06/2019 NOV/DEZ

NACHRICHTEN AUS TECHNIK, NATURWISSENSCHAFT UND WIRTSCHAFT

TECHNIK IN BAYERN

Das Regionalmagazin für VDI und VDE

Cyber-Sicherheit

Eventkalender & Aktuelles
Wann wird Stahl müde?
Zu Gast in München: VDI Italia

Foto: Silvia Stettmayer

Walter Tengler
Redaktion TiB

Cyber-Sicherheit geht jeden an

Es vergeht kein Tag, an dem nicht über Datendiebstahl, versuchte Hackerangriffe auf IT-Infrastrukturen oder das Ausspionieren von persönlichen Kontodaten berichtet wird.
Cyber-Sicherheit geht alle an, weil die Sicherheit von Daten, die vertrauensvolle Kommunikation über elektronische Medien und digitale Netze, weil stabile und sichere kritische Infrastrukturen, wie unser Stromnetz, unsere Krankenhäuser, Industrie- und Bankennetze einen Eckpfeiler für die technologische Souveränität Deutschlands bilden. Die digitale Vernetzung durchdringt alle Lebensbereiche und birgt ein großes Potential für technologische und soziale Innovationen. Cyber-Sicherheit ist damit eine Grundvoraussetzung für das Gelingen der digitalen Transformation geworden, im öffentlichen Bereich, in der Industrie, wie im Privaten.

Mehr Aufklärungsarbeit erzeugt ein höheres Problembewusstsein

Unsere wichtigste Cyberbehörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI), hat im Digitalbarometer 09/2019 eine Bürgerbefragung herausgebracht. Die Ergebnisse der Studie verdeutlichen, dass Bürgerinnen und Bürger sich generell möglicher Gefahren im Internet bewusst sind. Trotzdem werden wichtige Schutzmaßnahmen nicht konsequent umgesetzt. Nur 61 % haben ein aktuelles Virenschutzprogramm, 58 % verwenden sichere Passwörter und nur 32 % erneuern sie auch regelmäßig, verfügbare Updates installieren 36 % sofort, E-Mail-Verschlüsselung, der wichtigste Schutz gegen Abhörmaßnahmen, wird mit 19 % noch stiefmütterlich behandelt. Dabei hat das BSI am 20.08.19 der Presse mitgeteilt: Mit der quelloffenen Browser-Erweiterung „Mail-velope“ können Anwender unter Verwendung des Verschlüsselungsstandards OpenPGP verschlüsselte E-Mails deutlich nutzerfreundlicher austauschen.

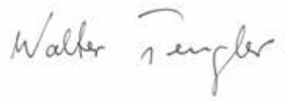
Digitales Erbe, kaum jemand kümmert sich darum

Es kann also fast jeder etwas zur Cybersicherheit beitragen, indem er seine Defizite erkennt und behebt. Eine weitere Aufgabe wäre die Sicherung seiner digitalen Hinterlassenschaft – in den sozialen Netzwerken, Cloud-Diensten, auf Smartphones, Laptops und PCs. Die wenigsten haben sich überlegt, was einmal mit ihrem digitalen Erbe passieren soll und erzeugen damit nicht selten große Probleme bei Nachkommen und Erben. Passwörter sind verschwunden, Zugriff auf Rechner, Smartphones und digitale Services geblockt, viele persönliche Daten, Konten, Texte und Bilder nicht auffindbar. Regeln Sie daher Ihr digitales Erbe rechtzeitig und legen Sie fest, was damit einmal passieren soll. Betrauen Sie am besten eine Person ihres Vertrauens mit der Aufgabe. Aber wie ist Deutschland insgesamt aufgestellt?

Deutschland ist in der Forschung zu Cyber-Sicherheit gut aufgestellt

In den Bereichen Kryptographie, Quanten Computing und Security Engineering, um nur einige zu nennen, zählen „wir“ zur Spitzenklasse. Jedoch fehlt die Umsetzung von Forschungsergebnissen in wirtschaftlich erfolgreiche Sicherheitsprodukte und -dienstleistungen. Ein schönes Beispiel ist der Einsatz von KI, um die IT-Sicherheit zu erhöhen. KI kann Unregelmäßigkeiten erkennen, Unbekanntes aufspüren, schneller und genauer bei der Erkennung und Behebung kritischer Bedrohungen reagieren und damit Kosten senken. Weiteres Interessantes gibt es in unseren Schwerpunktaufsätzen.

Viel Spaß beim Lesen wünscht Ihnen



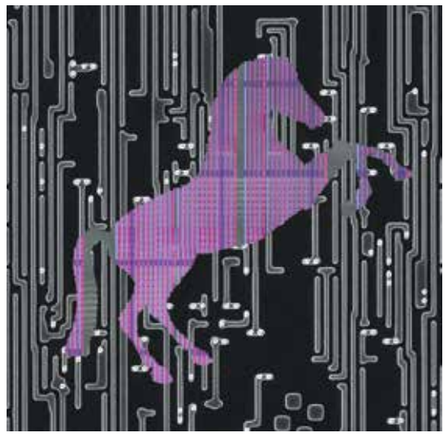
Cyber-Sicherheit

Durch die Digitalisierung von immer mehr Daten wächst die Gefahr einer missbräuchlichen Verwendung und damit auch die Bedeutung der IT-Sicherheit. Die Aufsätze befassen sich mit den Problemen und auch mit ermutigenden Lösungsansätzen.

Foto: T-Systems

Spurensuche zwischen Bits und Bytes: Das Labor eines IT-Forensikers

SCHWERPUNKT



Montage: H. Gieser, Fraunhofer EMFT 2019

Auch im Chip kann sich heute ein Trojanisches Pferd verstecken

HOCHSCHULE UND FORSCHUNG

AKTUELLES

RUBRIKEN

Beilagenhinweis – Wir bitten um freundliche Beachtung.
SCHULTZ GmbH & Co. KG

Titelbild: Fotolia
Foto: Weissblick

VDI Landesverband Bayern
VDI Bezirksverein München, Ober- und Niederbayern e.V.
Westendstr. 199, D-80686 München
Tel.: (0 89) 57 91 22 00, Fax: (0 89) 57 91 21 61
www.vdi-sued.de, E-Mail: bv-muenchen@vdi.de

VDI Bezirksverein Bayern Nordost e.V.
c/o Ohm-Hochschule, Keßlerplatz 12, D-90489 Nürnberg
Tel.: (09 11) 55 40 30, Fax: (09 11) 5 19 39 86
E-Mail: vdi@th-nuernberg.de

VDE Bayern, Bezirksverein Südbayern e.V.
Hohenlindener Straße 1, D-81677 München
Tel.: (0 89) 91 07 21 10, Fax: (0 89) 91 07 23 09
www.vde-suedbayern.de, E-Mail: info@vde-suedbayern.de

Eine hundertprozentige Sicherheit gibt es nicht

Wir sprachen mit Prof. Dr. Gabi Dreo Rodosek, Lehrstuhl für Kommunikationssysteme und Netzsicherheit an der Universität der Bundeswehr München und Leitende Direktorin des Forschungsinstituts CODE (Cyber Defence) über Cyberangriffe und Bedrohungsszenarien.

TiB: *Frau Prof. Dreo: Cyber Security bedeutet ja Sicherheit von Daten in Netzwerken. Stimmt das und wie kann man sicher im Netz kommunizieren?*

Prof. Gabi Dreo Rodosek: Die Informations- und Kommunikationstechnologie (IKT) ist heute in allen Bereichen der Gesellschaft von zentraler Bedeutung: Gesundheit, Mobilität, Bildung, Unterhaltung, Produktion, Logistik, Handel, Finanzen oder auch der Versorgung (z. B. Energie, Wasser) sowie militärisch vernetzter Operationen. Eine vertrauenswürdige IT ist die Grundvoraussetzung für eine sichere Nutzung der IKT in unserer digitalen Gesellschaft. Daher ist Cyber-Sicherheit umfassender und bezieht sich nicht nur auf die Datensicherheit. Vielmehr umfasst sie die Sicherheit der kompletten IKT von den Geräten und Netzen bis hin zu Anwendungen und Diensten.
Der Schutz des Anwenders, insbesondere seiner Privatsphäre, ist ein weiterer wesentlicher Faktor. Da es eine hundertprozentige Sicherheit nicht gibt, können wir Systeme und Kommunikation nur kontinuierlich immer sicherer machen, z. B. durch Verschlüsselung der Kommunikation.

TiB: *Das Gebiet der Cyber-Sicherheit ist demnach sehr umfangreich. Könnten Sie es etwas strukturieren?*

Dreo: Cyber-Sicherheit adressiert unterschiedliche Aspekte, die jedoch holistisch betrachtet werden müssen. Die Sicherheit der Internet of Things (IoT)-Geräte steht da genauso im Fokus wie die Netzsicherheit, die Sicherheit von Systemen und Software bis hin zur Anwendungs- und Benutzersicherheit.

TiB: *Wenn wir an das IoT (Internet of Things) denken, wie kann man eine so große Anzahl an Geräten absichern?*

Dreo: Prognosen gehen davon aus, dass wir bis 2022 um die 50 Milliarden vernetzter IoT-Geräte (z.B. IP-Kameras, Lautsprecher, Sensoren) haben werden. Daher ist es notwendig, bereits bei der Entwicklung von IoT-Geräten die Sicherheitsaspekte zu berücksichtigen und mit zu entwickeln (Security-by-Design).
Ein nachträgliches Umsetzen der Sicherheitsmaßnahmen ist viel aufwändiger, teurer und fast ein Ding der Unmöglichkeit. Ferner ist durch die Komplexität und Vernetzung die Einbringung von Schwachstellen viel wahrscheinlicher.

TiB: *Die nächste Stufe ist dann das Netz?*

Dreo: Bei der Netzsicherheit geht es um die Absicherung von Rechnernetzen gegen Cyberangriffe. Da die Angriffe komplexer werden, bedarf es auch einer Reihe von Sicherheitsmechanismen zur Abwehr, die von Firewalls, Intrusion Detection and Prevention Mechanismen bis hin zu neuartigen Ansätzen wie Moving Target Defence (MTD) reichen. MTD ist derzeit im Blickpunkt der Forschung, da es die Angriffsfläche dynamisiert und es somit dem Angreifer sichtlich erschwert in die Systeme einzudringen.

TiB: *Die nächste Stufe ist die Usable Security – die handhabbare Sicherheit der Benutzer?*

Dreo: Die Sicherheit aus Sicht des Benutzers ist teilweise viel zu komplex. Es ist notwendig Technologie, wie z. B. Passwortmanager, einzusetzen, um ein höheres Sicherheitsniveau zu erlangen.
Biometrische Verfahren wie Fingerprint, Gesichts- oder Venenscan sind weitere Beispiele.

TiB: *Sind diese biometrischen Verfahren wirklich sicher?*

Dreo: Wie bereits erwähnt existiert keine hundertprozentige Sicherheit. Auch biometrische Verfahren können überlistet werden. Jedoch bieten sie im Vergleich zu anderen Systemen wie Kennwörtern häufig ein Mehr an Sicherheit und vor allem ein Mehr am Komfort. Idealerweise sollten auch biometrische Verfahren mit anderen Verfahren (z. B. PIN) kombiniert werden. Eine Multi-Faktor-Authentifizierung, wobei verschiedene Kategorien wie Wissen (Etwas, das Sie kennen), Besitzen (Etwas, das Sie haben) und Inhärenz (Etwas, das Sie sind) kombiniert werden, ist nach aktuellem Stand der Forschung am sichersten.

Wir müssen im Sinne einer Digitalen Souveränität Europas mehr in digitale Plattformen investieren

TiB: *Die Gefährdungsszenarien aus dem Netz sind vielfältig. Gab es nicht Bestrebungen, das Internet ganz neu aufzusetzen?*

Dreo: Das Internet, dessen Entwicklung vor mehr als fünf Jahrzehnten anfing, war nie für die Anforderungen in Bezug auf Sicherheit oder auch Dienstqualität der heutigen Zeit gedacht. Die Stanford Universität versuchte in einem interdisziplinären Projekt zu untersuchen, wie das Internet konzipiert werden müsste, um den heutigen Anforderungen zu entsprechen. Dieses Projekt war später unter dem Namen Clean Slate bekannt geworden.

TiB: *Die letzte Stufe ist die Anwendungssicherheit. Wie kann man verhindern, dass der Anwender Schadsoftware durch Apps auf sein Gerät lädt?*

Dreo: Das ist schwierig, da Apps auch mit Malware infiziert sein können. Mobile Malware wird zu einer immer größeren Bedrohung. Allein 2017 wurden 27.000 neue Varianten registriert. Eine gute Schutzmöglichkeit ist Apps nur von den offiziellen Stores von Apple und Google zu laden. Aber auch hier gelang es Kriminellen Schadsoftware in die Plattformen einzuschleusen. Der beste Schutz des Anwenders ist aus meiner Sicht die Aufklärung, das Bewusstsein für Informationssicherheit und nicht zuletzt gesunder Menschenverstand. Die Kombination dessen, gepaart mit dem Security-by-Design Ansatz, führt sicherlich zu einem deutlich besseren Sicherheitsniveau des Anwenders.

TiB: *Wer steckt hinter diesen Angriffen?*

Dreo: Mit diesen Angriffen versuchen Angreifer unberechtigten Zugriff auf Systeme und Daten zu erlangen, um Informationen abzugreifen, und teilweise auch die befallenen Endgeräte selbst für kriminelle Zwecke zu missbrauchen. Das Problem bei der Aufklärung von Cyberattacken ist die sogenannte Attribution.

TiB: *An der Attribution wird gearbeitet?*

Dreo: Unter Attribution wird die Zuordnung von Cyberattacken zu bestimmten Angreifern verstanden. Dies ist jedoch äußert schwierig, da die Angreifer eine Vielfalt an Verschleierungstechniken nutzen können, um eigene Spuren zu verwischen. Je besser die Angreifer sind, desto schwieriger ist die Attribution.

TiB: *Sind Kritische Infrastrukturen durch mögliche Angreifer besonders gefährdet?.*

Dreo: Kritische Infrastrukturen (KRITIS) sind besonders gefährdet [1] und ein attraktives Ziel für Angreifer. Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI), als auch Telekommunikationsbetreiber wie die Deutsche Telekom belegen den extremen Anstieg von Angriffen, teilweise exponentiell. Kritische Infrastrukturen werden auch immer stärker angreifbar, da die Betreiber auf Vernetzung und Digitalisierung setzen, um die Effizienz zu steigern und die Kosten zu senken. Neben den Vorteilen werden jedoch auch neue Gefahrenpotentiale aufgezeigt, da u.a. Systeme aus dem Internet erreichbar sind.

