer auch immer Bildungsminister/in werden wird – tatsächlich das Ziel umsetzen will, Deutschland zur führenden Bildungsnation machen zu wollen, wird sie ja für Vorschläge dieser Art vielleicht offen sein. Die Diskussion darüber ist zumindest eröffnet und das ist genau das, was der Ausschuss damit bezweckte. „Die eine oder andere These mag überraschend sein, aber wir wollten auch ganz bewusst etwas querdenken“, sagt Prof. Berger. Digitalisierung sei schließlich kein Selbstzweck. Am Ende sollte sie ja schließlich allen nutzen. Und alle sollten begreifen, dass die damit verbundenen Umwälzungen zwar erheblich seien, aber eben nicht nur eine Gefährdung, sondern auch eine große Chance böten, wenn man sie denn richtig gestalte.

Wie schnell die Stimmung kippen kann, zeigen die Zahlen des aktuellen Bildungsbarometers des Münchener Ifo-Instituts. Demnach sehen sich derzeit 54 Prozent der Befragten als Gewinner der Digitalisierung, aber immerhin 16 Prozent als Verlierer. Es sollten nicht mehr werden.

MARTIN SCHMITZ-KUHL
ist freier Journalist und Autor in Frankfurt am Main sowie Redakteur beim VDE dialog.

MIKROELEKTRONIK

Regie hinter den Kulissen

Ohne Mikroelektronik ist die Digitalisierung nicht denkbar. Mikrosysteme halten durch das Internet der Dinge Einzug in nahezu alle Bereiche. Der VDE hat auf zwei hochkarätig besetzten Veranstaltungen die Mikrosystemtechnikbranche versammelt, um die neuesten Trends und Themen zu beleuchten. Ein Rückblick auf den von VDE und dem Bundesministerium für Bildung und Forschung gemeinsam organisierten MikroSystemTechnik Kongress in München und das VDE/ZVEI Symposium Mikroelektronik in Berlin.

MikroSystemTechnik Kongress, *München*

Die Karten werden neu gemischt

Der MikroSystemTechnik Kongress ist der größte Branchentreff im Bereich Elektronik- und Mikrosysteme im deutschsprachigen Raum. Ende Oktober 2017 informierten sich dort rund 800 Teilnehmer über die neuesten Trends aus Bereichen wie Mikro-Nano-Integration, innovative Materialien und Technologien sowie Aufbau- und Verbindungstechnik. Auch im Fokus waren aufkommende Themen wie RF-MEMS, chemische Sensorik und Biosensorik.

Mikrosysteme, darüber herrschte Einigkeit, werden künftig zunehmend hinter den Kulissen Regie führen. „Die Vielfalt an Anwendungen wird weiter rasant zunehmen und der Beruf des Mikrotechnologen noch vielfältiger und spannender werden“, erklärte 1 Tagungsleiter Prof. Dr. Christoph Kutter, Direktor der Fraunhofer-Einrichtung für Mikrosysteme und Festkörper-Technologien EMFT (rechts, im Bild mit Dr. Reinhard Ploss, VDE-Präsidiumsmitglied und Vorstandsvorsitzender der Infineon Technologies AG).

Bei der Eröffnung des Kongresses forderten 2 Staatsminister a. D. Erwin Huber und 3 VDE-Präsident Dr. Gunther Kegel, die Mikroelektronik nicht aus der Hand zu geben. Durch die Digitalisierung würden die Karten auf dem internationalen Parkett neu gemischt. „Ohne wettbewerbsfähige Mikroelektronik-Industrie werden wir abhängig und zum Importeur von Schlüsseltechnologien“, warnte Kegel in seiner Keynote.

4

5

6

INVENT a CHIP: Die Spezialisten von morgen

Bereits zum 16. Mal veranstalteten das Bundesministerium für Bildung und Forschung (BMBF) und der VDE den weltweit einmaligen Wettbewerb INVENT a CHIP (IaC), der jährlich bundesweit mit über 3000 Schulen durchgeführt wird. 2017 fand die **4** IaC-Siegerehrung im Rahmen des MikroSystemTechnik Kongresses statt.

5 Die Bandbreite der von Schülern entwickelten Mikrochips war auch diesmal enorm groß. Stolz präsentierten die Zweitplatzierten vom Gymnasium Lindlar ihre intelligente Krankenliege, die Schwerverletzte schonend im Rettungswagen transportiert.

6 Prof. Dr. Wolf-Dieter Lukas (unten rechts) vom BMBF zeigte sich begeistert von den guten Ideen und dem versierten Umgang des Techniknachwuchses mit digitalen Technologien. Den mit 3000 Euro dotierten ersten Platz sicherte sich der 18-jährige Philipp Grube (oben rechts und unten links) für sein chipgesteuertes Zukunfts-WC.

Alle Preisträger und prämierten Projekte finden Sie unter:
www.invent-a-chip.de

Rohstoff der digitalen Zukunft

1 Treffen der Halbleiterszene: Über 200 Experten aus Wirtschaft, Wissenschaft und der Politik kamen Anfang November 2017 in die Akademie der Wissenschaften zum 7. VDE/ZVEI Symposium „Mikroelektronik für die digitale Zukunft“.

Im Zentrum der Diskussionen stand die Frage: Was muss Europa tun, um den Wettlauf um die digitale Zukunft mitzubestimmen? Klar ist: Die Zeit drängt. Denn Big Data wird zum Rohstoff neuer Geschäftsmodelle. Und hier sind bekanntlich die US-Amerikaner besser. Die automatische Generierung, die Verarbeitung und der Austausch dieser Daten erfolgt im Internet der Dinge zwischen den Objekten. Die technologische Basis dafür bilden: Mikroelektronik, Sensoren und „embedded systems“, 5G und Cyber Security. Und da ist Deutschland noch marktführend. Ein Hoffnungsschimmer, immerhin, aber reicht das zukünftig aus?

1

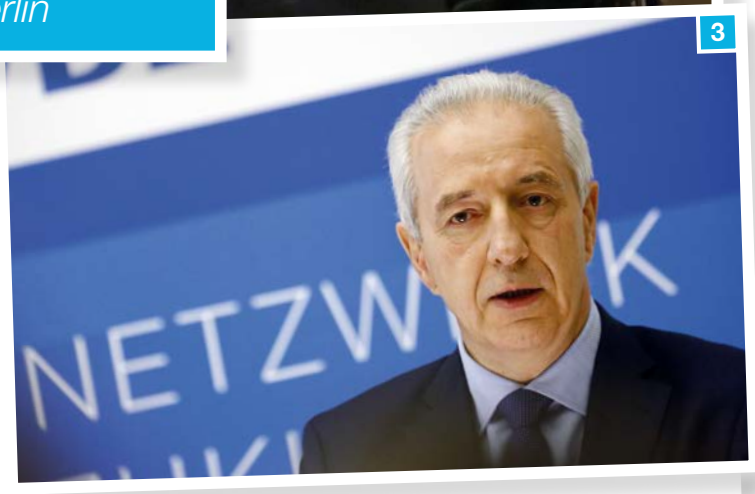
VDE /ZVEI Symposium Mikroelektronik,

2

Mehr Tempo!

„Die Mikroelektronik ist das Nervensystem der Digitalisierung, sie ist systemrelevant“, betonte VDE-Präsident Gunther Kegel. An die Politik – unter den Anwesenden 2 Prof. Dr. Wolf-Dieter Lukas vom BMBF – richtete er daher den Appell, die Rahmenbedingungen für Unternehmen und Forschungseinrichtungen zu verbessern und mehr in Bildung zu investieren. Und zwar jetzt. „Wir müssen ein höheres Tempo bei Innovationen anschlagen, mehr in Hochschulen und Forschung investieren“, pflichtete ZVEI-Präsident Michael Ziesemer Kegel bei.

Berlin



3

Fast wie im Silicon Valley

3 Stanislaw Tillich, Ministerpräsident von Sachsen, umriss nicht ohne Stolz die Erfolge, die Sachsen bereits vorzuweisen hat. „Noch vor einigen Jahren hätte keiner gedacht, dass sich die Chipindustrie mit Infineon, Globalfoundries und Bosch in Dresden konzentrieren wird. Oder dass wir 5G weltweit vorantreiben werden. Seit 1990 setzt Sachsen auf seine Hochschulen und das zahlt sich jetzt aus. Unser Ziel war es immer, mindestens mit Asien und den USA mitzuhalten“, so der Ministerpräsident. Gemeinsam mit dem Wirtschafts- und Forschungsministerium und der Europäischen Kommission etablierte er Dresden zum Halbleiter-Hub mit wertvollen Synergien. In Leipzig und Dresden entstehe gerade eine Start-up-Szene, die sich mit München messen ließe. Wenn auch noch nicht mit dem Silicon Valley.

Der Algorithmus der Ameisen

Nicht immer ist das Silicon Valley die Messlatte in Sachen Innovationen. Das bewies der „Exot“ des Symposiums, 4 Prof. Dr. Martin Wikelski (r.), Geschäftsführender Direktor des Max-Planck-Instituts für Ornithologie in Pöcking, der selbstbewusst behauptete: Was Big Data angeht, kann Pöcking bei Starnberg in Oberbayern mit Kalifornien mithalten! „Wir stehen kurz vor dem Durchbruch zu verstehen, wie die Welt funktioniert. Wir haben Big Data – die Big Data der Tiere“, so Wikelski. Und das dank der Mikroelektronik.

Das Max-Planck-Institut für Ornithologie hat bereits weltweit Hunderttausende von Tieren mit Chips ausgestattet. „Mithilfe dieser Chips zapfen wir die Intelligenz der Tiere und ihren sogenannten sechsten Sinn an“, so Wikelski. Sein Institut sammelt und wertet die Daten aus. Am Beispiel von Ameisen zeigte er auf, wie daraus Rückschlüsse für das autonome Fahren gezogen werden: „In den tropischen Regenwäldern sind Millionen von Ameisenstraßen. Die Ameisen bauen keine Unfälle. Über ihren sechsten Sinn regeln sie den Verkehr. Anhand ihrer Intelligenz und ihres Verhaltens auf den Ameisenstraßen leiten wir Algorithmen für autonomes Fahren ab.“

4

FOTOS: SEITE 30/31: VDE/MICHAELA HANDREK-REHLE; SEITE 32/33: HANNIBAL/VDE; EMER/FOTOLIA (R.)

