AMPERE

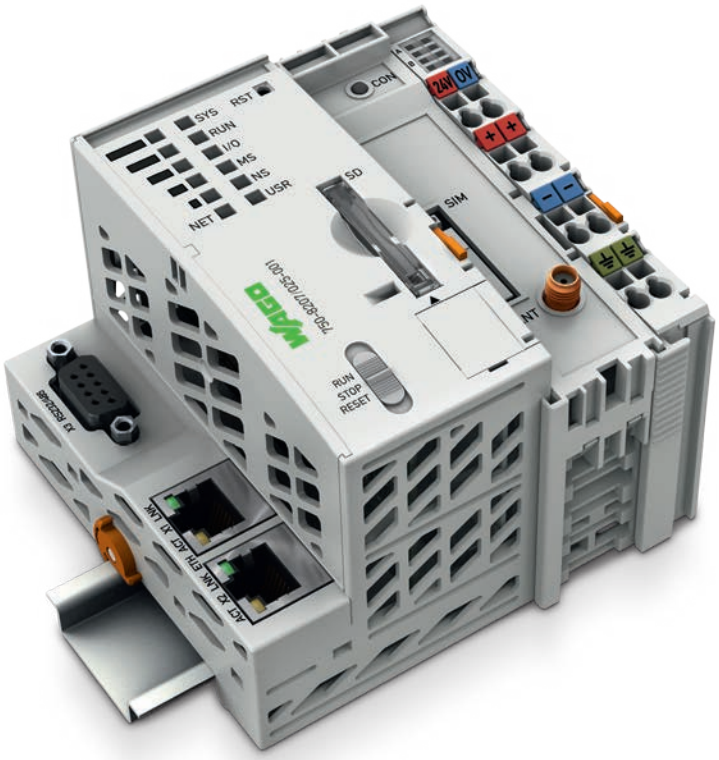
4.2016

DAS MAGAZIN DER ELEKTROINDUSTRIE

Cybersicherheit: Schutz vor versteckten Gefahren

ZVEI: Die Elektroindustrie

VERBINDET DIE WELT DER AUTOMATISIERUNG MIT DEM INTERNET OF THINGS



Der PFC200 von WAGO – Die sichere Basis für den Weg aus der Feldebene

- Leistungsstarke Steuerung mit integriertem 3G-Modem und Standard-Mini-SIM-Karte
- Drahtlose Datenübertragung über große Distanzen
- GPRS-Verbindung zum Internet und bidirektionale Kommunikation via SMS
- Höchste Sicherheitsstandards dank IPsec und OpenVPN

www.wago.com/pfc200

sps ipc drives

Nürnberg, 22.–24.11.2016

Besuchen Sie uns:
Halle 7, Stand 130

WE INNOVATE!

WAGO

Ohne das Vertrauen der Gesellschaft werden wir mit digital vernetzten Produkten langfristig nicht am Markt erfolgreich sein.

Liebe Leserin, lieber Leser,

auf Nummer sicher zu gehen, das ist tief in unserer Mentalität verankert. Sichere Produkte begründen den Weltruf von „Made in Germany". Doch was bedeutet Sicherheit in einer Zeit des raschen digitalen Wandels? Wie weit ist sie angesichts der im Cyberraum wartenden Gefahren überhaupt herzustellen? Und wie kann ein normaler, technisch nicht versierter Kunde ein sicheres von einem unsicheren Produkt unterscheiden?

Ich bin zutiefst davon überzeugt, dass die Industriezweige, die die Digitalisierung vorantreiben, diese Fragen dringend beantworten müssen. Ohne das Vertrauen der Gesellschaft werden wir mit digital vernetzten Produkten langfristig nicht am Markt erfolgreich sein. Die Antworten zu finden, ist gewiss nicht einfach. Doch in einem Punkt bin ich mir sicher: Wenn jeder nur an sich, an sein Unternehmen, an seine Produkte denkt, werden wir sie nicht finden.

Daher gilt es nun, Allianzen zu bilden, zwischen Unternehmen der Real- und der Digitalwirtschaft genauso wie Allianzen zwischen Politik und Wirtschaft. Dies wiederum bedingt, dass wir Fragen der Cybersicherheit offen diskutieren – so wie wir es mit der vorliegenden Ausgabe von AMPERE versuchen.

Gehen wir also den Weg in das Neuland eines digitalen Zeitalters – aber gemeinsam!

Ihr

DR. KLAUS MITTELBACH
Vorsitzender der Geschäftsführung des ZVEI und
Vorsitzender des Beirats der Allianz für Cybersicherheit

Illustration: Indi Davies | Titelfoto: REUTERS/Amir Cohen

Sicher im Cyberraum

Das Internet der Dinge, Dienste und Menschen kommt. Doch die Vernetzung von technischen Systemen benötigt neue Antworten auf die zunehmende Bedrohung durch Cyberkriminalität.

Auftakt: Politik, Wirtschaft und Behörden arbeiten immer enger zusammen, um sich gegen Cyberkriminalität zu schützen.

Praxis: Das inhabergeführte Unternehmen Block begreift Informationssicherheit als Chefsache. Und redet offen über Cyberangriffe.

Praxis: Um Geschäfte im Internet sicher abzuwickeln, gibt es bessere Verfahren als Passwörter.

Download & Bestellung
Sie können diese Ausgabe von AMPERE über den QR-Code downloaden oder unter zsg@zvei-services.de bestellen.
QR-Code Reader im App Store herunterladen und Code mit Ihrem Smartphone scannen.

www.zvei.org/ampere

ISSN-Nummer 2196-2561
Postvertriebskennzeichen 84617

Standpunkte: Klaus Helmrich (links) und Ammar Alkassar geht es vor allem um die Kronjuwelen.

Energieeffizienz erleben: Wie Energiemanager Pascal Meury Abwärme in Nutzwärme verwandelt.

Heißes Eisen: Rittal-Chef Karl-Ulrich Köhler hat keine Angst vor amerikanischen IT-Konzernen.

Chefsache: In einer vernetzten Welt, so NXP-Topmanager Kurt Sievers, gehört das Nachdenken über Sicherheit zu guter Unternehmensführung.

Impressum

CHEFREDAKTEUR
Thorsten Meier

HERAUSGEBER
ZVEI-Services GmbH
Dr. Henrik Kelz, Patricia Siegler
(Geschäftsführung)
Lyoner Straße 9,
60528 Frankfurt am Main
Telefon +49 69 6302-412
E-Mail: zsg@zvei-services.de
www.zvei-services.de

ZSG ist eine 100-prozentige Servicegesellschaft des ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

ANSPRECHPARTNER ZVEI
Thorsten Meier
(Abteilungsleiter Kommunikation und Marketing),
meier@zvei.org
Karen Baumgarten, Stella Loock
(Referenten Kommunikation und Marketing),
baumgarten@zvei.org, loock@zvei.org
www.zvei.org

VERLAG, KONZEPT & REALISIERUNG
PICS publish-industry Corporate Services GmbH, München
Projektleitung: Julia Rinklin,
j.rinklin@publish-industry.net

Inhalt: Redaktionsbüro delta eta Paschek & Winterhagen GbR

Art-Direktion: Barbara Geising

ANZEIGEN
Thomas Burkert, burkert@zvei-services.de

DRUCK
SEW-EURODRIVE GmbH & Co KG

Der Bezug des Magazins ist im ZVEI-Mitgliedsbeitrag enthalten. Alle Angaben sind ohne Gewähr, Änderungen vorbehalten. Nachdruck, Vervielfältigung und Onlinestellung sind nur mit schriftlicher Genehmigung des Herausgebers gestattet.

Stand: 11/2016.

FSC www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C004592

Dieses Magazin wurde auf FSC®-zertifiziertem Papier gedruckt. Mit der FSC®-Zertifizierung (Forest Stewardship Council) wird garantiert, dass sämtlicher verwendeter Zellstoff aus nachhaltiger Forstwirtschaft stammt. Der FSC® setzt sich für eine umweltgerechte, sozial verträgliche und wirtschaftlich tragfähige Bewirtschaftung der Wälder ein und fördert die Vermarktung ökologischer und sozial korrekt produzierten Holzes.

Ausweiskontrolle

1953

Unbefugten ist der Zutritt zu Industrieanlagen schon immer verboten. So gilt am Werkstor der Kieler Howaldtswerke AG, die in den 1950er-Jahren unter anderem für den Tanker-König Aristoteles Onassis tätig ist, strenge Ausweispflicht. Werksspione bleiben so meist vor dem Tor.

Foto: Jochen Blume/ullstein bild via Getty Images

Kontrollzentrum

2015

Großunternehmen müssen jeden Tag mehrere Tausend Cyberangriffe abwehren. Denn die wahren Schätze eines Unternehmens wie Kunden- und Konstruktionsdaten befinden sich hinter der Firewall, die der Chief Information Security Officer bewacht.

Foto: Helen H. Richardson/Kontributor

Gesichtslos, aber gefährlich: Immer öfter greifen Hacker auch kritische Infrastrukturen an.

Die Bedrohung durch Cyberangriffe nimmt weiter zu. Doch auch die Gegenwehr formiert sich: Politik, Wirtschaft und Behörden arbeiten in Deutschland und in Europa immer enger zusammen. Ein wirksamer Schutz ist auch für mittelständische Unternehmen möglich, wenn sie nicht nur auf technische Maßnahmen vertrauen.

Text: **Johannes Winterhagen** | Illustration: **Marek Haiduk**

Gefahrenabwehr

Lisa taucht 1983 auf und ist ein Jahr später wieder verschwunden. Dem ersten von Apple hergestellten PC mit grafischer Benutzeroberfläche ist kein Erfolg beschieden – auch wegen des horrenden Preises von rund 10.000 Dollar. Dass es zu diesem Zeitpunkt bereits möglich ist, Rechner über Telefonleitungen miteinander zu verbinden und so Informationen auszutauschen, ist für die meisten Menschen damals pure Science-Fiction, so weit außerhalb der eigenen Vorstellungswelt wie das Beamen oder ein Smartphone in der eigenen Jackentasche. Und doch: Im gleichen Jahr erscheint „War Games", der erste Spielfilm über Hacker. Der Schüler David Lightman dringt darin in ein lernendes Expertensystem ein, das vom Pentagon errichtet wurde, um im Fall eines sowjetischen Nuklearangriffs richtig zu reagieren. Unbeabsichtigt löst der Teenager so fast den Dritten Weltkrieg aus. Hacker, das sind damals Technikbegeisterte mit einem Hang zum Anarchismus. So wie Wau Holland, Mitgründer des Computer Chaos Clubs, der erklärt: „Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann." Erst als Anfang der 1990er-Jahre die elektronische Datenverarbeitung in immer mehr Büros und sogar in erste Haushalte Einzug hält, kann eine kriminelle Hacker-Szene entstehen – so wie der Beruf des Autodiebs erst lohnte, als das Auto zum Massenverkehrsmittel geworden war. Mittlerweile ist Internetkriminalität zum Massenphänomen geworden.

„Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann."

WAU HOLLAND, MITGRÜNDER DES COMPUTER CHAOS CLUBS

Die in der Öffentlichkeit gehandelten Schadenssummen variieren. Noch recht überschaubar scheint die Summe von rund 40 Millionen Euro, die in der Statistik des Bundeskriminalamtes (BKA) auftaucht. Sie bezieht sich jedoch nur auf die 45.000 Fälle, die im Jahr 2015 tatsächlich zur Anzeige gebracht wurden. BKA-Chef Holger Münch geht wie viele Experten von einer hohen Dunkelziffer aus. Am anderen Ende der Skala liegt ein – allerdings zwei Jahre alter – Bericht, der im Auftrag von McAfee entstand. Auf 400 Milliarden Euro weltweit schätzt die Studie den Schaden durch Cyberkriminalität, eine Summe, die in etwa dem Bruttoinlandsprodukt Österreichs entspricht. „Am Ende sind das zugegebenermaßen alles Schätzungen", sagt Lukas Linke, der für Cybersicherheit zuständige Referent des ZVEI. „Klar ist, dass sich die Angreifer professionalisiert haben. Der Hacking-Markt mit Lösegeldern und dem Verkauf von ▷

Soft- und Hardwareschwachstellen hat sich zu einer regelrechten Wachstumsbranche mit Milliardenumsätzen entwickelt."

Noch vor wenigen Jahren galten vor allem Großkonzerne als lukrative Angriffsziele. So muss Volkswagen als größtes europäisches Unternehmen mehr als 6.000 Angriffe täglich abwehren. Doch mittlerweile ist auch der Mittelstand im Visier. Ein anonymer Hacker, interviewt von PWC-Beratern, berichtet: „Große Unternehmen haben zwar mehr Daten gespeichert, aber kleine Firmen sind oft schlecht gesichert. Für Hacker ist das leicht verdientes Geld. Dann ist es vom Zeitaufwand her fast egal, ob man eine Firma angreift oder 500. So kommen große Mengen an Kundendaten zusammen. Und auch die kleinen Unternehmen haben durchaus lohnende Firmendaten." Mit der Gefahr wächst allerdings auch das Bewusstsein. „Awareness für das Problem ist inzwischen vorhanden", berichtet Linke. Das zeigt eine kürzlich vom ZVEI-Fachverband Automation durchgeführte Umfrage. 63 Prozent der Teilnehmer geben an, dass Cybersicherheit inzwischen ein Top-Thema der jeweiligen Geschäftsführungen ist. Als wichtigste Bedrohungen gelten Schadprogramme (29 Prozent der Vorfälle), menschliches Fehlverhalten (20 Prozent) und technisches Versagen (19 Prozent). Insbesondere Ransomware stellt eine zunehmende Herausforderung dar. Generell bestätigt die Umfrage, dass die meisten Angriffe über die Büro-IT-Systeme erfolgen.

Angesichts dieser Situation liegt der Ruf nach dem Staat nahe. Denn Sicherheit ist ein klassisches öffentliches Gut, aus dem sich die Existenzberechtigung des Staates ableitet. „Die klassische Aufgabenteilung zwischen Staat und Wirtschaft greift jedoch bei der Cybersicherheit nicht mehr", sagt Dr. Klaus Mittelbach, Vorsitzender der ZVEI-Geschäftsführung. „Cyberkriminalität hält sich nicht an nationalstaatliche Grenzen." Auch die Abgrenzung zwischen Einzelunternehmen und gesamtgesellschaftlichen Aufgaben fällt schwer. So wird in Europa der Großteil der kritischen Energie-Infrastrukturen von Privatunternehmen betrieben. Die Politik hat erstaunlich früh auf dieses Phänomen reagiert. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 1991 gegründet, um die Aufgaben einer bereits zuvor existierenden Zentralstelle zu erweitern. Diese hatte sich im Auftrag des Bundesnachrichtendienstes vor allem um die IT-Sicherheit staatlicher Einrichtungen gekümmert. Fortan sollte die neue Behörde einen „staatlichen Beitrag zur Förderung der IT-Sicherheit" leisten. Mit den Jahren wurden die Kompetenzen des BSI zunehmend erweitert, zuletzt durch das zuvor umstrittene IT-Sicherheitsgesetz, das den Betreibern kritischer Infrastrukturen eine engere Kooperation mit dem BSI vorschreibt.

Wichtig ist die Zusammenarbeit von Staat und Wirtschaft vor allem dann, wenn es um besonders komplexe Angriffe geht. Das gilt nicht für jede Attacke aus dem Internet – ähnlich wie im realen Leben hat sich ein differenziertes System des Verbrechens entwickelt. Es beginnt mit dem Kleinkriminellen, der mit geringem Ressourcen-Einsatz vorgeht und nur dann Erfolg hat, wenn Standard-Schutzmaßnahmen wie Firewalls und Virenscanner versagen – meist durch Fehler der Nutzer. Aber auch im Cyberraum existiert organisiertes Verbrechen, das mit erheblichen Ressourcen auf Jagd nach Daten geht und Lösegeld erpresst. Für mittelständische Unternehmen können solche Attacken bereits schwierig abzuwehren sein. Die größte Herausforderung sind jedoch APT-Angriffe („Advanced Persistent Threat"), hinter denen beispielsweise staatlich gesteuerte Industriespionage stecken kann.

„Die klassische Aufgabenteilung zwischen Staat und Wirtschaft greift jedoch bei der Cybersicherheit nicht mehr. Cyberkriminalität hält sich nicht an nationalstaatliche Grenzen."

DR. KLAUS MITTELBACH,
VORSITZENDER DER ZVEI-GESCHÄFTSFÜHRUNG

Auch die 2012 erfolgte Gründung der Allianz für Cybersicherheit, deren Beiratsvorsitzender Mittelbach derzeit ist, kann als neue Form der Zusammenarbeit von Wirtschaft und Staat gedeutet werden. Neben den 100 Partnern der Allianz nehmen rund 2.000 Institutionen das Angebot zu einem Austausch wahr – auf Geschäftsführungsebene genauso wie in Expertenkreisen, in denen über Abwehrkonzepte diskutiert wird. Die in der Allianz organisierten Partner können ihre Schutzkonzepte – beispielsweise für Fernwartungszugänge oder Identitätsmanagement – einreichen. Checklisten, Leitfäden und andere Dokumente werden dann vom BSI geprüft und allen Mitgliedern zugänglich gemacht – online genauso wie auf regionalen Fachtagungen. „Hier ist ein Informationspool entstanden, der einem bei der Prävention und der Gefahrenabwehr wirklich weiterhilft", sagt Linke. Darüber hinaus betreibt die Allianz eine freiwillige Meldestelle: Jedes Unternehmen kann Vorfälle anonymisiert melden. Je nach Ausmaß des Vorfalls steht dann sogar das BSI als Ansprechpartner zur Verfügung. Allerdings: Eine FBI-Einheit, die mit schwarzen Sonnenbrillen getarnt innerhalb weniger Minuten ausrückt, darf man nicht erwarten.