TiB: *Abseits der offiziellen Definition: Sehen Sie weitere kritische Infrastrukturen, bspw. IoT oder Industrie 4.0?*

Dreo: Neben KRITIS gibt es auch andere wichtige Infrastrukturen z. B. Suchmaschinen. Mit der Nutzung von Suchmaschinen wie Google trainieren wir nicht nur die Algorithmen von Google (Machine Learning), sondern geben auch indirekt Auskunft über Themenfelder, an denen wir arbeiten. Durch die Korrelation der einzelnen „Bausteine“ ergibt sich dann das gesamte „Mosaikbild“.
Die eigentliche Frage ist doch, ob wir nicht im Sinne der digitalen Souveränität Europas mehr in die Entwicklung eigener digitaler Plattformen investieren müssen. Denn wenn wir USA und China betrachten, dann gibt es Amazon und Alibaba oder Google und Baidu oder Facebook und Tencent. In Europa gibt es keine derartigen Plattformen.

TiB: *Wie beurteilen Sie den großen Einfluss sozialer Medien?*

Dreo: Auch soziale Medien sind eine wichtige Infrastruktur, da diese die Demokratie und das Selbstverständnis der Bürger fördern, aber auch bedrohen können. Wenn nicht mehr Personen Meinungen verbreiten, sondern Programme, sog. Social Bots, dann ist das ein Angriff auf unsere Demokratie. Gezielte Desinformation gefährdet die demokratische Willensbildung und bedarf daher gesteigerter Aufmerksamkeit und gezielter Gegenmaßnahmen.
Die Möglichkeit über soziale Medien jedoch direkt eigene Meinungen kundzutun ist wiederum eine Stärkung der Demokratie. Die Herausforderung ist, mit KI und Algorithmen Desinformation, Manipulationen oder Social Bots zu erkennen und Gegenmaßnahmen einzuleiten, ohne jedoch die Meinungsfreiheit zu behindern.

Foto: Privat

TiB: *Brauchen wir dazu die KI?*

Dreo: Heutzutage wird die Verbreitung von KI-Systemen durch Fortschritte im Bereich des maschinellen Lernens vorangetrieben. Im Gegensatz zum expliziten Programmieren lernt das System eigenständig und durch die Analyse der vorliegenden Daten. Die enormen Mengen von Daten und die hohe Komplexität der IT-Umgebung bedürfen des Einsatzes des maschinellen Lernens.

TiB: *Wo steht Europa in Bezug auf Cybersicherheit?*

Dreo: Mit der Billigung des Rechtsakts zur EU-Cyber-Sicherheit hat die EU einen wesentlichen Schritt gemacht, um der zunehmenden Zahl von Cyberbedrohungen zu begegnen. Die Stärkung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA), die Schaffung eines gemeinsamen Zertifizierungsrahmens, die Vernetzung von Cybersicherheitskompetenz wie im Rahmen des H2020-Projektes CONCORDIA, die neuen Forschungs- und Entwicklungsprogramme wie Horizon Europe oder Digital Europe Programme sind u. a. wesentliche Schritte zur Stärkung der Cyber-Sicherheit in Europa. Das ist gut so, denn Cyber-Sicherheit ist das Fundament unserer digitalen Gesellschaft.

Das Interview führten Fritz Münzel, Walter Tengler und Silvia Stettmayer

Anmerkungen

[1] https://www.bsi.bund.de/DE/Themen/KRITIS

Die Sicherheit von Betriebssystemen

Auch Handys, Consumer-Elektronik-Geräte und eingebettete Systeme sind heute Rechner mit einem Betriebssystem. Was kann das Betriebssystem zur Sicherheit beitragen, wo liegen typische Schwachstellen?

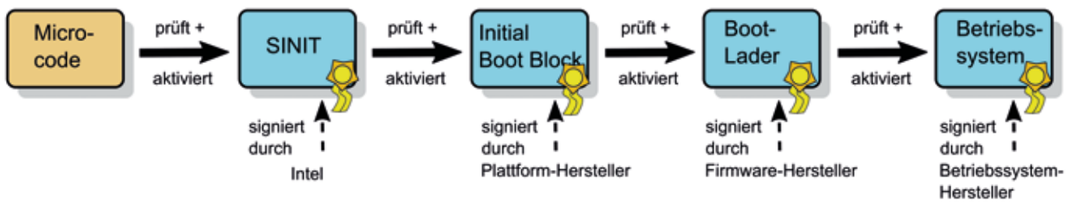
Welches Betriebssystem ist jetzt sicherer, Windows oder Linux? Diese Frage am Beginn der Vorlesung über Betriebssystemsicherheit führt schnell zur Diskussion, was es denn bedeutet, dass ein Betriebssystem sicher ist. Soll es die Hardware schützen, die Anwendungen oder den Nutzer? Soll es vor Angriffen aus dem Netz schützen, vor Datendieben, die sich physikalischen Zugang zum Rechner verschafft haben, oder vor Nutzern, die die Daten anderer Nutzer ausspähen wollen? Oder soll es sogar verhindern, dass sein Nutzer illegal Videos vervielfältigt?

Alte Zeiten

Vor 50 Jahren war das alles viel einfacher. Rechner hatten die Größe von Schränken, wurden weder herumgetragen noch verloren und waren für Privatpersonen unerschwinglich. Die Institutionen, die sich weltweit Sorgen um die IT-Sicherheit machten ließen sich an einer Hand abzählen, prominentester Vertreter war das US-Verteidigungsministerium. Hier entstanden die Wurzeln der Forschung über IT-Sicherheit im Allgemeinen und über sichere Betriebssysteme im Besonderen.
Der „use case“ war ähnlich wenig vielfältig: Zu ermöglichen, dass militärisch klassifizierte Dokumente („vertraulich“, „geheim“) auf Computern verarbeitet werden können. Dazu müssen die Nutzer unterschiedliche Berechtigungen haben und das Betriebssystem muss sie voneinander isolieren. Dabei sollte das Betriebssystem aber beispielsweise auch verhindern, dass ein Nutzer mit Zugriffsberechtigung auf ein Dokument dieses versehentlich oder absichtlich an Nutzer ohne diese Berechtigung weitergibt.
Veröffentlichungen aus dieser Zeit lesen sich sprachlich schon etwas antiquiert, inhaltlich aber hochaktuell. So wurde damals bereits erkannt, dass das Betriebssystem diese Aufgaben nur garantiert erfüllen kann, wenn es selbst vor Änderung seines Binärcodes und seiner Daten geschützt ist. Dies war eine von drei Anforderungen („tamper proof“) des „Referenzmonitor-Konzepts“, das eine Arbeitsgruppe unter James P. Anderson 1972 formulierte. Und zwischen der unberechtigten Weitergabe geheimer Dokumente und der illegalen Verbreitung digitalisierter Blockbuster besteht technisch kaum ein Unterschied.

Selbstschutz

Praktisch hatte der Selbstschutz des Betriebssystems wegen der stark eingeschränkten Zugänglichkeit allerdings keine hohe Priorität. Das ist heute durch Vernetzung und Mobilität anders: Ein Handy ist ständig von Milliarden anderer Computer aus erreichbar und kann leicht gestohlen oder in einem unbeaufsichtigten Moment manipuliert werden.
Typische Selbstschutzmaßnahmen sind Signierung oder verschlüsselte Speicherung des Betriebssystems und seiner Daten. Dies ermöglicht es beim Systemstart die Integrität durch den Boot-Lader zu verifizieren. Doch wer kontrolliert den Kontrolleur? Auch die Boot-Lader-Software kann manipuliert werden. Eine moderne UEFI Firmware, die „secure boot“ mit entsprechenden Maßnahmen realisiert, ist im Flash-ROM gespeichert und kann relativ leicht ersetzt werden (das ist auch notwendig, wenn mal wieder eine Schwachstelle erkannt und ein Update bereitgestellt wird).
Man „löst“ dieses Problem durch immer längere Ketten sich kontrollierender Kontrolleure. Bei heutigen Systemen reichen diese Ketten bis in die Hardware: der Mikrocode moderner Intel-Prozessoren mit der Technologie „Verified Boot“ hat die Fähigkeit, kryptografische Signaturen der Firmware zu prüfen (Abb. 1). Damit basiert die Integrität des Betriebssystems auf der (Prozessor-)Hardware. Da die Hardware auch alle Maschinenbefehle des Betriebssystems ausführt, muss ihre Integrität sowieso immer vorausgesetzt werden. Leider kann auch diese Voraussetzung heute problematisch sein.



Grafiken: Gunnar Teege

Abb. 1: Die Boot-Lader-Kette bei „Verified Boot“ beginnt im Mikrocode der Prozessor-Hardware

Schutz für Nutzer und Daten

Die wichtigste Aufgabe des Betriebssystems in Bezug auf Sicherheit ist nach wie vor die Isolation verschiedener Nutzer oder Anwendungen voneinander, sowohl im Hauptspeicher als auch im Dateisystem. Gleichzeitig sollen aber auch kontrollierte Kanäle zum Informationsaustausch ermöglicht werden. Im Dateisystem geschieht dies durch die Verwaltung von Zugriffsrechten. Das Betriebssystem garantiert, dass nur ein Prozess mit den nötigen Rechten auf eine bestimmte Datei zugreifen kann.
Während das in den 1970er Jahren entstandene Rechtesystem von Unix, das auch heute in den meisten Linux-Systemen verwendet wird, noch relativ einfach war, sind seitdem hochkomplexe Rechtesysteme entstanden mit dem Ziel, Sicherheitsanforderungen immer besser erfüllen zu können. Insbesondere Rechte zur Rechtevergabe tragen zur Steigerung der Komplexität bei. Bereits die Windows-Systeme seit 2000 haben ein deutlich komplexeres Rechtesystem. Die von der NSA und RedHat entwickelte open-source Linux-Erweiterung SeLinux („Security enhanced Linux“) übertrifft dies noch bei weitem.

Diese Komplexität wird zum Problem. Schwachstellen bestehen heute nicht in einer fehlerhaften Rechteprüfung durch das Betriebssystem, sondern aus fehlerhaft vergebenen Zugriffsrechten. Als Lösung wird gerne die systembestimmte Zugriffskontrolle („mandatory access control“) propagiert. Dabei werden alle grundlegenden Rechte durch den (Sicherheits-)Administrator verwaltet.
Das reduziert zwar den Personenkreis, der Fehler bei der Rechtevergabe machen kann, aber auch Administratoren sind nur Menschen.
Und das schönste Rechtesystem ist wirkungslos, wenn der Angreifer (oder Forensiker) die Festplatte ausbaut und auf einem Rechner ausliest, der die auf der Platte gespeicherten Rechte einfach ignoriert. Das ist der Grund, warum die Festplatteninhalte verschlüsselt sein sollten. Im Betrieb besitzt das Betriebssystem den Schlüssel und ver- bzw. entschlüsselt alle Daten beim Transport zwischen Hauptspeicher und Festplatte. Da es dies allerdings auch für einen Angreifer machen würde, ist die Verschlüsselung im Betrieb wiederum als einzelne Sicherheitsmaßnahme wirkungslos. Erst die Kombination aus Rechtesystem und Verschlüsselung ergibt einen hinreichenden Schutz der gespeicherten Daten (siehe Abb. 2). Dieses Beispiel ist typisch für Sicherheitseigenschaften: nicht die Stärke einzelner Mechanismen oder ihre Anzahl ist alleine entscheidend, sondern häufig erst ihre geeignete Kombination.

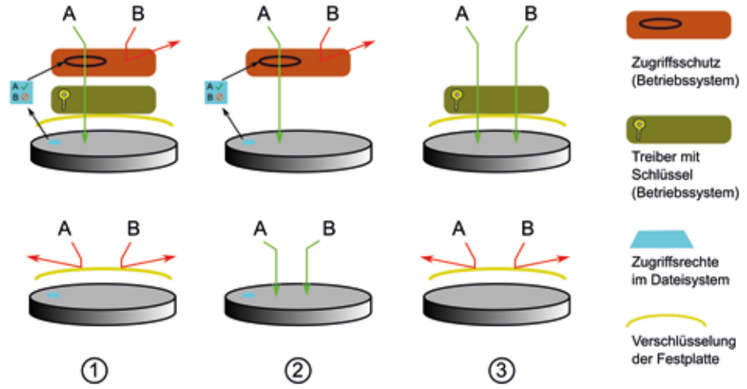


Abb. 2: Erst die Kombination (1) aus Zugriffsschutz und Verschlüsselung schützt die Dateisystem-Inhalte des Nutzers A wirksam im aktiven (oben) und inaktiven Rechner (unten) vor dem Zugriff durch einen Angreifer B. Jede Sicherheitsmaßnahme für sich (2), (3) reicht nicht aus

Sicherheitsbewertung

Auf der siebenstufigen Skala der Sicherheitszertifizierung von IT-Systemen gemäß „Common Criteria“ ist Windows 10 auf der untersten Ebene EAL1 zu finden. Standard-Betriebssysteme von PCs, Servern, Handys etc. erreichen maximal die Ebene *EAL4* (u.a. Windows-Server-Varianten, Enterprise-Linux-Versionen und Windows Mobile). Das einzige komplett auf EAL5 zertifizierte Betriebssystem ist das Spezialsystem PR/SM von IBM, kein Betriebssystem erreicht eine höhere Stufe. Und selbst Stufe EAL7 garantiert noch nicht, dass das System keine Schwachstellen enthält.

Die Forschung ist hier etwas weiter. 2013 wurden für das Mikrokern-Betriebssystem *seL4* alle wesentlichen Sicherheitseigenschaften formal bewiesen. Der Aufwand dafür betrug allerdings das 15-fache des reinen Entwicklungsaufwands. Die Funktionalität des 10.000 Code-Zeilen umfassenden seL4 ist zwar grundlegend, aber rudimentär. Bis vergleichbare Sicherheit für ein Standard-Betriebssystem mit vielen Millionen Code-Zeilen erreichbar ist, dürften noch einige Jahre vergehen. Die Frage ist also nicht, ob Windows oder Linux, sondern wie und wann überhaupt hinreichend sichere Betriebssysteme praktisch einsetzbar sind und wie diese aussehen werden.

Prof. Dr. Gunnar Teege
Institut für Technische Informatik
Universität der Bundeswehr München

Software Diversity

Was die Computersicherheit von der Natur lernen kann

Ein Virus breitet sich aus, aber nicht jeder Mensch erkrankt daran. Wenn Computer-Viren sich ausbreiten, dann ist praktisch jeder Computer in irgendeiner Form davon betroffen. Was kann die Natur, was Software nicht kann?