PHOTOVOLTAIK & CO.

Am Wendepunkt

Erneuerbare Energien im Allgemeinen und Photovoltaik im Besonderen überraschen mit hohen Zuwächsen. Jetzt kommt es auf neue Energiespeicher und digitale Energiemanagementsysteme an. Und auf entsprechende Standards und Bewertungskriterien. Die VDE Renewables leisten auf diesem Gebiet international Pionierarbeit.

VON **MARTIN SCHMITZ-KUHL**

„Noch eine Veranstaltung zur Energiewende?“, fragte die Energietechnische Gesellschaft (ETG) im VDE in ihrer Einladung zum großen Kongress Ende November 2017 in Bonn. Dabei war die Frage natürlich nur rhetorisch gemeint, die Antwort war ein selbstbewusstes Ja!

Das wundert nicht, denn die Themen Energiewende und Erneuerbare Energien sind aktueller denn je. Und nicht nur in Deutschland, auch in anderen Ländern wird die Stromversorgung immer „grüner“. Der Grund dafür ist nicht zuletzt, dass erneuerbare Energien zunehmend konkurrenzfähig sind. Bereits heute sind Sonne und Windkraft vielerorts sogar die günstigere Stromalternative. So werden in Abu Dhabi und Dubai, aber auch zum Beispiel in Chile gerade Solarfelder konzipiert, deren Strom noch nicht einmal drei Cent pro Kilowattstunde kosten wird. Weder Kohle- und Gaskraftwerke noch Atomreaktoren können da mithalten.

Der Zuwachs im Bereich erneuerbarer Energien ist enorm. So erwartet die Internationale Energieagentur (IEA) für das abgelaufene Jahr einen weiteren Anstieg um zwölf Prozent. Bis 2022, so steht es in ihrem Bericht „Renewables 2017“, soll der Beitrag

der Erneuerbaren zur Stromerzeugung um mehr als ein Drittel auf über 8000 Terawattstunden ansteigen – dies entspräche dem summierten Gesamtverbrauch von China, Indien und Deutschland! Und damit würde die Erneuerbaren-Erzeugung doppelt so schnell ansteigen wie die von Gas und Kohle zusammen.

Besonders interessant in diesem Zusammenhang: das Wachstum bei der Photovoltaik. Diese habe im vergangenen Jahr alle Erwartungen übertroffen, so die IEA. Erstmals sei sie stärker als alle anderen Energiequellen gewachsen. „Wir sind Zeuge der Geburt einer neuen Ära für die Photovoltaik“, schwärmte Fatih Birol, Direktor der IEA, bei der Vorstellung des Berichts. Allein: Die Erkenntnis kommt nach Meinung vieler Fachleute reichlich spät. Von einem „jahrelang währenden Dornröschenschlaf“ spricht gar manch ein Kritiker, aus der die Organisation nun endlich erwacht sei. So hätte die traditionell als eher atomfreundlich geltende Internationale Energieagentur ebenso wie der Weltklimarat IPCC das Wachstumspotenzial der Erneuerbaren im Allgemeinen und das der Photovoltaik im Besonderen bislang stets unterschätzt. Und das wäre durchaus nicht folgenlos geblieben. Denn viele Volkswirte würden sich an den Aussagen dieser beiden Organisationen orientieren und hätten sich im Zweifelsfall dann eben mit ihrem Engagement etwas zurückgehalten.

Die Bankability gilt als wichtiger Schlüsselfaktor

Dies zu ändern ist nicht zuletzt das Anliegen der VDE Renewables GmbH. Damit Investoren, Banken und Versicherungen auf erneuerbare Energien setzen und ihr Vertrauen entgegenbringen, kommt es neben den zu erwartenden Wachstumspotenzialen jedoch auch darauf an, dass man den Anwendungen selbst vertrauen kann. Bankability, Investability und Insurability gelten dabei weltweit als die entscheidenden Schlüsselfaktoren. Denn nach der Finanzkrise 2008/2009 sind Kapitalgeber noch vorsichtiger geworden, wenn es darum geht, Investitionsentscheidungen zu treffen. Ähnliches gilt für Versicherungen. Auch sie wollen nicht die „Katze im Sack“ kaufen, respektive versichern. Deshalb unterstützt VDE Renewables die gesamte Branche der erneuerbaren Energien bei der Erreichung von bestimmten Kriterien von Finanzorganisationen und der Versicherungsbranche. Dabei sind an den jeweiligen Bedarf angepasste Qualitäts-Zertifikate entstanden. Sie gehen über die internationalen Standards hinaus und beschreiben verlässlich die Vertrauenswürdigkeit und Stabilität eines Unternehmens (siehe auch Interview auf der nächsten Seite).

Die Geschäftspotenziale und Herausforderungen der Branche standen auch im Fokus des Asia Clean Energy Summit, der Ende Oktober 2017 in Singapur stattfand. Der Kongress gilt als die führende Veranstaltung in diesem Bereich und als Plattform für Experten aus Finanzwirtschaft, Industrie, Forschung und Politik. Zwei der sechs Tracks wurden dabei von VDE Renewables in Partnerschaft mit der Sustainable Energy Association of Singapore organisiert: zum einen der „Financial Summit“ und zum anderen der Track „Digital Transformation of Energy“. „Wir haben uns sehr gefreut, bereits zum siebten Mal Partner des Kongresses zu sein“, erklärt Burkhard Holder, Geschäftsführer der VDE Renewables. „Gerade die beiden von uns organisierten Tracks helfen uns, kontinuierliches Feedback zu erhalten. Das brauchen wir, um die Kriterien für die erneuerbaren Energien weiter zu entwickeln und auszubauen.“

Auf dem Kongress wurde zudem das Global Energy Storage Competence Cluster (GECC) vorgestellt. Zusammen mit ihren Partnern, dem Fraunhofer-Institut für Solare Energiesysteme ISE und dem Energy Research Institute der Nanyang Technological University, kommen die VDE Renewables damit dem Ziel ein gutes Stück näher, ihr Test- und Zertifizierungs-Produktportfolio für Energiespeicherprodukte und -systeme auf internationaler Ebene auszuweiten. Das ist auch nötig. Denn die Nachfrage nach Batterien sowie nach stationären und mobilen Speichern wird weltweit weiter steigen. Und damit verbunden ist eben auch der Bedarf

INFORMATION

»From Grid to Bit«

Unter dem Titel „From Grid to Bit: Key factors for enabling the sustainable growth of the smart grid“ hielt VDE-Vorstandsvorsitzender Ansgar Hinz anlässlich des Asia Clean Energy Summits in Singapur eine Keynote. In seinem Vortrag* beantwortete er die Fragen: Was sind die Treiber der Digitalisierung und Dezentralisierung? Und welches sind die Erfolgsfaktoren für die Weiterentwicklung der Stromnetze?

* Der Vortrag wurde vorab im VDE-Institut in englischer Sprache aufgezeichnet. Zum Abspielen des Videos folgen Sie dem Link oder scannen den unten stehenden QR-Code ein.

www.vde.com/topics-de/energy/erneuerbare-energien-weltweit

FOTOS: SEITE 34: YANGPHOTO/FOTOLIA; SEITE 35: HANNIBAL/VDE

VDE RENEWABLES

»Wir müssen miteinander reden!«

Die VDE Renewables GmbH bietet Qualitätssicherung, Zertifizierung und Bankability-Dienstleistungen für erneuerbare Energien weltweit. Was darunter zu verstehen ist, erklärt Geschäftsführer Burkhard Holder.

BURKHARD HOLDER,
Geschäftsführer
VDE Renewables GmbH

Herr Holder, die VDE Renewables GmbH ist die jüngste Tochter der VDE-Familie. Was machen Sie eigentlich genau?
Wir sind 2016 aus dem VDE-Institut hervorgegangen. Ziel war, dass wir als kommerzielle Gesellschaft das ganze Thema „Erneuerbare Energien" beim VDE zentral bearbeiten. Begonnen haben wir mit der Photovoltaik, von der einzelnen Komponente bis hin zu Gesamtsystemen. Und seit etwa einem halben Jahr haben wir zudem die Windenergie im Portfolio. In Zukunft werden wir es allerdings auch mehr mit Fragen rund um die Speichertechnologien zu tun haben. Also einerseits der Einbindung des Stroms in die Energienetze der Zukunft – Stichwort: Grid-Codes – und andererseits mit autonomen Systemen, die gar nicht an das Energienetz angeschlossen sind – Stichwort Mini-Grids.

Wie viele Leute arbeiten inzwischen für Sie?
Wir haben mit zehn Mitarbeitern hier im bayerischen Alzenau angefangen. Jetzt sind wir 16 Mitarbeiter – mit steigender Tendenz. Daneben haben wir ein weltweites Netzwerk mit Mitarbeitern in China, Japan, Korea, Singapur aber auch in den USA, sodass insgesamt rund 40 Leute für uns arbeiten.

Warum in Alzenau?
Wir haben hier zusammen mit der Fraunhofer-Gesellschaft eine Plattform für das Thema „Recycling von Erneuerbaren Energiesystemen" gegründet. Fraunhofer investiert in diesen Bereich in den nächsten Jahren mehr als 100 Millionen Euro für Forschungsprojekte und Laborinfrastruktur. Dieses Thema ist extrem wichtig – aus betriebswirtschaftlichen Gründen, aber auch aus Gründen des Umweltschutzes. Denn schließlich werden ja nicht nur immer mehr Systeme installiert, sondern gleichzeitig werden wir immer mehr deinstallieren müssen, weil sich ihre Lebenszeit dem Ende nähert. Dafür brauchen wir vernünftige Lösungen.