Für 63 Prozent der CEOs in der deutschen Automatisierungsbranche ist Cybersicherheit ein Top-Thema.

Auch auf europäischer Ebene schreitet die Zusammenarbeit voran. Im Juli 2016 wurde die European Cyber Security Organisation (ECSO) gegründet, eine von der EU gemeinsam mit Unternehmen und Verbänden als „Public Private Partnership" betriebene ▷

Ganz gleich, was Sie bewegt:
Wir treiben es an – und das seit 85 Jahren.

Halle 3
Stand 3-420

Unterschiedliche Branchen. Unterschiedliche Herausforderungen. Und ein kompetenter Partner: SEW-EURODRIVE. Unsere innovativen Antriebstechnologien bieten höchste Qualität bei niedrigem TCO. Und dazu maximale Leistung bei einer Energieeffizienz, die schon heute die gesetzlichen Anforderungen von morgen erfüllt. Das gilt von der Baustoffindustrie über die Getränke- und Nahrungsmittelproduktion bis zur Automobilindustrie oder Flughafenlogistik. Von klein bis gewaltig groß: Wir entwickeln für nahezu jede Branche richtungsweisende Antriebssysteme – und haben auch für Sie die passende Lösung. Weil wir das Ganze sehen. **Und das seit 1931.**

www.sew-eurodrive.de

SEW EURODRIVE

Studie von BSI und ZVEI zur Sicherheitslage in der Automationsbranche
www.zvei.org/Verband/Publikationen

Plattform. Wesentliches Ziel ist es, die Frage zu beantworten: Wie kann das EU-Forschungsprogramm „Horizon 2020“ genutzt werden, um Innovationen auf dem Gebiet der Cybersicherheit zu fördern? Keine einfache Aufgabenstellung, sind doch klassische Forschungsprogramme in der Regel auf drei bis vier Jahre angelegt – angesichts der sich rasch wandelnden Bedrohungslage im Cyberraum wäre ein solches Instrumentarium viel zu langsam. Eine weitere Herausforderung für die ECSO: Auf sicherheitsrelevanten Feldern wie der Kryptologie existiert in Europa bereits herausragende Forschung. „Oft kommen die Ergebnisse jedoch in Industrieanlagen nicht zur Anwendung, weil die Performance zu gering ist“, erläutert Linke. „Die Produktivität darf sich durch Sicherheitsmaßnahmen nicht verschlechtern.“ Die Lösung liegt nicht darin, noch mehr Geld in Forschung zu stecken, so der Experte, sondern deren industrielle Verwertbarkeit zu fördern. „Wir müssen mehr an Industrial Security und nicht nur allgemein an IT-Sicherheit denken.“

Laut aktuellem Bericht des BSI zur IT-Sicherheit nimmt die Gefährdung industrieller Steuerungsanlagen stark zu. Neben den Herstellern von Komponenten – gemeint sind die klassischen Automatisierer – seien auch die Maschinenhersteller sowie die Betreiber gefordert. Für den Mittelstand eine Herausforderung, die ohne spezialisierte Dienstleister kaum zu lösen ist. Doch welche Kriterien sollte ein Unternehmer seiner IT oder einem Dienstleister vorgeben? Checklisten für IT-Sicherheit gibt es bereits, doch sie enthalten in der Regel so viele Unterpunkte, dass sie eher für die Kommunikation unter Experten geeignet sind. Fragt man Experten, geht es im Kern aber immer darum, ob Sicherheit wirklich Chefsache ist. So steht an erster Stelle nicht eine bestimmte Technik, sondern eine ausführliche und regelmäßig durchgeführte Risikoanalyse im Auftrag der Unternehmensleitung. Dahinter steht die Frage: Was sind die Kronjuwelen eines Unternehmens, die es unbedingt zu schützen gilt? Ist sie beantwortet, fällt es leichter, die letztendlich immer begrenzten Mittel für IT-Sicherheit richtig zu investieren. Und auch sonst sind es klassische Aufgaben der Unternehmensführung, die Inhaber und Geschäftsführer mittelständischer Betriebe im Blick haben sollten: Wer ist für was verantwortlich? Und wer darf was und was nicht? Es reicht nicht, einen Mitarbeiter beim Eintritt ins Unternehmen einmal eine EDV-Richtlinie unterschreiben zu lassen. Empfohlen wird vielmehr eine regelmäßige Schulung, die auf aktuelle Bedrohungen und Verhaltensweisen eingeht. Vor diesem Hintergrund wagt die AMPERE-Redaktion einen ungewöhnlichen Schritt: Neun Punkte nur umfasst unsere Checkliste für den Unternehmer.

„Die Produktivität darf sich durch Sicherheitsmaßnahmen nicht verschlechtern.“

LUKAS LINKE, REFERENT FÜR CYBERSICHERHEIT IM ZVEI

Was dem einen Kopfzerbrechen bereitet, ist das Geschäftsmodell des anderen. Als noch vor allem Bürorechner von Viren befallen wurden, entstanden Unternehmen wie McAfee, heute selbst ein IT-Gigant, dessen Wert aktuell auf rund sechs Milliarden Dollar taxiert wird. In der Welt der vernetzten Dinge, deren Boomphase gerade erst beginnt, sind Spezialisten gefragt – damit haben auch mittelständische Unternehmen aus Deutschland eine Chance. Ein Beispiel dafür ist Wibu-Systems aus Karlsruhe. Gründer und Vorstandschef Oliver Winzenried begann Ende der 1980er-Jahre nach seinem Studium zunächst damit, einen Kopierschutz für Software zu entwickeln. Seit 2008 arbeiten die Karlsruher auch an Security-Lösungen für das industrielle Umfeld, mittlerweile konnten namhafte Hersteller von Industriesteuerungen als Kunden gewonnen werden. „Heute ist die Vernetzung industrieller Anlagen zwar in aller Munde“, sagt Winzenried. „Doch wir stehen noch immer ganz am Anfang.“ Geschützt werden momentan vor allem die Zugänge ins Internet, nicht aber die Maschine-zu-Maschine-Kommunikation. Dies aber ist nach Ansicht des Experten zwingend notwendig, wenn komplexe Anlagen sich weitgehend selbst steuern. Winzenried setzt dabei auf die Kombination von Hard- und Software: „Nur wenn sichergestellt ist, dass zum Beispiel Sensordaten von einem authentifizierten Sender stammen, können diese in einer Produktionsumgebung über offene Netzwerke kommuniziert werden.“ Dafür sorgen im Idealfall Hardware-basierte Sicherheitselemente. Die zunehmende Vernetzung schlägt sich bei Wibu-Systems bereits in einem zweistelligen Umsatzwachstum nieder. „Aber es wird aktuell noch immer mit spitzem Bleistift gerechnet, wenn es um die Sicherheit geht“, sagt der Unternehmer. Blickt er weiter in die Zukunft, sieht er große Chancen. Ganzheitliche Sicherheitslösungen „Made in Germany“ könnten zum Exportschlager werden. „Wir Deutschen haben in der ganzen Welt einen Vertrauensvorsprung“, so Winzenried.

Vernetzte Autos, vernetzte Produktionsmaschinen, vernetzte Energiesysteme. Die in Deutschland traditionell starken Branchen erhoffen sich von der Digitalisierung einen neuen Produktivitätsschub. Zudem soll die Vernetzung zu weniger Verkehrstoten, geringeren CO_2-Emissionen und höherer Produktivität führen. Doch Sicherheit ist die Grundvoraussetzung dafür, dass die Digitalisierung gesellschaftliche Akzeptanz findet. „Es darf kein Fatalismus entstehen“, warnt Linke. „Wenn wir konsequent sind, können wir ein hohes Maß an Sicherheit herstellen und die Digitalisierung konsequent vorantreiben.“ Für einen Hightech-Standort wie Deutschland gäbe es nichts Gefährlicheres, als aus Angst den Fortschritt auszubremsen. □

CHECKLISTE

1. Lassen Sie in regelmäßigen Abständen eine **Sicherheits- und Risikoanalyse** durchführen, um Ihre wichtigsten Unternehmenswerte und -prozesse zu identifizieren? Diskutieren Sie die Ergebnisse im Vorstand/in der Geschäftsführung? ☐

2. Haben Sie – idealerweise außerhalb der IT-Abteilung – einen **„Chief Security Officer (CSO)"** benannt, der für Sicherheit verantwortlich ist? Wenn das Unternehmen dafür zu klein ist: Haben Sie einen darauf spezialisierten Dienstleister beauftragt? ☐

3. Wie hoch ist der **Anteil des IT-Budgets**, der für Standardmaßnahmen der IT-Sicherheit verwendet wird? Liegt er im Bereich des Empfehlungswertes von zehn Prozent? ☐

4. Ist Ihr Unternehmen direkt oder über Dienstleister in ein **Erfahrungs- und Austauschnetzwerk** für Cybersicherheitsvorfälle eingebunden? Gibt es Kontakte zum Bundesamt für Sicherheit in der Informationstechnik (BSI), zum ZVEI oder zur Allianz für Cybersicherheit? ☐

5. Gibt es in Ihrem Unternehmen einfache, verständliche Regeln für die Nutzung von IT-Systemen? Werden Ihre **Mitarbeiter** für die Gefahren durch Cyberkriminalität sensibilisiert und mindestens einmal im Jahr geschult? ☐

6. Besteht ein definierter **Notfallplan**, falls es doch zu einer Störung relevanter Bestandteile der Informations- und Kommunikationstechnik kommt? Wird der Notfall regelmäßig durchgespielt? ☐

7. Wie sieht Ihr Konzept für die physikalische **Datensicherung** und die Herstellung von Backups aus? Ist geregelt, welche Daten für **Cloud-Anwendungen** zur Verfügung gestellt werden und welche angesichts von Datenschutz und Cybersicherheit nicht? ☐

8. Ist über ein definiertes **Rechte- und Rollenmanagement** geregelt, welcher Mitarbeiter auf welche Daten und Programme zugreifen darf? Verfügt Ihre IT über ein Log-in-System, das – datenschutzrechtlich unbedenklich – erfasst, wer wann auf was zugreift? ☐

9. Sprechen Sie regelmäßig mit Ihren Kunden und vor allem den eigenen **Zulieferern** über Cybersicherheit in Produkten und Lösungen? Wie stellen Sie sicher, dass gelieferte Produkte, die Sie selbst einsetzen oder weiterverarbeiten, keine gravierenden Schwachstellen haben? ☐

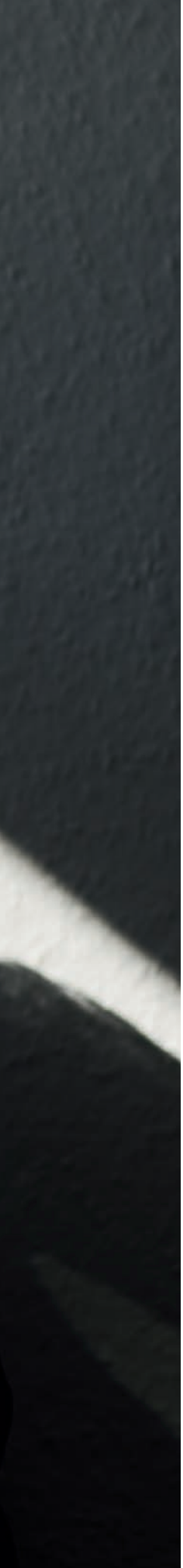
Cybersicherheit in neun Schritten

Unternehmer müssen sich um Kunden und Mitarbeiter kümmern, Strategien entwickeln und Märkte erschließen, Budgets und Kommunikation steuern – da bleibt nicht viel Zeit, sich um Details der IT-Sicherheit zu kümmern. Experten müssen her. Doch den Rahmen für deren Arbeit sollte der Unternehmer selbst setzen. Orientierung bieten die Fragen auf der umseitigen Checkliste.

ZUR CHECKLISTE

„Hardware zählt"

Cybersicherheit ist eine Chance für die deutsche Exportwirtschaft, meint Kurt Sievers, General Manager bei NXP.



Sicherheit im Cyberraum – das ist nach Ansicht von Kurt Sievers möglich. Der Topmanager des Halbleiterherstellers NXP spricht dennoch offen über die Gefahr, die von Hackerangriffen ausgeht. In einer vernetzten Welt, so sein Credo, gehört das Nachdenken über Sicherheit zu guter Unternehmensführung.

Text: **Johannes Winterhagen** | Fotografie: **Matthias Haslauer**

Hamburg, ein Verwaltungsgebäude aus den 1920er-Jahren. Im Büro von Kurt Sievers finden sich dezente Hinweise auf seine Leidenschaft: das Bergsteigen. Auf mehr als 6.000 Meter Höhe war er schon. Wer solche Abenteuer wagt, weiß, wie wichtig eine realistische Risikoeinschätzung ist. Die spielt auch in Sievers beruflicher Aufgabe eine wichtige Rolle: Er verantwortet das weltweite Automobilgeschäft von NXP.

Herr Sievers, wie schließen Sie Ihr Auto auf?
Ich nutze die normale Funkfernbedienung. Aber meinen neuen Dienstwagen kann man auch mit dem Smartphone öffnen und verriegeln. Ich habe mich während der Registrierung dabei ertappt, wie ich darüber nachdachte, ob das wirklich sicher ist. Technisch kann es das sein. Aber auch das Nutzungsverhalten bestimmt darüber, wie sicher eine Lösung ist.

Die meisten Autofahrer dürften gar nicht wissen, dass die Funksignale eines Schlüssels von Autodieben abgehört werden können.
Insgesamt ist das Bewusstsein für Sicherheitsrisiken nicht sehr groß, egal um welches Endgerät es sich handelt. Ich denke sogar, dass die Achtsamkeit bei jungen Menschen, die mit dem Internet aufgewachsen sind, eher abnimmt. Denken Sie nur an das Bezahlen mit der Kreditkarte im Internet. Je jünger die Menschen sind, desto eher nutzen sie diesen Bezahlweg.

Gleichzeitig steigt das Bedrohungspotenzial.
Eindeutig. Vernetzung steigert das potenzielle Risiko. Und der Vernetzungsgrad steigt in nahezu allen Bereichen unseres Lebens.

Kann es durch spektakuläre Hacks zu einem Bumerang-Effekt kommen und die Akzeptanz wieder abnehmen?
Es ist unabdingbar, dass die Sicherheit mit der Vernetzung Schritt hält. Wenn wir das Vertrauen der Konsumenten nicht haben, stellt das einen Hemmschuh für die Entwicklung dar. Die Industrie steht hier in der Verantwortung, nicht nur, indem sie sich um die bestmögliche Sicherheit auf Systemebene kümmert, sondern auch indem sie das Thema erklärt und so Vertrauen schafft.

Auch wo sehr sichere technische Lösungen möglich sind, etwa bei der elektronischen Gesundheitskarte, führt das nicht zwangsläufig dazu, dass diese genutzt werden.
Eine gute Lösung ist nie nur technisch eine gute Lösung, sondern eine, die gesellschaftlich genutzt wird. Dafür muss sie von der öffentlichen Hand unterstützt werden. Das gilt nicht nur für das Gesundheitswesen, sondern auch für den Verkehr, zum Beispiel wenn man Autos und Ampeln vernetzen will. Es muss durch entsprechende Authentifizierung sichergestellt sein, dass Grün wirklich Grün ist, davon hängt im Zweifelsfall menschliches Leben ab.

Haben denn die Planungsämter in den Kommunen das Know-how dafür?
Sicher nicht, dafür gibt es spezialisierte Unternehmen. Aber die Kommune muss hier eine neue Rolle übernehmen: die Rolle des Schiedsrichters, der darüber entscheidet, wer an einem solchen System unter welchen Bedingungen teilnehmen darf. Das Sicherheitskonzept für vernetzten Verkehr beruht im Wesentlichen darauf, dass jedes einzelne Signal daraufhin geprüft wird, ob es von einem authentifizierten Absender stammt. Es geht also weniger um technisches Verständnis als darum, die Rolle des Systemeigners zu akzeptieren.

Was bedeutet Sicherheit im Cyberraum eigentlich?
Wenn wir über Cyberattacken sprechen, ist es sinnvoll, sich darüber klar zu werden, was da angegriffen wird: zunächst unsere Gesundheit und sogar unser Leben. Das ist neu und spielte bei früheren Sicherheitskonzepten eine untergeordnete Rolle. Zweitens gibt es Attacken auf unser Eigentum. Damit meine ich neben physischem Eigentum explizit auch geistiges Eigentum, unsere Daten und unser Wissen. Und drittens Angriffe auf die industriellen Prozesse. ▷

„Heute sind die sichersten Lösungen immer Hardware-basiert. In Zukunft werden ideale Lösungen immer aus der Kombination von Hard- und Software bestehen. Das bedeutet auch: Ohne entsprechende Hardware wird es nicht gehen."

KURT SIEVERS

Das sind Kernbereiche unserer Gesellschaft. Sicherheit kann daher nur bedeuten, diese drei Bereiche so zu schützen, dass sich der Bürger im Cyberraum bewegen kann, ohne dass ihm Schaden entsteht.

Aber so etwas wie ein absolut sicheres, vernetztes IT-System ist doch gar nicht möglich, oder?
Ja und nein. Was man nicht hundertprozentig absichern kann, ist das Fehlverhalten von Menschen. Leichter abzusichern ist hingegen die Maschine-zu-Maschine-Kommunikation. Technische Systeme können schon weitgehend sicher gestaltet werden – wenn man nur alles anwendet, was verfügbar ist. Eine Studie von Kaspersky zeigt jedoch, dass 92 Prozent aller vernetzten Industrieanlagen weltweit nicht den aktuellen Sicherheitsstandards entsprechen. Auch Deutschland schneidet – aufgrund seiner industriellen Historie und der Vielzahl älterer Anlagen – dabei übrigens nicht besonders gut ab.