Nicht alle Menschen werden von einer Grippeepidemie erfasst: Manche werden angesteckt, andere hingegen bleiben gesund. Die Natur hat sich durch den ständigen Prozess der Evolution einen besonders schlauen Mechanismus einfallen lassen, um diese Immunität zu gewährleisten: die sogenannte Biodiversität. Da sich die einzelnen Individuen einer Gruppe in mehrfacher Hinsicht unterscheiden, kann ein einzelnes Virus nicht alle Individuen in gleichem Ausmaß befallen. Dadurch ist unter anderem auch ein Fortbestand der Gruppe auch bei schwerwiegenden Erkrankungen gesichert. Dieser Effekt nutzt nicht nur den Menschen, sondern allen Lebewesen.

Heutige Computersysteme folgen einer Monokultur

In der Computersicherheit konstatieren wir das genaue Gegenteil: Malware breitet sich nicht nur rasend schnell aus, sondern befällt alle verwundbaren Systeme. Würde man einen Biologen um Rat fragen, dann wäre die Ursache schnell identifiziert: Computersysteme – also Hardware und Software – folgen von der Organisationsform her einer Monokultur. Mithin sind wenige Komponenten in praktisch allen Systemen vorhanden, z. B. Betriebssysteme (Windows in Desktop Computern, Android & iOS in mobilen Geräten), Browser (Google Chrome, Mozilla Firefox, Apple Safari), CPUs (Intel x86, ARM Prozessoren), etc. Diese Komponenten sind absolut identisch und bieten daher keine prophylaktische Diversität an.

Ein konkretes Beispiel: Google Chrome hat derzeit einen Marktanteil von über 60 %. Da es mehrere hundert Millionen Desktop PCs gibt, verwenden also fast zwei Drittel davon – im Mittel gesehen – Google Chrome. Findet ein Angreifer eine Schwachstelle in Google Chrome, sind also genau diese zwei Drittel aller Desktop PCs von exakt der gleichen Schwachstelle betroffen und können durch einen gemeinsamen Angriff ausgenutzt werden (Abb. 1). Gleiches gilt für Apple Safari auf iPhones, iPads und Apple Watches.

Warum also folgen Computersysteme einer Monokultur? Dies liegt im Wesentlichen an der Geschichte und den für Computer hilfreichen Vorteilen der Monokultur. Ein solcher Vorteil ist z. B. eine äußerst einfache Verteilung von Software- und Hardware-Komponenten. Software wurde bis vor kurzem auf physikalischen Medien, mithin Disketten oder CDs, ausgeliefert. Diese Medien automatisch mit der exakt gleichen Software zu bespielen oder exakt die gleiche Hardware in großen Mengen herzustellen erlaubt es Herstellern, erhebliche Größeneffekte zu erzielen. Minimale Veränderungen in diesen Herstellungsprozessen wären exorbitant teuer und daher betriebswirtschaftlich nicht zu rechtfertigen.

In der ersten wissenschaftlichen Arbeit zu dem Thema [1] werden diese physikalischen Medien als eines der größten Hindernisse zur praktischen Umsetzung einer Diversifizierung von Software gesehen. Erst seit kurzem erfolgt die Verteilung von Software nicht mehr durch die physikalischen Medien, sondern durch Netzwerke, allen voran das Internet.

Windows holt sich Updates automatisch über das Internet und mobile Endgeräte verwenden durchwegs App Stores der jeweiligen Hersteller. Diese „Digitalisierung“ der Verteilung ermöglicht es uns erstmalig, Software durch den Hersteller oder den App Store Betreiber kosteneffizient zu diversifizieren. Eine Studie aus dem Jahr 2015 hat die Kosten der Diversifizierung des Firefox Web Browsers auf ca. 7 US Cents beziffert [2]. Die damals berechneten Kosten sind heute aufgrund der gestiegenen Effizienz und gleichzeitig gesunkenen Kosten im Cloud Computing und Storage Bereich weiter gesunken.

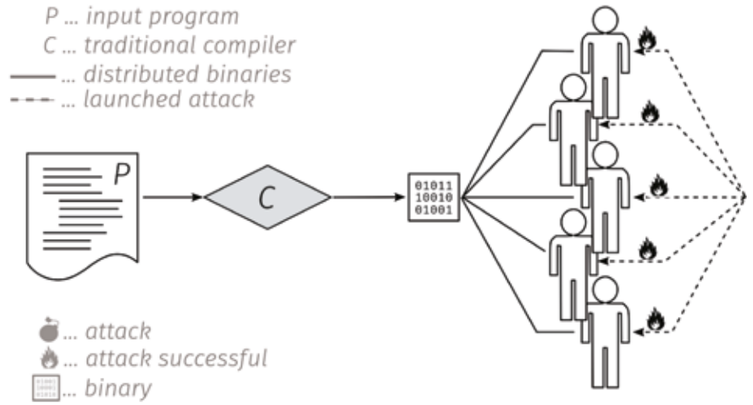


Abb. 1: Heutige Computersysteme folgen einer Monokultur

Wie lässt sich Software diversifizieren?

Ziel der Forschung im Bereich „Software Diversity“ ist es, auch große Software Systeme vollständig automatisch und transparent zu diversifizieren. Diese Charakteristika – automatisch und transparent – gelten dabei in zweifacher Hinsicht. Zum einen sollen Anwender nicht durch die Diversifikation ihrer Software beeinträchtigt werden. Idealerweise wissen die Anwender gar nicht, dass ihre Software diversifiziert wurde. Zum andern sollen auch Programmierer möglichst nicht durch die Diversifizierung beeinträchtigt werden. Sollten Programme durch den Programmierer manuell verändert werden müssen, entstehen zusätzliche Kosten, welche die wenigsten Hersteller tragen können oder wollen. Grundsätzlich eignen sich sogenannte sprachbasierte Transformationen, wie sie z. B. im Compilerbau verwendet werden, besonders gut, um Software automatisch und transparent zu diversifizieren. Um beispielsweise das Speicherabbild eines Programms zu diversifizieren, kann ein Compiler während des Übersetzungsvorgangs verschiedene Zufallsexperimente durchführen, um entweder Entscheidungen des Compilers zu randomisieren oder aber auch zufallsgesteuerte, separate und benigne Code Fragmente in ein Programm einzubauen (Abb. 2). Ein derartig diversifiziertes Programm verändert die grundlegenden Annahmen, die ein Aggressor tätigen muss, um einen Angriff erfolgreich durchzuführen.

In unserer heutigen Monokultur kann ein Angreifer mit hoher Wahrscheinlichkeit erraten, welche Software verwendet wird und wie sich deren Speicherabbildungen zur Laufzeit manifestieren. Diversifizierte Software invalidiert derartige Annahmen zum Großteil, was Angreifer in einen Zugzwang bringt. Selbstverständlich bleibt ein gewisses Restrisiko, da die Diversifizierung von Software ipso facto nur probabilistische Sicherheit bieten kann – analog zur Biodiversität in Biologie und Natur: Einzelne Individuen sind betroffen, aber die Gesamtheit bleibt bestehen.

Der Fokus auf Compiler-gestützte Diversifizierungstechniken hat einen anderen wichtigen Vorteil: Größtmögliche Kompatibilität mit existierenden Software Systemen. Durch die Diversifikation während der Übersetzungszeit können beispielsweise auch komplexe Software-Komponenten diversifiziert werden. So konnten in vorangegangener Forschungsarbeit ganze Betriebssysteme (Linux) und Web Browser (Chrome und Firefox) vollständig kostenneutral durch Software Diversity abgehärtet werden.

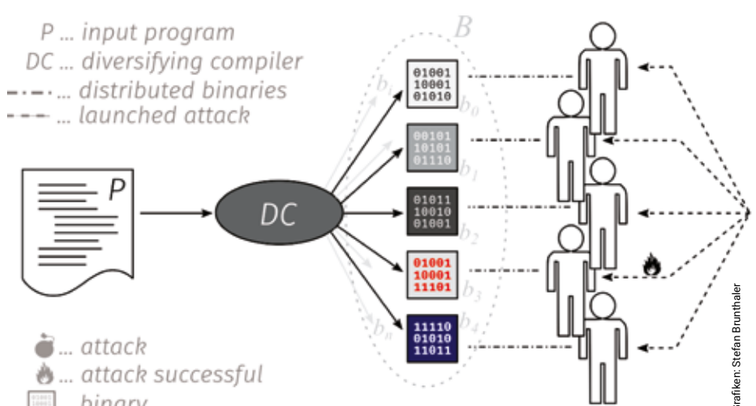


Abb. 2: Computersystem mit diversifizierten Programmen

Urheber der Grafiken: Stefan Brunthaler

Was sind die Grenzen und Möglichkeiten der Diversifizierung?

Software Diversity kann keine Logikfehler im Programm erkennen und verhindern. Diese Art von Fehler wird also auch in einem diversifizierten Programm angreifbar sein. Die Manifestation des Fehlers kann aber vom Originalprogramm divergieren und somit auch die Angriffsfläche eines Programms verändern und idealerweise auch verkleinern. Software Diversity eignet sich u. a. besonders gut dazu, die Laufzeit Darstellung eines Programms zufallsgesteuert zu variieren. Als solches eignet sich Software Diversity unter anderem dazu, verschiedene Varianten von mikro-architektonischen Seitenkanälen (z. B. Spectre) signifikant zu erschweren. Dies ist derzeit ein Forschungsgegenstand am Lehrstuhl des Autors und erste positive Resultate wurden bereits erzielt.

Prof. Dr. Stefan Brunthaler
Institut für Systemsicherheit
Universität der Bundeswehr München

Literatur

[1]: F. B. Cohen, Operating System Protection through Program Evolution. http://all.net/books/tech/evolve.pdf
[2]: A. Homescu, T. Jackson, S. Crane, S. Brunthaler, P. Larsen, M. Franz, Large-Scale Automated Software Diversity-Program Evolution Redux, IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2015.2433252

IT-Forensiker: Spurensuche zwischen Bits und Bytes

Datenklau, Sabotage oder Spionage: Um in solchen Fällen keine Spuren zu zerstören, sollten Unternehmen sofort einen IT-Forensiker zu Hilfe rufen. Denn der sichert und untersucht im Schadensfall die Beweise gerichtsverwertbar.

Die Honeypots der Telekom, die digitalen Lockfallen von T-Systems, zählen an einem einzigen Tag 31 Millionen Angriffe auf unser Netz. Aber nicht nur die Deutsche Telekom und T-Systems sind das Angriffsziel von Digital-Kriminellen. 43 Prozent [1] der großen Unternehmen geben an, 2018 Opfer einer Cyber-Attacke [2] gewesen zu sein und 87 Prozent der von einer IT-Attacke Betroffenen berichteten dabei von Betriebsstörungen oder -ausfällen [3].

Im Verdachtsfall: IT-Forensiker alarmieren

Spätestens dann schlägt die Stunde der IT-Forensik und des Incident Handlings (siehe Abbildung). Oft ermitteln die Telekom Security Experten bereits, bevor externe Stellen die Unternehmen darüber informieren, dass sich in ihre Systeme Cyberkriminelle eingeschlichen haben. Sie kommen etwa dann zum Einsatz, wenn die IT-Administratoren der Kunden merken, dass sich das IT-System anders verhält als sonst. Wenn der Buchhalter zum Beispiel über Überweisungen stolpert, für die er keine Rechnungsbelege findet. Oder sich der Geschäftsführer wundert, dass seine Firma seit einiger Zeit bei jeder Ausschreibung unterboten wird oder die Konkurrenz aus Fernost mit einer Innovation auf den Markt kommt, die den eigenen Entwürfen verblüffend ähnelt.

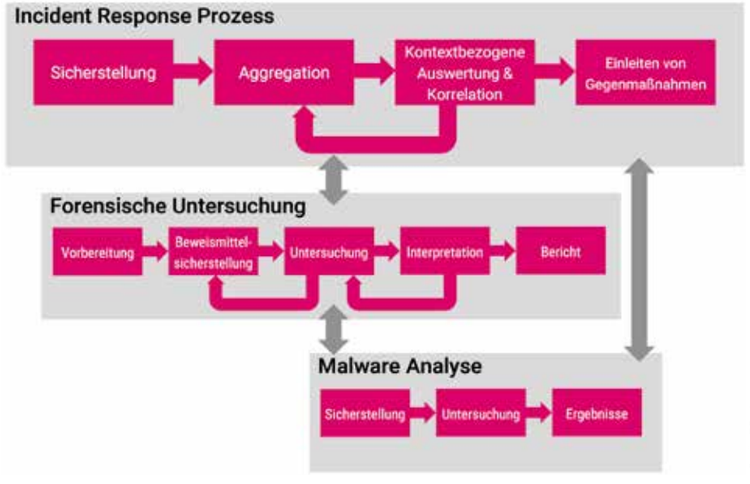
In solchen und ähnlichen Verdachtsfällen wenden sich die Kunden an die Security-Experten. Zu den Aufgaben des Incident Handlings gehören: Das Ausmaß des Schadens bestimmen und begrenzen, die Schuldigen und deren Motive ausfindig machen und deren Vorgehensweise analysieren. Dann verschließen die Experten die Einfallstore und leiten Gegenmaßnahmen ein. Die IT-Forensik, ein Teilgebiet des Incident Handlings, liefert dabei gerichtsverwertbare und nachweisbare Tatsachen, damit das Gericht die digitalen Beweismittel in einem späteren Prozess nicht ablehnt. Oder das Unternehmen auf Probleme stößt, wenn es den entstandenen Schaden bei der Versicherung geltend machen möchte.

Beweismittel sichern, Datenverlust minimieren

Voraussetzung dafür: ein standardisierter IT-Forensik-Prozess. Der Ablauf einer IT-forensischen Analyse muss strukturiert sein und methodisch immer den gleichen Vorgaben folgen. Zuerst sichern die IT-Forensiker Datenträger, Speicherimages und Logdateien gerichtsverwertbar. Das bedeutet, dass sie die Beweismittel nicht verändern oder gar zerstören dürfen. Aus diesem Grund dokumentieren und fotografieren sie bei der Beweissicherung auch alles. Es könnte beispielsweise wichtig werden, wie die Umgebung aussieht oder wo welches Kabel im Laptop steckte. Natürlich weiß man zu Beginn nicht, welches Details sich am Ende wirklich als relevant herausstellen wird, ob die Fotos beispielsweise tatsächlich von Belang sein werden. Deshalb müssen die IT-Forensiker zu diesem frühen Zeitpunkt zuallererst eine verlässliche Grundlage für die weiteren Untersuchungen schaffen.