Auch in dem neuen Labor in Singapur arbeiten Sie mit Fraunhofer zusammen. Wie sieht Ihre Arbeitsteilung aus?
Mit Fraunhofer steht uns ein technischer Kompetenzpartner zur Seite, der eine international führende Forschungseinrichtung im Bereich der erneuerbaren Energien ist. Wir bringen unsere Kompetenzen in Sachen Standardisierung und Zertifizierung ein und gemeinsam können wir so viel erreichen. Über die globale Plattform, die der VDE in den letzten sieben Jahren aufgebaut hat, können wir so mehr als 2000 Banken, Versicherungen und Marktaufsichten zusammenbringen, die diesen Ansatz sehr zu schätzen wissen. Und die uns bei der Zertifizierung und Sicherstellung von Bankability und Insurability auch sehr vertrauen.

Was heißt das denn genau? Ist das eine technische Prüfung – also, dass Sie zum Beispiel schauen, ob bei einer Photovoltaik-Anlage an Strom hinten rauskommt, was der Anbieter verspricht? Oder handelt es sich auch um eine betriebswirtschaftliche Prüfung?
Wir machen beides. Allerdings übernimmt die Finanzüberprüfung dann eher ein Partner aus dem Finanz- und Versicherungswesen. Insgesamt geht es darum, ein Renewables-Produkt oder -System quasi auf Herz und Nieren zu prüfen. Dafür gibt es zwar die internationalen Standards. Die sind natürlich sehr wichtig, und der VDE mit seiner Standardisierungsorganisation DKE ist in diesem Bereich ja auch sehr aktiv. Oft reichen diese Standards aber trotzdem nicht aus. Und deshalb haben wir auf diese Standards eben noch Tests und Kriterien aufgesockelt, die an die Bedürfnisse der Banken, Ratingagenturen und Versicherungen angepasst sind.

»Die Kriterien und Standards werden in unseren globalen Plattformen definiert.«

Wie entwickeln Sie die?
Wir definieren sie gemeinsam in der eben erwähnten Plattform, dem sogenannten VDE Financial Dialogue. Wenn wir dann nach diesen gemeinsam beschlossenen Kriterien eine Anlage zertifizieren, ist es sehr viel einfacher, dafür eine Finanzierung zu bekommen. Und auch die Versicherung wird dadurch deutlich günstiger, weil sich unser Partner – zum Beispiel die Allianz oder die Münchener Rück – darauf verlassen kann, dass das jeweilige System oder Produkt etwas taugt.

Das heißt, am Anfang steht immer der Dialog?
Unbedingt! Darum geht es uns auch bei dem Global Energy Storage Competence Cluster, das wir Ende Oktober in Singapur vorgestellt haben. Denn das miteinander Reden und Netzwerken ist extrem wichtig. Gerade wenn es sich um neue Technologien handelt, bei denen es noch nicht so viele Erfahrungswerte und letztlich auch noch nicht so viele Experten gibt. Da geht es um Kompetenzaufbau, gemeinsame Standards und den Austausch von Erfahrungen, also „best practices" und „lessons learned". Dies brauchen wir dringend, und all das geht nur durch Kooperation und Dialog.

Anfang November 2017 eröffnete die VDE Renewables GmbH zusammen mit dem Fraunhofer-Institut für Solare Energiesysteme ISE in Singapur ein Testlabor. Zeitgleich hat auch das Global Energy Storage Competence Cluster (GECC) die Arbeit aufgenommen.

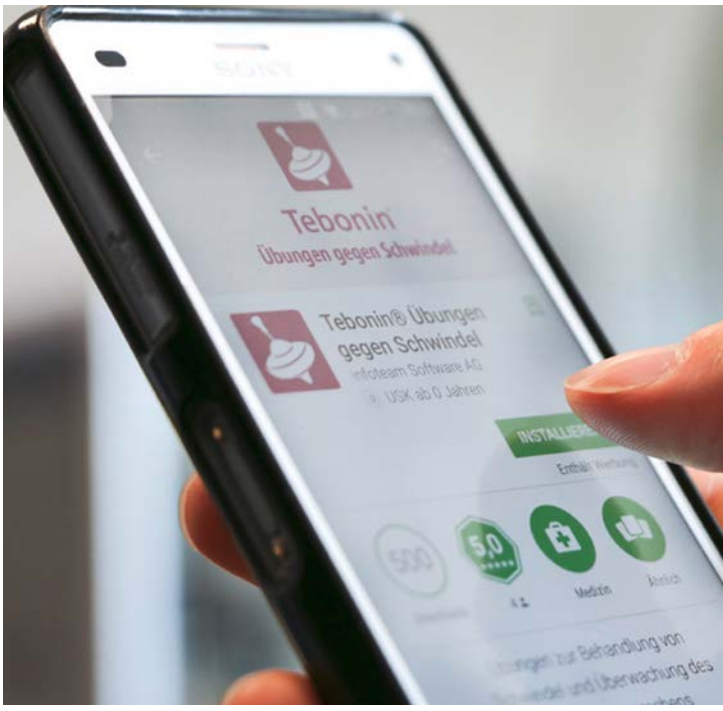
an der Weiterentwicklung unabhängiger, entwicklungsbegleitender Qualitäts- und Sicherheitsprüfungen sowie die Etablierung internationaler Zertifizierungen. „Das Cluster mit seinem regionalen Hub in Singapur ist ein weiterer Meilenstein in unserer Erfolgsgeschichte, maßgeschneiderte Lösungen anzubieten, die die Finanzierung und Versicherbarkeit von Produkten und Systemen im Energiebereich unterstützen“, freut sich auch Ansgar Hinz, Vorstandsvorsitzender des VDE (siehe Link/QR-Code auf Seite 35).

Nächste Herausforderung: Mikro- und Mini-Grids

Was das Engagement der VDE Renewables perspektivisch bedeuten kann, wurde indes am Rande der Veranstaltung in Singapur deutlich. Dort nämlich unterzeichnete die VDE-Tochter ein Memorandum of Understanding mit dem Energy Research Institute. Dabei geht es um das Mikro-Grid-Demonstrationsprojekt „Renewable Energy Integration Demonstrator – Singapore“ (REIDS). Dieses steht auf einer Insel, auf der noch vor wenigen Jahren Müll abgeladen wurde. Doch inzwischen entsteht hier gerade eine große Testplattform, in der verschiedene Mikronetze – also komplett abgeschlossene Einheiten, die autonom erneuerbare Energie erzeugen und eben nicht an das Stromnetz angeschlossen sind – getestet werden. Damit verbunden ist ein riesiger Markt. Denn allein Indonesien, die Philippinen und Thailand haben zusammen mehr als 24.000 Inseln. Rund 100 Millionen Menschen leben dort ohne Energieversorgung, weite Teile dieser Staaten werden von kleinen Diesel-Grids versorgt. Doch nicht nur für Inseln sind solche autonomen Energiesysteme zukunftsweisend. Auch auf dem Festland und selbst in Industrieländern wie Deutschland gibt es zahlreiche Anwendungsfelder.

Noch ist das alles zwar Zukunftsmusik, doch die Zukunft ist nah. So sind die REIDS-Grids schon weit entwickelt und stehen kurz vor der Kommerzialisierung durch große Konzerne wie Rolls-Royce oder Schneider Electric. Doch bevor diese Systeme in Serie gehen, müssen zunächst noch Test- und Qualitätssicherungsprogramme entwickelt werden. Und hier kommt eben wieder VDE Renewables ins Spiel, die mit ihrem neuen Singapur Lab in der Region bestens aufgestellt ist. Und damit zurück nach Deutschland, zum ETG-Kongress „Die Energiewende geht weiter“. Auf diesem stellte VDE-Präsident Dr. Gunther Kegel zur Eröffnung seine eigene Vision von „Smart Energy, Smart Grid, Smart Meter & Co. Made in Germany“ vor. Diese solle zur „Blaupause für einen globalen Paradigmenwechsel in der Energieversorgung“ und unsere Industrie zum weltweiten Systemanbieter für die Integration erneuerbarer Energien und Elektromobilität, für Sektorkopplung, Versorgungssicherheit und Cyber Security werden, so Kegel. Zumindest in Singapur scheint seine Vision schon Wirklichkeit zu werden.

MARTIN SCHMITZ-KUHL
ist freier Journalist und Autor in Frankfurt am Main sowie Redakteur beim VDE dialog.



1

WISSENSCHAFTSJAHR 2018

Arbeitswelten der Zukunft

Arbeit und Arbeiten verändern sich so rasant wie nie zuvor. Menschen, Maschinen, Anlagen, Logistik und Produkte kommunizieren direkt miteinander. Neue Arbeitswelten entstehen. Bei der Gestaltung dieser neuen Arbeitswelten leisten Wissenschaft und Forschung einen wesentlichen Beitrag. Diesen so konkret und anschaulich wie möglich darzustellen – darum geht es im Wissenschaftsjahr 2018 – Arbeitswelten der Zukunft. Der VDE unterstützt die Initiative als Partner mit zahlreichen Veranstaltungen, darunter der VDE Tec Summit 2018.

Thematisch steht die Frage nach Reichweite und Tiefe der Veränderungen in der Arbeitswelt im Mittelpunkt des Wissenschaftsjahres 2018. Zentral ist die Frage, welchen Einfluss der Einzelne auf den Veränderungsprozess nehmen kann, nach dem Motto: „Nicht die digitale Vernetzung lenkt uns, sondern umgekehrt". Dabei geht es um die Auswirkungen technischer Innovationen genauso wie um ökonomische und soziale Einflüsse neuer Technologien. Eine deutliche Mehrheit der Menschen in Deutschland ist sich bewusst über die bevorstehenden Veränderungen. Dies ergab eine repräsentative Befragung im Auftrag des Bundesministeriums für Bildung und Forschung. Demnach gaben 90 Prozent der Befragten an, es sei in Zukunft unerlässlich für den beruflichen Erfolg, sich ständig weiterzubilden. Und bereits 75 Prozent rechnen mit einer spürbaren Veränderung der Arbeitswelt.