Das zeigt auch, dass Sicherheit immer nur für den Moment existiert.
Was heute sicher ist, muss noch lange nicht in fünf Jahren sicher sein. Man muss immer Schritt halten. Auch bei den Hackern gibt es so etwas wie Moden.

Was ist denn gerade in Mode?
Sehr viel kriminelle Energie fließt momentan tatsächlich in den Autodiebstahl durch sogenannte Relais-Angriffe. Was sowohl Unternehmen als auch Privatpersonen sehr beschäftigt, ist das Hacken von Accounts. In der Regel wird der Besitzer des Computers dann mit der Sperrung seiner Festplatte erpresst. Eine dritte Mode besteht darin, Identitäten und E-Mails zu fälschen. Passiert so etwas in einem Unternehmen und kommen dadurch gefälschte Anweisungen in Umlauf, kann erheblicher Schaden entstehen. Aber alle drei Angriffsformen können systemtechnisch abgefangen werden.

Welche Branche geht denn bei der Anwendung neuer Sicherheitslösungen voran?
Grundsätzlich hat die Automobilindustrie die Chance, die Rolle des Leithammels zu übernehmen. Mit dem automatisierten Fahren übernimmt sie mehr denn je Verantwortung für Leib und Leben ihrer Kunden. Aber die Autobranche täte sehr gut daran, das aufzunehmen, was anderorts bereits getan wird, zum Beispiel um Bezahlfunktionen abzusichern. Ich würde mir hier mehr Offenheit wünschen.

Wollen Sie sagen, dass die Entwickler von Embedded Systems, nicht nur in der Autoindustrie, zu stolz sind, um sich bei der Finanzbranche etwas abzuschauen?
Natürlich gibt es begründete Unterschiede. So können Sie im Auto oder in einer Maschine nicht alle Berechnungen in Echtzeit auf zentralen Servern ausführen lassen. Aber mein Credo besteht darin, dass es in einer komplexen Welt keine Schande ist, sich 70 bis 80 Prozent einer Lösung abzuschauen und nur für den Rest eigene Wege zu gehen. Ich sage das deshalb, weil ich beobachte, dass der Expertenfluss von Branchen, die viel mit Absicherung zu tun haben, in die klassische Industrie eher gering ausfällt. Manchmal wundere ich mich darüber.

Bei Cybersicherheit denkt man zunächst an Software. Welche Rolle spielt denn die Hardware?
Heute sind die sichersten Lösungen immer Hardware-basiert. In Zukunft werden ideale Lösungen immer aus der Kombination von Hard- und Software bestehen. Das bedeutet auch: Ohne entsprechende Hardware wird es nicht gehen.

Name:
Kurt Sievers

Firma:
NXP

Position:
Executive Vice President und General Manager für das weltweite Automobilgeschäft

Geboren:
19. August 1969 in Augsburg

Ausbildung:
Diplom-Physiker, Diplom-Informatiker

Lieblings-Elektrogerät:
sein Autoschlüssel

Out of Office anzutreffen:
im Gebirge

Warum ist das so?
Sie steigert die Geschwindigkeit einer sicheren Transaktion deutlich. Nehmen wir das Beispiel elektronischer Reisepass. Ohne den Chip mit einem „Embedded Secure Element" im Inneren würden das Einlesen und der Abgleich mit biometrischen Werten und den Datenbanken im Hintergrund viel zu lange dauern. Sprich, die Schlangen am Flughafen würden länger. Das ist übrigens auch der Grund, warum alle Kredit- und EC-Karten mittlerweile einen Chip haben: Der Kunde wägt in der Regel Bequemlichkeit und Sicherheit gegeneinander ab.

Künftig bezahlen wir vermutlich ohnehin mit dem Smartphone ...
In vielen Ländern ist das heute schon möglich. Dann sorgt ein „Hardware Secure Element" dafür, dass die Nahfeldkommunikation zwischen Terminal und Smartphone absolut sicher ist. Das wird in die meisten Smartphones schon heute eingebaut und kann auch für andere Funktionen genutzt werden. Ich war kürzlich in einem Hotel in Singapur. Dort kann man statt der üblichen Plastik-Magnetkarte einen virtuellen Zimmerschlüssel für die Dauer des Aufenthalts auf das Smartphone laden.

Wenn schon sichere Hardware verbaut wird, was muss darüber hinaus passieren?
Ein gutes Sicherheitskonzept bedingt, dass schon in einer frühen Entwicklungsphase über die spätere Anwendung nachgedacht wird. Man darf nicht erst über die Funktion und das Gerät nachdenken und sich ganz am Schluss um die Sicherheit kümmern. Wir nennen das ideale, synchrone Vorgehen daher „Security by Design".

Bleibt der Haken, dass es Konsumenten sehr schwer fallen dürfte, zu erkennen, ob ein technisches Gerät dem neuesten Stand in Sachen Sicherheit entspricht.
Auch hier stehen wir als Industrie in der Verantwortung. Es liegt an uns, das Vertrauen der Bevölkerung für vernetzte Technologien zu gewinnen. Dafür ist es wichtig, einheitliche Zertifizierungsstandards zu entwickeln.

Sie meinen eine Art TÜV-Siegel?
Grundsätzlich ja. Nur sollte das auf europäischer Ebene passieren, damit eine hohe Wiedererkennbarkeit gegeben ist. Auch sonst denke ich, dass wir auf europäischer Ebene eng zusammenarbeiten sollten. Deshalb beteiligt sich NXP als Gründungsmitglied an der öffentlich-privaten Partnerschaft „Europäische Cybersicherheitsorganisation", die Anfang Juli ins Leben gerufen wurde. Insgesamt mobilisieren die EU und die Unternehmen 1,8 Milliarden Euro. Damit lässt sich schon etwas erreichen.

Viele mittelständische Unternehmen dürften sich an einem solchen Großvorhaben nicht beteiligen.
Einerseits werden sie von ihren Verbänden, etwa dem ZVEI, vertreten. Andererseits muss man aber auch kritisch sagen: Viele Unternehmer haben noch nicht erkannt, dass Cyberangriffe heute das größte unternehmerische Risiko bedeuten, wenn man die Wahrscheinlichkeit des Eintritts und die Schadenshöhe gemeinsam betrachtet. Jeder Unternehmer und jeder Topmanager sollte das zu seinem persönlichen Thema machen und nicht den IT-Spezialisten überlassen.

Das Gleiche müsste dann für Spitzenpolitiker gelten.
Ja. So sollte Cybersicherheit in der Forschungsförderung den gleichen Stellenwert wie Elektromobilität oder die Energiewende besitzen. Wir sollten auch die Chance sehen, die Cybersicherheit für unser Exportgeschäft besitzt. Wo immer auf der Welt ich hinkomme und erwähne, dass wir die Chips für den elektronischen Reisepass entwickelt haben, gewinne ich sofort die volle Aufmerksamkeit. „Secured in Germany" ist Exportschlager.

Herr Sievers, herzlichen Dank für das Gespräch. □

Vorbeugen ist besser als heilen

Im Jahr 2015 führt die Kriminalstatistik für Deutschland 45.793 Fälle von Internet- und Kommunikationskriminalität auf, davon wurden nur rund 30 Prozent aufgeklärt.

Illustration: Barbara Geising

Aus Schaden wird man klug – nicht so bei Block Transformatoren. Das inhabergeführte Unternehmen begreift Informationssicherheit als Chefsache. Dazu gehört auch: über Cyberangriffe offen reden. Denn zahlreiche Studien zeigen: Auch der Mittelstand ist zunehmend betroffen.

Text: **Johannes Winterhagen**

Eines Tages steht ein erboster Kunde vor dem Werktor am Stadtrand von Verden an der Aller. Wo seine Ware bleibt, will er wissen. Schließlich habe er bereits Vorkasse geleistet und nun sei die Lieferung wirklich fällig. Der Haken an der Sache: Die Bestellung lief über eine Internetseite, die gar nicht von dem Unternehmen betrieben wurde. Auch das österreichische Konto, auf das der Kunde in der Hoffnung auf einen besonders günstigen Preis sofort überwies, gehört nicht dem Unternehmen, sondern einem Cyberkriminellen. Was sich auf den ersten Blick nach einer unwahrscheinlichen Geschichte anhört, hat Jörg Reichelt wirklich erlebt. Er ist Geschäftsführer der AC-Elektronik GmbH, einem internen Zulieferer von Block Transformatoren, die sein Vater Wolfgang Reichelt als CEO leitet. Rechtlich war die Sache klar: Zwar war auf der gefälschten Internetseite die Anschrift der Firma korrekt angegeben, aber da diese Seite selbst gefälscht war, kam ein rechtlich gültiger Vertragsabschluss nicht zustande. Auch wenn kein materieller Schaden entstanden ist, sagt Jörg Reichelt: „Diese Erfahrung zeigt, wie groß das Risiko durch Identitätsdiebstahl ist." Erst kürzlich habe die USA-Gesellschaft von Block eine E-Mail erhalten, in der sie dazu aufgefordert wurde, 8.000 Dollar auf ein bestimmtes Konto zu überweisen. Unter der Mail prangte die Signatur „W. Reichelt". Auch dieser Betrugsversuch flog jedoch auf: Die Gesellschaft fragte bei Block-Chef Reichelt nach, ob die Anweisung tatsächlich von ihm stammte.

Beide Fälle brachte Jörg Reichelt zur Anzeige. Bislang konnten die Täter jedoch nicht ermittelt werden. Die Kripobeamten versprachen dies auch nicht. „Wir haben zu wenig Leute und nicht ausreichend Technik", so die Entschuldigung. Trotzdem zeigen sich Vater und Sohn überzeugt: „In einem solchen Fall muss sofort Anzeige erstattet werden." Ein derart ausgeprägtes Verständnis von Rechtsstaatlichkeit lässt sich nicht durch geringe Aufklärungsquoten abschrecken. Im Jahr 2015 führt die Kriminalstatistik für Deutschland 45.793 Fälle von Internet- und Kommunikationskriminalität auf, davon wurden nur rund 30 Prozent aufgeklärt. In der Realität ist die Anzahl von Cyberattacken um ein Vielfaches höher, nur gelangt die überwältigende Mehrzahl niemals zur Anzeige. Es scheint, als haben sich weite Kreise in Bevölkerung und Wirtschaft damit abgefunden, dass das Internet teilweise ein rechtsfreier Raum ist. ▷

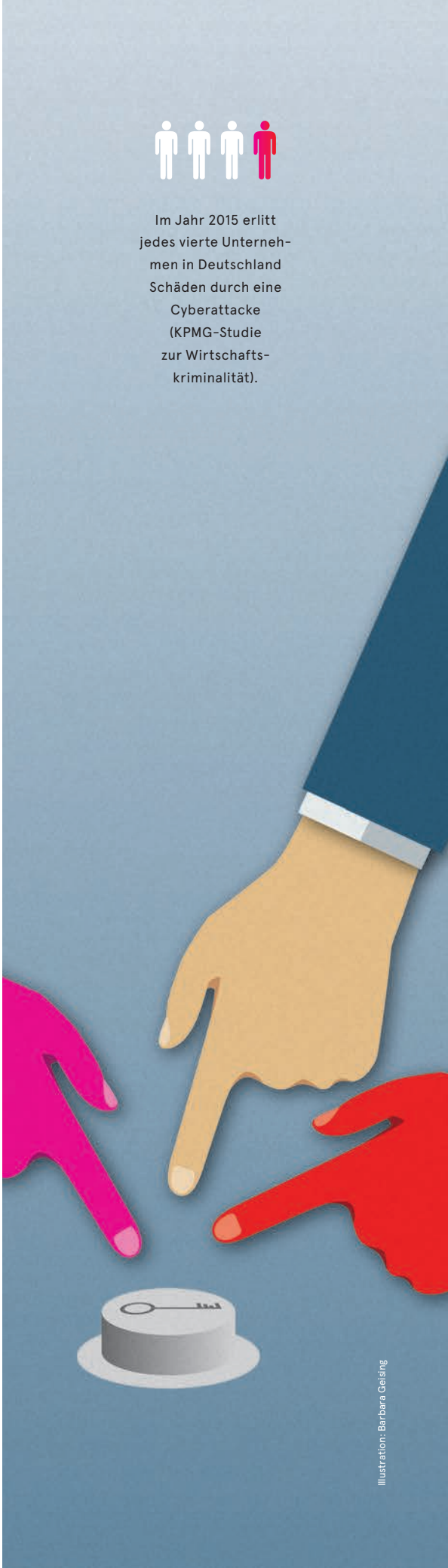
Wolfgang und Jörg Reichelt haben das nicht. Und deshalb scheuen sie sich nicht, anders als viele andere Unternehmer, offen über Cyberkriminalität zu reden. Zum Gespräch erscheinen sie mit Udo Thiel, die Geschäftsführung von Block ist nun komplett. „Das größte Risiko sind wir selbst“, sagt der gleich zu Beginn. Denn in vielen Unternehmen gelten Sonderregeln für die Geschäftsführung. Nicht so bei Block. „Wir halten uns an die Regeln, die für alle Mitarbeiter gelten“, sagt dann auch Wolfgang Reichelt. Wenn er eine neue App auf seinem Smartphone installieren will, konsultiert er zuvor die IT-Abteilung. Und sein Sohn, der unter anderem für die Produktion verantwortlich ist, hat zwei Laptops im Büro. Mit dem einen kommuniziert er nach außen, der andere ist für interne Abfragen gedacht. „Es ist manchmal etwas anstrengend, das konsequent durchzuhalten“, so Jörg Reichelt. „Doch man muss sich klarmachen, dass jede Form der Vernetzung die Gefahr birgt, dass Fremde auf die eigenen Daten zugreifen.“

Das hohe Bewusstsein für Cybersicherheit, das in dem Familienunternehmen herrscht, hat seinen historischen Ursprung in gänzlich analogen Zeiten. Denn bei Block herrscht schon seit Jahrzehnten zollrechtlich die höchste Sicherheitsstufe: Das Unternehmen darf direkt ans Flugzeug liefern. Da gilt es, unter allen Umständen sicherzustellen, dass niemand unbefugt auf das Firmengelände gelangt und in die Prozesse eingreift, sei es nur, um ein „Päckchen“ zu schmuggeln. Auf das digitale Zeitalter übertragen, heißt das: kapseln, was immer zu kapseln ist. So ist es einem Lieferanten von Werkzeugmaschinen zwar erlaubt, Ferndiagnosen durchzuführen – doch die Verbindung dafür muss für jede Wartung einzeln freigeschaltet werden, sie wird anschließend wieder gekappt. „Wir diskutieren die Risiken bei jeder einzelnen IT-Neuerung“, sagt Thiel. Zum Beispiel bei der derzeit anstehenden Beschaffung einer neuen Telefonanlage, die mit dem Internetprotokoll IP arbeitet.

„Man muss sich klarmachen, dass jede Form der Vernetzung die Gefahr birgt, dass Fremde auf die eigenen Daten zugreifen.“

JÖRG REICHELT

Ist mit dieser Philosophie eine vernetzte Produktion, wie sie durch die Vision von „Industrie 4.0“ verkörpert wird, überhaupt machbar? „Natürlich“, sagt Wolfgang Reichelt. „Innerhalb der eigenen Fabrik können Sie vernetzen, so viel Sie wollen.“ Kritischer sieht er die Vernetzung mit der Außenwelt, wie sie zunehmend unter dem Aspekt durchgängiger Prozessketten diskutiert wird. Es gilt das Motto: Unsere Daten sind unsere Daten, sie werden auch physikalisch nicht bei irgendeinem Cloud-Dienstleister gespeichert, sondern auf verteilten Servern auf dem eigenen Firmengelände. Denn auch bei dem Trafohersteller liegt immer mehr Know-how in der Software. So ist die neueste Generation der Maschinen, die für das Aufwickeln der Kupferspulen verwendet werden, mit einer im Haus entwickelten Steuerung versehen. Auf dem freien Markt waren entsprechend leistungsfähige Anlagen nicht zu erhalten. „Es hat schon seinen Grund, dass wir als einziges Unternehmen unserer Branche noch immer vorrangig ▷



Im Jahr 2015 erlitt jedes vierte Unternehmen in Deutschland Schäden durch eine Cyberattacke (KPMG-Studie zur Wirtschaftskriminalität).