Im Schadensfall: Ruhe bewahren

Entscheidend ist, dass die Unternehmen den Forensiker frühzeitig an den Tatort rufen – ehe sie ungewollt die Spuren der Angreifer verwischt haben. Der wichtigste Tipp: Bewahren Sie im Schadensfall Ruhe, rühren Sie nichts an und alarmieren Sie sofort einen Spezialisten. Denn digitale



Quelle: T-Systems

Voraussetzung für den Erfolg sind standardisierte Abläufe: Der Incident-Handling-Prozess mit seinen Unterprozessen Forensik und Schadsoftwareanalyse

Beweise sind flüchtig. Ein falscher erster Schritt kann fatale Folgen haben und den Schaden noch vergrößern. Wie bei jedem anderen Kriminalfall gilt auch in der Welt der IT: Erst einmal den Tatort absperren und bloß nichts verändern.
Forensiker arbeiten mit den betroffenen Unternehmen eng zusammen – sie brauchen das Vertrauen ihrer Kunden und den Zugriff auf Logfiles, Festplatten, Laptops, Handys, Netzwerkdaten und -pläne oder E-Mails mit Headern. Selbstverständlich sammelt der Forensiker auch die Aussagen der Betroffenen, um sich ein Bild zu machen. Anschließend erstellt er eine vollständige forensische Kopie der Festplatte oder sichert den Laptop.
Der Tatort eines IT-Forensiker ist also stets gleichzeitig analog und digital: Neben der Analyse einzelner Systeme, dabei handelt es sich zumeist um Arbeitsplatzrechner oder Server, kann sich die Untersuchung auch auf die gesamte IT-Landschaft aus Hardware, Software, Services, Organisation und Planung ausdehnen. Bei diesen Recherchen sucht der Experte auch nach Spuren im Netzwerk und auf den Rechnern. Mitunter tauchen dann Daten an Stellen auf, wo sie nicht hingehören. Das ist immer ein guter Ansatzpunkt, um tiefer zu bohren. Stets verfolgen die IT-Forensiker den Weg der Schadsoftware: Wo kam es zur Erstinfektion? Wie hat sich der Schädling im Unternehmensnetzwerk weiterverbreitet? Was ist der Ursprung? Kommt er von innen oder von außen? Wer zählt zu den Opfern und wie groß ist der Schaden?

Viele Täter bleiben lange unbemerkt

Kein Angriff gleicht dem anderen, aber das Gros der Cyber-Attacken zielt derzeit noch auf die breite Masse der Privatanwender. Die Cyber-Kriminellen leitet also die Hoffnung, dass es am Ende irgendwen schon erwischen wird. Angriffe von Verschlüsselungstrojanern, Emotet, Cryptolocker oder dem Erpressungstrojaner Locky sind daher im Grunde wenig komplex, gegen sie können die aktuellen Schutzmechanismen im Grunde greifen. Interessante Schlupflöcher finden die Angreifer dennoch: So hat die berüchtigte Hackergruppe Turla vor zwei Jahren den Instagram-Account von Britney Spears für eine Malware-Steuerung benutzt – und damit viele Fans in die Falle gelockt – darunter auch etliche Musikliebhaber, die sich mit ihren Firmenrechnern in den infizierten Account klickten.

Anders sieht es bei der Industriespionage oder staatliche Sabotage aus: So genannte Advanced Persistent Threats (APT) [3] suchen sich ihre Opfer gezielt aus – und werden laut BSI von den Unternehmen erst nach durchschnittlich 205 Tagen bemerkt. Sehr viel Zeit, um tief in die Unternehmensstrukturen einzudringen und den Systemen die gewünschten Informationen abzupressen. Mitarbeiter werden ungewollt zu Sprungbrettern ins Unternehmen. Die Angreifer kommunizieren mit dem Opfer über eine Spear-Phishing-Mail [4]. Man nennt diese Methode Social Engineering. Das bedeutet, dass die Angreifer den Empfänger erst ausforschen, auch sein Privatleben, um ihm dann eine maßgeschneiderte Mail zu schicken. Der Fußballfan bekommt dann eine manipulierte Einladung zu einem Spiel seines Lieblingsvereins und die Controllerin eine bösartige Rechnung. Wenn das funktioniert, wird der Mitarbeiter beziehungsweise dessen Rechner ohne böse Absicht vom Opfer zum unfreiwilligen Innentäter.

Der Notfallplan als Krisenvorbereitung

Bedeutet: Nicht jeder Cyberangriff lässt sich durch technische Schutzmaßnahmen verhindern: Daher zahlt sich für Unternehmen eine gute Krisenvorbereitung aus. Mit einem Notfallplan steigt die Wahrscheinlichkeit, dass die Beschäftigten in einer Ausnahmesituation richtig reagieren. Lassen Sie sich im Vorfeld von einem erfahrenen Sicherheitsdienstleister beraten: Mit einem Penetrationstester spüren Sie die Schwachstellen Ihrer IT-Infrastruktur auf. Vereinfacht kann man sich das so vorstellen: Der Tester verhält sich wie ein Einbrecher, rüttelt an jeder IT-Sicherheitstür und schaut, ob sie wirklich gut und sicher verschlossen ist. Mit dem Forensiker kann man typische Bedrohungsszenarien durchspielen und danach die Frage beantworten: „Könnte ich mein Unternehmen gegen diese Art von Angriff verteidigen?“ Es gibt keinen hundertprozentigen Schutz vor einer Cyber-Attacke. Deshalb braucht jedes Unternehmen einen Notfallplan. Er sorgt nicht nur dafür, dass Sie sich richtig verhalten – er erhöht auch die Chance, dass Sie im Vorfeld auf Schwachstellen stoßen und diese rechtzeitig beseitigen können.
Der beste Notfallplan wird Sie nicht retten, wenn Sie mit Ihren Mitarbeitern nicht regelmäßig üben, wie man sich bei einem Cyber-Angriff richtig verhält.

Dr. Alexander Schinner
T-Systems

Quellen

[1] Laut der Online-Umfrage „Cyber-Risiken & Schutzmaßnahmen in Unternehmen“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom April 2019 https://bit.ly/2XWw4eU
[2] Computerwoche: Cyberangriffe haben sich verdoppelt. https://bit.ly/2M69FEY
[3] TecChannel: Wenn Virenscanner und Firewalls nicht mehr ausreichen. https://bit.ly/2JLQMp2
[4] Datenschutzbeauftragter-Info: Die 8 häufigsten Angriffe auf die IT-Sicherheit. https://bit.ly/30Rp6VO

Videos auf Youtube

http://easyurl.net/c5d98
http://easyurl.net/c4e06

Cyber Security aus dem Blickwinkel der Bayerischen Polizei

Die Nutzung digitaler Informations- und Kommunikationstechnologien ist Basis des modernen gesellschaftlichen und wirtschaftlichen Lebens, sie bietet aber auch die Möglichkeit, Straftaten zu begehen.

Für Industrieunternehmen und Dienstleistungsanbieter sowie für öffentliche Institutionen sind funktionierende Kommunikationsinfrastrukturen ein entscheidender Faktor. Mit der Zunahme informationstechnischer Systeme und Geräte erhöht sich ebenso die Möglichkeit der Begehung von Straftaten in diesem Umfeld.
Kriminalitätsfördernd wirken sich dabei unzureichende Absicherungen und veraltete Technologien, aber auch unzureichendes Risikobewusstsein von Nutzern dieser Technologien aus. Die fortschreitenden Entwicklungen bei Stichworten wie Internet der Dinge/Internet of Things (IoT), Industrie 4.0, Smart Home oder Automotive IT bieten ein breites Feld an Tatgelegenheiten. So erweitern die stark zunehmenden „adressierbaren" Objekte im Internet das Spektrum potentieller Ziele für Cyberkriminelle.

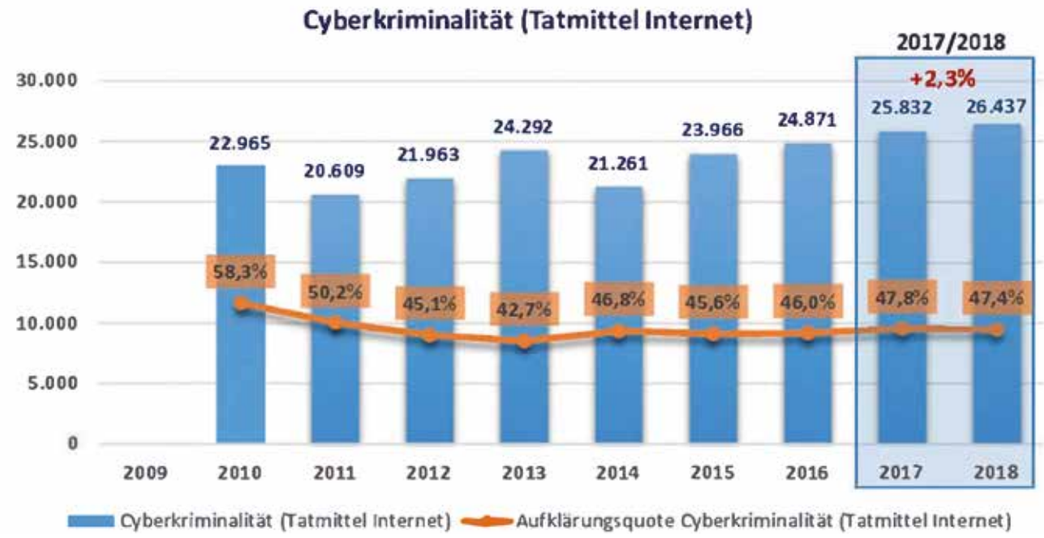
Abbildungen: LKA Bayern

Wie reagiert die Bayerische Polizei auf diese Entwicklung?
Cybercrime stellt demzufolge eine herausragende und hochdynamisch weiter wachsende Kriminalitätsform dar, auf die die Bayerische Polizei entsprechend reagiert hat. So wurde neben einer verbesserten Sachausstattung und einer personellen Stärkung der Ermittlungsbeamten in diesem Bereich auch die Notwendigkeit einer Spezialisierung erkannt. Aus diesem Grund wurde bei der Bayerischen Polizei die Sonderlaufbahn des „IT-Kriminalisten" eingeführt. Hierbei handelt es sich um Informatikstudenten, die nach Abschluss ihres Studiums im Rahmen einer sog. „polizeifachlichen Unterweisung" zu Polizeivollzugsbeamten ausgebildet werden, um deren technischen Hintergrund für die polizeiliche Ermittlungsarbeit nutzen zu können. Da sich diese Sonderlaufbahn bewährt hat, wird sie auch zukünftig fortgeführt; d. h. die Bayerische Polizei ist auch weiterhin auf der Suche nach IT-Fachkräften, die ihr Wissen bei der Bekämpfung von Computer- und Internetkriminalität einsetzen wollen.
Die Spezialisierung zeigt sich ferner in der Gründung eigener Dienststellen. So existiert seit April 2017 bei jeder Kriminalpolizeiinspektion in Bayern ein eigenes Kommissariat Cybercrime. Ferner wurde bundesweit bei jedem Landeskriminalamt eine Zentrale Ansprechstelle Cybercrime (ZAC) installiert. Die ZAC ist im Bereich der Polizei der Single-Point-of-Contact für alle Behörden, Unternehmen und Verbände in Fragen der Cybersicherheit. Sie steht im präventiven Bereich für Vorträge und Beratungsgespräche zur Verfügung. Sollte es zu einem Angriff gekommen sein, steht die ZAC in der Angriffsphase beratend zur Seite und zeigt die zu bedienenden Kommunikationswege auf. Im Nachgang steht sie auch für eine intensive Aufarbeitung des Vorfalls zur Verfügung. Die ZAC im Bayerischen Landeskriminalamt ist unter der Hotline 089/1212-3300 bzw. über das E-Mail-Postfach: zac@polizei.bayern.de erreichbar.

Welche Gefahren lauern im Netz?
Die Auswertung der bei der Polizei zur Anzeige gebrachten Straftaten zum Nachteil von Unternehmen ergab folgende Schwerpunkte:

- Online-Erpressung mittels Ransomware/Kryptotrojaner
- Online-Erpressung mittels DDoS (Destributed-Denial-of-Service)
- Man-in-the-middle-Angriffe (z. B. Abfangen und Verändern von per E-Mail versandten Rechnungen)
- Datendiebstahl/Veröffentlichung von Daten
- CEO-Fraud (Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden).

Wie können sich Unternehmen davor schützen?
Hierzu muss man wissen, dass Cyber-Kriminelle grundsätzlich drei Schwachstellen ausnutzen. In vielen Unternehmen herrschen noch organisatorische Mängel im Hinblick auf Cyberangriffe. Die Abläufe im Falle einer Attacke sind noch gar



nicht bzw. nur mangelhaft geregelt oder bei den Mitarbeitern nur rudimentär bekannt. Es herrschen Wartungsmängel (keine Updates) oder die Benutzerrechte sind überdimensioniert angelegt. Ferner profitieren die Angreifer von technischen Mängeln wie fehlendem oder veraltetem Virenschutz, offenen Ports in der Firewall, fehlendem Backup, unverschlüsselter Kommunikation oder WLAN-Sicherheitslücken. Die größte Schwachstelle ist und bleibt jedoch das menschliche Fehlverhalten. Cyber-Kriminelle nutzen dies in Form des sogenannten „Social Engineering" für ihre Zwecke aus. „Social Engineering" bedeutet, dass die Mitarbeiter durch geschickte psychologische Manipulation zu Handlungen verleitet werden, die die Sicherheit der Unternehmensdaten gefährden. Potentielle Opfer werden beispielsweise anhand von Angaben in Sozialen Netzwerken ausgewählt und gezielt kontaktiert (z. B. Mitarbeiter aus Finanzabteilungen der Unternehmen).
Als Konsequenz ist es für Unternehmen wichtig, die Schwachstellen im eigenen Betrieb zu identifizieren und zu schließen. Während die organisatorischen und technischen Mängel relativ leicht behoben werden können, ist der Aufwand zur Verhinderung menschlichen Fehlverhaltens ungleich größer. In vielen Unternehmen ist jedoch selbst bei den Führungskräften das Bewusstsein für diese Thematik noch nicht vorhanden. Es ist von entscheidender Bedeutung, seine Mitarbeiter zu sensibilisieren. Jedem Angestellten sollte bekannt sein, welche Gefahren aktuell im Internet lauern und welche Vorsorgemaßnahmen zu treffen sind.
Grundsätzlich sollten Unternehmen sich bereits im Vorfeld Gedanken hinsichtlich des Vorgehens machen und ein Sicherheitskonzept entwickeln.

Was ist bei einem Cyber-Angriff zu tun?
Bei einem Verdacht auf eine Cyberattacke sollten alle Informationen zum Vorfall gesammelt und aufgezeichnet werden. Dabei sollten sich Unternehmen an die intern festgelegten Meldewege halten. Es sollte eine identische Kopie des betroffenen Systems erstellt werden, um den Schaden abzuschätzen, die Schwachstellen zu identifizieren oder den Angreifer zurückzuverfolgen. Ferner sollte geprüft werden, ob von Seiten des Unternehmens dafür die Polizei (ZAC) einzuschalten ist. Die Kopie des betroffenen Systems sollte möglichst von anerkannten Forensikern der Polizei erstellt werden, um gerichtsfeste Beweise sichern zu können. Dadurch können zugleich Spuren und Hinweise gesichert werden. Das kann auch für das Unternehmen selbst in einem Arbeitsgerichtsverfahren von Bedeutung sein, wenn es sich um einen „Innentäter" handelt. Für die Kontaktaufnahme sollte nicht das betroffene System benutzt werden. Ist bereits ein Schaden eingetreten, sollten alle damit zusammenhängenden Ereignisse (z. B. Anrufe, E-Mails, Systemstörungen, Logdaten) dokumentiert werden.