1

STROMAUSFÄLLE

Aufwand steigt

Das Forum Netztechnik Netzbetrieb im VDE (VDE|FNN) konnte in seiner Störungs- und Verfügbarkeitsstatistik 2016 eine Rekordzahl melden: Nur 11,5 Minuten Stromausfall im letzten Jahr, eine Steigerung von vier Sekunden zu 2015. Werden Fälle höherer Gewalt berücksichtigt, betrug die durchschnittliche Unterbrechungsdauer pro Stromkunde im Jahr 2016 12,1 Minuten (2015: 15,3 Minuten). Ereignisse höherer Gewalt waren im vergangenen Jahr vor allem die durch starke Regenfälle in Süddeutschland verursachten Hochwasser Ende Mai und Anfang Juni. Die Häufigkeit der Versorgungsunterbrechung pro Stromkunde lag 2016 inklusive der auf höhere Gewalt zurückgeführten Ereignisse bei 0,24 Ausfällen (2015: 0,29). Konkret heißt das: Ein Kunde muss durchschnittlich nur alle vier Jahre mit einem Ausfall rechnen. Dies ist neben günstigen Wetterbedingungen vor allem auf den steigenden Aufwand der Netzbetreiber zurückzuführen, unser Stromnetz stabil zu halten. Stromnetze werden immer häufiger an ihren Grenzen betrieben, weil der Ausbau der erneuerbaren Energien – insbesondere der Offshore-Windenergie – eine stärkere Netzauslastung verursacht. Die Netzbetreiber müssen immer häufiger Redispatch-Maßnahmen ergreifen, das heißt, sie passen die Einspeisung von Kraftwerksleistung an. Außerdem regeln sie die Einspeisung von Erneuerbare-Energien-Anlagen ab.

Für die Anpassung von konventionellen Kraftwerken haben die Netzbetreiber im vergangenen Jahr 219 Millionen Euro an Entschä-

Jetzt bewerben!

Deadlines zur Einreichung folgender Preise:

31.01.2018
Klee-Preis der Deutschen Gesellschaft für Biomedizinische Technik im VDE
www.vde.com/klee-preis

02.06.2018
Preis für Patientensicherheit der Deutschen Gesellschaft für Biomedizinische Technik im VDE
www.dgbmt.de/patientensicherheit

digungen gezahlt (2015: 412 Mio. Euro). Die Entschädigungen für Erneuerbare-Energien-Anlagen schlugen 2016 mit 373 Mio. Euro zu Buche (2015: 478 Mio. Euro). Um eine zuverlässige Stromversorgung zu gewährleisten, muss das Netz weiterentwickelt und – wo nötig – ausgebaut werden, so die Forderung des VDE.

MEDIZINISCHE SOFTWARE 2

Leitfaden für Marktzugang

Medizinische Software in Form eines eigenständigen Produktes wie eine Smartphone App oder als integraler Bestandteil eines Medizinprodukts unterstützen Ärzte in der Diagnostik und Therapie. Das Problem: Schon bei der Produktentwicklung müssen Hersteller komplexe Anforderungen für rechtskonforme und damit marktfähige Produkte berücksichtigen. Um Start-ups und mittelständischen Herstellern von medizinischer Software Orientierung zu bieten, haben die Experten der Deutschen Gesellschaft für Biomedizinische Technik im VDE (VDE|DGBMT) zur Medica 2017 die Publikation „Entwicklung und Herstellung medizinischer Software“ herausgegeben. Neben Best-Practice-Empfehlungen gibt der Wegweiser auch einen Ausblick auf künftige rechtliche Verschärfungen im neuen europäischen Rechtsrahmen und dient als Kompass zur Orientierung im „Anforderungs-Dschungel“.

Die Autoren beschreiben alle relevanten Normen mit ihren wesentlichen Inhalten und geben Tipps zur Anwendung. Ausgehend von der Produktidee starten die Vorentwicklungsaktivitäten mit der Erstellung des technologischen Konzepts und ersten Überlegungen zur regulatorischen Strategie. Die nachfolgende Entwicklung berücksichtigt möglichst frühzeitig alle gesetzlichen und normativen Anforderungen. Dabei werden die notwendigen regulatorischen Aktivitäten entlang des Entwicklungsprozesses praxisorientiert dargestellt. Denn: „Ziel des Leitfadens ist, Mitarbeitern aus Unternehmensbereichen, die sich nicht schwerpunktmäßig mit den gesetzlichen Anforderungen und den einschlägigen Normeninhalten beschäftigen, einen praxisorientierten Einstieg in diese Thematik zu vermitteln“, so die Autoren.

BLITZSCHUTZ 3

Höchste Auszeichnungen

Bei der 12. Blitzschutztagung des VDE-Ausschusses Blitzschutz und Blitzforschung am neuen Tagungsstandort in Aschaffenburg verlieh der Ausschuss seine zwei höchsten Auszeichnungen. Die Benjamin-Franklin-Medaille ging an Dr. Wolfgang Zischank von der Universität der Bundeswehr München für seine Verdienste in der Blitzforschung sowie seine Forschungsergebnisse, die maßgeblichen Einfluss auf die nationale und internationale elektrotechnische Normung hatten.

Die zweithöchste Auszeichnung für herausragendes Engagement für den Blitzschutz, die Goldene Ehrennadel, erhielt Wolfgang Heuhsen für den VDE-Kindercomic „Donner-Wetter!“. Sein Comic klärt Kinder und Jugendliche über die Gefahren von Blitz und Donner und das richtige Verhalten bei Gewitter auf. Zudem erstellte Heuhsen eine jährliche Blitzunfallstatistik.

1 2

MINI-PV-ANLAGEN 1

Weg für sicheren Betrieb gebahnt

Was lange währt, wird endlich gut! Nun ist sie da, die Vornorm für steckbare Photovoltaikmodule. Der VDE hatte Experten zur Einreichung von Kommentaren des Normentwurfs aufgerufen und anschließend zur offiziellen Einspruchsberatung im Vorfeld der Messe Intersolar in München an einen runden Tisch geladen. Gefolgt waren Vertreter der Deutschen Gesellschaft für Sonnenenergie (DGS), des Elektrohandwerks, der Versicherungswirtschaft, der Komponentenhersteller, der Netzbetreiber sowie Vertreter der wissenschaftlichen Institute. Alle hatten sie ein Ziel: Den steckbaren „Mini-PV-Anlagen“ den Weg auf Deutschlands Balkone zu ebnen und gemeinsam die Anforderungen zu identifizieren, unter denen steckbare Photovoltaikmodule ohne Einschränkungen beim Thema Sicherheit betrieben werden können – zunächst auf nationaler, dann auf europäischer und schließlich auch auf internationaler Ebene. Mehr als 300 Kommentare zum Entwurf DIN VDE 0100-551-1 (VDE 0100-551-1):2016-09 waren im Vorfeld bei der VDE-Normungsorganisation DKE eingegangen. Diese galt es zu diskutieren und auszuwerten.

Zu dem Ergebnis der offiziellen Einspruchsberatung, das an alle Beteiligten ging, wurden erneut Kommentare eingereicht. Diese konnten in einer weiteren Gesprächsrunde geklärt werden. Somit steht der Veröffentlichung einer Nationalen Vornorm DIN VDE V 0100-551-1 (VDE V 0100-551-1), die auch in die europäische und internationale Normung eingebracht werden soll, nichts mehr im Weg. Der nächste Schritt wird die Fertigstellung der Produktnorm sein, um die Anforderungen an die anzuschließenden steckbaren Photovoltaikmodule festzulegen. Als dritte Säule neben den Anforderungen an die Errichtung sowie an das Produkt selbst arbeiten die VDE-Experten aktuell an der Veröffentlichung eines Standards zu einer speziellen Energiesteckvorrichtung für die Einspeisung in einem separaten Stromkreis, der ebenfalls kurz vor der Fertigstellung steht.

Die auch als „Balkon-PV“ oder „Plug-in-PV“ bekannten steckbaren Photovoltaikmodule sind für Privathaushalte von großem Nutzen: Sie ermöglichen auch Mietern, den selbst erzeugten Strom direkt zu nutzen. Um die Geräte ohne Sicherheitslücken schnell auf die Balkone zu bringen, hat der VDE bereits 2016 die Normungsinitiative für Plug-in-PVs gestartet.

VDE RENEWABLES 2

Globaler Austausch

Auf dem Asia Clean Energy Summit in Singapur Ende Oktober 2017 wurde in Anwesenheit des Industrie- und Handelsministers Dr. Koh Poh Koon (4. v. l.) die Einführung des Global Energy Storage Competence Cluster (GECC) beschlossen. Unterzeichner der Vereinbarung waren (v. l. n. r.) der Geschäftsführer der VDE Renewables, Burkhard Holder, Dr. Matthias Vetter vom Fraunhofer ISE, der VDE-Vorstandsvorsitzende Ansgar Hinz sowie Prof. Choo Fook Hoong von der Nanyang Technological University Singapore (2. v. r.). Der neu aufgesetzte globale Wissensaustausch soll für eine kontinuierliche

3

Verbesserung der Qualitäts- und Prüfkriterien sorgen. „Um ein sicheres und nachhaltiges Wachstum des Energiespeicher-Marktes zu ermöglichen, werden wir unsere langjährigen Erfahrungen und unser Know-how in der Bankability-Zertifizierung nutzen und zusätzliche Leistungen abdecken, die weit über etablierte Sicherheitsstandards hinausgehen“, so VDE-CEO Ansgar Hinz.

PROJEKTSTART

HARBSAFE

Nur wer die gleiche Sprache spricht, versteht sich. Ist in der Normung ein und derselbe Begriff in verschiedenen Anwendungsfällen unterschiedlich definiert, kann dies zu erheblichen Problemen führen. Hier setzt das vom Bundesministerium für Wirtschaft und Energie geförderte Verbundprojekt HARBSAFE von DKE und TU Braunschweig zur Harmonisierung unterschiedlicher Begriffsverständnisse in den Bereichen IT-Sicherheit, funktionale Sicherheit und Zuverlässigkeit für kritische Infrastrukturen an.