Illustration: Barbara Geising

sps ipc drives

Nürnberg, 22.–24.11.2016

Besuchen Sie uns in Halle 4, Stand 4-311

„IT-SICHERHEIT IST EIN ELEMENTARER BESTANDTEIL UNSERER UNTERNEHMENS-PHILOSOPHIE“ W. REICHELT, CEO

Transformatoren • Stromversorgungen • Drosseln • EMV-Filter

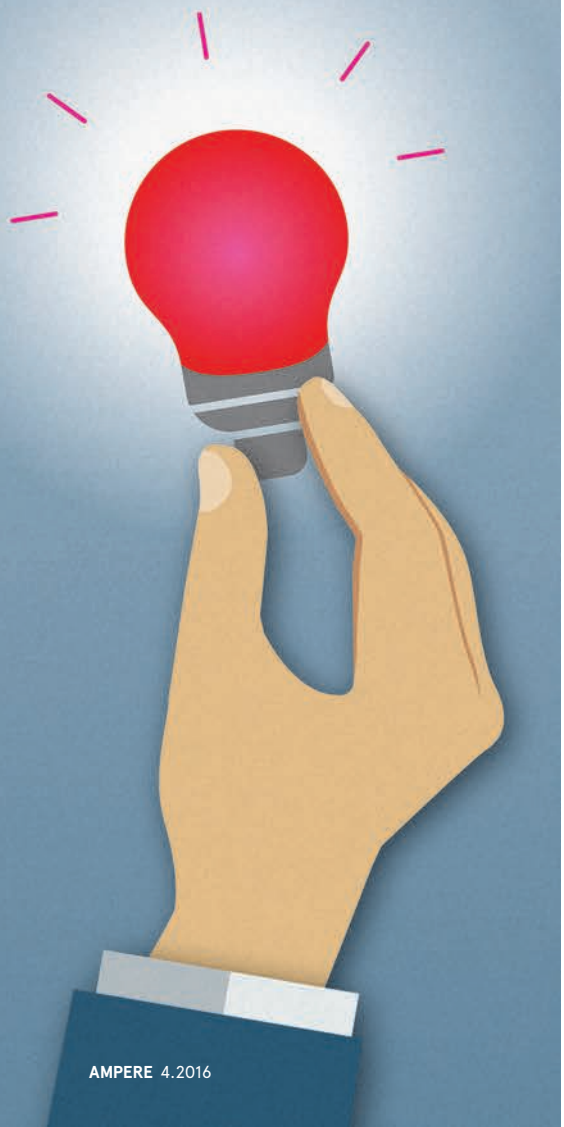
BLOCK Transformatoren-Elektronik GmbH
Max-Planck-Straße 36-46 • 27283 Verden
Phone +49 4231 678-0 • Fax +49 4231 678-177
info@block.eu • block.eu

BLOCK
block.eu

Laut KPMG schätzen

82 %

der Unternehmen das Risiko Cyberkriminalität als hoch oder sehr hoch ein.



in Deutschland produzieren“, sagt Wolfgang Reichelt. „Aber damit werden wir als Angriffsziel auch attraktiver.“

Technische Schutzmaßnahmen sind nur eine Seite der IT-Sicherheit. „Den Faktor Mensch darf man nicht unterschätzen“, warnt Jörg Reichelt. Die Gefährdungsanalyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gibt ihm Recht. Als besonders stark wachsende Angriffsmethode wird im aktuellen Lagebwricht die Installation von Schadsoftware genannt, insbesondere sogenannte Ransomware, die Dateien, Computer oder sogar Server verschlüsselt und erst nach Zahlung eines „Schutzgeldes“ wieder freigibt. Die Erpressung bedarf der Installation eines Programmes auf dem entsprechenden Rechner oder Netzwerk. Möglich wird das meist, indem Mitarbeiter unbedacht einen E-Mail-Anhang öffnen oder auf einen Link klicken. Verschickt werden solche E-Mails selten gezielt, sie landen als Spam in einem entsprechenden Filter. So auch bei Block – mit dem Unterschied zu vielen anderen Betrieben, dass die Mitarbeiter selbst keinen Zugriff auf die Spam-Mails haben, sondern dass diese zunächst von der hauseigenen IT freigegeben werden müssen. „Völlige Sicherheit gibt es nirgends, wo Menschen arbeiten“, ist sich Jörg Reichelt bewusst. „Allerdings kann man das Risiko deutlich minimieren, indem man menschliches Fehlverhalten einkalkuliert.“

„Nur wenn mittelständische Unternehmen untereinander ihr Wissen teilen, können wir uns wirksam gegen Angriffe wappnen.“

WOLFGANG REICHELT

Auf Nummer sicher gehen heißt daher auch: Schwachstellen identifizieren. Zum Beispiel, indem Block regelmäßig einen externen Dienstleister damit beauftragt, das Firmennetzwerk zu hacken. Und sich selbst ajour halten, indem man Veranstaltungen besucht, mit Vertretern des Computer Chaos Clubs spricht, IT-Fachmagazine liest. „IT-Sicherheit ist Kernaufgabe einer guten Unternehmensführung“, sagt Wolfgang Reichelt. „Das sind wir als Familienunternehmen unseren Mitarbeitern schuldig.“ Und wenn eines Tages doch etwas Gravierendes passiert? Auch den Fall hat die Block-Geschäftsführung schon durchgespielt. Für maximal fünf Tage wäre der Betrieb beeinträchtigt, dafür sorgt eine Systematik kaskadierter Back-ups. Unschön wäre das, aber nicht existenzgefährdend.

Auch in einem solchen, hoffentlich nie eintreffenden Fall würde Wolfgang Reichelt seine Erfahrung gerne teilen. Nicht offen, aber doch in anonymisierter Form. „Nur wenn mittelständische Unternehmen untereinander ihr Wissen teilen, können wir uns wirksam gegen Angriffe wappnen.“ Das kürzlich in Kraft getretene IT-Sicherheitsgesetz sieht die Meldung von Vorfällen nur bei Angriffen auf kritische Infrastrukturen vor – insbesondere Großunternehmen hatten sich gegen eine umfassende Meldepflicht gewehrt. Den Austausch anonymisierter Schadensmeldungen könnte, so die Vorstellung Reichelts, der ZVEI auf freiwilliger Basis organisieren. „Wir können doch nur davon profitieren“, wirbt er für seine Idee. Versteckspiel war seine Sache noch nie. □

Illustration: Barbara Geising

Einfach zuverlässig: Anlagensicherheit von Endress+Hauser

Ein Griff, ein Klick – mit einer einfachen Handbewegung haben Sie gerade Ihre Sicherheit entscheidend erhöht. Vielleicht denken Sie dabei: „Wenn das doch nur immer so einfach wäre!“ Für die Sicherheit von Prozessen in Industrieanlagen braucht es mehr als eine Handbewegung. Und ist trotzdem so einfach: Denn Feldinstrumente von Endress+Hauser tragen zuverlässig zur Sicherheit Ihrer Anlagen bei. Ob beim Explosionsschutz nach Ex ia/Ex d sowie der funktionalen und konstruktiven Sicherheit. Sie haben Fragen? Sprechen Sie uns an!

www.de.endress.com/anlagensicherheit

sps ipc drives

Nürnberg, 22.–24.11.2016
Halle: 4A, Stand: 135

Endress+Hauser
Messtechnik GmbH+Co. KG
Colmarer Straße 6
79576 Weil am Rhein

Telefon 0 800 348 37 87
Telefax 0 800 343 29 36
info@de.endress.com
www.de.endress.com

Endress+Hauser
People for Process Automation

Identitätsdiebstahl gehört zu den häufigsten und am stärksten wachsenden Kriminalitätsformen in hochtechnisierten Ländern. Systeme, die allein auf Benutzernamen und Passwort setzen, gelten als nicht sicher. Doch erste Lösungen sind bereits in Sicht.

Text: **Laurin Paschek**

Ausweiskontrolle 4.0

Wie war die Welt doch früher so einfach. Wenn Lieschen Müller ein Konto eröffnen oder einen Kredit aufnehmen wollte, dann ging sie einfach in die nächste Bankfiliale. Der Filialleiter, den sie seit ihrer Kindheit kannte, erkundigte sich höflich nach dem Wohlergehen der Familie. Vielleicht wurde noch eine Kopie des Personalausweises angefertigt, und die Sache war erledigt. Mit der Digitalisierung der Wirtschaft sind aber gerade im Finanzsektor Anbieter auf den Markt gekommen, die ihr komplettes Geschäft online abwickeln. Alles funktioniert digital: Bankkonten eröffnen, Kreditkarten oder Mobilfunkverträge beantragen, Kredite aufnehmen. Aber wie weiß der Anbieter, dass der Kunde auch wirklich seine wahre Identität angibt?

In wichtigen Fällen nehmen die Anbieter das Postident-Verfahren in Anspruch, das aber aufwändig ist und einen Medienbruch darstellt. Denn der Kunde muss für jeden Authentifizierungsvorgang in die Postfiliale gehen. Ansonsten setzt beinahe die gesamte digitale Wirtschaft auf Benutzernamen und Passwort. „Das ist aber nicht sicher“, sagt André Zilch, Geschäftsführer von ValiPic in Eppstein bei Frankfurt am Main. „Im Grunde leben wir wie im Mittelalter – da konnte auch jeder Gaukler eine beliebige Identität annehmen.“ Im Vorfeld der neuen Zahlungsdienste-Richtlinie (PSD2) der Europäischen Union, die bis 2018 von den Mitgliedsstaaten in nationales Recht umgesetzt sein muss, haben sich Unternehmen wie ValiPic jetzt auf andere Formen der Identitätsfeststellung spezialisiert, die mehr Sicherheit versprechen. Denn die neue Richtlinie verpflichtet die Anbieter von Online-Zahlungsdiensten bei hohen Strafen, die Identität ihrer Kunden zu verifizieren. Wir stellen drei Firmen vor, die unterschiedliche Verfahren entwickelt haben.

IDENTIFIZIEREN PER VIDEO-CHAT

Als Armin Bauer 2012 ein Konto eröffnen wollte, schickte ihn seine Bank erst einmal zur nächsten Postfiliale. „Das Postident-Verfahren empfand ich als nicht mehr zeitgemäß“, berichtet er. So entwickelte der heutige Technikchef des Münchener Dienstleisters IDnow eine Alternative, die mittlerweile von mehr als 100 Banken und Finanzanbietern eingesetzt wird und nach eigenen Angaben den Anforderungen des Geldwäschegesetzes (GwG) und der am 1. Juli 2016 in Kraft getretenen eIDAS-Verordnung des Europäischen Parlaments und des Rats der Europäischen Union für die qualifizierte elektronische Signatur (QES) entspricht. Bei dem Verfahren wird ein Kunde, der per Smartphone oder am Rechner beispielsweise einen Kredit beantragt, auf die IDnow-Seite geleitet, auf der ein Video-Chat startet.

Ein Kundenbetreuer von IDnow führt den Kunden dann durch den Authentifizierungsvorgang: Über die Kamera im Computer oder Smartphone wird ein Foto des Anrufers angefertigt und mit dem Bild auf dem Personalausweis oder Reisepass verglichen, den der Kunde mit Vorder- und Rückseite in die Kamera hält. „Dabei laufen im Hintergrund ständig automatische Überprüfungen – etwa, ob die Hologramme auf dem Ausweis echt sind oder ob die Schriftgröße den Vorgaben entspricht“, erläutert IDnow-Geschäftsführer Sebastian Bärhold. Außerdem werden sämtliche Ausweisdaten erfasst und Prüfziffern abgeglichen. Das Ergebnis der Online-Identifizierung wird dann direkt nach Abschluss der Legitimation über eine Datenschnittstelle an die Bank oder den Finanzdienstleister übertragen – der eigentliche Geschäftsvorgang kann weiterlaufen. „Der audiovisuelle Kanal kommt einer Präsenzsituation sehr nahe“, meint Bärhold. „Wir bieten damit ein Verfahren an, das bequem ▷

Die Iriserkennung dient unter den biometrischen Merkmalen als besonders sicher. Selbst bei eineiigen Zwillingen unterscheidet sich die Struktur des Bindegewebes zwischen Iris und Hornhaut.

Foto: stocksy/Cameron Whitman, Fotolia/Jürgen Fälchle

Foto: stocksy/Mattia Pelizzari, Fotolia/treek

Maschinelle Erfassung und Bildverarbeitung von Fingerabdrücken sind technisch weit entwickelt. Noch in der Forschung sind Ultraschallverfahren, die den durch die Furchen variierenden akustischen Widerstand messen.

und kundenfreundlich ist, gleichzeitig aber ein hohes Maß an Sicherheit bietet."

Ergänzend zum sogenannten Video-Ident-Verfahren hat IDnow auch eine Methode für die qualifizierte elektronische Signatur entwickelt, mit der Verträge online abgeschlossen werden können – bei gleicher Rechtssicherheit wie bei einer handschriftlichen Unterzeichnung. Auch hier wird die Person über einen Video-Chat von einem IDnow-Mitarbeiter identifiziert. Per Mausklick kann diese Person dann einen Vertrag unterzeichnen; das System erzeugt im Hintergrund eine elektronische Signatur und ordnet sie dem jeweiligen Vertrag oder anderem wichtigen Dokument zu. „Neben Banken, Versicherungen und Finanzdienstleistern können auch andere Branchen diese Technologie nutzen", sagt Bärhold. Dabei hat er unter anderem die Gesundheitsbranche mit der digitalen Krankenakte, aber auch die öffentliche Verwaltung im Blick: So könnten beispielsweise auch Wohngeldanträge über die Schnittstelle abgewickelt werden.

PERSONEN UND UNTERNEHMEN ZUORDNEN

Einen ähnlichen Ansatz bietet WebID an, identifiziert dabei aber nicht nur Einzelpersonen, sondern auch Unternehmen. Darüber hinaus können die Nutzer auch hier Verträge rechtsgültig mit einer qualifizierten digitalen Signatur unterschreiben, Vollmachten erteilen oder Lastschriftmandate einrichten. „Anfang 2014 waren wir das erste Unternehmen, das vom Bundesfinanzministerium als GwG-konform zugelassen wurde", berichtet Geschäftsführer Frank S. Jorga, der das Berliner Unternehmen gemeinsam mit Franz Thomas Fürst aufgebaut hat und inzwischen mehr als 160 Mitarbeiter beschäftigt. Auch WebID nutzt das Tablet oder Smartphone des Kunden, damit ein Mitarbeiter in einem verschlüsselten Video-Chat die jeweilige Person identifiziert und das Ausweisdokument auf Echtheit prüft. Durch Eingabe einer sechsstelligen Transaktionsnummer, die der Kunde per SMS oder E-Mail erhält, wird der Vorgang abgeschlossen. Neben der reinen Personenidentifikation bietet WebID mit diesem Verfahren auch gezielt eine Altersprüfung an, etwa für Lottogesellschaften. „Es ist aber auch möglich, den Führerschein als Dokument zu überprüfen, beispielsweise für Car-Sharing-Anbieter", erläutert Jorga.

Zum Authentifizieren von Unternehmen werden zunächst – ebenfalls per Video-Chat – die handelnden Personen identifiziert. Dann prüfen die Mitarbeiter von WebID anhand eines gescannten Handelsregister-Auszugs oder mit Hilfe des elektronischen Handelsregisters die Vertretungsberechtigung und gleichen gegebenenfalls zusätzliche wirtschaftlich Berechtigte ab, etwa die Inhaber des Unternehmens. „Das kann in Einzelfällen auch schon mal eine Handvoll Ansprechpartner sein", erläutert Jorga. „Die Identifikation von Unternehmen ist weitaus komplexer als die von Einzelpersonen und wird nur von wenigen Dienstleistern angeboten."

Seit März 2014 hat WebID rund 1,5 Millionen Überprüfungen durchgeführt, etwa 15 Prozent der Überprüften wurden unter anderem wegen mangelhafter Bildqualität, aber auch wegen dringenden Tatverdachts auf Identitätsbetrug abgelehnt. „Wir hatten bislang nach erfolgreicher Prüfung aber noch keinen einzigen Betrugsfall", berichtet Jorga.

BIOMETRISCHE MERKMALE ERFASSEN

André Zilch vom Dienstleister ValiPic verfolgt einen anderen Lösungsansatz. Er verweist auf die Neufassung der Zahlungsdienste-Richtlinie (PSD2) der Europäischen Union. „Die Richtlinie verpflichtet die Anbieter, die Identität ihrer Kunden sicher festzustellen", berichtet Zilch. „Das stellt neue Anforderungen an die zuverlässige Zuordnung digitaler Identitäten an real existierende Personen."

Mit seinem System ValiPro setzt Zilch auf ein Verfahren, das auf der persönlichen Überprüfung beruht. Dabei geht der Kunde, der zum Beispiel ein Konto bei einem Internet-Zahlungsdienstleister eröffnen will, zu einer Registrierstelle, die ähnlich einer Postagentur in einem Partnerbetrieb eingerichtet ist. Bislang betreibt ValiPic 100 solcher Registrierstellen, will das Angebot aber bis 2018 bundesweit auf 2.000 Filialen ausweiten. Mit Hilfe des Personalausweises oder Reisepasses werden dort die administrativen Daten überprüft. Zusätzlich können je nach Geschäftsvorgang vor Ort aber auch einzelne biometrische Merkmale des Kunden erfasst und dem Datensatz hinzugefügt werden, etwa biometrische Gesichtsmerkmale, die Stimme, der Iris-Scan oder das Bild der Handvenen. Die vor Ort erfassten Daten werden dann an den Geschäftspartner des Kunden weitergegeben und sind fortan verfügbar, in diesem Beispiel für Internet-Zahlungen des Kunden.

Der große Vorteil an biometrischen Merkmalen ist, dass damit auf Benutzernamen und Passwörter völlig verzichtet werden kann. „Nach der PSD2-Richtlinie wird bei Internetzahlungen von mehr als zehn Euro eine Zwei-Faktor-Authentifizierung notwendig", sagt Zilch. „Von den Faktoren Besitz, Wissen und Biometrie müssen zwei erfüllt werden." So kann der Faktor Besitz über ein Smartphone erfüllt werden – mit einem biometrischen Merkmal wie der Stimme wäre dann bereits die sichere Identifizierung möglich. □

Auf der guten Seite der Macht

Foto: cartoonstock/Harris, S

Programme, Internetseiten und Passwörter – vor den Teilnehmern des Schüler- und Studentenwettbewerbs „Cyber Security Challenge Germany“ ist nichts sicher. Die Initiative verfolgt das Ziel, junge IT-Talente frühzeitig zu fördern – und sich damit den Nachwuchs zu sichern, den Unternehmen brauchen, um sich in einer vernetzten Welt vor Hackern zu schützen.