Ausblick
Die hochdynamischen Entwicklungen in der digitalen Welt sind nicht mehr aufzuhalten, insbesondere auch im Bereich der Künstlichen Intelligenz (KI). Sie beinhalten jedoch nicht nur Fluch, sondern weitaus mehr Segen.
Hält man sich stets die aufgezeigten Gefahren vor Augen und trifft die entsprechenden Vorsorgemaßnahmen, besteht keinerlei Anlass ängstlich zu sein.
Unternehmen, die sich hierbei externer Hilfe bedienen wollen, stehen die Bayerische Polizei und die Industrie- und Handelskammern gerne beratend zur Seite.

Werner Kretz
Erster Kriminalhauptkommissar
Bayerisches Landeskriminalamt

Hardware-Attacken auf kryptographische Implementierungen

Kryptographische Algorithmen bilden die Grundlage für die Informationssicherheit in allen modernen vernetzten Systemen, und nur durch ihre Anwendung kann die Vertraulichkeit und Echtheit von Daten garantiert werden. Doch sie sind in Chips implementiert, die man bei der Ausführung kryptographischer Berechnungen beobachten kann, z. B. über den Stromverbrauch, oder auch gezielt stören kann, um Rückschlüsse auf den verwendeten Schlüssel zu erhalten.

Bestimmte Anwendungsbereiche wie hoheitliche Dokumente, Bankkarten, TPMs (Trusted Plattform Module zur Absicherung von PCs), oder auch Zugangssysteme bestehen fast ausschließlich aus einer Implementierung von kryptographischen Algorithmen und Speichermöglichkeiten für die dafür notwendigen Schlüssel.

Der Stand der Technik in Bezug auf die mathematische Sicherheit von kryptographischen Algorithmen ist dabei seit vielen Jahren auf einem sehr hohen Niveau. Es gibt standardisierte kryptographische Algorithmen (z. B. AES, ECC, RSA), die mathematisch gesehen noch eine lange Zeit Informationssicherheit gewährleisten können. Leider gilt das schon heute nicht im selben Maß für die sogenannte Implementierungssicherheit derselben Algorithmen. Die Implementierungen der Algorithmen, beispielsweise in einem Chip als Hardware oder Software für eine Automobil- oder Industriesteuerungsanwendung, befinden sich nämlich schlussendlich „im Feld", daher im Zugriffsbereich von möglichen Angreifern. Solche Angreifer versuchen dann, Schlüssel aus diesen Chips oder Geräten zu extrahieren, um damit über die entsprechenden Möglichkeiten frei zu verfügen. Der wesentliche Unterschied, der sich durch diesen physischen Zugang zu Geräten mit kryptographischen Implementierungen ergibt ist, dass ein Angreifer nun nicht darauf beschränkt ist, abgefangene Nachrichten zu analysieren, um eine Verschlüsselung zu brechen. Der Angreifer kann vielmehr das Gerät während der Durchführung von kryptographischen Berechnungen „beobachten" oder gezielt stören. Der Angreifer konzentriert sich dabei weniger auf die (guten) mathematischen Eigenschaften der kryptographischen Algorithmen, sondern auf konkretere Eigenschaften der Implementierung, beispielsweise auf elektrische bzw. physikalische Eigenschaften. Man nennt dies Hardware Angriffe, weil sie durch den Zugriff auf die Hardware – die Chips – möglich werden. Das angegriffene Gerät wird dazu vom Angreifer zumindest für eine Zeit entwendet, was in einigen Fällen entdeckt werden könnte. Extrahierte Schlüssel erlauben aber beispielsweise das beliebige Klonen von Geräten oder sind für mehrere Geräte gültig, sodass der Angreifer mehr gewinnt als den Schlüssel eines individuellen Gerätes. Bei einem Einsatz von Geräten „im Feld" ist es teilweise denkbar, dass ein Angriff nicht entdeckt würde und ein individueller Schlüssel bereits großes Missbrauchspotential hätte. Dies ist zum Beispiel der Fall bei Smartmetern, wo ein Angreifer seinen eigenen manipulierten Stromverbrauch per extrahiertem Schlüssel authentisch kommunizieren könnte.

Ein Teil dieser breiten Klasse von Hardware-Angriffen zielt direkt darauf ab, geheime Schlüssel aus den entsprechenden Speicherstellen zu extrahieren, beispielsweise mit hochpräzisen Ladungsdetektoren nach einer aufwändigen und nicht zerstörungsfreien Präparation des Chips. Diese Angriffe sind daher relativ aufwändig und stehen nicht im unmittelbaren Zusammenhang mit der eigentlichen kryptographischen Ausführung. Sogenannte Implementierungsangriffe aber beschäftigen sich mit der Ausführung von Kryptographie und sind häufig attraktiver für den Angreifer, weil sie weniger Aufwand erfordern. Wesentliche Ausprägungen dieser Implementierungsangriffe auf kryptographische Algorithmen sind Seitenkanalangriffe und Fehlerangriffe.

Seitenkanalangriffe

Seitenkanalangriffe zielen darauf ab, ein Gerät während der Ausführung einer kryptographischen Berechnung genau zu beobachten, beispielsweise durch eine möglichst präzise Messung des Stromverbrauchs während der Berechnung. Dieser steht in direkter Abhängigkeit zu den intern über die Zeit verarbeiteten Bits. Daher versucht der Angreifer, den Stromverbrauch oder auch das Magnetfeld, das durch diesen verursacht wird, möglichst genau aufzuzeichnen, um daraus Informationen über einen geheimen Schlüssel zu erlangen. Wesentlich ist, dass dem Angreifer durch solche Messungen ein Paradigmenwechsel gelingt. Anstatt anhand der Ausgangsdaten einen vollständigen kryptographischen Schlüssel brechen zu müssen, beobachtet der Angreifer bei einem Seitenkanalangriff kleine Zeitausschnitte der kryptographischen Berechnung, in denen nur Teile des kryptographischen Schlüssels in Zwischenergebnissen enthalten sind. Auf Basis der Messungen versucht der Angreifer dann, diese kleinen Schlüsselteile getrennt voneinander zu brechen. Er muss dabei immer nur Geheimnisse der Größenordnung von z. B. 8 bit auf einmal brechen, was eine deutliche Erleichterung darstellt. Dieser Vorteil ist immens, auch wenn die

Fotos: ASEC

Abb. 1: Hochpräzise Seitenkanalmessung des Magnetfeldes als Angriff gegen die kryptographische Implementierung.

verwendeten Messungen keinesfalls erlauben, die Werte direkt zu bestimmen. Die Messwerte werden zu diesem Zweck üblicherweise mit umfangreichen statistischen Methoden analysiert, da die Signale sehr schwach und das Rauschen sehr stark sind. Schlussendlich kann ein Angreifer aber durch den Einsatz von einigen Tagen Laboranalyse kryptographische Schlüssel aus Geräten extrahieren, die mit herkömmlichen mathematischen Angriffen auf Basis von ausgegebenen Nachrichten selbst unter Zuhilfenahme der besten verfügbaren Rechner-Ressourcen nicht in endlicher Zeit gebrochen werden könnten. Daher sind solche Angriffe immens gefährlich.

Die Implementierungssicherheit kryptographischer Algorithmen ist seit sehr vielen Jahren ein aktives Forschungsgebiet. Es gibt zahlreiche Methoden, um Angriffe zu erschweren, aber auch immer wieder neue und verbesserte Angriffe. So lassen sich zum Beispiel Seitenkanalangriffe bis heute nicht gänzlich ausschließen, was auch an immer präziseren Messmethoden liegt. Die Abbildung 1 zeigt eine sehr hochentwickelte Form eines Seitenkanalangriffs aus dem Labor des Fraunhofer AISEC in Garching bei München. Das Bild zeigt einen Chip, der eine kryptographische Berechnung ausführt, und dessen Gehäuse mit Hilfe von Säure für die Präzisionsmessung entfernt wurde. Über dem Silizium sind 3 spezielle Messsonden für magnetische Felder positioniert, deren Spitzen Messspulen von nur ca. 100 µm Durchmesser enthalten. Solche hochwertigen Messplätze erlauben äußerst präzise Seitenkanalanalysen. Dies ist notwendig, um auf einem hohen Niveau die Sicherheit von kryptographischen Implementierungen und die Wirksamkeit von integrierten Schutzmaßnahmen bewerten zu können. Es erlaubt, sichere Implementierungen für verschiedenste eingebettete Systeme bis hin zu Geräten mit hohen Sicherheitsanforderungen zu entwickeln. Fraunhofer AISEC hat zu diesem Zweck über die letzten 10 Jahre ein hochentwickeltes Hardware-Sicherheitslabor aufgebaut, das in der Lage ist, solche Untersuchungen durchzuführen. Dabei wurde insbesondere an der schlussendlich erreichbaren Präzision von Seitenkanalmessmethoden und Laserbasierten Fehlerangriffen geforscht, um abzuleiten, welcher Aufwand im Schutz gegen Angriffe betrieben werden muss.

Fehlerangriffe

Die genannten Fehlerangriffe sind eine weitere wichtige Form von Implementierungsangriffen auf kryptographische Algorithmen und basieren darauf, ein elektronisches Gerät während der Berechnung eines kryptographischen Algorithmus gezielt zu stören. Dafür gibt es grundsätzlich einfache, vergleichsweise unkontrollierte Methoden, bei denen dem Chip beispielsweise kurz die Spannungsversorgung entzogen wird. Für gezielte Untersuchungen gibt es hochpräzise Formen, bei denen ein kurz gepulster Laserstrahl auf einen sehr kleinen Bereich des Siliziums gerichtet wird. Aufgrund eines photoelektrischen Effekts kann so während der Berechnung ein Fehler in sehr bestimmte Zellen der Schaltung eingebracht werden; es werden dadurch zum Beispiel gezielt Zwischenwerte der kryptographischen Berechnung verändert.

Ein Angreifer nutzt dann fehlerhafte Ausgabewerte, um den geheimen Schlüssel zu brechen. Umso präziser ein Angreifer Fehler einbringen kann, desto höher die Chance, auch geschützte Implementierungen zu brechen. Daher muss auch die Untersuchung der Wirksamkeit von Gegenmaßnahmen mit einem hochentwickelten Messplatz erfolgen (s. Abb. 2).

Was ist zu tun?

Veröffentlichte Angriffe auf Produkte zeigen leider, dass viele eingebettete Systeme selbst gegen einfache Varianten dieser Angriffe nicht oder nur unzureichend geschützt sind. Beim Einsatz von kryptographischen Algorithmen muss daher dringend auf deren Implementierungssicherheit und die Untersuchung derselben im Labor geachtet werden. Zum Erhöhen der Implementierungssicherheit gibt es nämlich eine große Auswahl an Gegenmaßnahmen aus der Forschung und dem Bereich der dedizierten Sicherheitsprodukte. Diese gilt es nun in eingebetteten Systemen in einem sinnvollen Maß einzusetzen.

Dr. Johann Heyszl
Fraunhofer AISEC

Abb. 2: Laser-Messplatz, der in der Lage ist, mit zwei parallelen Laserstrahlen einzelne Bits in Chips wahlfrei auf logisch 0 oder logisch 1 zu setzen

Quantencomputer

Steht die Revolution vor der Türe?

Seit mehr als 20 Jahren wird zum Thema Quantencomputer geforscht und in letzter Zeit mehren sich die Erfolgsmeldungen. Mit ausgefeilter Technik können quantenmechanische Schwebezustände der aktiven Rechenelemente immer länger aufrechterhalten werden, eine Voraussetzung für das Funktionieren dieses Konzeptes. Viele große Konzerne versprechen die baldige Marktreife der Geräte, im IT-Bereich sieht man Probleme mit den gängigen Verschlüsselungen.

Eine Binärziffer, die zwei Zustände aufweist, die als 1 oder 0 dargestellt werden, also das bekannte Bit, ist die grundlegende Speicher- und Arbeitseinheit eines klassischen Computers. Der Wert eines Bits wird meist durch die Ladung eines Kondensators in Verbindung mit einem festgelegten Schwellwert definiert.

Was ist ein Quantencomputer?

Beim Quantencomputer (QC) ist die logische Grundeinheit eine Quanten-Binärziffer, das „Quantenbit" oder „Qubit".
Abhängig von der Art des QCs kann ein Qubit durch Zustände von Photonen, Atomen, Ionen usw. repräsentiert sein. Weitere technisch interessante, makroskopischere Varianten solcher Quantensysteme sind supraleitende Schaltungen. In ihnen können unter bestimmten Bedingungen beide Stromrichtungen bzw. zwei Ladungszustände überlagert sein. Ein solches Quantenobjekt kann entsprechend codierte logische Zustände „0" oder „1" annehmen, aber auch beliebige überlagerte Zwischenzustände.
„Überlagerung" und „Verschränkung" sind zwei von vielen quantenmechanischen Begriffen, die im Zusammenhang mit QCs auftauchen. In der Quantentheorie bedeutet Überlagerung die Fähigkeit eines Quantenobjekts, mehrere mögliche Zustände gleichzeitig einzunehmen.
„Verschränkung" ist die Fähigkeit von zwei oder mehr Quantenobjekten, sich in einem Zustand zu befinden, in dem sie auf seltsame Weise miteinander verbunden sind. Die Gesetze der Quantentheorie sind vielfach überprüft, aber unintuitiv, und sie stehen im Widerspruch zu einer anderen etablierten physikalischen Theorie – Einsteins Relativitätstheorie. Einer Ansicht nach ist die Natur inhärent so, wie wir sie beobachten, und wir müssen sie so akzeptieren. Nach einer anderen Ansicht deuten beide Konzepte auf eine Unvollständigkeit der Quantentheorie hin. Wenn man also QCs hat, bei denen Quantenkonzepte direkt verwendet werden, eröffnen sich damit neue Möglichkeiten um neue Theorien jenseits der heutigen Quantentheorie zu entwerfen und entsprechende Experimente durchzuführen.