DKE

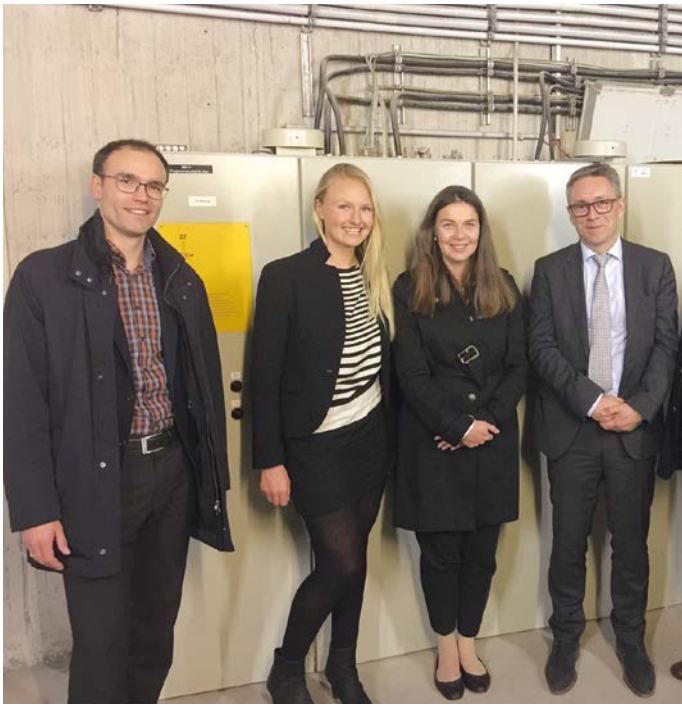
Auf Zukunft getrimmt

3

Cyber Security, E-Mobility, Industrie 4.0 – die Technologien wandeln sich rasant, sie werden vernetzter und komplexer. Damit ändern sich auch die Anforderungen an die Normung, sie muss agiler werden. Um frühzeitig Veränderungen aufzunehmen, hat sich die DKE deshalb komplett neu ausgerichtet und in die vier Bereiche Technology, Production, Finance & Controlling sowie External Relations & Support aufgeteilt. „Unser Ziel ist es, in der Normung den neuesten Technologien immer voraus zu sein“, erklärt Michael Teigeler (im Bild), alleiniger Geschäftsführer der DKE. Unterstützt wird Teigeler durch die Bereichsleiter Kevin Behnisch, der für den Bereich Technology verantwortlich zeichnet, Johannes Stein, der den Bereich Production leitet, und Klaus-Wolfgang Klingner, verantwortlich für Finance & Controlling. Mit der neuen Organisation trimmt sich die vom VDE getragene DKE auf die Zukunft ein. Im Bereich Technology bearbeiten Experten aus Industrie, Wissenschaft, Handwerk und Politik unter der Federführung von VDE|DKE aktuelle, aber auch zukünftige Normungs- und Standardisierungsthemen. „Die zunehmende Konvergenz der Technik erfordert neues Denken. Neben den klassischen Produktnormen nehmen wir daher verstärkt Systemaspekte ins Visier und zugleich innovative Themen durch flexible und agile Ansätze und Strukturen auf. Gleichzeitig sorgen wir für eine bessere Vernetzung der Experten untereinander“, erklärt Teigeler. Der Bereich External Relations & Support erweitert die bereits sehr gut etablierten nationalen und internationalen Netzwerke von VDE|DKE und befasst sich unter anderem mit strategischen Fragen der gesamten Normungspolitik. Er unterstützt die Managementgremien von IEC und CENELEC und beobachtet die normungsrelevanten Entwicklungen in mehr als 70 Nationen. Die beiden Bereiche Production und Finance & Controlling sind als interne Services beispielsweise für die Umsetzung von Normungsprojekten und der IT-Unterstützung der Gremien zuständig.

FOTOS: BAXI/PADMA/ISTOCK (1), VDE (2), MICHAEL HANSCHEKE (3)

1



1

VDE RHEIN-MAIN

Kollaborative Robotik

Humanoide Zeitarbeiter, die die Arbeitswelt 4.0 revolutionieren, sowie mit Künstlicher Intelligenz ausgestattete kollaborative Roboter standen unter anderem auf dem Programm der Fachtagung „Kollaborative Robotik“, zu der der VDE Rhein-Main Anfang November 2017 in die Industrie- und Handelskammer Gießen eingeladen hatte. „Wir erleben gerade eine wahre Explosion an neuen Anwendungen für Sensoren und Aktoren, angetrieben vom Internet der Dinge und Industrie 4.0. Eine zentrale Rolle spielt hierbei die Künstliche Intelligenz, die Maschinen mit der Intelligenz eines Menschen ausstattet. Dabei verwischen die Grenzen zwischen ‚dummen‘ Industrierobotern und futuristisch anmutenden Humanoiden, wie wir sie aus Science-Fiction-Filmen kennen, immer mehr“, sagt Armin Belle vom VDE Rhein-Main. Die Fachtagung nahm daher generell das Zusammenspiel von Mensch und Maschine ohne räumliche und körperliche Trennung ins Visier. Während der Pausen gab es für die Teilnehmer die Möglichkeit, sich auf der begleitenden Ausstellung die Exponate der Unternehmen und Forschungseinrichtungen demonstrieren zu lassen.

VDE SÜDBAYERN

Design Thinking

Durch die Digitalisierung entstehen völlig neue Wettbewerbssituationen für die Unternehmen in Deutschland. „Da die bisherigen Ansätze bei Forschung & Entwicklung häufig zu schwerfällig sind, um aufkommenden Disruptionen zu begegnen, investieren heute viele Unternehmen vor allem in neue Formen der Zusammenarbeit“, erklärt Rainer Klos vom VDE Südbayern. Letztendlich aber seien es die neuen Arbeitsweisen, die über Erfolg oder Misserfolg entscheiden. Deshalb lud der VDE Südbayern Mitte November 2017 Dr. Steffen Gackstatter, Partner bei Roland Berger, und Lisa Glassner, Community Designer bei Steelcase, ein, um das aus der Produktentwicklung bekannte „Design Thinking“ den Mitgliedern vorzustellen. Während Gackstatter aus Sicht eines Unternehmensberaters Innovationsansätze von verschiedenen Industrien und Ländern vorstellte, konzentrierte sich Glassner auf Praxisbeispiele.

2

VDE DÜSSELDORF

Ganz weit vorn? Ganz weit oben!

„Hoch hinaus mit dem VDE“, hieß es Ende September 2017 für Mitsubishi Electric Europe. Der VDE Düsseldorf begrüßte das neue korporative Mitglied im Drehrestaurant auf dem 240 Meter hohen Rheinturm in Düsseldorf. Hier tauschte man sich über gemeinschaftliche Projekte und Ideen zur Bekämpfung des Fachkräftemangels aus. Abschließend warfen die Teilnehmer einen Blick hinter die Kulissen des berühmten Wahrzeichens Düsseldorfs und bekamen Einblicke in dessen technische Ausstattung, den Brandschutz und die moderne Klimatisierung. „Dieser Be-

2 3

reich ist nicht öffentlich zugänglich. Zum Glück konnte ich uns in die heiligen Hallen des Rheinturms bringen. Das hat auf unser neues Mitglied großen Eindruck gemacht", freut sich Axel Dietrich (2.v.r.) vom Bezirksverein über den Erfolg der Veranstaltung. Die anwesenden Gäste von Mitsubishi Electric (im Bild: Pia Müller (2.v.l.), Barbara Sutter (3.v.l.) und Georg Jennen (3.v.r.)) hätten sich zudem beeindruckt von den beiden jungen Vorstandsmitgliedern des VDE Köln, Daniel Mertens (l.) und Jürgen Kreienkamp (r.) gezeigt. Dietrich hatte anlässlich eines Vortrags zum Thema Gebäudeautomation bei Mitsubishi Electric gleich die Chance genutzt, den Gastgeber als korporatives Mitglied zu werben. Als Nächstes plant Tausendsassa Dietrich weitere Kooperationen, unter anderem mit Tesla.

3

VDE SÜDBAYERN

VDE Awards 2017

Es ist schon Tradition: Auch 2017 lud der Bezirksverein wieder Gäste aus Industrie, Hochschule, Politik und Medien in den Bayerischen Hof zum Münchener VDE-Abend mit Verleihung der VDE Awards in den Kategorien „Wirtschaft", „Wissenschaft" und „Schule". Moderiert wurde die Veranstaltung im historischen Ambiente von Heike Götz vom Bayerischen Fernsehen.

VDE KASSEL

Komm, mach MINT

Die MINT-Messe (MINT = Mathematik, Informatik, Naturwissenschaft und Technik) „Technik zum Anfassen" in Witzenhausen lockte Ende September 2017 Tausende Besucher an. Mehr als 70 Aussteller aus dem MINT-Bereich präsentierten sich dem Publikum. Mit dabei: Der VDE Kassel. Am Stand des Bezirksvereins lernten die Schülerinnen und Schüler, aber auch ihre Eltern und Großeltern das Löten. Ebenso konnten sie sich über das Studium oder eine Ausbildung im Bereich Elektro- und Informationstechnik informieren. „Für jedes Alter, jeden Geschmack und jede Begabung ist auf dieser Messe etwas dabei. Gerade für die Eltern und Großeltern ist sie interessant. Das wissen auch die Aussteller zu schätzen", sagt Stefan Bothe vom VDE Kassel. In erster Linie ginge es aber darum, Kinder und Jugendliche für Technik zu begeistern und so dem zunehmenden Fachkräftemangel etwas entgegenzusetzen.

VDE THÜRINGEN

E-Mobility für Thüringen

Zusammen mit Thüringer Versorgungsunternehmen veranstaltete der Bezirksverein Anfang November 2017 das eintägige Symposium „Elektromobilität für Thüringen" bei den Stadtwerken Erfurt. Themen waren dabei die Thüringer Ladeinfrastrukturstrategie für Elektrofahrzeuge bis 2020 sowie der Aufbau kommunaler Stromtankstellen. Zu den Referenten zählten unter anderen Josef Karl von Schneider Electric und Xaver Pfab von BMW. Abgerundet wurde die Veranstaltung durch eine Fachausstellung mit Produkt- und Fahrzeugpräsentation.

FOTOS: FRANKA EMIKA GMBH (1); VDE (2); STEFAN SCHUMACHER (3)

1

YOUNGNET CONVENTION

Richtig gute Stimmung!