Text: **Marc-Stefan Andres**

Tobias Scharnowski klappt seinen Laptop auf. Er fährt den Rechner hoch und ruft die Website der Cyber Security Challenge Germany auf. Zwei Minuten lang liest er die Aufgabe. Klingt einfach. Er soll das Autorisierungsprotokoll einer Internetseite austricksen und sich als Administrator einloggen. Der 25-Jährige überlegt kurz und hat die Lösung. Er muss sich in die Kommunikation zwischen dem Server und der Seite schalten, sich anschließend einer sogenannten „Injection“ bedienen. Er installiert in der Anfrage, die zwischen den Computern hin und her geschickt wird, eine eigene URL, die ihm – sehr vereinfacht gesagt – Administratorrechte zuspielt. Zehn Minuten später hat er die Aufgabe im Grunde gelöst. „Das kam mir aber alles viel zu einfach vor“, sagt Scharnowski. „Ich habe anschließend noch fünf, sechs Stunden darüber gebrütet, bis ich am Ende doch wieder zur ersten Lösung kam.“

Etwas ausprobieren, kreativ sein, um die Ecke denken, sich selbst infrage stellen und doch mit viel Selbstbewusstsein ein Ergebnis erzielen: Mit diesen Eigenschaften und Fähigkeiten hat der Student zum zweiten Mal das Finale der Cyber Security Challenge Germany erreicht. Mehr als 1.000 Schüler und Studenten nahmen im Jahr 2016 an dem Wettbewerb teil, den das Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen, Bocholt, Recklinghausen gemeinsam mit dem Bundesverband IT-Sicherheit e.V. (TeleTrusT) organisiert. Qualifizieren muss sich der IT-Nachwuchs über neun Aufgaben, die sie zu Hause am eigenen Rechner lösen. Die 20 Besten von ihnen fahren nach Berlin, wo sie in Teams gegeneinander antreten. Zusätzlich findet in der Hauptstadt eine Recruiting-Messe statt, auf der sich potenzielle Arbeitgeber präsentieren.

„Wer es nach Berlin geschafft hat, wird keine Probleme haben, in der Branche zu landen“, sagt Norbert Pohlmann. „Im Gegenteil, die jungen Spezialisten sind sehr gefragt. Die Studenten bekommen direkt Jobangebote, die Schüler können Werkspraktika machen“, fügt der Professor am Institut für Internet-Sicherheit hinzu. Große wie kleine Unternehmen und Behörden suchen händeringend nach Nachwuchskräften, die sich mit dem Thema auskennen. Der Grund: Je virtueller und vernetzter die Wirtschaft wird – Stichwort Industrie 4.0 –, desto gefährdeter sind auch die Produktionsprozesse und die Kommunikation. „Die IT befindet sich noch im Anfangsstadium, wenn es um Sicherheit geht“, zieht Pohlmann Bilanz. „Die Angreifer brauchen eben nur einen Fehler zu finden, während die Verteidiger alle Lücken schließen müssen.“ Umso wichtiger sei es, dass sich Schüler und Studenten mit diesen Fragen auseinandersetzen und schließlich auf der richtigen Seite stehen.

Das funktioniert vor allem über Begeisterung, ist der Organisator überzeugt. „Die Welt der Hacker fasziniert viele junge Leute. Das wollen wir ausnutzen.“ Mit Erfolg: Die Teilnehmerzahl hat sich 2016 fast verdoppelt. Dabei geht es um maximale Offenheit: „Wir sind nicht nur auf der Suche nach Informatikstudenten, sondern schauen auch in benachbarten Bereichen wie Elektrotechnik oder Wirtschaftsingenieurwesen.“ Pohlmann hat so auch Talente entdeckt, die er vorher nicht auf dem Schirm gehabt hätte. „Ich erinnere mich zum Beispiel an einen 15-jährigen Schüler, mit dem ich im vergangenen Jahr bei der Challenge zusammengesessen habe“, erzählt Norbert Pohlmann. „Er war sehr schüchtern und hat erst nach einer Weile angefangen, sich zu öffnen. Was ich herausfand: Er hatte noch nie Informatikunterricht gehabt, konnte aber hacken wie ein Weltmeister.“

Die Hacker-Karriere von Tobias Scharnowski sieht ähnlich aus. „In der Schule hatte ich zwar vier Sprachen, die erste Informatikstunde aber erst in der neunten Klasse. Da habe ich aber gemerkt, dass mich Software fasziniert“, erzählt Scharnowski. „Es war ein bisschen wie ein Spiel, das mich nicht mehr losgelassen hat.“ Ihn interessiert, was sich unter der Oberfläche verbirgt. Er arbeitet sich tief in die Probleme ein, versucht zu verstehen, warum Sicherheitslücken in Programmen entstehen oder wie man Verschlüsselungen knacken kann. Dafür recherchierte er im Internet, suchte Anleitungen und Programme und drang in die Welt des Hackings ein. „Ich bin ein detailliebender Mensch, habe ich gemerkt. Das kann ich so extrem gut ausleben.“ Wie viele der Schüler und Studenten, die bei der Challenge mitmachen, fasziniert ihn auch die Grauzone zwischen Legalität und Illegalität. „Ich kann mir sehr gut vorstellen, für ein Unternehmen zu arbeiten und dessen Systeme anzugreifen, um sie damit zu verbessern.“

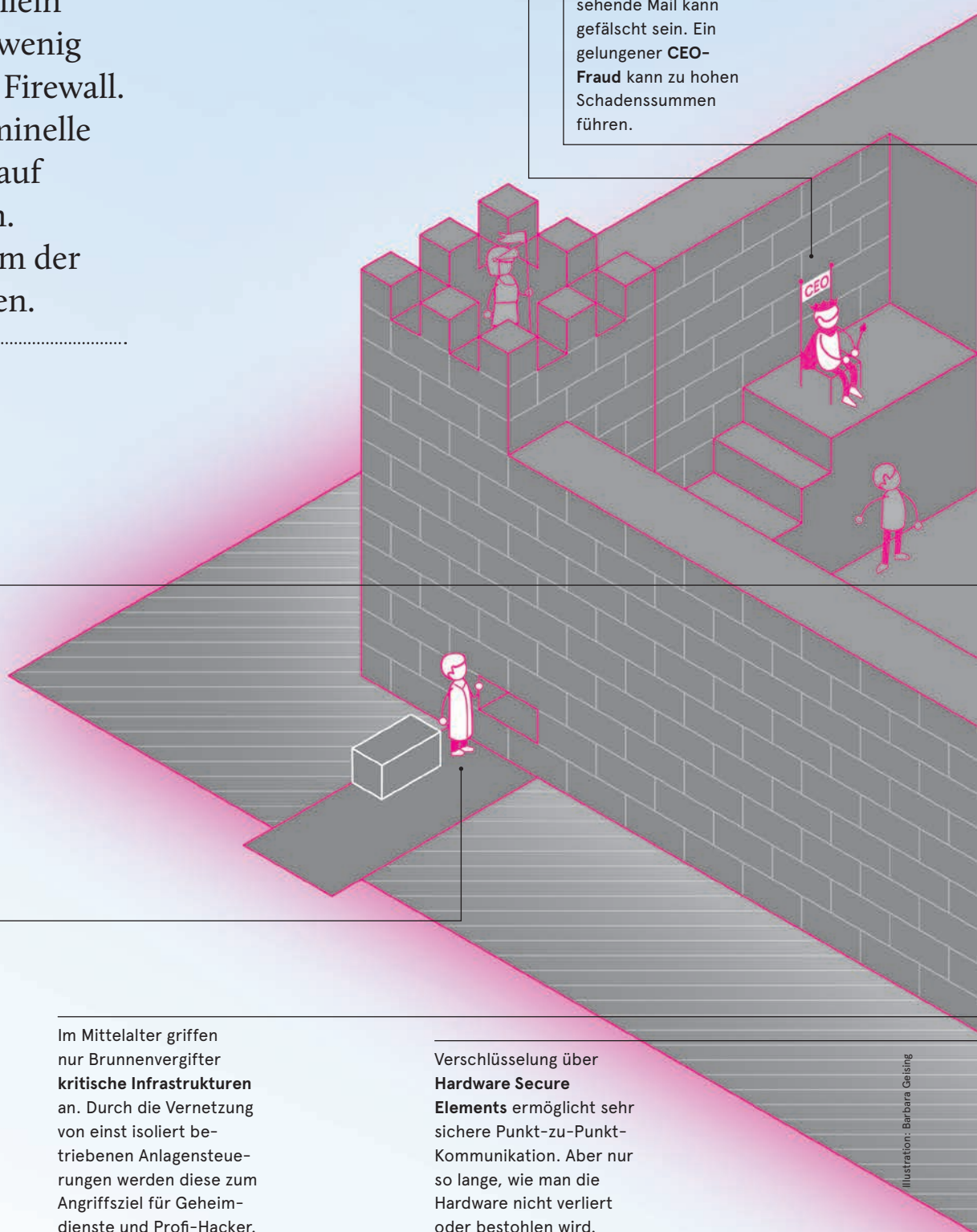
Hacker müssen breite Kenntnisse besitzen. Können Verschlüsselungstechniken vor allem mathematisch geknackt werden, kommt es im wachsenden Bereich der Industrie 4.0 hingegen auch auf Kenntnisse der Elektrotechnik an. „So kann man durch einen veränderten oder ungewöhnlichen Stromverbrauch Rückschlüsse auf mathematische Zusammenhänge ziehen und damit Systeme aushebeln“, erläutert Tobias Scharnowski. Der Student plant seine Ausbildung daher auf den Punkt. Nach dem Abitur, einem Work-and-Travel-Jahr in Australien und einem dualen Bachelor-Studium der Wirtschaftsinformatik an der privaten Fachhochschule der Wirtschaft in Paderborn geht er nun den nächsten Schritt. Er absolvierte ein Semester Mathematik in Bielefeld – „das brauchte ich, um in der Theorie fit zu werden“ – und startet nun zum Wintersemester an der Ruhr-Universität Bochum ein Studium der IT-Sicherheit. „Ich möchte hier die theoretischen Hintergründe der Informatik besser verstehen lernen“, sagt Scharnowski. „Erst danach möchte ich mich entscheiden, wo es für mich hingehen soll.“ □

Eine feste Burg?

Dicke Mauern allein bieten genauso wenig Schutz wie eine Firewall. Denn Cyberkriminelle schleichen sich auf vielen Wegen an. Ein Kompendium der größten Gefahren.

In vielen Unternehmen wird Cybersicherheit noch immer als Aufgabe für IT-Spezialisten betrachtet. Der **CEO** wähnt sich angesichts des ohnehin üppigen IT-Budgets in Sicherheit.

Wer würde nicht unmittelbar handeln, wenn er vom eigenen CEO aufgefordert wird, eine bestimmte Summe zu überweisen? Doch Vorsicht: Selbst eine völlig authentisch aussehende Mail kann gefälscht sein. Ein gelungener **CEO-Fraud** kann zu hohen Schadenssummen führen.



Wenn Sie nicht mehr an die Daten auf Ihrem eigenen Computer oder Server kommen, dann haben Sie entweder das Passwort vergessen oder sind Opfer eines Angriffs mit **Ransomware**. Die Schad-Software wird erst gegen Zahlung eines Lösegeldes entfernt.

Trauen Sie eigentlich allen Anbietern, deren Hard- und Software Sie verwenden? In komplexen Systemen können sich **„backdoors"** verbergen, über die Angreifer mühelos zum Ziel kommen.

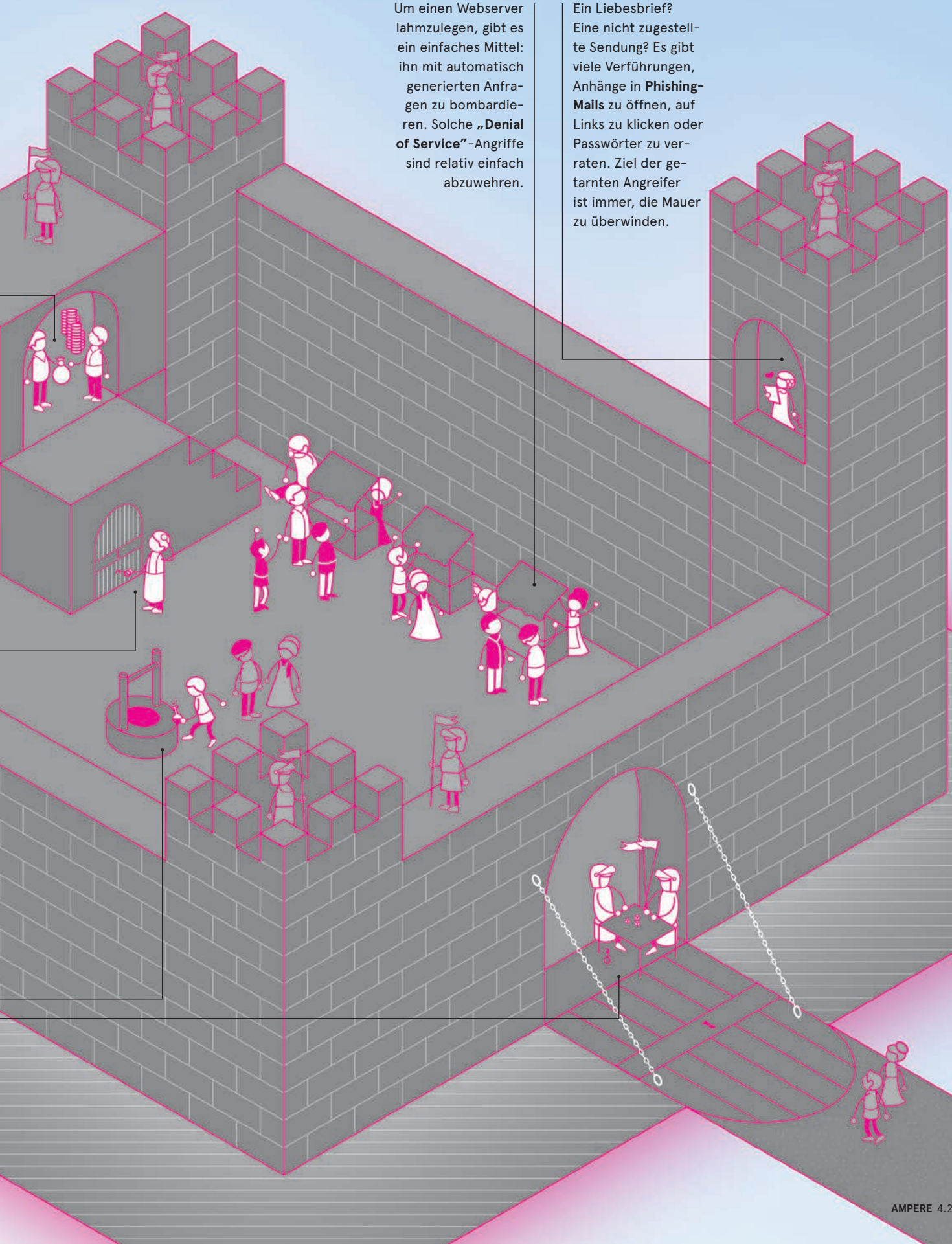
Im Mittelalter griffen nur Brunnenvergifter **kritische Infrastrukturen** an. Durch die Vernetzung von einst isoliert betriebenen Anlagensteuerungen werden diese zum Angriffsziel für Geheimdienste und Profi-Hacker.

Verschlüsselung über **Hardware Secure Elements** ermöglicht sehr sichere Punkt-zu-Punkt-Kommunikation. Aber nur so lange, wie man die Hardware nicht verliert oder bestohlen wird.

Illustration: Barbara Geising

Um einen Webserver lahmzulegen, gibt es ein einfaches Mittel: ihn mit automatisch generierten Anfragen zu bombardieren. Solche **„Denial of Service"**-Angriffe sind relativ einfach abzuwehren.

Ein Liebesbrief? Eine nicht zugestellte Sendung? Es gibt viele Verführungen, Anhänge in **Phishing-Mails** zu öffnen, auf Links zu klicken oder Passwörter zu verraten. Ziel der getarnten Angreifer ist immer, die Mauer zu überwinden.



Kronjuwelen in den

Technisch ist Cybersicherheit herzustellen. Da sind sich Ammar Alkassar, CEO von Rohde & Schwarz Cybersecurity, und Siemens-Vorstand Klaus Helmrich rasch einig. Doch ist eigentlich definiert, was geschützt werden soll? Und wer ist dafür verantwortlich?

Text: **Johannes Winterhagen** | Fotografie: **Dominik Gigler**

Sehen die Digitalisierung als Chance: Klaus Helmrich (links) und Ammar Alkassar

Wenn man die Bevölkerung fragt, was die größten Risiken für das Leben der Menschen in Deutschland sind, so werden Altersarmut und Pflegebedürftigkeit am häufigsten genannt. Geht die Diskussion über Cybersicherheit an den Menschen vorbei?

Helmrich: Die Digitalisierung beeinflusst mittlerweile alle unsere Lebensbereiche. Das gilt nicht nur im privaten Bereich, sondern zunehmend auch in der Industrie. Denn mit digitalen Technologien lassen sich neue und individuelle Produkte schneller entwickeln und mit neuartigen Methoden produzieren – bis hin zur individualisierten Massenfertigung. So entstehen durch die Digitalisierung ganz neue Chancen für Deutschland mit seiner ausgeprägten Fertigungsindustrie. Traditionell starke Branchen in unserem Land wie Elektrotechnik, Maschinen- und Automobilbau können damit ihre internationale Wettbewerbsfähigkeit steigern. Aber dazu müssen wir Anlagen, Daten und nicht zuletzt auch Menschen vor neuen Risiken schützen. Deswegen ist Cybersicherheit bei Siemens ein integraler Bestandteil von Automatisierungslösungen.

Alkassar: Es ist ganz normal, dass Menschen ihre Ängste auf das richten, was ihnen am nächsten liegt. Mit dem Älterwerden haben sie jeden Tag zu tun. Noch nicht für jeden ist die Bedeutung absehbar,

Panzerschrank

die die Digitalisierung für alle Menschen bekommen wird. Gesellschaftlich ist mit der Digitalisierung eine große Chance verbunden, insbesondere in Deutschland. Wir können auf Kompetenzen aufbauen, die hierzulande ohnehin schon ausgeprägt sind. Automatisierung und Cybersicherheit als Teil einer Smart Factory sind dafür ein gutes Beispiel.