Konzepte von Quantencomputern

Es gibt zwei Arten von QCs: Quanten-Annealer und Gatter-basierte QCs. Annealer beruhen darauf, dass gekoppelte Qubits von einem definierten Ausgangszustand hin und her springen und sich so lange umstellen, bis das gesamte System seine minimale Energie erreicht hat. Dieses Minimum entspricht dann der Lösung des Problems, das wir zu lösen versuchen. Gatter-basierte QCs basieren auf Schaltungen, bei denen der Rechenprozess auf den Zuständen einer Folge von reversiblen Quantengattern beruht. Gatter-basierte QCs mögen auf lange Sicht besser sein, da sie eine hohe Flexibilität bieten, kurzfristig sind Annealer jedoch leistungsfähiger.
Steuern lassen sich die Zustände der Qubits z. B. durch Mikrowellenpulse auf supraleitende Schaltungen, wie sie im Google-Quantenprozessor verwendet werden, oder durch Laserpulse auf Quantenobjekte in Ionenfallen. Beim Annealer werden die Quantenobjekte durch das Anlegen von Magnetfeldern gesteuert. Für beide Arten von QCs ist es eine große Herausforderung, Probleme und Algorithmen für einen konventionellen Computer in solche für den QC zu übersetzen. Eine große technische Herausforderung ist es aber auch, die Quantenobjekte für eine ausreichende Zeit, mindestens einige Mikrosekunden, in ihrem Überlagerungszustand zu halten.

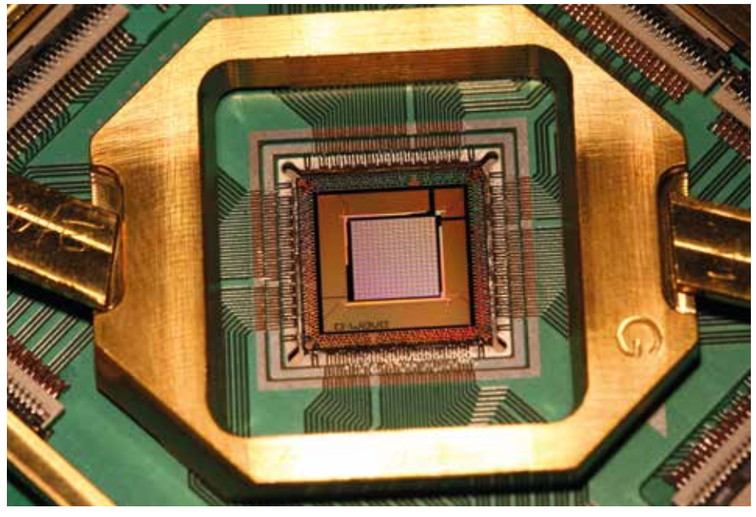


Foto: D-Wave Systems

Quanten Annealer: D-Wave 2000Q Quantenprozessor mit etwa 2000 supraleitenden Schleifen (Qubits), Arbeitstemperatur bei 15 mK.

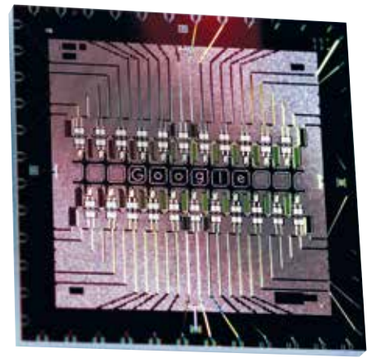
Wer braucht den Quantencomputer?

Quantencomputer stoßen bei Industrie- und Wissenschaftsgruppen, die bereits Supercomputer für ihre Forschungsprogramme und Anwendungen einsetzen, auf zunehmendes Interesse. Die Pilot-QC-Anwender sind in erster Linie daran interessiert zu testen, ob die verfügbaren QCs heute oder in absehbarer Zeit zur Lösung der für sie relevanten Probleme geeignet sind. Es ist wichtig, dass sich die Industrie schnell auf den Einsatz von QCs zur Lösung spezifischer Probleme vorbereitet. Die Konkurrenz schläft nicht.
Ein eminent wichtiger Punkt im Kontext der Cyber-Sicherheit ist aber, dass der Quantencomputer die heute gebräuchlichsten Verschlüsselungsmethoden unwirksam machen könnte. Dies liegt daran, dass die Public-Key-Codierung auf der Produktbildung zweier (sehr großer) Primzahlen basiert. Diese ist leicht durchzuführen, aber die Umkehrung, nämlich die Faktoren aus einem bekannten Produkt zu finden, die sogenannte Primfaktorisierung, ist heute noch praktisch unmöglich. 1994 stellte der amerikanische Mathematiker und Informatiker Peter Shor jedoch einen Algorithmus vor, der, auf einem QC verwendet, die Primfaktoren exponentiell schneller berechnen würde als ein klassischer Computer und somit die Standard-RSA-Verschlüsselung brechen könnte. Dieses wurde an Simulatoren von QCs, die auf den schnellsten heutigen Supercomputern der Welt betrieben wurden, positiv getestet. Es gibt also nur einen Ausweg: Die Verschlüsselungsstandards müssen gehärtet werden, um in einer post-quantum Welt zu überleben.

Mythen und Realitäten

Persönliche Pocket QCs in naher Zukunft: Möglicher Mythos

Unsere täglich genutzten (klassischen) Computer sind bereits sehr gut und es wird erwartet, dass sie für die meisten Zwecke nützlich bleiben. Ein QC, der in der Praxis nützlich sein kann, ist immer noch Zukunftsmusik, auch wenn große Unternehmen wie IBM, Google und Intel seit einigen Jahren erhebliche Ressourcen in ihre Entwicklung investieren. Auf lange Sicht kann es jedoch anders sein, wenn die Entwicklung der QCs fortschreitet.



Gatter-basierter Prozessor: Googles Quantenchip „Foxtail" mit 22 supraleitenden Schaltungen (Xmon-Qubits). Arbeitstemperatur bei 10 mK. *Bildquelle: Google*

QCs werden klassische Computer ersetzen: Mythos

Es wird erwartet, dass der Einsatz von QCs hauptsächlich im Bereich von Berechnungen bleiben wird, wo klassische Computer entweder ineffizient sind oder eine Berechnung algorithmisch nicht möglich ist. QCs, die zusammen mit Supercomputern im Hybridmodus betrieben werden, können wahrscheinlich viel bessere Rechen- und Energieeffizienz erreichen als Supercomputer allein. Es wird erwartet, dass klassische Computer für den täglichen Gebrauch durch den Endbenutzer weiterhin nützlich bleiben.

Extrem schnelles Rechnen: Mögliche Realität

Im Prinzip gibt es nichts, was ein QC leisten kann, ein klassischer Computer aber nicht. In der Praxis machen Größe, Energieverbrauch, Rechenleistung und -zeit große Unterschiede aus. Bestimmte Probleme können schneller gelöst werden – exponentiell schneller. Diejenigen Probleme, die sich derzeit und in naher Zukunft außerhalb des Bereichs der leistungsfähigsten Supercomputer, aber im Rahmen der QCs befinden, sind von besonderem Interesse und werden voraussichtlich die Industriestandards revolutionieren.

Die Nutzung von QCs wird langfristig zunehmen: Mögliche Realität

Es ist zwar richtig, dass sich die QCs in naher Zukunft in erster Linie auf sehr spezifische Probleme konzentrieren werden, aber man kann nicht behaupten, dass dies langfristig der Fall sein wird. Ganz grob ausgedrückt könnten wir uns bei der Entwicklung der QCs derzeit in einem Stadium befinden, in dem klassische Computer bei der Erfindung des Transistors standen. Mögliche Anwendungen von QCs wurden für Verschlüsselung, Verkehrsoptimierung, Produktionsplanung, Pharmazie, Luftfahrt, autonomes Fahren, Satellitenoptimierung, quantengestütztes Maschinenlernen, um nur einige zu nennen, gefunden. Es gibt auch anstehende wissenschaftliche Anwendungen von QCs, z. B. im Bereich der Materialwissenschaft und der Simulation von Quantensystemen.

Und die Zukunft?

Obwohl wir einige Mythen und Realitäten im Zusammenhang mit QCs und ihren Einsatzmöglichkeiten für industrielle und wissenschaftliche Anwendungen aus heutiger Sicht diskutiert haben, wären langfristige Vorhersagen unwissenschaftlich. Wir arbeiten an der Zukunft, aber die Zukunft wird stets anders aussehen als das, was wir uns heute vorstellen können!

Manpreet Jattana M.Sc. und
Prof. Dr. Kristel Michielsen
Jülich Supercomputing Centre

Originalsprache Englisch
Ins Deutsche übersetzt von
www.DeepL.com und Fritz Münzel

Resiliente Kritische Infrastrukturen

Kritische Infrastrukturen wie das Stromnetz oder Verkehrswege sind zunehmend von digitalen Komponenten abhängig. Dies ermöglicht zwar einerseits eine flexible und dezentrale Steuerung, erhöht aber andererseits die Anfälligkeit für Cyberangriffe.

Seit knapp vier Jahren ist bekannt, dass Angriffe gegen kritische Infrastrukturen in den Bereich des Möglichen gerückt sind. Im Dezember 2015 wurde etwa das Stromnetz der Ukraine Opfer eines Cyberangriffs. Forensische Daten legen nahe, dass die Angriffe über einen Zeitraum von fast 9 Monaten geplant und durchgeführt wurden. Durch einen initialen „Spear Phishing" Angriff über ein infiziertes Word-Dokument gelangte Schadcode in die Netzwerke verschiedener Betreiber. Dies ermöglichte den Angreifern, die befallenen Netzwerke über einen langen Zeitraum zu analysieren und einen weiteren komplexen Angriff vorzubereiten, der schließlich zum Ausfall mehrerer Umspannwerke für mehrere Stunden führte. Der Betrieb konnte letztendlich nur durch das Umschalten auf manuelle Steuerung behoben werden.

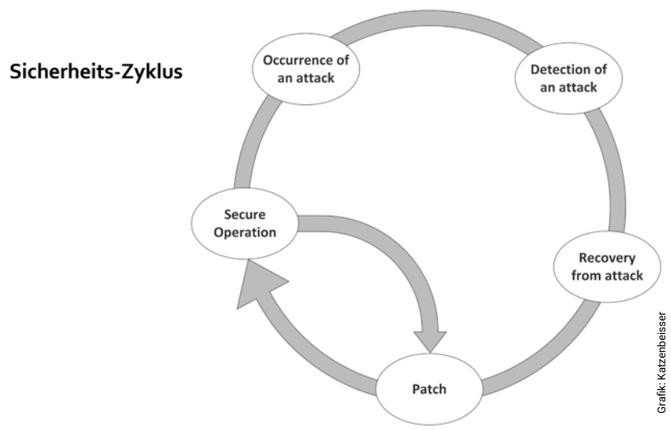
Die Software und Hardware vieler kritischer Infrastrukturen wird nach den Kriterien der funktionalen Sicherheit entworfen – und kann daher beispielsweise mit Ausfällen von einzelnen Komponenten bereits umgehen. Allerdings sind funktional sichere Komponenten in der Regel nicht robust gegen Cyberangriffe. Konzepte zur Erzielung von funktionaler Sicherheit basieren nämlich oftmals auf Redundanz sowie der Annahme, dass Komponenten unabhängig und zufällig ausfallen. Dies ist jedoch im Kontext der Cyber-Sicherheit nicht der Fall, da ein Angreifer üblicherweise gezielt das „schwächste Glied" eines Systems ausnützt. Sind daher funktional sichere Komponenten auch Cyberangriffen ausgesetzt, so müssen spezielle Schutzmaßnahmen vorgesehen werden.

Security Engineering-Prozess

Kritische Infrastrukturen sollten immer mit einem Fokus auf Cyber-Sicherheit entworfen werden. Stand der Technik ist hierbei die Etablierung eines „Security Engineering" Prozesses: Statt ein System erst nach dessen Implementierung oder Inbetriebnahme abzusichern, muss Cybersicherheit in allen Phasen des Entwicklungsprozesses mitgedacht werden – vom Design über die Entwicklung bis hin zur Einführung sowie der Stilllegung.

Ein Security Engineering Prozess umfasst üblicherweise mehrere Schritte: In einem ersten Schritt werden dabei die „Assets" untersucht, also alle schützenswerten Betrachtungsgegenstände, bestehend aus physischen Komponenten oder immateriellen Größen wie Reputation. Danach wird analysiert, welche Angreifer gegen das zu entwickelnde System zu erwarten sind und welche Ressourcen bzw. welche Motivation diese aufweisen – das Spektrum reicht dabei von Amateur-Hackern über kriminelle Vereinigungen bis hin zu staatlichen Akteuren im Kontext von Cyberwar. Diese Analyse bildet die Basis einer Risikobetrachtung, bei der geklärt wird, gegen welche Angreifer ein Schutz nötig ist und welche man bewusst in Kauf nimmt. Beispielsweise wird ein Schutz gegen staatliche Angreifer aus Kostengründen oftmals nicht betrachtet. Nach dem Risikomanagement müssen nun zielgerichtete Maßnahmen zum Schutz gegen Cyberangriffe abgeleitet werden; diese können technischer oder organisatorischer Natur sein. Während der Implementierung muss speziell auf die Qualität der Software geachtet werden, um etwa die Zahl der kritischen Softwarefehler auf ein Minimum zu beschränken.

Nach der Installation sowie der Anpassung des implementierten Systems (auch hierbei sollte man die Cyber-Sicherheit mitbedenken, etwa durch das Ändern von Standardpasswörtern) erfolgt die Aufrechterhaltung des sicheren Betriebs. Da jedoch kein System gegen alle in der Zukunft zu erwartenden Angriffe sicher sein kann, müssen Angriffsversuche laufend detektiert werden. Noch während eines Angriffs sollte es zeitnah zu dessen Abwehr kommen, etwa durch die Einleitung von kurzfristigen Notmaßnahmen. Sobald der dem Angriff zugrundeliegende Fehler durch den Hersteller behoben wurde, muss der entsprechende Patch eingespielt werden, um einen neuerlichen Angriff über den gleichen Weg zu unterbinden. Erfahrungsgemäß ist dies aus mehreren Gründen schwierig.



Sicherheits-Zyklus: Reaktion auf einen Angriff – von der Erkennung eines Angriffs über kurzfristige Sofortmaßnahmen bis hin zum Patchen

Erstmals ist die zeitnahe Detektion eines Angriffes eine Herausforderung, da Angreifer gezielt versuchen, über einen längeren Zeitraum unentdeckt zu bleiben. Zum anderen müssen Systeme in kritischen Infrastrukturen oftmals eine Zertifizierung aufweisen, was das Patchen der Systeme erschwert bzw. den Zeitraum bis zur Verfügbarkeit von Patches verlängert.

Resilienz

Trotz aller Vorkehrungen können erfolgreiche Angriffe nie ausgeschlossen werden. Da unsere Gesellschaft in hohem Maße vom Funktionieren kritischer Infrastrukturen abhängig ist, sollten diese daher derart entworfen und implementiert sein, dass sie selbst unter Angriffen nicht komplett versagen, sondern ein Mindestmaß an Funktionalität und Verfügbarkeit aufweisen. Diese Eigenschaft bezeichnet man als „Resilienz".