Natürlich kommt es bei (fast) jeder Veranstaltung vor allem auf die Inhalte an. Die VDE YoungNet Convention in Unterschleißheim bei München hatte hier ohnehin schon vorgelegt: Eine Keynote des Wissenschaftsphilosophen Prof. Klaus Mainzer, Vorträge zu Themenbereichen wie Verkehr, Security oder Personal Growth gehörten ebenso dazu wie eine Karrieremesse oder das Come-together am Vorabend. Mindestens ebenso wichtig aber war die Frage, wie die Stimmung und die „Teamqualitäten" der rund 160 Mitglieder des VDE YoungNet sein würden, die Ende Oktober 2017 nach Unterschleißheim gekommen waren. Und auch in diesen Punkten waren Thorben Fohlmeister, der die Organisation der Convention mit übernommen hatte, sowie VDE YoungNet-Sprecherin und Convention-Moderatorin Sylvia Schmitz mehr als zufrieden. „Bestes Beispiel für die richtig gute Laune hier auf der Convention war der Science Slam. Den Teilnehmern ist es nicht nur gelungen, fachlich interessanten Input zu liefern, sondern auch gemeinsam mit den Besuchern richtig Stimmung zu machen", sagt Fohlmeister. Da könne sich der ein oder andere Dozent noch eine Scheibe abschneiden.

2

JUNGES FORUM BMT

Am Puls der Medizintechnik

Für Studierende, Promovierende und Young Professionals hält das Junge Forum BMT ein exklusives Programm bereit, um die Kommunikation und Vernetzung im Bereich der Biomedizinischen Technik zu fördern. Im Rahmen der Jahrestagung der Deutschen Gesellschaft für Biomedizinische Technik (DGBMT) im VDE bot das Junge Forum BMT im September 2017 rund 35 Teilnehmerinnen und Teilnehmern die Möglichkeit, während interaktiver Workshops zu Themen wie der extrakorporalen Perfusion und Bildgebung in der Rehabilitation in aktuelle Forschungen einzutauchen, sich bei einem „Connected Café" über Risikomanagement und Karrieremöglichkeiten auszutauschen oder eine umfangreiche Industrieausstellung zu besuchen. Zusätzlich organisierte das Junge Forum BMT die Session „Junges Forum trifft Alte Hasen". Im Zentrum dieses Austausches zwischen Einsteigern und Erfahrenen: die Entwicklung von Medizinprodukten und die Bedeutung der Normenvielfalt.

3

POLEN-EXKURSION

Willkommen in Posen!

Im Juli 2017 haben vier Mitglieder des VDE YoungNet die Stadt Posen in Polen besucht. Mit auf der Agenda des fünftägigen Programms: Das Kennenlernen der TU Politechnika Poznanska und der persönliche Erfahrungsaustausch mit Wissenschaftlern verschiedener Institutionen, Treffen mit dort ansässigen Unternehmen, eine Besichtigung von Posen (der fünftgrößten Stadt des Landes) und natürlich die Come-together:

Dazu gehörten unter anderem ein Grill- beziehungsweise ein Bowlingabend mit polnischen Studierenden der Elektrotechnik. „Wir hatten hier fantastische Leute bei uns und freuen uns auf unseren Gegenbesuch im Mai 2018“, sagt Marek Dura vom VDE Büro in Polen. Wegen des Erfolgs ist nun sogar eine Ausweitung des Angebots geplant.

BUNDESTEAMTREFFEN

Über 50 Teilnehmer erwartet

Schon das erste Treffen des Bundesteams Anfang vergangenen Jahres war ein voller Erfolg. Nun soll die Agenda nochmals ausgeweitet und die deutschlandweite Zusammenarbeit verbessert werden. Mit dem Konzept eines breit aufgestellten, übergreifenden Bundesteams und regelmäßigen Treffen wurden bereits grundlegende Ergebnisse und Erfolge erzielt. Beim zweiten Bundesteamtreffen werden diese Ergebnisse nun weiterverfolgt. Auch sollen neue Themen bearbeitet werden. Ziel ist zudem der Ausbau der Zusammenarbeit zwischen Young Professionals und Studierenden im VDE, damit die Organisatoren und Ressortleiter gemeinsam Akzente zur Zukunft des VDE YoungNet setzen können. Zu dem Treffen werden über 50 Teilnehmer erwartet. Es findet vom 12. bis 14. Januar auf dem Rittergut Hof Largesberg statt. Alle Interessierten sind herzlich eingeladen. Weitere Infos auf der Veranstaltungsseite unter: www.vde.com/de/vde-youngnet/veranstaltungen

Gut verlinkt

- www.vde.com/youngnet
- www.facebook.com/VDE.youngnet
- www.twitter.com/vdeyoungnet
- www.youtube.com/vdepresse

PROJEKTENTWICKLUNG

Evolution im Nahverkehr

Seit drei Jahren entwickelt ein Team an der Hochschule Trier den proTRon EVOLUTION – ein hocheffizientes Nahverkehrsfahrzeug. Im Interview erklärt Fahrzeugleiter Christian Endres das Projekt und welche besonderen Aufgaben die rund 70 beteiligten Studierenden leisten.

CHRISTIAN ENDRES,
Fahrzeugleiter im Team proTRon der Hochschule Trier

Ihr habt ehrgeizige Ziele …
… und wir sind kurz davor, sie zu erreichen! Ende kommenden Jahres werden wir der Öffentlichkeit unseren proTRon EVOLUTION vorstellen. Dann haben wir an der Hochschule Trier ein Nahverkehrsfahrzeug mit vier Sitzen entwickelt. Es wird über eine Reichweite von 100 km verfügen.

Euer Team besteht unter anderem aus Fahrzeugtechnikern, Maschinenbauern und Elektrotechnikern.
Das war einmal. Mittlerweile sind wir deutlich interdisziplinärer aufgestellt. Auf der diesjährigen IAA haben wir eines unserer Herzstücke präsentiert: Unsere Fahrgastzelle, die nahezu ausschließlich aus Naturfasern besteht und trotzdem alle gesetzlichen Anforderungen erfüllt. Allein um die Virtual-Reality-Präsentation und den Stand hinzukriegen, waren neben Informatikern beispielsweise auch Kommilitonen aus dem Bereich Design oder Architektur aktiv.

Die Probleme bei der angestrebten Leichtbauweise und dem elektrischen Antrieb sind mittlerweile weitgehend gelöst?
Es wäre illusorisch anzunehmen, dass schon alles perfekt ist. Wir arbeiten zwar seit drei Jahren am proTRon EVOLUTION, aber das ist in Anbetracht dessen, dass es immer wieder „Generationswechsel“ und damit Wissensverluste gibt, ohnehin sehr schnell.

Was ist so faszinierend an der Mitarbeit, dass einige von euch sogar „Vollzeit“ an der Entwicklung arbeiten?
Das sind in der Regel Studenten, die die Konstruktion und den Bau mit ihrer Abschlussarbeit verknüpfen können – und somit das Angenehme mit dem Nützlichen verbinden. Denn wo sonst sind Theorie und Praxis so eng verknüpft? Generell ist das ohnehin einer der vielleicht größten Vorzüge des Projekts: Die Chance, erlerntes Wissen unmittelbar „auf die Straße“ zu bringen.

FOTOS: SEITE 44: VDE / MIKIJRA GELHAUSEN (1), DANIEL LAQUA (2), PRIVAT (3); SEITE 45: TEAM PROTRON UND HOCHSCHULE TRIER

KONGRESSE / VERANSTALTUNGEN

Energietechnik

23.–24.01.2018, Nürnberg
Workshop „Der zellulare Ansatz“
Seit Jahren bereiten sich innovative Versorgungsunternehmen und Systemlieferanten in zahlreichen Forschungsinitiativen der Länder, des Bundes und der EU auf die Umstellung einer zentralen auf eine dezentrale Energieversorgung vor. Der VDE hat dazu mit seiner Studie „Der zellulare Ansatz“ die technischen Bedingungen dieses Paradigmenwechsels dokumentiert. Diskutieren Sie gemeinsam mit Experten, wie konkrete Rollout-Szenarien für dezentrale Systeme und Lösungen aussehen können.
www.vde.com/workshopzellularer ansatz

20.–21.02.2018, Berlin
Schutz- und Leittechnik 2018
Die Schwerpunkte der Veranstaltung von FNN und ETG sind: Schutztechnik auch zukünftig sicher beherrschen, sichere Kommunikation in der Schutz- und Leittechnik, Vielfalt der Digitalisierung der Schutz- und Leittechnik und schließlich: Wie kann man aus den Erfahrungen mit realisierten Projekten lernen?
www.schutz-leittechnik.de

19.03.2018, Stuttgart
Schaltungstechnik für GaN-Bauelemente in der Leistungselektronik
GaN-Bauelemente haben in den letzten Jahren eine rasante Entwicklung durchlaufen und etablieren sich mehr und mehr in der angewandten Leistungselektronik. Immer mehr Anwender investieren in Forschung und Entwicklung, um das Potenzial der schnellen GaN-Halbleiterschalter für ihre Systeme zu nutzen.
www.vde.com/GaN2018

20.–22.03.2018, Stuttgart
CIPS 2018 – 10th International Conference on Integrated Power Electronics Systems
CIPS is consequently focused on the following main aspects: assembly and interconnect technology for power electronic devices and converters, integration of hybrid systems and mechatronic systems with high power density, systems‘ and components‘ operational behavior and reliability.
www.cips-conference.de

18.04.2018, Frankfurt
Online-Monitoring von Betriebsmitteln im Hochspannungsnetz
Vor dem Hintergrund der Energiewende steigen die Anforderungen an das elektrische Energienetz und die Ferndiagnose der Komponenten. Im Workshop werden Lösungen zum kontinuierlichen Monitoring von Betriebsmitteln des Hochspannungsnetzes vorgestellt und diskutiert. Die Schwerpunkte bilden Transformatoren, Generatoren, Freileitungen und Schaltanlagen.
www.vde.com/monitoring2018

04.–05.09.2018, Leipzig
18.–19.09.2018, Bad Neuenahr
09.–10.10.2018, Ulm
30.–31.10.2018, Hannover
TAR-Fachforum 2018
Das TAR-Fachforum von VDE|FNN und ZVEH gibt Verteilnetzbetreibern, dem Elektrohandwerk sowie Herstellern und Planern einen Überblick über alle Neuerungen rund um die Niederspannung in der Gesetzgebung, in Normen und VDE-Anwendungsregeln sowie sonstigen Vorschriften.
www.vde.com/de/fnn/veranstaltungen/tar-fachforum