Wie groß ist denn objektiv die Bedrohung durch Cyberkriminalität?
Alkassar: Die Bedrohung ist real. Der entscheidende Punkt ist dabei allerdings die Wahrnehmung. Denn an der einen oder anderen Stelle herrscht die Auffassung: Die Bedrohung ist so groß, dass wir bei der Digitalisierung auf die Bremse treten müssen. Es ist genau umgekehrt! Ich bin davon überzeugt, dass die Digitalisierung eine große Chance für uns bedeutet und dass Cybersicherheit die Voraussetzung dafür schafft. Ein gutes Beispiel dafür ist die Frage: Können wir im industriellen Bereich auch Cloud-Lösungen nutzen? Die Frage ist nicht unberechtigt angesichts der Nachrichten über Datenklau bei Dienstleistern im Konsumentenbereich. Wir müssen zeigen, dass wir im industriellen Bereich einen anderen Sicherheitsstandard erreichen, als er bei klassischer Office-IT bisher zum Zuge kam.
Helmrich: Datensicherheit hat verschiedene Aspekte: Zunächst einmal geht es um Know-how-Schutz; er bekommt einen ganz neuen Stellenwert für die Industrie. Wie beispielsweise ein Bier gebraut wird, das ist Kern-Know-how einer Brauerei – und lässt sich anhand von Daten nachvollziehen. Ein zweiter wichtiger Aspekt ist der Schutz von Anlagen vor Manipulation. Aber egal, welche Daten und was man schützen will: Eine Cloud ist zunächst einmal eine Cloud. Es gibt Untersuchungen, die zeigen, dass per se die Sicherheit nicht höher ist, wenn die Daten auf dem eigenen Firmengelände gehostet werden. Der Unterschied liegt im Umgang mit den Daten. Und mit dem steigenden Datenvolumen muss natürlich die Sicherheit noch stärker in den Fokus rücken. Da muss der deutsche Mittelstand noch mehr in ganzheitliche Ansätze für die digitale Fabrik investieren.
Alkassar: Darin – in dem ganzheitlichen Ansatz – besteht der Unterschied, zwischen dem, was wir mit Industrial Security meinen, und der klassischen Office-IT. Das ist auch kulturell geprägt. Der Ansatz von Software-Entwicklern im Silicon Valley ist ein anderer als das deutsche Ingenieursdenken. Wir denken erst einmal darüber nach, was wir eigentlich tun wollen, definieren die Anforderungen und setzen das dann um. Die angelsächsische ▷

„Wir müssen Anlagen, Daten und nicht zuletzt auch Menschen schützen. Deswegen ist Cybersicherheit bei Siemens ein integraler Bestandteil von Automatisierungslösungen."

KLAUS HELMRICH

Software-Industrie entwickelt – überspitzt formuliert – erst mal ein Programm und denkt dann darüber nach, wie man es verbessern kann. So sind Programme entstanden, mit Sicherheitslücken groß wie Scheunentore. Dergleichen können wir uns im industriellen Bereich nicht leisten. Entscheidend ist hier der ganzheitliche Ansatz, da bin ich ganz bei Herrn Helmrich. Übrigens gibt es heute schon gute technische Lösungen, wie eine von uns im Auftrag des BMWi durchgeführte Studie zeigt.
Helmrich: Auf der technischen Seite muss man zunächst drei Dinge sicherstellen: Anlagensicherheit, Netzwerksicherheit, Systemintegrität. Und dann kommen die organisatorischen Maßnahmen. Die beginnen mit der Frage: Was sind eigentlich die Kronjuwelen meines Unternehmens? Denn Kronjuwelen brauchen natürlich eine ganz andere Schutzhülle als allgemein zugängliche Informationen. Viele der Ängste im Mittelstand beruhen auf der Unsicherheit, welche Elemente eigentlich zwingend geschützt werden müssen. Wenn diese Frage erst einmal beantwortet ist, lässt sich die dafür notwendige Technik leicht installieren.

Nun wachsen ja aber Office-IT und industrielle Anlagen im Zuge von Industrie 4.0 stärker zusammen.
Alkassar: Natürlich nutzen wir am Ende des Tages das gleiche Internet. Aber wir können sicherheitskritische Anlagen mit relativ einfachen technischen Maßnahmen schützen – etwa durch eine Firewall für Industrie 4.0.
Helmrich: Technologisch sind wir uns einig: Man kann Netze separieren und trotzdem über abgesicherte Tunnel miteinander verbinden. Die Lösungen sind da.

„Wir müssen weg von der Erwartung, dass jeder Nutzer ein Experte für Cybersicherheit sein wird."

AMMAR ALKASSAR

Alkassar: Die Herausforderung für kleinere Mittelständler besteht darin, die für sie passende Lösung aus Hunderten von Lösungen auszuwählen. Ist dann die von Ihnen, Herr Helmrich, aufgeworfene Frage nach den Kronjuwelen nicht sauber beantwortet, dann kann das dazu führen, dass aus Furcht vor der Komplexität gar nichts unternommen wird. Dabei gibt es bedarfsgerechte Lösungen, die von „streng geheim" für die NATO bis hin zum Basisschutz für den Einzelhändler reichen.
Helmrich: Im Kern muss der Eigentümer oder CEO eines mittelständischen Unternehmens die Frage beantworten, wie er die digitale Transformation aller Prozesse im Unternehmen und somit die Zukunftsfähigkeit sicherstellt. Die zweite strategische Weichenstellung, die ebenfalls Chefsache ist: Wie sieht denn mein digitales Angebot nach außen aus? Welche Daten liefere ich denn mit meinem Produkt in Zukunft aus? Und wie stelle ich deren Integrität sicher? Noch einmal: Sicherheit ist ein unverzichtbarer Teil der digitalen Transformation.

Nun gibt es neben der Technik ja noch den Faktor Mensch, der zum Beispiel aus Versehen einen infizierten E-Mail-Anhang öffnet. Was empfehlen Sie?
Alkassar: Wir müssen weg von der Erwartung, dass jeder Nutzer ein Experte für Cybersicherheit sein wird. Auch Netzwerkadministratoren sind in erster Linie Netzwerkexperten. Wir müssen also technische Systeme so gestalten, dass das Risiko für unbeabsichtigtes Fehlverhalten systembedingt reduziert wird. Und auch gegen kriminelles Vorgehen helfen Technologien, zum Beispiel Systeme zur Informationsflusskontrolle. Sich allein darauf zu verlassen, dass sich alle Menschen in einem Unternehmen korrekt verhalten, wäre sträflich.

Helmrich: Auch hier arbeiten wir von zwei Seiten. Einerseits benötigt man natürlich geeignete Technik, etwa um nachzuverfolgen, wann wer auf welche Informationen zugreift. So etwas bauen wir in unsere digitalen Lösungen bereits ein. Andererseits brauchen aber auch die eigenen Mitarbeiter ein Gefahrenbewusstsein. Daher schulen wir fortlaufend in Fragen der IT-Sicherheit. Wichtig ist, dass man das nicht einmal macht, sondern das Wissen permanent auffrischt.

Noch einmal zur technischen Seite: Wo sehen Sie denn den größten Forschungs- und Entwicklungsbedarf in Sachen Cybersicherheit?
Helmrich: Wir müssen verstehen, dass wir über stetig wachsende Datenmengen reden. In der Produktion müssen die Systeme, an denen wir arbeiten, in Echtzeit reagieren. Hier sehe ich noch Felder, in denen Forschung und Wissenschaft uns neue Möglichkeiten eröffnen können. Zudem sollten wir überlegen, wie wir in der Kombination von Software und Hardware ein noch höheres Sicherheitsniveau erreichen können. Das sind aus meiner Sicht wichtige Zukunftsfelder.
Alkassar: Wir sollten auch berücksichtigen, dass sich die Rahmenbedingungen für Cybersicherheit ändern. So können wir erwarten, dass in den nächsten Jahren Quantencomputer marktreif werden. Die setzen aber einige der Mechanismen außer Kraft, die wir heute im Bereich der Kryptologie verwenden. Darüber hinaus sollten wir die Mikrokern-Technik, die heute zum Teil schon in der Luftfahrt verwendet wird, auf ihre Einsatzfähigkeit im industriellen Umfeld prüfen. Ein dritter Bereich ist die Kombination von Künstlicher Intelligenz und IT-Sicherheit, vor allem, wenn es um den Umgang mit großen Datenmengen geht.

Im industriellen Bereich müssen andere Wege gegangen werden als in der klassischen Office-IT. Nur welche?

Auch die gegnerische Seite entwickelt sich weiter. Ist denn absolute Sicherheit überhaupt zu erreichen?
Helmrich: Auch vor der Digitalisierung gab es keine absolute Sicherheit. Als man noch mit Bargeld

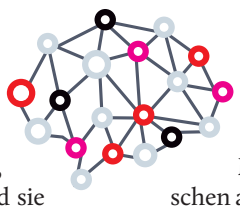
gezahlt hat, haben Diebe versucht, Panzerschränke zu knacken. Trotzdem haben sich Panzerschränke bewährt, um große Mengen Bargeld aufzubewahren. Für eine Geldbörse reichte hingegen ein abschließbarer Wandschrank. Das kann man auf das digitale Zeitalter übertragen: Kritische Infrastrukturen wie ein Elektrizitätswerk brauchen eine andere Absicherung als ein Einfamilienhaus. Und dazu reicht keine einmalige Entscheidung, sondern man muss ständig überprüfen, ob der Schutz noch gut genug ist.
Alkassar: Man darf nicht vergessen: Der wirtschaftlich größte Schaden entsteht durch Kollateralschäden. Diese sind nicht zielgerichtet und treffen jeden, der sich im vernetzten öffentlichen Raum bewegt. Cyberkriminalität ist ein funktionierendes Ökosystem, das heute schon die Größenordnung des Drogenhandels überholt hat. Aber wenn wir wissen, was die jeweiligen Kronjuwelen sind, die in den Panzerschrank sollen, können wir diese sehr gut schützen.

Herzlichen Dank für das Gespräch! □

DIE VERANTWORTUNG TRÄGT DER MENSCH

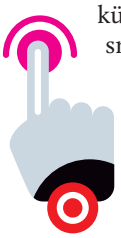
Binnen zehn Jahren gehören intelligente Maschinen zu unserem Alltag, prognostiziert der Wissenschaftsjournalist Ulrich Eberl. Damit sie nicht zu einer Gefahr für uns werden, müssen wir dem Einsatz künstlicher Intelligenz jedoch Grenzen setzen.

Text: **Ulrich Eberl**

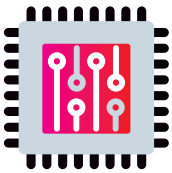


Maschinen werden sprechen und uns zuhören, unsere Gesten und Mimik verstehen, Texte, Bilder und Videos interpretieren und sie werden lernfähig sein. Sie werden vergleichen, beobachten, nachahmen und über Belohnungen lernen. Wir werden diesen smarten Maschinen schon in zehn Jahren überall begegnen, sie werden für uns ein ebenso selbstverständlicher Bestandteil unseres Alltags sein wie heute das Smartphone.

Es gibt bereits lernfähige Software, die Verkehrsschilder besser und schneller erkennt, als es die meisten Menschen vermögen, und sie kann vorhersagen, was in bestimmten Verkehrssituationen wahrscheinlich passieren wird. In Zukunft werden wir immer öfter unsere Fahrzeuge auf Autopilot schalten. Viele Transporte werden autonom erfolgen, elektrisch und vernetzt – mit fahrerlosen Elektrotaxis, elektronisch gekoppelten Lkw und mehr noch: Auf den Bürgersteigen werden automatische Einkaufswagen Bestellungen ausliefern, in der Luft bringen Drohnen eilige Pakete und in den Lagerhallen der Internet-Versandhändler suchen Roboter die Waren und machen sie versandfertig. In Fabriken werden die Maschinen Hand in Hand mit den Menschen arbeiten, in Hotels, Museen und Geschäften werden uns Roboter bedienen und Auskünfte geben und in den Küchen werden Maschinen selbsttätig das Essen zubereiten. Wir werden den Analysen der von uns befragten Smartphones oft stärker vertrauen als menschlichen Experten. Denn schon heute gibt es Computersysteme, die Millionen von Patientenakten durchforsten und bessere Diagnosen stellen als viele Ärzte. Solche kognitiven Systeme haben auch Märkte und Börsen besser im Blick als Bankberater und sie wissen Tage im Voraus, wann Züge oder Windturbinen gewartet werden sollten, damit sie gar nicht erst ausfallen.

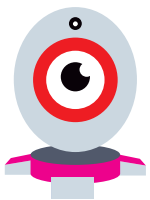


Letztlich ist der Trend eindeutig: Wir werden künftig in einer Gemeinschaft von Menschen und smarten Maschinen leben. Die heute noch meist getrennten Entwicklungsstränge des maschinellen Lernens, der Datenanalyse und Wissensverarbeitung, der Robotik und der autonomen Fahrzeuge sowie der Industrie 4.0 und des Internets der Dinge wachsen zusammen und



lösen eine Revolution aus, die alle Lebensbereiche radikal verändert: in den Haushalten und auf den Straßen ebenso wie in Fabriken und Büros. In den nächsten 25 Jahren wird sich die Leistung von Mikrochips noch einmal vertausendfachen, Sensoren werden kleiner und billiger und auf der Software-Seite werden die Techniken der Künstlichen Intelligenz immer leistungsfähiger. Viele Maschinen lernen anhand von Daten im Internet, deren Anzahl explosionsartig wächst. Es gibt Milliarden von Bildern, Videos, Audiodateien und Texten, die als Lerninhalte dienen können.

Kein Zweifel: Wir brauchen smarte Maschinen, als Assistenten für die älter werdende Bevölkerung ebenso wie für nachhaltige Energiesysteme, lebenswerte Städte und eine wettbewerbsfähige Industrie. Dennoch birgt auch diese Entwicklung neue Gefahren: Wenn Maschinen immer besser darin werden, Videobilder zu interpretieren, dann können sie auch gezielt nach Gesichtern suchen und im Extremfall als autonome Killerroboter – wie der Terminator im Film – auf Menschenjagd gehen. Wenn sie immer stärker vernetzt sind, entstehen ganz neue Einfallstore für Hacker, die dann autonome Fahrzeuge ebenso manipulieren können wie Industrieanlagen oder Energiesysteme.



Und wenn smarte Maschinen Daten aller Art analysieren und logisch zusammenführen, dann gibt es immer weniger technische Hürden für die lückenlose Überwachung von Personen – ein Alptraum für die Verteidiger der Privatsphäre. Mehr noch: Aus dem Einkaufsverhalten lassen sich detaillierte Kundenprofile und extrem personalisierte Werbemaßnahmen ableiten. Ebenso kann man aus der Kommunikation in sozialen Netzwerken auf Team- und Führungsfähigkeiten schließen, und sogar auf Persönlichkeitsstrukturen und Krankheiten. So haben Forscher herausgefunden, dass allein die Art und Weise, wie jemand das Internet nutzt, Hinweise auf eine Depressionserkrankung zulässt – sogar, bevor dies dem Betroffenen bewusst ist.

Etliche Städte setzen bereits mit Erfolg das Predictive Policing ein, ein Verfahren, das aus Daten wie Ort, Tatzeit, Beute und Vorgehen der Täter Muster destilliert und Vorhersagen über mögliche Folgetaten trifft. In Großbritannien hat die Polizei sogar schon ein Programm getestet, das – gefüttert mit Daten wie Zeugnissen, Jobs, Einkäufen oder Internetsurfverhalten – Wahrscheinlichkeitsaussagen trifft, ob bestimmte Personen erneut Gewalttaten begehen könnten.

Wie lange wird es dann noch dauern, bis Computer darüber entscheiden, ob jemand Kredite bekommt, welche Jobs er ausführen oder gar wo er sich aufhalten darf? Hitachi hat bereits ein lernfähiges System mit künstlicher Intelligenz eingeführt, das die Arbeitsabläufe von Angestellten analysiert und entscheidet, wo sie am besten eingesetzt werden sollten. China ist mit seinem Internet-Überwachungssystem auf dem Weg zum gläsernen Bürger und digitale Vordenker wie Tim O'Reilly propagieren die algorithmische Regulierung: Computersysteme, so sagen sie, wären in der Lage, Städte und Staaten effektiver und effizienter zu steuern als Menschen. Dabei würden allerdings nicht nur Verkehrs- und Energiesysteme optimiert, sondern das menschliche Verhalten an sich. Das geht dann so weit, dass Algorithmen das Einkaufsverhalten mit der Steuererklärung abgleichen, dass Überwachungskameras selbstständig Übeltäter verfolgen und dass sogar Mülleimer Passanten ermahnen, ihren Abfall korrekt zu entsorgen.

Wollen wir das? Wohl kaum! Was also tun, damit uns die smarten Maschinen mehr nützen als schaden? Wir müssen frühzeitig eine gesellschaftliche Debatte beginnen, Chancen und Risiken abwägen und festlegen, was sozial erwünscht ist und was nicht. Autonome Killerroboter sollten weltweit genauso geächtet werden wie Biowaffen oder Atombomben im Weltall. Was Maschinen eigenständig entscheiden dürfen, muss klar definiert sein. Existenzielle Entscheidungen – etwa im Gesundheitsbereich, der Rechtsprechung oder über die Kreditwürdigkeit von Personen – müssen letztlich von Menschen getroffen werden. Maschinen dürfen hier nur beratend tätig werden. Die Maßnahmen zum Schutz der Privatsphäre und der Datensicherheit müssen an die neuen Möglichkeiten lernender und wissensverarbeitender Systeme angepasst werden: durch klare Regeln, was etwa Arbeitgeber oder Versicherungen tun dürfen, ebenso wie durch möglichst sichere, gegenseitige Authentifizierungen von Menschen und Maschinen, durch hohe Transparenz, dezentrale Datenstrukturen und nutzergesteuerte Informationsfilter. Und wenn die Maschinen dann einmal so weit sind, dass sie eigenständig lernen, neugierig ihre Umgebung erforschen und sich selbst Ziele setzen, dann muss ein unverrückbares Ziel an oberster Stelle ihres einprogrammierten Belohnungssystems stehen: den Menschen helfen zu wollen. □

Ulrich Eberl, Jahrgang 1962, promovierte an der TU München in Biophysik, arbeitete bei Daimler und leitete 20 Jahre lang bei Siemens die Kommunikation zu Forschung, Innovationen und Zukunftstrends. 2016 veröffentlichte er das Sachbuch „Smarte Maschinen – Wie Künstliche Intelligenz unser Leben verändert".