Resilienz ist oftmals schwer zu erreichen, kann jedoch durch entsprechendes modulares Systemdesign verbessert werden. Hierbei wird versucht, ein großes System in entsprechend kleinere Subsysteme zu partitionieren, sodass sich Angriffe nicht über Systemgrenzen hinweg ausbreiten können und das Gesamtsystem selbst bei Kompromittierung einzelner Subsysteme nicht zusammenbricht.

Die Arbeitsgruppe CYSIS, initiiert durch die Deutsche Bahn sowie die TU Darmstadt, hat weitere grundlegende Empfehlungen erarbeitet, wie die Resilienz kritischer Infrastrukturen erhöht werden kann. Eine der zentralen Empfehlungen ist die Absicherung jeder Kommunikation „Ende zu Ende", also von der Datenquelle bis hin zum Empfänger. Stand der Technik für die Ende-zu-Ende-Sicherung der Kommunikation sind Verfahren zur Verschlüsselung und sowie zur Generierung digitaler Signaturen.

Neben der Absicherung der Kommunikation selbst spielt auch die Integrität der Endgeräte eine herausragende Rolle, da Angreifer oftmals versuchen, Schadcode auf eingesetzte Geräte aufzuspielen. In Zukunft sollten daher die wichtigsten Systeme in der Lage sein, ihre eigene Software-Integrität zu prüfen und diese gegenüber Dritten zu übermitteln – man spricht von „remote attestation".

Zur frühzeitigen Detektion von Angriffen sollten zudem entsprechende Sensoren im Gesamtsystem platziert werden. Die Meldungen aller Sensoren können dann an einer zentralen Stelle in einem „Security Operations Center" aggregiert werden, um eine fundierte Bewertung der Sicherheitslage durch Experten vorzunehmen. Ist ein Angriff detektiert, so müssen dessen Auswirkungen auf das System zeitnah begrenzt werden.

Fazit

Kritische Infrastrukturen rücken zunehmend in den Fokus von Angreifern, ihre Absicherung ist daher von essentieller Bedeutung für unsere Gesellschaft.

Viele Systeme kritischer Infrastrukturen wurden jedoch bisher ohne Betrachtung der Cyber-Sicherheit konstruiert. Hier gilt es, durch einen entsprechenden „Security Engineering" Prozess gegenzusteuern, um das Ziel der größtmöglichen Resilienz zu erreichen.

Prof. Stefan Katzenbeisser
Lehrstuhl für Technische Informatik
Universität Passau

Verifizierter Schutz über die gesamte Lieferkette

Troja Today

Hätten die Trojaner seinerzeit auf die Warnungen der Königstochter Kassandra gehört und das riesige Holzpferd – ein vermeintliches Weihgeschenk der Griechen – nicht in ihre Stadt geholt, wären sie wohl unbesiegt geblieben. Doch die Geschichte ging bekanntlich anders aus.

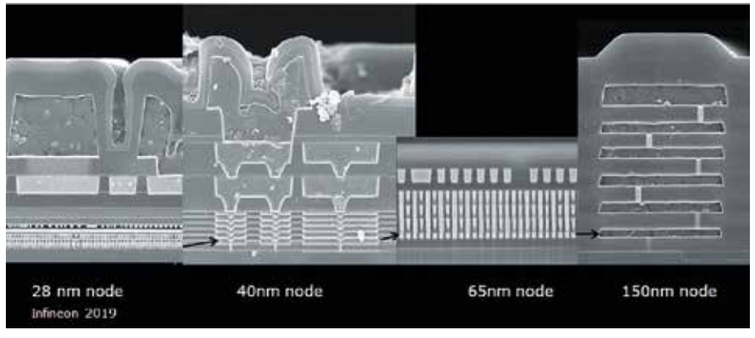
Ähnlich wie im alten Troja macht die Freude am technischen Fortschritt und seinen Möglichkeiten oft blind für die verborgenen Risiken.
Vor allem die Integrität und der Schutz von Daten haben eine ebenso hohe gesellschaftliche wie wirtschaftliche Bedeutung. Moderne komplexe Informations- und Kommunikationssysteme in Anwendungsgebieten wie Internet of Things (IoT), Industrie 4.0, Health, autonomes Fahren oder kritische Infrastrukturen bieten unschätzbar viele Möglichkeiten – doch wirklich akzeptieren werden Nutzerinnen und Nutzer solche Systeme nur, wenn diese wirklich sicher vor unbefugtem Zugriff sind.

Nur der kombinierte verifizierte Schutz auf Soft-, Firm- und Hardwareebene über die gesamte Lieferkette kann den Aufwand für Angriffe von Datendieben und Manipulatoren erhöhen und Risiken minimieren.
Hardwareseitig kann er nur durch den Einsatz von Sicherheitskomponenten mit hardwarebasierter Verschlüsselung erreicht werden. Diese können integraler Bestandteil von Systemen auf dem Chip (SOC – System on a Chip), als eigenständiger Chip im selben Gehäuse (SIP – System in a Package) oder als zusätzlicher Baustein (TPM – Trusted Platform Module) in einem System sein. Die höchsten Sicherheitsanforderungen werden dabei an Bausteine gestellt, die in Reisedokumente und Bankkarten integriert werden. Auch wenn diese noch in etwas älteren Technologien in Europa hergestellt werden, haben die Kosten für Entwicklung und Massenherstellung von Bausteinen mit Strukturen von aktuell weniger als 10 nm die Fertigung von Europa zunehmend zu wenigen Auftragsfertigern (Foundry, Assembly, Test) vorwiegend nach Fernost verlagert.
Diese sind Grundlage für die vorgenannten Anwendungen. Für europäische Nutzer gilt es, in der gesamten Wertschöpfungskette von den Entwurfsdaten bis hin zum fertigen Baustein oder gefertigten System Gefährdungen durch Angriffe, Manipulation und Fälschungen an der Quelle vorzubeugen.
Bei den zunehmend komplexen Bausteinen und Systemen ist keine vollständige Abdeckung durch elektrische Tests möglich. In manchen Fällen wird die Testbarkeit sogar bewusst eingeschränkt, um die Sicherheit zu erhöhen.
Vor diesem Hintergrund müssen exemplarisch zumindest die sicherheitskritischen Teile von gefertigten Bausteinen physisch analysiert und verifiziert werden können. Dies kann am wirksamsten durch Vergleich mit bekannten Entwurfsdaten erfolgen. Dieser Analyse- und Verifikationsprozess umfasst, wie von Lippmann et al. [1] gezeigt, grundsätzlich folgende Schritte:

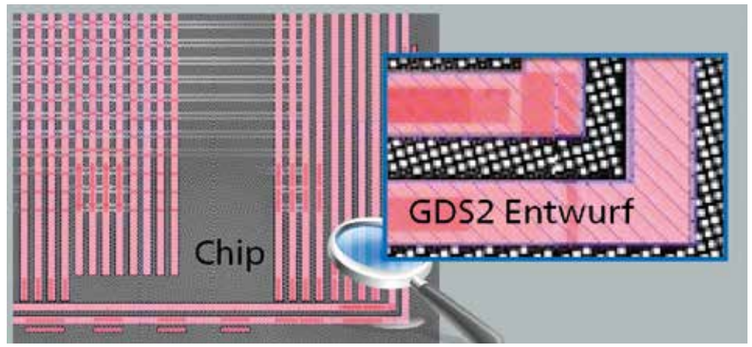
1) Analyse und Entfernung des Gehäuses in welchem sich auch mehrere integrierte Schaltungen neben- oder übereinander befinden können
2) Selektiver, planparalleler Abtrag der einzelnen Isolationsschichten und Freistellen der Metallisierungsebenen oder aktiven Ebenen auch bei gewölbten Bausteinen
3) Abscannen der Strukturen mittels eines speziellen Rasterelektronenmikroskops mit einer Auflösung von wenigen Nanometer
4) Erzeugung globaler Bilder (z. B. Metallisierungsebenen) aus den einzelnen Bildern (Stitching)

Bei vorhandenen Entwurfsdaten kann hier bereits der Vergleich mit den Analysedaten erfolgen. Bei unbekannten Bausteinen schließen sich die folgenden Stufen an:

5) Erkennung und Differenzierung von Strukturen (Leiterbahnen, Vias, Transistoren) und Zellen
6) Vergleich mit Entwurfsdaten im GDS2-Format
7) Passgenaue Überlagerung dieser Ebenen und vertikalen Verbindungen



Querschliffe zeigen exemplarisch die Abnahme der Strukturgrößen und Schichtdicken für CMOS-Technologien unter 150 nm und die damit verbundenen Herausforderungen für die Analyse [1]



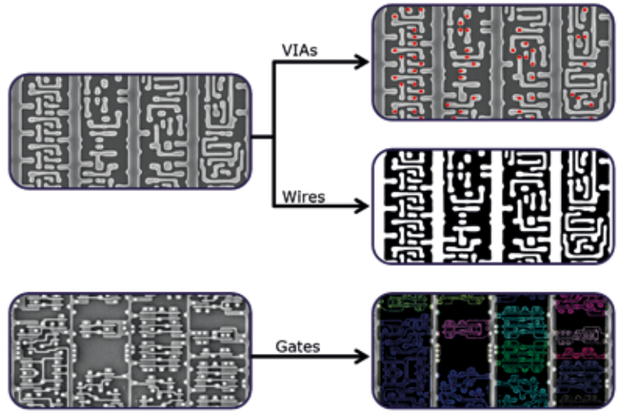
Exemplarischer Vergleich der eingescannten integrierten Schaltung mit dem Layout im GDS2-Format [1]

8) Erkennung von Schaltungsblöcken und Erzeugung eines Schaltplans
9) Analysen auf höherer Abstraktionsebene

Die Schlüsselherausforderungen dieses Prozesses, die insbesondere für die aktuellen Technologien zum Teil noch gelöst werden müssen, sind:

- Bei der Rückpräparation von 40 nm Technologien müssen für Chipgrößen bis über 100 mm² hinweg Toleranzen von wenigen 10 nm eingehalten werden.
- Die über mehrere Tage hinweg stabile Präzision und hohe Effizienz der Erzeugung von Bildern mit höchster Auflösung
- Die effiziente Verarbeitung der bei der Analyse entstehenden riesigen, mit Präparationsartefakten und Rauschen behafteten Datenmengen
- Vertikal integrierte Multi Chip Module.

Die sich daraus ergebenden interdisziplinären Aufgaben und die Weiterentwicklung der Werkzeuge und Programme können nur in enger Zusammenarbeit eines Konsortiums mit den unterschiedlichen Schwerpunkten und Ressourcen sowie öffentlicher Förderung ganzheitlich bearbeitet werden.
Im Rahmen des durch das Bundesministerium für Bildung und Forschung BMBF geförderten Investitionsprojektes FMD [2] werden auch hochwertige Geräte für das Sicherheitslabor der Fraunhofer EMFT, das noch 2019 nach CC-EAL6 zertifiziert werden soll, beschafft. Die Methoden werden seit 2017 auch im Rahmen der von BMBF geförderten Forschungsprojekte SyPASS [3] und RESEC [4] angewandt und weiterentwickelt. Zudem ist die Fraunhofer EMFT koordinierende Partnerin des vom Freistaat Bayern und der Fraunhofer Gesellschaft geförderten Münchner Leistungszentrums »Sichere intelligente Systeme« [5].
Auch wenn aktuell die Realisierung und Entdeckbarkeit von integrierten Hardware Trojanern in der wissenschaftlichen Literatur akademischen Charakter besitzt und noch keine Fälle öffentlich bekannt geworden sind, sollten wir nicht vergessen: die grundsätzliche technische Möglichkeit dazu besteht und so könnte aus der Theorie schneller Praxis werden als gedacht. Solide Risikoanalysen in den verschiedenen kritischen Bereichen sollten daher eine realistische Bewertung der technischen Möglichkeiten, des Aufwands für Manipulationen sowie die Verfügbarkeit von Methoden zu deren Erkennung in integrierten Schaltungen beinhalten.



Bildverarbeitung vom Rasterelektronenmikroskopbild (REM-Bild) zur identifizierten Zelle [1]

Dr.-Ing. Horst Gieser
Leiter CS Analyse & Test
Fraunhofer EMFT, Einrichtung für Mikrosysteme u. Festkörpertechnologien München

Quellen

[1] Bernhard Lippmann, Michael Werner, Niklas Unverricht, Aayush Singla, Peter Egger, Anja Dübotzky, Horst Gieser, Martin Rasche, Oliver Kellermann, Helmut Graeb, 2019. Integrated Flow for Reverse Engineering of Nanoscale Technologies. In Proceedings of the 24th Asia and South Pacific Design Automation Conference (ASPDAC, 19). ACM, New York, NY, USA, pp. 82-89. https://doi.org/10.1145/3287624.3288738
[2] FMD Forschungsfabrik Mikroelektronik Deutschland https://www.bmbf.de/foerderungen/bekanntmachung-1513.html
[3] SyPASS – Systeme und Verfahren für die fehlerfreie Präparation und Abbildung sicherer höchstintegrierter Schaltungen https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/sypass
[4] RESEC – Systeme und Methoden für die Analyse und Rekonstruktion höchstintegrierter Sicherheitsschaltungen https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/resec
[5] Leistungszentrum Sichere intelligente Systeme LZ SiS ein Zusammenschluss der sechs Fraunhofer-Institute AISEC, EMFT, ESK, IBP, IGCV und IVV aus dem Großraum München mit der TU München und der Universität der Bundeswehr München, https://www.lz-sis.de/

Unsere moderne Zivilisation ist verletzlich


Europa bei Nacht – nur mit Strom

Quelle: ESA/NASA

Im Jahre 2010 hatte eine vom Deutschen Bundestag in Auftrag gegebene Studie die „Gefährdung und Verletzbarkeit moderner Gesellschaften“ untersucht und kam zu dem Ergebnis: „Aufgrund der nahezu vollständigen Durchdringung der Lebens- und Arbeitswelt mit elektrisch betriebenen Geräten würden sich die Folgen eines langandauernden und großflächigen Stromausfalls zu einer Schadenslage von besonderer Qualität summieren.
Betroffen wären alle Kritischen Infrastrukturen, und ein Kollaps der gesamten Gesellschaft wäre kaum zu verhindern. Trotz dieses Gefahren- und Katastrophenpotenzials ist ein diesbezügliches gesellschaftliches Risikobewusstsein nur in Ansätzen vorhanden.“ [1, S. 4]
Hintergrund ist, dass in modernen Gesellschaften die Versorgung der Bevölkerung mit notwendigen Gütern und Dienstleistungen über ein eng verflochtenes Netz „Kritischer Infrastrukturen“ erfolgt. Dazu gehören die Informationstechnik und Telekommunikation, das Transport- und Verkehrswesen sowie die Energieversorgung oder das Gesundheitswesen. Diese sind nicht zuletzt wegen ihrer gegenseitigen Abhängigkeiten hochgradig verletzbar, etwa durch terroristische Anschläge, Naturkatastrophen oder Unfälle.