Mikroelektronik/-technik

20.–21.02.2018, Fellbach
EBL 2018 – 9. DVS/GMM-Fachtagung Elektronische Baugruppen und Leiterplatten
„Sind die Integrations- und Leistungsdichten für die Baugruppentechnologie auf Leiterplatten am Limit angelangt oder geht es noch weiter?“ Diese Frage steht im Mittelpunkt der EBL 2018, die sich als führende Präsentations- und Diskussionsplattform für Experten aus Industrie und Wissenschaft präsentiert. Sie stellt aktuelle Entwicklungstrends und Praxisergebnisse vor, die begleitende Ausstellung zeigt Geräte- und Prozessentwicklungen.
www.ebl-fellbach.de

07.–08.03.2018, Dortmund
AmE 2018 – 9. GMM-Fachtagung Automotive meets Electronics
Der Weg in die Welt des autonomen Fahrens ist klar aufgezeigt, dennoch ist die Diskussion über die technische Realisierung in komplexen Alltagsumgebungen notwendig, um die notwendige Sicherheit in allen Situationen gewährleisten zu können.
www.ame-konferenz.de

19.–20.06.2018, Grenoble
EMLC 2018 – The 34th European Mask and Lithography Conference
Der ungebremste Trend zu immer kleineren Strukturen in der Mikroelektronik zwingt die Maskenhersteller in die Innovationsoffensive. Um die Herausforderungen der Zukunft meistern zu können, scheint der Einstieg in die Lithographie mit extrem kurzwelligem UV-Licht (EUV) unausweichlich. Bevor diese Technologie jedoch wirtschaftlich sinnvoll eingesetzt werden kann, sind noch technologische Hürden zu überwinden.
www.emlc-conference.com

Medizintechnik

23.01.2018, Frankfurt
3. Praxis-Workshop „Notfallmedizin für Ingenieure“
Das Programm besteht aus Fachvorträgen zu Grundlagen der Notfallmedizin. Im Praxisteil vermitteln Führungen durch die zentrale Notaufnahme und die Radiologie des Klinikums Frankfurt-Höchst den Teilnehmern detaillierte Einblicke in den Einsatz der Medizintechnik durch die dort tätigen Ärzte.
www.vde.com/Praxis-Workshop-Notfallmedizin-3

28.02.2018, Frankfurt
Software in der Medizin – Anforderungen und Best Practice
Der europäische Gesetzgeber hat die Anforderungen für Medizinprodukte drastisch verschärft. Die Veranstaltung bietet einen Überblick von der Entwicklung medizinischer Software bis zu neuen regulatorischen Anforderungen und die Anwendung einschlägiger Normen.
www.vde.com/software-in-der-medizin

Normung und Standardisierung

30.01.2018, Dortmund
IEC Smart Cities Workshop 2018
Are you interested in how the development of international good practice and standards may support your efforts in becoming an even smarter city? Why not take the opportunity to spend a day with the IEC Smart City Systems Committee to review your own smart city challenges and plans and to help develop international Smart City good practice and standards? The workshop provides you with ample opportunity to further your interest.
www.dke.de/smart-cities-workshop-2018

27.02.2018, Frankfurt
Symposium „Ethik in der Technik“
Mit der fortschreitenden Digitalisierung von vernetzten Prozessen in Gesellschaft und Wirtschaft muss der Mensch aus seiner geschützten Rolle des Architekten und Betreibers solcher Prozesse heraustreten. Untersuchungen dazu haben Prof. Steusloff (Fraunhofer IOSB) und Prof. Decker (KIT) unter dem Titel „Der Mensch als Akteur in Prozessketten – Modellierung und Modellvalidation mittels Ethiken“ publiziert. Die Veröffentlichung bildet den Ausgangspunkt des VDE|DKE-Symposiums.
www.dke.de/de/ueber-uns/symposium-ethik-in-der-technik

Informationstechnik

12.–14.03.2018, Freiburg
GeMiC 2018 – German Microwave Conference
GeMiC 2018 offers plenty of opportunities to exchange scientific and technical information. The conference will be hosted by Fraunhofer IAF and University of Freiburg in cooperation with IMA e.V. and VDE|ITG. The Topics are: Electronics and Active Circuits, Systems and Sensors, Passives, EM and Antennas.
www.gemic2018.de

16.–18.04.2018, München
ICMIM 2018 – International Conference on Microwaves for Intelligent Mobility
This conference covers a broad range of topics that enable intelligent mobile systems through RF/microwave/millimeter-wave components, circuits and systems. Potential applications include cognitive and autonomous automobiles and robots, wireless communications between automobiles and industrial machines.
http://icmim-ieee.org

18.–19.04.2018, Berlin
12. ITG-Fachkonferenz Breitbandversorgung in Deutschland
Ziel der Fachkonferenz ist es, ein Forum sowohl für politisch-regulatorische als auch technische und wirtschaftliche Fragen zur Breitbandversorgung in Deutschland anzubieten. Die Konferenz richtet sich an Entscheidungsträger, Netz- und Produktplaner bei den Kommunen, an Versorger, Netzbetreiber und Hersteller.
www.vde.com/breitbandversorgung 2018

Blitzschutz

08.–09.11.2018, Schieder
5. Workshop Koordinierung Blitz- und Überspannungsschutz
Auf der Agenda stehen aktuelle Entwicklungen in VDE 0100-534 und VDE 0100-443, außerdem sind Beiträge zu relevanten VDE-Anwendungsregeln, zum Überspannungsschutz für Gefahrenmeldeanlagen sowie zur dritten Ausgabe der Blitzschutz-Normenreihe VDE 0185-305 geplant. In Ergänzung findet eine Besichtigung des „Erdungsgartens“ statt.
www.vde.com/kbue2018

ALLE TERMINE FINDEN SIE UNTER WWW.VDE.COM/DE/VERANSTALTUNGEN

VDE Seminare

19.–23.02.2018, Berlin
04.–08.06.2018, Offenbach/M.
03.–07.12.2018, München
Fachkraft für Photovoltaik (VDE/DGS)
Zertifikats-Lehrgang zu fach- und normgerechter Planung, Installation, Montage und Inbetriebnahme von PV-Anlagen
www.vde-verlag.de/seminare/pi0300040

27.–28.02.2018, München
05.–06.06.2018, Berlin
Energieeffizienz in der Gebäudeautomation
Anforderungen an die Gebäudeautomation in Nichtwohngebäuden
www.vde-verlag.de/seminare/pi0300050

12.–13.03.2018, München
26.–27.09.2018, Offenbach/M.
IT-Sicherheit – Kompaktkurs zum Schutz vernetzter Industrieanlagen. Aktuelle Darstellung der Sicherheit von Automatisierungssystemen (inkl. Live-Demonstration und Handlungsansatz)
www.vde-verlag.de/seminare/pi0100025

21.03.2018, Erkrath
25.09.2018, München
EU-Datenschutzgrundverordnung
Neue Anforderungen durch EU-Datenschutzgrundversorgung und BDSG-neu #ITS
www.vde-verlag.de/seminare/pi0700030

Alle Seminare sind auch als Inhouse-Angebot erhältlich. Sprechen Sie uns an unter seminare@vde-verlag.de

Das aktuelle Seminarprogramm finden Sie unter: www.vde-verlag.de/seminarkatalog.

INFOCENTER

Aktuelle Positionspapiere, Studien und Reports

VDE-Leitfaden Medizinische Software

Medizinische Software umfasst zahlreiche Produkte, die im therapeutischen oder diagnostischen Kontext eingesetzt werden und deren Bedeutung vor dem Hintergrund der Digitalisierung des Gesundheitswesens stark zunimmt. Normen unterstützen die Hersteller medizinischer Software bei der Erfüllung vielfältiger gesetzlicher Anforderungen, die sich erst kürzlich in Europa grundlegend geändert haben. Der VDE-Leitfaden „Medizinische Software“ bietet Herstellern einen umfassenden Überblick von der Entwicklung über die neuen gesetzlichen Anforderungen bis hin zur Anwendung der einschlägigen Normen. Der Leitfaden ist im VDE Verlag erhältlich. VDE-Mitglieder erhalten einen 10-prozentigen Rabatt.

VDE|FNN-Störungs- und Verfügbarkeitsstatistik

Durchschnittlich nur 11,5 Minuten war ein Kunde 2016 ohne Strom. Zu diesem Ergebnis kommt die jährlich erscheinende VDE|FNN-Störungs- und Verfügbarkeitsstatistik, die die Qualitätsentwicklung der Stromversorgung in Deutschland transparent macht. Die Statistik steht im VDE Shop als Download zur Verfügung. FNN-Mitglieder erhalten einen Rabatt.

VDE-Studie Young Professionals der Elektro- und Informationstechnik

Maximal fünf Bewerbungsschreiben und zwei Vorstellungsgespräche benötigten Absolventen der Elektro- und Informationstechnik im Schnitt bis zur Zusage der ersten Arbeitsstelle. Zu diesem Ergebnis kommt die Studie „Young Professionals der Elektro- und Informationstechnik 2017“, für die der VDE 232 Elektroingenieure und Elektroingenieurinnen bis 35 Jahre mit einer durchschnittlichen Berufserfahrung von etwas über zwei Jahren befragt hat. Die Studie steht VDE-Mitgliedern kostenlos im VDE Shop als Download zur Verfügung.

Der VDE auf Messen

06.–08.02.2018, Essen E-world energy & water

Am 06.02.2018 beteiligt sich der VDE mit Experten der DKE und des VDE-Instituts erstmals an der Messe E-world energy & water im Rahmen des Smart Tech Forums im Themenblock „Energy Ecosystems“.
www.vde.com/messen

18.–23.03.2018, Frankfurt light + building

Das VDE-Institut präsentiert sein umfangreiches Dienstleistungsangebot im Bereich Licht und Smart Home in Halle 4 D 90. Bereits zum dritten Mal organisieren ZVEI und VDE den Nachwuchstag „Industry meets Students“. Studierende der Elektrotechnik, Informatik, Physik und Lichttechnik ab dem zweiten Semester treffen hier auf namhafte Unternehmen der Elektroindustrie. Die Veranstaltung findet am Freitag, dem 23.03.2018, ab 11 Uhr im Rahmen des Technologieforums in Halle 8.0 statt.
https://www.vde.com/nachwuchstag_auf_der_light_building_2018

23.–27.04.2018, Hannover Hannover Messe

Freier Eintritt zur Hannover Messe 2018 für VDE-Mitglieder!