Alles im Fluss

Pascal Meury, Energiemanager bei Endress+Hauser, betrachtet Abwärme nicht als Abfall, sondern als Rohstoff.

Abwärme entsteht in der Produktion von Endress+Hauser reichlich. Energiemanager Pascal Meury nutzt sie, um Warmwasser aufzubereiten und um im Winter zu heizen. Aber das ist nur ein Baustein in seinem Effizienz-Plan, der alle Mitarbeiter einbezieht.

Text: **Laurin Paschek** | Fotografie: **Matthias Haslauer**

Pascal Meury sitzt in einem Konferenzraum und versucht sich einzuloggen. Der Energiemanager bei Endress+Hauser im schweizerischen Reinach will sein Energiemonitoring-System anhand einer Datei erklären. Doch die Tastatur reagiert nicht. Auch ein zweiter Versuch bleibt erfolglos. Dann aber kommt Meury der Grund dafür in den Sinn: „Ach ja, ich muss sie erst manuell wieder einschalten. Diese Tastatur wird nicht häufig benutzt, so dass sie nicht dauernd im Standby-Betrieb laufen muss." Für Meury ist das keine Kleinigkeit: „Alleine wenn wir dort, wo es möglich ist, die Computer und Monitore nach Feierabend ganz ausschalten, können wir jedes Jahr 200.000 Kilowattstunden Strom einsparen – genug, um 40 Einfamilienhäuser zu versorgen."

Bei Endress+Hauser Flowtec in Reinach entwickeln und fertigen rund 1.000 Mitarbeiter Durchfluss-Messgeräte, zum Beispiel für Chemiewerke, Lebensmittel-Abfüllanlagen oder kommunale Wasserversorger. Der jährliche Stromverbrauch summiert sich auf fast neun Gigawattstunden. „Als ich Anfang 2015 als Energiemanager anfing, war mein erster Auftrag, hier die internationale Energiemanagement-Norm ISO 50001 einzuführen", berichtet Meury. „Unser Ziel war dabei, die zahlreichen Maßnahmen, die hier schon seit vielen Jahren umgesetzt wurden, unter einem Dach zusammenzuführen und nach innen und nach außen sichtbar zu machen. So wollen wir nicht zuletzt bei den Mitarbeitern ein Bewusstsein für den effizienten Umgang mit Energie schaffen."

Mit deren Ideen konnte Meury bereits neue Projekte realisieren und bestehende Installationen optimieren, so bei der Wärmerückgewinnung. Abwärme ist reichlich vorhanden in der Produktion. Sie entsteht etwa in den großen und mehr als 1.000 Grad Celsius heißen Öfen, in denen die Lötstellen von Rohren behandelt werden. Die Abwärme der Produktionsanlagen wird über einen Wasserkreislauf zu einer großen Kältemaschine mit 550 Kilowatt Leistung geführt, die im Keller steht und dem Wasser die Wärme entzieht – das kältere Wasser fließt dann wieder zu den Anlagen, um diese zu kühlen. Im Winter wird die Abwärme der Kältemaschine genutzt, um Heizungswasser aufzubereiten, das in einem 5.000-Liter-Tank gespeichert werden kann. Darüber hinaus gewinnt Endress+Hauser in mehreren Produktionshallen die Wärme aus der Raumluft über Wärmetauscher in der Lüftung und einer weiteren, mit Wärmerückgewinnung ausgestatteten Kältemaschine zurück. „Wir arbeiten uns mit jeder Modernisierung oder Ausbaumaßnahme schrittweise vor", berichtet Meury. „Bereits jetzt können wir im Winter unser neuestes Gebäude, das etwa ein Viertel der gesamten Energiebezugsfläche ausmacht, überwiegend mit Abwärme beheizen." Zwei Pelletöfen mit je 200 Kilowatt Leistung sorgen zudem dafür, dass in diesem Gebäude nur noch in Ausnahmefällen fossiler Brennstoff benötigt wird.

Meury ruft eine Datei auf, in der alle weiteren Maßnahmen zu sehen sind, die in letzter Zeit umgesetzt wurden. Etwa die Wärmepumpen-Boiler für Prozesswasser, das in der Produktion benötigt wird und 60 Grad Celsius heiß sein muss. „Das haben wir bislang zentral über einen Elektroboiler aufgewärmt", sagt er. Die neuen Boiler nutzen die Abwärme aus den Produktionsanlagen und benötigen 80 Prozent weniger Strom. Oder die LED-Leuchten, die bei jeder Modernisierung installiert werden. „Die amortisieren sich schon nach zweieinhalb Jahren. Denn wir betrachten nicht nur die Energiekosten, sondern auch die Wartungskosten, die bei LEDs deutlich niedriger sind."

Den größten Effekt sieht Meury aber in der Betriebsoptimierung, die mit Hilfe von rund 500 Messgeräten am Standort und eines online abrufbaren Energiemonitoring-Systems möglich geworden ist. „Die Messtechnik, die wir bei unseren Kunden installieren, hilft uns auch im eigenen Betrieb. Damit können wir überprüfen, ob wir tatsächlich von den richtigen Annahmen ausgehen", sagt er. „Häufig arbeitet man ja mit Alltagstheorien, die sich dann als falsch herausstellen." Mit dem Energiemonitoring kann er beispielsweise die Sollwerte der Energieflüsse überwachen, als effizient geltende Anlagen überprüfen, Stromfresser lokalisieren und mit dem Gebäudeleitsystem eingreifen, wenn etwa der Stromverbrauch unerwartet ansteigt. Neben Strom, Wärme, Kälte und Lüftung behält der Energiemanager auch die Versorgung mit den Industriegasen Stickstoff und Argon im Auge. „Damit habe ich das perfekte Werkzeug für meine Arbeit an der Hand", sagt Meury.

Mit regelmäßigen Schulungen sorgt Meury dafür, dass das auch bei seinen Kollegen ankommt. „Jeder hier am Standort sollte wissen, dass wir auf den Energieverbrauch schauen. Denn jeder kann dazu beitragen, ihn zu senken – im Kleinen wie im Großen." Schon während seiner Ausbildung zum Elektromonteur und während seines Bachelorstudiums der „Life Science Technologies" spielte Nachhaltigkeit eine wichtige Rolle für Meury. „Effizienz bedeutet, eine Sache besser zu machen, ohne auf etwas verzichten zu müssen. Mit Technologien für mehr Effizienz können wir dafür sorgen, dass auch die kommenden Generationen so leben können, wie wir leben dürfen." Auch wenn dafür mal eine Tastatur nicht gleich ihren Dienst tut. □

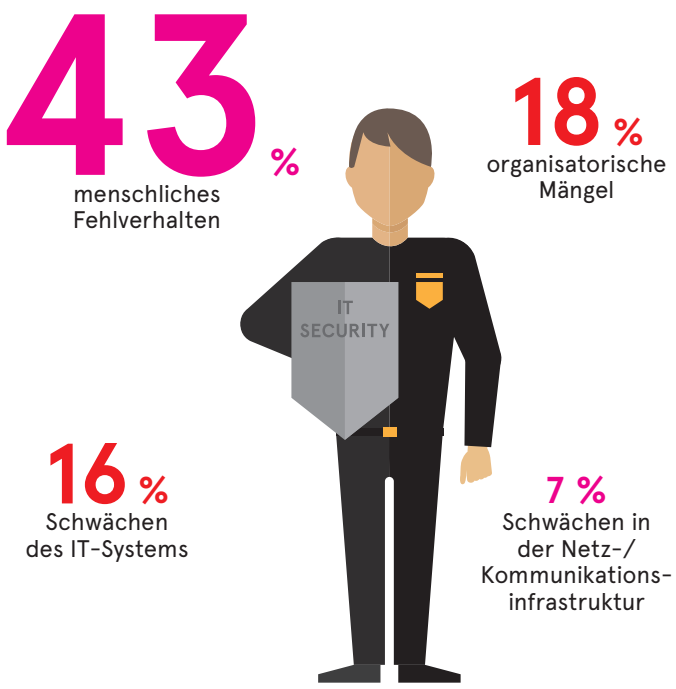
Hinweis der Redaktion: Dieser Bericht erscheint auch im ZVEI-Portal „Energieeffizienz erleben". Die Microsite berichtet regelmäßig von Überzeugungstätern, die sich für mehr Effizienz im Umgang mit Energie einsetzen.

Weitere Beispiele finden Sie unter http://www.energieeffizienz-erleben.de

Vorurteil 1: Schutz vor Cyberangriffen bietet vor allem ein ausgefeiltes technisches Abwehrsystem.

Fakt ist: Die meisten realen Vorfälle in Unternehmen sind auf menschliches Fehlverhalten zurückzuführen.

Interne Schwachstellen, die zum Eintreten eines Schadens durch einen Cyberangriff geführt haben:



Quelle: „Cybersicherheit: Wie sich die Automationsbranche schützt", ZVEI, 2016

Vorurteil 2: Der Datendiebstahl durch Cyberkriminelle und der daraus resultierende Know-how-Abfluss stellt die größte Gefahr für deutsche Unternehmen dar.

Fakt ist: Die größte Gefahr stellen die finanziellen Schäden durch Ausfall der IT dar.

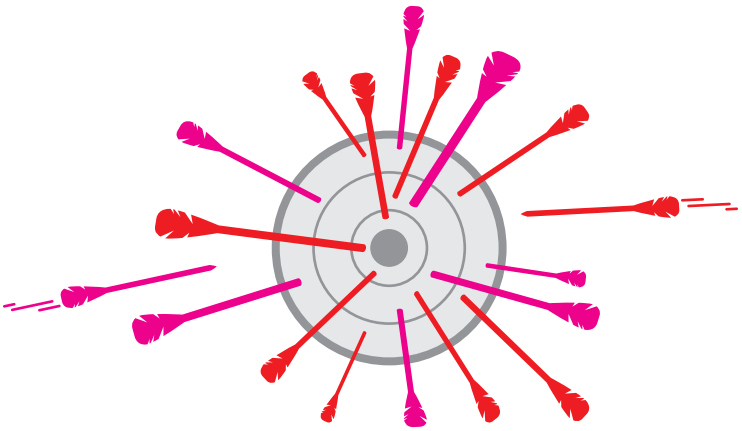
Entstandene Schäden durch nicht oder nicht vollständig abgewehrte Cyberangriffe auf Unternehmen der Automatisierungsbranche:

Quelle: „Cybersicherheit: Wie sich die Automationsbranche schützt", ZVEI, 2016

Vorurteil 3: Cyberangriffe sind doch vor allem gegen große Konzerne gerichtet.

Fakt ist: Mittelständische Unternehmen werden oft massiv angegriffen.

Angriffe auf Unternehmen mit bis zu 1.000 Mitarbeitern:



Ein Mittelständler muss mit durchschnittlich 18 Angriffen pro Jahr rechnen.

18 % aller Unternehmen werden häufiger als zehn Mal pro Jahr angegriffen.

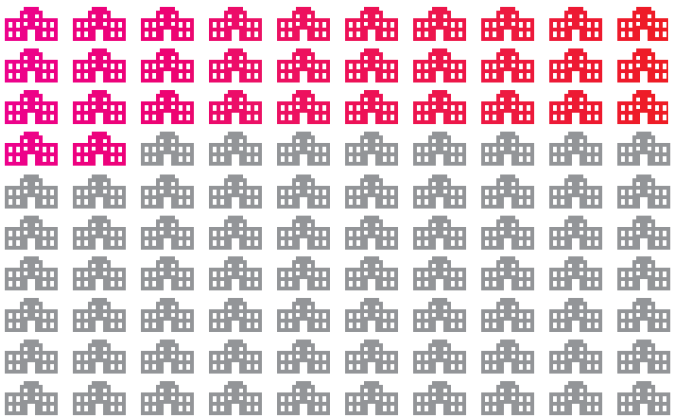
Jeder zweite Angriff (51 %) sollte die IT-System-verfügbarkeit reduzieren.

Quelle: Studie „Angriff aus dem Cyberraum", PWC, 2015

Vorurteil 4: Ich bin nicht erpressbar, schon gar nicht im virtuellen Raum.

Fakt ist: Erpressung über Ransomware gehört zu den am stärksten wachsenden Zweigen der Cyberkriminalität.

Online-Umfrage unter deutschen Unternehmen:



32 % aller Unternehmen waren innerhalb von sechs Monaten betroffen.

In 82 % aller Fälle erfolgte der Angriff über einen E-Mail-Anhang.

Bei 18 % der betroffenen Unternehmen dauerten die aus dem Angriff resultierenden Einschränkungen länger als 48 Stunden.

Quelle: Umfrage zur Betroffenheit durch Ransomware, Allianz für Cyber-Sicherheit, 2016

Heißes Eisen
Digital ist uns nicht egal

Digitalisierung ist eine Sache amerikanischer IT-Konzerne? Dr. Karl-Ulrich Köhler, seit Juli Vorsitzender der Geschäftsführung von Rittal, widerspricht: Die von Familienunternehmen geprägte Struktur der hiesigen Elektroindustrie spielt beim Rennen um die industrielle Zukunft ihre Vorteile aus.

Text: **Johannes Winterhagen** | Fotografie: **Markus Hintzen**

Mehr als Schaltschränke: Karl-Ulrich Köhler, CEO von Rittal, setzt auf die Digitalisierung.

Ein Flachbau, von außen unscheinbar, von dem Schild „Innovation Center“ abgesehen. Büroräume vermutlich, vielleicht ein Ausstellungsraum. Drinnen dann die Überraschung: eine lichtdurchflutete Halle, in der Hightech-Produktionsmaschinen stehen. „Hier sind Sie richtig“, sagt Karl-Ulrich Köhler einladend. Der Geschäftsführungsvorsitzende von Rittal erläutert, warum man in Haiger eine Musterfertigung von Schaltschränken betritt: „In unserem Innovation Center bilden wir den kompletten Wertschöpfungsprozess unserer Kunden ab. Das ist für uns die Arbeitsumgebung, in der unsere Entwickler miteinander und mit den Kunden neue Lösungen erarbeiten.“ Begeistert führt Köhler an einem Montage-Arbeitsplatz vor, wie ein zuvor digital geplanter Schaltschrank entsteht. Jeder einzelne Arbeitsschritt wird auf einem Tablet angezeigt, in der exakt richtigen Reihenfolge. Fehlmontagen sollen so ausgeschlossen werden – für Köhler nur ein Beispiel dafür, welches Potenzial in einer durchgängigen Digitalisierung von der Planung über Bestellung, Produktion bis hin zur Nutzungsphase steckt.

Köhler, der auch schon mal selbst zum Schraubendreher greift, fühlt sich sichtlich wohl in seiner neuen Aufgabe. Erst zum 1. Juli dieses Jahres übernahm er den Vorsitz der Geschäftsführung, nachdem er mehr als 35 Jahre bei verschiedenen Stahlkonzernen tätig war, zuletzt als CEO. Es ist eher selten, dass Topmanager aus börsennotierten Großunternehmen zu einem kleineren Familienunternehmen wechseln. „Die Unternehmensgröße ist für mich nicht relevant“, so Köhler. „Es geht vielmehr um den Systemansatz. Nach dem Motto ‚Denke groß, starte klein und handle jetzt‘ – und genau das entspricht der Kultur, die ich hier vorgefunden habe.“ Überraschend war das für Köhler nicht, schließlich war er bereits mehr als zehn Jahre Mitglied des Beirats der Loh-Gruppe, zu der Rittal gehört.

Digitalisierung wird in Deutschland oft mit IT-Unternehmen aus den Vereinigten Staaten verbunden. Dagegen ordnet Köhler ein: „Die mittelständisch geprägte Elektroindustrie ist ein großer volkswirtschaftlicher Faktor mit starker Innovationskraft.“ Dass sich Unternehmen auf die Digitalisierung einzelner Teilschritte industrieller Prozesse oder aber wie bei Rittal auf die gesamte Wertschöpfungskette konzentrieren, ermögliche eine hohe Geschwindigkeit in der Umsetzung neuer Ideen.

Tatsächlich zeigt eine im Auftrag des Bundesministeriums für Bildung und Forschung erstellte Studie zum Innovationsverhalten der deutschen Wirtschaft, dass die Elektroindustrie 9,9 Prozent ihres Umsatzes in Innovationen investiert. Dieser Wert umfasst auch Investitionen in Anlagen, die für Forschung und Entwicklung genutzt werden. Die Elektroindustrie ist damit auf Augenhöhe mit dem Fahrzeugbau und deutlich innovationsintensiver als die Chemie- und Pharmabranche, die 7,7 Prozent ihres Umsatzes in die Zukunft investiert. Allerdings zeigt dieselbe Studie auch: 78 Prozent der gesamten Innovationsausgaben entfallen auf Großunternehmen. Die Autoren mahnen: „Der Anteil kleiner und mittlerer Unternehmen (KMU) ist seit vielen Jahren rückläufig.“ Ein Problem dieser Betrachtung: Als KMU gelten nach amtlicher Definition nur Unternehmen mit bis zu 499 Beschäftigten, alle anderen werden in der Statistik als Großunternehmen geführt. „Man kann sich schon fragen, ob diese Einteilung ausreicht“, sagt Köhler vorsichtig. „Familienunternehmen, die nicht die Ressourcen eines DAX-Konzerns haben, aber wie wir mit 11.500 Mitarbeitern weltweit tätig sind, fallen da durch das Raster.“ Zum Beispiel, wenn das Bundesforschungsministerium ein 320-Millionen-Euro-Programm für die „Stärkung des Mittelstandes“ auflegt.

Das Modell Familienunternehmen hat sich für Köhler jedenfalls auch in einer digitalisierten und globalisierten Welt nicht überholt. „In einer wissensgetriebenen Industrie ist Langfristigkeit von Vorteil. Und Familienunternehmen pflegen eine Mentalität des ständigen Re-Investierens.“ Wichtig sei das auch, weil niemand bislang die allumfassende Lösung für Industrie 4.0 habe. „Wir befinden uns alle auf einer Lernkurve. Dazu benötigen Unternehmen eine Kultur, die es erlaubt, aus Fehlern zu lernen.“ Die vernetzten Wertschöpfungsstrukturen, die für die deutsche Wirtschaft so typisch sind, seien dabei hilfreich, Gelerntes schnell zu teilen und damit zu vermehren. Genauso wie das weltweit einmalige Ausbildungssystem. Auch wenn die Kleinstadt Haiger nicht mit hippen Lokalen glänzen kann, Nachwuchssorgen plagen Köhler nicht. Derzeit erhält Rittal jedes Jahr mehr Bewerbungen, als es weltweit an Beschäftigten hat. „Wir haben beachtliche Möglichkeiten und wollen diese nutzen“, zeigt sich Köhler optimistisch.

Ausprobieren: Im Innovation Center können neue Ideen sofort getestet werden.

Trotz der guten Voraussetzungen brauche es einen kritischen Blick auf die Rahmenbedingungen, mahnt Köhler. Als großen Konkurrenten sieht er neben den USA vor allem China. Im neuen, bis ins Jahr 2020 reichenden Fünf-Jahres-Plan ist festgeschrieben, dass 60 Prozent des künftigen Wirtschaftswachstums aus Fortschritten in Wissenschaft und Technologie resultieren sollen. Der Digitalisierung kommt dabei eine entscheidende Rolle zu. „Auf diesen staatlichen Fokus muss die Politik in Deutschland und Europa eine Antwort finden. In den Unternehmen wird es kreative und bedarfsgerechte Lösungen geben“, sagt Köhler. Durch die Glasscheibe des Besprechungsraums weist er auf die Musterfabrik. „Das ist die richtige Plattform, um solche Lösungen zu erarbeiten.“ □

Die kommende Ausgabe der AMPERE erscheint im Januar 2017 zum Themenschwerpunkt

Energieeffizienz erleben.

Ehrgeizige Ziele

Selbstbewusst: Die Schülerinnen Anja Dücker (links) und Roxana Esmaili (rechts) mit Anke Hüneburg, ZVEI

Berlin-Mitte. Unweit des Reichstags treffen Anja Dücker (16) und Roxana Esmaili (17) auf Anke Hüneburg, die für Energiepolitik verantwortliche Bereichsleiterin des ZVEI. Die Schülerinnen an der Herder-Oberschule verbindet die Teilnahme an „Jugend forscht“ und die Liebe zur Mathematik. Als Reporterinnen für AMPERE wollen sie herausfinden, was für höhere Energieeffizienz getan werden sollte.

Text: **Johannes Winterhagen** | Fotografie: **Michael Jungblut**

Wie halten Sie es persönlich mit der Energieeffizienz? Sie reisen doch sicher beruflich viel ...
Natürlich fliege ich viel. Wenn man häufig reist und es schnell gehen muss, stehen oft keine Alternativen zur Verfügung. Aber jetzt komme ich gerade mit dem E-Bike aus dem Bundesministerium für Wirtschaft und Energie.

Bedeutet Energieeffizienz eigentlich das Gleiche wie Energie sparen?
Nein, denn sparen könnte man ja auch, indem man die Produktion drosselt oder die Raumtemperatur im Winter auf 18 Grad absenkt und einen Pullover mehr anzieht. Auch wenn es etwas akademisch klingt: Energieeffizienz bedeutet, für eine gleich bleibende Ausgangsmenge weniger Energie einzusetzen – oder die Ausgangsmenge zu erhöhen, ohne den Energieeinsatz zu steigern. Wir müssen schon gucken, dass wir den richtigen Maßstab ansetzen und nicht nur auf die absolute Höhe des Energieverbrauchs schauen. Zumal Energieeffizienz kein Selbstzweck ist: Letztlich geht es um Klimaschutz, also darum, so wenig CO_2 wie möglich in die Atmosphäre zu entlassen.

Geld regiert die Welt. Warum also sollten Unternehmen in Energieeffizienz investieren?
Das wird im Unternehmen nicht anders betrachtet, als wenn eure Eltern über eine neue Heizung nachdenken. Man schaut sich an, was eine Anlage mit einem höheren Wirkungsgrad kostet und wie viel man bei den Betriebskosten dann über die Jahre einspart. So betrachtet, kann es sich daheim lohnen, etwas mehr Geld in eine Wärmepumpe zu investieren, weil die Energie ja dann kostenlos von der Umwelt zugeliefert wird. Wenn man sich die Kosten, die über den Lebenszyklus einer Anlage oder eines Produkts anfallen, genauer ansieht, dann rechnen sich ganz viele Effizienzmaßnahmen schon heute. Zum Beispiel, wenn man die Abwärme, die in industriellen Prozessen entsteht, nicht entweichen lässt, sondern in einem anderen Bereich des Unternehmens nutzt. Oder wenn man stromsparende LED-Beleuchtung mit Bewegungsmeldern kombiniert.

Das heißt, dass Energie eigentlich noch teurer werden müsste, damit sich energieeffiziente Technologien schneller durchsetzen?
Das würde ich nicht so sehen. Man muss ja auch die volkswirtschaftlichen und die sozialpolitischen Folgen sehen, die teure

„Insgesamt hat sich die Politik ehrgeizige Ziele gesetzt, was die Energieeffizienz betrifft."

ANKE HÜNEBURG

Energie hat. Energie muss bezahlbar bleiben. Wir haben im internationalen Vergleich schon heute nicht die günstigsten Strompreise.

Erneuerbare Energien werden vor allem dezentral erzeugt. Ist das effizient?
Ideal ist es natürlich, wenn dezentral erzeugter Strom möglichst in der gleichen Region verbraucht wird. Dazu braucht man eine intelligente Vernetzung zwischen Verbrauchern und Erzeugern. Durch Vernetzung und Digitalisierung werden wir Potenziale heben, von denen wir zum Teil heute noch gar nichts ahnen. Mit einer intelligenten Steuerung der Nachfrage in dezentralen Netzwerken lässt sich mit Sicherheit viel Energie einsparen.

Sie meinen so etwas wie das „Smart Home", das wir auf der IFA gesehen haben?
Neben dem Komfort ist Energieeffizienz ein ganz zentraler Punkt beim Smart Home. So kann ich zum Beispiel meine Heizung über mein Smartphone steuern, jeden einzelnen Heizkörper. Wenn ich mehrere Tage nicht da bin, kann ich die Heizung herunterfahren, das aber so einstellen, dass es bei meiner Rückkehr wieder warm ist. Aber das ist nur ein Beispiel, jeden Tag lerne ich neue Ideen kennen, was man durch Vernetzung noch tun kann.

Wie weit sollte Politik solche Technologien fördern?
Die Technologien, die wir für das Gelingen der Energiewende benötigen, sind größtenteils vorhanden. Forschungsbedarf besteht an einigen Stellen, vor allem bei den Speichertechnologien. Insgesamt hat sich die Politik ehrgeizige Ziele gesetzt, was die Energieeffizienz betrifft. Gerade bei diesem Punkt sollte man schon überlegen, wie man das Tempo erhöhen kann.

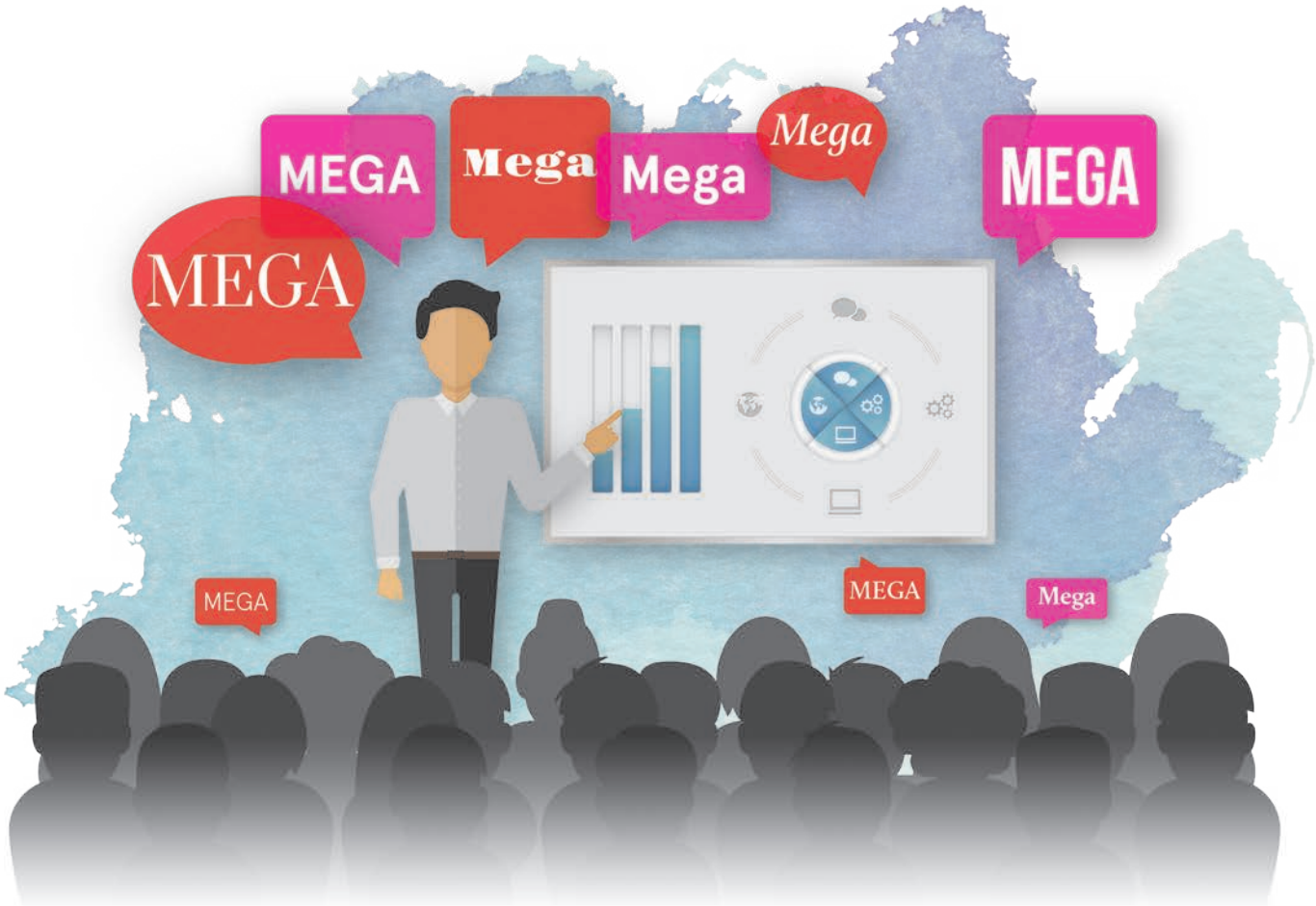
Sind die Ziele der Politik nicht zu ehrgeizig?
Für uns ist die politische Zielsetzung der Bundesregierung der Rahmen, in dem wir uns bewegen. Das gilt sowohl für den Ausbau erneuerbarer Energien als auch die Energieeffizienz. Beides gehört untrennbar zusammen.

Was bedeutet der Klimaschutzplan 2050, an dem die Bundesregierung derzeit arbeitet, für uns?
In der Vergangenheit war die Diskussion um erneuerbare Energien stark auf den Strombereich fokussiert. Nun stehen alle Sektoren, also auch Verkehr oder Gebäude, in der Diskussion. Die Sektoren sollen vermehrt gekoppelt werden – und das wiederum geht nur über den Energieträger Strom. Die Welt wird also noch elektrischer.

In der Zeitung lesen wir viel über die Flüchtlingskrise, aber kaum über Energiepolitik. Haben die Politiker keine Zeit mehr für das Thema?
Natürlich ist die Flüchtlingskrise ein wichtiges Thema für die Bundesregierung. Aber im Bundeswirtschaftsministerium, das für die Energiepolitik zuständig ist, arbeitet man weiter an den Dingen, die man sich für die aktuelle Legislaturperiode vorgenommen hat. Die Herausforderungen sind ja nicht kleiner geworden. So klafft beim Thema Energieeffizienz nach wie vor eine große Lücke zwischen der politischen Zielsetzung und dem, was wir heute erreicht haben.

Was fasziniert Sie persönlich am Thema Energie?
Meine Eltern waren beide in einem Braunkohlekraftwerk tätig. Nach der Schule begann ich dort zunächst eine Lehre. Das war eine harte Zeit mit vielen Nachtschichten. Danach habe ich dann Kraftwerkstechnik studiert und dann bei einem Energieversorger begonnen. Seit mehr als 15 Jahren bin ich nun in Berlin im politischen Umfeld tätig. Es war für mich als Ingenieurin anfangs eine ungewohnte Arbeit, die mir aber bis heute großen Spaß macht. □

Mega, der neue Trend



Ich besuche gerne Tagungen. Ob es um Elektromotoren oder um Smart Grids geht, ich lerne fachlich immer etwas dazu. Darüber hinaus schätze ich den gleichförmigen Rhythmus von halbstündigen Vorträgen, die ab und an durch eine Kaffeepause unterbrochen werden. Mittags und abends stärkt ein Buffet, meist kulinarisch nicht anspruchsvoll, dafür trifft man interessante Menschen. Und wenn das einmal nicht der Fall ist, so hat man über das gemeinsam Gehörte zumindest einen Anlass für eine fachliche Diskussion. Kurzum, eigentlich gehören Tagungen zu meinen liebsten Reiseanlässen.

In letzter Zeit leidet mein Wohlbefinden aber gelegentlich. Viele Vorträge beginnen mit beliebig austauschbaren Folien zu gesellschaftlichen Megatrends. Digitalisierung, Klimaschutz, Urbanisierung, alles ist megawichtig, auch wenn im Anschluss daran nur die Entwicklung eines Hochvolt-Wechselrichters thematisiert wird. Für die Beweisführung müssen stets dieselben Zahlen herhalten – etwa die 50 Milliarden vernetzter Geräte, die bis 2020 Einzug halten sollen. (Die Schätzung stammt übrigens von Cisco aus dem Jahr 2012, auch wenn die Quellenangabe meist fehlt.) Selbst auf Fachtagungen sehe ich immer mehr eingebundene Animationen, die die Grenzen von Powerpoint genauso ausreizen wie die Nerven des Vortragenden, wenn sie nicht funktionieren wie vorgesehen. Grafiken, die die Ergebnisse von Analysen und empirischer Arbeit darstellen, oder gar die mathematische Formel eines verwendeten Algorithmus scheinen heutzutage eine Zumutung darzustellen. Nach dem Vortrag darf man überdies immer häufiger keine Rückfragen stellen – es gibt ja nach dem Ende der Sektion noch ein Panel. Es mag an mir liegen, aber oft habe ich bis dahin vergessen, was genau ich zuvor fragen wollte.

Wie lieb sind mir doch die gelegentlich noch auftretenden Wissenschaftler alter Schule, die ohne den Umweg über Megatrends direkt zur Sache kommen, wenig Arbeit in die Gestaltung ihrer Folien investieren, dafür aber ihr Thema tief durchdrungen haben. Denn dabei lerne ich etwas über die Welt, etwa warum das eine funktioniert und das andere nicht. Ich ahne schon, was mancher denken mag: Alles zu akademisch, und um Wissen geht es doch in unserer schnelllebigen Zeit ohnehin nicht mehr. Wir sollten unsere knappe Zeit eher für den gegenseitigen Austausch, neudeutsch das „Networking“, nutzen. Aber worüber sollen wir reden, wenn wir nichts mehr wissen und nichts mehr verstehen? □

Text: **Johannes Winterhagen** | Illustration: **Barbara Geising**

Johannes Winterhagen, leitender Redakteur der AMPERE, ist beruflich viel unterwegs. Rund 100 Nächte pro Jahr verbringt er in Hotels. Auf der letzten Seite teilt er seine Reise-Beobachtungen mit den Lesern.


Digitalisierung live erleben –
Software-Einsatz in der Wertschöpfungskette
20. – 24. März 2017
Hannover ▪ Germany
cebit.com
Mobility &
Financial
Services
Produktion &
Maschinenbau
Multichannel &
After Sales
Deutsche Messe
Global Event for Digital Business
CeBIT

Die intelligente Produktion von morgen

Phoenix Contact – Ihr Partner für Industrie 4.0

„Mit unserer Erfahrung im Maschinenbau und in der Automatisierung sind wir bestens gerüstet, um die Digitalisierung unserer Welt in die intelligente Produktion von morgen zu verwandeln."

Roland Bent, Geschäftsführung Marketing & Entwicklung

Mehr Informationen unter Telefon (0 52 35) 3-1 20 00 oder
phoenixcontact.de/industrie40

PHOENIX CONTACT
INSPIRING INNOVATIONS

COM21-16.000.L1