VDE, DKE und das VDE-Institut sind in Halle 13 an Stand C 20 vertreten und beteiligen sich im Rahmen der Hannover Messe erneut am Energieforum Life Needs Power sowie an der Techniknachwuchsinitiative Tec2You. Außerdem ist der VDE Mitorganisator der Integrated Energy Plaza, die in spannenden Showcases das Energiesystem der Zukunft interaktiv erlebbar macht.
www.vde.com/messen

Impressum

VDE DIALOG
Mitgliedermagazin des VDE e. V.
HERAUSGEBER
VDE Verband der Elektrotechnik Elektronik Informationstechnik e. V.
VERLAG
HEALTH-CARE-COM GmbH
Ein Unternehmen der VDE VERLAG GmbH
Kaiserleistraße 8A, 63067 Offenbach
REDAKTION
VDE Kommunikation + Public Affairs
Dr. Walter Börmann (v.i.S.d.P.), Melanie Unseld (Chefredakteurin), Kontakt: dialog@vde.com
ERSCHEINUNGSWEISE
4 x im Jahr, zum Anfang des Quartals
DRUCKEREI
H. Heenemann GmbH & Co. KG
KONZEPTION UND UMSETZUNG
HEALTH-CARE-COM GmbH
Susanne Margraf, Martin Schmitz-Kuhl, Martin Wolczyk
ANZEIGEN
Beate Gehm, dialog@vde-verlag.de
Telefon: 069/840006-3030, Fax: -8030
Es gilt die Anzeigenliste 7 (November 2017)
AUFLAGE
40.000 Exemplare
BEZUGSBEDINGUNGEN:
Der VDE dialog ist im Mitgliedsbeitrag des VDE e. V. enthalten. Nichtmitglieder können das Magazin für eine jährliche Gebühr von 36 Euro (inkl. Versand) abonnieren sowie Einzelhefte für 9 Euro plus 1 Euro Versand bestellen. (Mail: dialog@vde-verlag.de, Telefon: 069/840006-3030, Fax: -8030)

Kontakt

VDE Kommunikation + Public Affairs
Dr. Walter Börmann
Melanie Unseld
Stresemannallee 15, 60596 Frankfurt;
Tel.: 069/6308-461, Fax: 069/6312925
oder per Mail: dialog@vde.com

FOTO: HANNIBAL / VDE

VDE VERLAG

Technik. Wissen. Weiterwissen.

Werb-Nr. 171176 / Bildquelle: © davis/fotolia

Messetermine 2018

Lernen Sie uns persönlich kennen

Wir sind auf zahlreichen Messen und Veranstaltungen vertreten. Erfahren Sie mehr über uns und unsere Angebote zu diesen Themenfeldern:

- **Elektroplanung und -installation, Gebäudetechnik**
- **Automatisierung**
- **Industrie**
- **Kälte-, Klima-, Lüftungstechnik**
- **Geodäsie, Geoinformation**

Wir freuen uns auf Ihren Besuch!

Merken Sie sich die wichtigsten Termine vor: www.vde-verlag.de/messen

EXPERTEN MEINUNG

Alles nur Teillösungen

Warum startet „Smart Home“ nicht so richtig durch? Smarte Lösungen sind doch eigentlich so beliebt – das Smartphone ist hierfür das beste Beispiel. Nur bei den eigenen vier Wänden scheinen erstaunlich viele Menschen zurückhaltend zu sein. Offenbar ist das Thema komplexer, als es auf den ersten Blick scheint. So manch eine (Detail-)Frage verlangt nach einer Antwort.

VON **PROF. DR. RÜDIGER KAYS**

Smart Home verbessert unser Leben. Und es verspricht den Herstellern ordentliche Umsätze. Zumindest im Prinzip. Denn wenn man die Marktentwicklung anderer Produkte wie etwa die des Smartphones betrachtet, geht es beim Smart Home doch recht gemächlich zu. Gerade Menschen, die sich nicht täglich mit Technologie befassen, sehen offenbar keine attraktive Relation zwischen Aufwand und Nutzen. Oft sind nur technikaffine Menschen mit ausgeprägtem Spieltrieb von heutigen Smart-Home-Konzepten begeistert.

Das Thema „Smart Home“ ist offenbar komplexer, als es auf den ersten Blick erscheint. Umso wichtiger sind Studien des VDE, wie das Positionspapier „Smart Living“ oder das Weißbuch „SmartHome 2 Market“. Denn sie benennen nicht nur die Chancen, sondern auch die Herausforderungen. So gibt es zum Beispiel eine Vielzahl von Lösungen, die im Wettbewerb zueinanderstehen. Der Kunde kann die Dauerhaftigkeit konkurrierender Konzepte nicht einschätzen, und eigentlich bieten alle Systeme nur Teillösungen an. Konvergenz wird teilweise durch Gateways möglich, die es erlauben, Sensoren und Aktuatoren unterschiedlicher Standards zu verbinden. Aber wo ist die einfache, geschlossene Gesamtlösung für jedermann? Wie schön wäre ein integriertes Konzept für alle technischen Komponenten des Wohnumfeldes, vergleichbar der Infrastruktur in einem modernen Automobil.

Vielleicht kommen wir um einen langwierigen Konvergenzprozess nicht herum. Und bei einzelnen Aspekten muss wohl noch genauer auf die wirklichen Kundenbedürfnisse geschaut werden. Denn vollständiger Internetzugriff oder Bedienung per Smartphone sind kein Selbstzweck. Die Frage sollte daher eher sein: Was sind die wirklichen Wünsche und Probleme im praktischen Alltag? Sicherlich hat jeder seine eigenen Vorstellungen. Ich verrate hier einige wichtige Aspekte, die begründen, warum mein persönliches „Home“ weniger „smart“ ist als nach Stand der Wissenschaft möglich. Denn mir ist zum Beispiel die Energieeffizienz sehr wichtig. Ich möchte wissen, wie viel Strom ich zusätzlich verbrauche, wenn ich etwa 40 Aktuatoren per Funk betätigen möchte. Mit etwas Glück erhält man zur Stand-by-Leistung dieser kleinen Helferlein eine Angabe, und die nennt in den meisten Fällen einen Wert über 0,5 Watt. Das macht zusätzlich 20 Watt Stand-by im Haus. Stromkosten, die übrigens vermeidbar wären, schließlich verbraucht ein guter Smart TV inzwischen noch nicht einmal 0,1 Watt. Und ich frage mich auch: Warum brauche ich in den meisten Fällen eine zusätzliche Zentrale, die eingerichtet sowie mit Strom und Softwareupdates versorgt werden muss, obwohl doch schon der Internetrouter rund um die Uhr läuft? Ich möchte keine weitere Plastikbox kaufen, um erstmals einen Heizkörper intelligent zu steuern.

> »Die Hersteller bieten eine Vielzahl von guten Lösungen. Aber wo ist die einfache, geschlossene Gesamtlösung für jedermann?«

Ich glaube, dass noch viele dieser Detailprobleme bestehen, von denen kein einziges unlösbar ist. Und so wird das Smart Home in den unterschiedlichsten Ausprägungen in den Markt kommen, Stück für Stück und evolutionär. Das wird aber einige Zeit und Mühe kosten. Schneller würde es durch mehr Abstimmung und Standards gehen. So oder so wird dieser – aus gutem Grund konservative – Massenmarkt sukzessive erschlossen werden, und die Nutzung intelligenter vernetzter Gebäudekomponenten ist dann hoffentlich eines Tages so selbstverständlich wie der elektrische Fensterheber im Auto.

PROF. DR. RÜDIGER KAYS
ist Inhaber des Lehrstuhls für Kommunikationstechnik an der Technischen Universität Dortmund (Fakultät für Elektrotechnik und Informationstechnik). Als Vorsitzender der Informationstechnischen Gesellschaft im VDE (VDE|ITG) ist er zudem Mitglied im VDE-Präsidium.

FOTO: TU DORTMUND

Good Job!

Chips für die Arbeit von übermorgen

INVENT a CHIP 2018

INVENT a CHIP 2018 – Work 4.0
Chips, die die Welt verändern

Schüler/innen aufgepasst! Im Februar 2018 fällt bundesweit der Startschuss für den Schülerwettbewerb INVENT a CHIP. Diesmal zum Thema „Work 4.0“ in Anlehnung an das aktuelle Wissenschaftsjahr.

Welche Idee hast du für die Arbeit der Zukunft?

Mehr unter **www.invent-a-chip.de**

Neu in 2018:
LABS for CHIPS – Elektronik-Initiative für Macher

EINE GEMEINSAME INITIATIVE VON

Bundesministerium für Bildung und Forschung

VDE

Eine Initiative des Bundesministeriums für Bildung und Forschung

Wissenschaftsjahr | 2018
ARBEITSWELTEN DER ZUKUNFT

SMART MOBILITY

E-HEALTH

Net.Law.S 2018

Konferenz für Recht, Gesellschaft & Industrie in der digitalen Welt

INDUSTRIE 4.0

Nürnberg, Germany
20.–21. Februar 2018

KEYNOTE:
PROF. DR. DR. UDO DI FABIO

Richter des Bundesverfassungsgerichts a. D., Direktor des Forschungskollegs normative Gesellschaftsgrundlagen der Universität Bonn

Digitalisierung, Vernetzung und Automatisierung werfen neue, wichtige Fragen auf. **Net.Law.S** führt Spezialisten und Entscheider unterschiedlichster Branchen zusammen, gibt wegweisende rechtliche Handlungsempfehlungen und beleuchtet neue Geschäftsmodelle angesichts von Haftungsverschiebungen in der vernetzten Wertschöpfungskette.

Sichern Sie sich Ihr Ticket zum Frühbuchervorteil:

netlaws.de/anmeldung

Vogel Business Media

robot|recht forschungs|stelle

NÜRNBERG MESSE