Blackout und die Folgen

Da die Funktion der Elektroenergie- und Kommunikationsnetze unabdingbar für alle anderen Infrastrukturen ist, haben massive Funktionsstörungen in diesem Bereich katastrophale Auswirkungen auf die Gesellschaft. In der Vergangenheit ließen verschiedene Blackouts die weitreichenden Folgen erahnen, etwa wenn 1977 beim einen Stromausfall in New York, der 25 Stunden dauerte, Plünderer und Brandstifter durch die Stadt zogen und die Polizei im Dauereinsatz war. Während das Stromnetz die Energie für die verteilten Infrastrukturkomponenten bereitstellt, erfolgt deren Steuerung meist über das Kommunikationsnetz.
Angriffe auf Computer sind zwar seit langem bekannt, aber nun werden nicht nur Daten verändert – was gleichfalls sehr problematisch ist –, sondern es besteht die Möglichkeit, direkt in unsere materielle Welt einzugreifen. Bereits 2011 forderte eine OECD-Studie die Erhöhung der Cyber-Sicherheit in diesem Bereich [2].

Cyberangriffe auf die Infrastruktur sind möglich

Die Relevanz der Cyber-Sicherheit hatte im Juni 2010 die Schadsoftware Stuxnet verdeutlicht. Diese war eigens zum Angriff auf eine Industriesteuerung von Siemens entwickelt worden. Derartige Steuerungssysteme werden vielfach in Industrie- und Infrastrukturanlagen eingesetzt. Bald wurde klar, dass der Computerwurm speziell für den Angriff auf die Steuerung von Uranzentrifugen u. a. in der iranischen Anreicherungsanlage Natanz programmiert worden war. Mittlerweile gilt als gesichert – was aber bisher nie bestätigt wurde! –, dass Geheimdienste in den USA und in Israel die Software programmiert hatten, um das iranische Atomprogramm zumindest um einige Zeit zu verzögern.
Der Computerwurm Stuxnet zeigt, dass Angriffsszenarien auf die Infrastruktur Realität werden könnten. Aber nicht nur Cyberwar-Attacken, über die im Nachgang von Stuxnet intensiv diskutiert wurde, sind als Ursache für einen Netzzusammenbruch denkbar; auch Kriminelle könnten dahinter stecken. Je mehr elektronische Komponenten in einer Wohnung über das Internet gesteuert werden, desto mehr Einstiegsmöglichkeiten haben potentielle Hacker, die Personen aber auch den Staat erpressen könnten. In der Folgezeit wurde nicht nur in Deutschland die Sicherheit „Kritischer Infrastrukturen“ auf den Prüfstand gestellt. Naturgemäß sind die zuständigen Unternehmen und Behörden zurückhaltend mit Informationen, aber die Tatsache, dass im Rahmen der 2011 von der Bundesregierung verabschiedeten Cyber-Sicherheitsstrategie ein Cyber-Abwehrzentrum gegründet wurde, zeigt, dass das Problem erkannt wurde.

Frank Dittmann
Deutsches Museum München

Literatur

[1] Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung. Bericht des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung. Deutscher Bundestag, Drucksache 17/5672, 27.04.2011
[2] Peter Sommer, Ian Brown: Reducing Systemic Cybersecurity Risk. OECD/IFP Project on “Future Global Shocks”, 14th January 2011
[3] Spektrum der Wissenschaft 2011, H. 10, Teil zur Energieversorgung

VDI BV München, Ober- und Niederbayern

Der VDI Italia zu Gast in München

Nächstes Jahr in München – mit diesen Worten verabschiedete sich der VDI Bezirksverein München, Ober und Niederbayern nach dem festlichen Goldenen Jubiläum des VDI Freundeskreis Italien 2018 in Ispra. Und am 12. September 2019 war es endlich so weit: der VDI Freundeskreis Italien folgte der herzlichen Einladung zum Jahrestreffen 2019 in die Bayerische Landeshauptstadt München.

Fotos: VDI

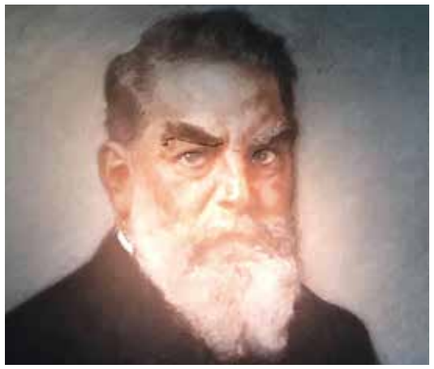
Im Angesicht Oskar von Millers höchst persönlich, dessen Ölportrait in der Hotel-Lobby ein wachsames Auge auf die Hotelgäste hatte, brach die Delegation des VDI München gemeinsam mit etwa 50 VDI-Mitgliedern aus Italien am 12. September gegen 16.00 Uhr auf, um das Druckhaus der Süddeutschen Zeitung zu besichtigen.
Ein viertägiges Programm wartete auf den Freundeskreis Italien, der seine Jahreshauptversammlung in jedem Jahr an einen anderen Ort verlegt. In diesem Jahr war also München an der Reihe.

50 km/h: die Zeitung auf der Überholspur

Dort gaben Uwe Seifert und Albert Vetter, beide langjährige Schichtleiter des Gesamtbetriebs, umfassenden Einblick in die Prozesse der Druckvorgänge.
Leider musste die Kamera, wie so oft, draußen bleiben. Glücklicherweise lässt sich so mancher Eindruck auch in Worte fassen.
Das SZ-Druckhaus jagt das Papier mit 50 km/h durch die Maschine. Mehr Elektronik sei in dieser Anlage verbaut, als in einem Jumbo-Jet, heißt es. Allein eine Papierrolle, die hier zum Einsatz kommt, enthält 21 km Papier, wobei gerade einmal 18 Minuten nötig sind, um eine Rolle komplett aufzubrauchen. Pro Nacht werden etwa 60 bis 70 solcher Rollen für den Druck verbraucht; rechnet man Fremdaufträge dazu, sind es sogar 90.
Im Anschluss an die gut zweistündige Führung ging es zum Hofbräukeller am Wiener Platz mit guten Gesprächen und in anregender Runde – ein gelungener Auftakt für ein Wochenende ganz im Zeichen der deutsch-italienischen Freundschaft.

Besuch bei MAN

Punkt 9:00 Uhr am Folgetag traf die Gruppe vor dem MAN Truck Forum ein. Die erste Gruppe startete die Besichtigung, während die zweite Gruppe eine halbe Stunde Zeit hatte, um historische Fahrzeuge und Modelle zu betrachten und in einigen Truck-Fahrerhäusern zur Probe zu sitzen.
Der Werksbus fuhr dann zuerst zur Achsfertigung. Hier werden in bunter Reihenfolge die Achsen für zwei-, drei- oder vierachsige Fahrzeuge montiert, dazu noch die Ausgleichsgetriebe für Allradfahrzeuge. Angebaut wurden für Baufahrzeuge noch Trommelbremsen und für Straßen-LKWs Scheibenbremsen. In der Rahmenfertigung wurden die Träger erst von der Unterseite her genietet oder geschraubt. Nach der Lackierung wurden die fertigen Achsen montiert.
Dann erfolgte das spektakuläre Umdrehen des Fahrgestells mit Hilfe einer Seilschlinge, der Einbau der Motoren und der weitere Anbau diverser Aggregate und der unterschiedlichen Fahrerhäuser.



Nach Montage der Räder wurde der Motor auf einem Rollenprüfstand gestartet. Beeindruckend war auch die Logistik der Kleinteile im „Warenhaus“, die in einem Anhänger dem selbstfahrenden Montageplatz folgten.

Schloß Nymphenburg und Jahreshauptversammlung am Königsplatz

Nach der zweistündigen Besichtigung war eine Pause am Schloß Nymphenburg angesagt. Ein Rundblick mit Erläuterung der Anlage und ein Blick in den Park drängte alle zur Stärkung in das Schloß-Café im Palmenhaus.
Die Fontäne verabschiedete uns zum nächsten Programmpunkt im Hansahaus des KKV-Hansa, wo die Jahreshauptversammlung des VDI Italia folgte.
Die Versammlung begann mit der Ehrung von Lorenzo Scandola für seine hervorragende Diplomarbeit mit dem Titel: „Implementation and Investigation of two distinct crystal-plasticity material models for polycrystalline nickel-base superalloys“. Scandola stellte die Arbeit kurz (weil zu schwierig für das Auditorium) vor. Er erhielt neben der Urkunde einen Geldbetrag und eine einjährige VDI-Mitgliedschaft.
Das Programm ging weiter mit dem Jahresbericht von Walter Brand und dem Kassenbericht von Reinhard Freidhof, beide wurden zustimmend angenommen. Klaus Haenel (stellvertretender Vorstand) und Reinhard Freidhof (Schatzmeister) wollten ihre Ämter niederlegen, und Neuwahlen standen an. Walter Brand wurde als erster Vorstand wiedergewählt. Für die vakanten Ämter fanden sich mit Bernd Hartmann (Schatzmeister) und Claus Quartz (stv. Vorstand) zwei Mitglieder der jüngeren Generation. So schloss die Versammlung sehr harmonisch, und die S-Bahn brachte alle zum Rosenheimer Platz und zum Hotel.

Gute Gespräche beim Gala-Abend

„Dahoam”, der bayrische Begriff für Heimat und Attribut für Gemütlichkeit, Wärme und Geborgenheit beschreibt die Atmosphäre beim Stangl Wirt am Freitagabend, zu dem der Vorstand des VDI München eingeladen hat, wohl tatsächlich am besten. Wobei es vor allem auch die Freundschaft ist, die in dieser Runde ausschlaggebend zu sein scheint – was für ein schöner und inspirierender Abend in freundschaftlicher Verbundenheit. Mit dabei an diesem Wochenende war Prof. Udo Ungeheuer, vormaliger VDI Präsident und seine Frau Susanne, sowie Agnes Galkowski von der VDI Hauptgeschäftsstelle, die auch die 15 internationalen Freundeskreise des VDI betreut.

Auf nach Landshut – der Hauptstadt Niederbayerns

Und auch am Samstag ging es schon früh auf Tour. Nach einer ausgedehnten Fahrt über das Rollfeld des Münchner Flughafens, bei der vor allem technisches Know-how, aber auch so manch lustige Anekdote aus rund 30 Jahren Flughafenbetrieb zum Besten gegeben wurde, war am Nachmittag Landshut das Ziel.
Nach einer dichten Stadtführung entlang der Martinskirche ging es die Stufen hinauf zur Burg Trausnitz. Dort führte der Kastellan Klaus Höchstetter überaus lehrreich und humorvoll durch die Räumlichkeiten. Zum Abschluss des Tages fanden sich alle im Bräustüberl Weihenstephan zum zünftigen Ausklang des Abends ein.
Der gemeinsame Stadtbummel am Sonntagmorgen führte vom Isar-Hochufer durch das Deutsche Museum zum Isartor und weiter über den Viktualienmarkt mit Karl Valentin-Brunnen, Jakobsplatz mit Synagoge und Marienplatz zum Franziskaner. Ein Frühschoppen mit Weißwürsten und Weißbier stärkte alle für die Rückfahrt nach Ispra, die hinter dem Nationaltheater begann.
Auf bald, liebe Freunde, liebe Italiener,
Arrivederci!
Besonderer Dank gilt dem Leiter des Arbeitskreises „Aktuelles Forum Technik“ Karl-Heinz Lohn, der dieses Wochenende maßgeblich organisiert hat.

VDI Landesverband Bayern

Gratulation zum Bayerischen Verdienstorden

Im Rahmen einer Feierstunde im Antiquarium der Residenz in München zeichnete Ministerpräsident Dr. Markus Söder, 58 Persönlichkeiten für ihre hervorragenden Verdienste um den Freistaat Bayern und das bayerische Volk mit dem Bayerischen Verdienstorden aus.


Foto: Bayerische Staatskanzlei

Prof. Dr. Reinhard Höpfl und Ministerpräsident Dr. Markus Söder (re.) bei der Ordensverleihung

Mit dabei ist auch unser ehemaliger VDI Landesverbandsvorsitzender und früherer Präsident der Hochschule Deggendorf, Professor Dr. Reinhard Höpfl. In seiner sechsjährigen Amtszeit, von 2009 bis 2014, als ehrenamtlicher Vorsitzender des VDI Landesverbandes Bayern stand Prof. Höpfl als kompetenter Ansprechpartner gegenüber Staatsregierung, Staatsministerien, Unternehmen, Wirtschafts- und Ingenieurverbänden sowie Universitäten und Hochschulen zur Verfügung. Für die Arbeit im VDI waren seine umfangreichen Verbindungen sehr hilfreich. Ebenso war Prof. Höpfl nicht nur der Impulsgeber für neue Kontakte und Projekte in Bildung, Wissenschaft und Technik, sondern er bezog geschickt und überzeugend in öffentlichen Veranstaltungen zu aktuellen Themen Stellung und vertrat dabei die berufspolitischen Interessen der Ingenieurinnen und Ingenieure. Zukunftsweisend setzte er auch auf ideenreiche Vorhaben, die das Interesse und die Begeisterung von Schülerinnen und Schülern für Technik und Naturwissenschaften wecken sollten. In seiner Zeit als Landesverbandsvorsitzender waren gerade sein Wirken und Handeln im Hochschulbereich in der Phase der Umstellung von Diplom auf Bachelor und Master, sowie weiterer Hochschulreformen sehr vorteilhaft. Aber auch die Medienarbeit und Koordinierung der Medienkontakte in Bayern spielten für ihn eine große Rolle.

Von 1996 bis 2012 war Prof. Dr. Höpfl Präsident der Hochschule Deggendorf, und in dieser Amtszeit sei die Hochschule „zu einem Anker der wissenschaftlich-technischen Infrastruktur in der Region“ geworden, sagte Ministerpräsident Markus Söder. Ebenso verwies er auf den Aufbau von Technologietransferzentren, die bayernweit einen Vorbildcharakter haben.

Ministerpräsident Dr. Markus Söder betonte bei der Verleihung auch: „Der Bayerische Verdienstorden ist eine sehr exklusive Auszeichnung. Nur maximal 2000 lebende Personen dürfen ihn tragen. Mit ihm ehren wir das vielfältige Engagement von großartigen Menschen, die Bayern einzigartig machen. Bekannte Sportler, Künstler und Wissenschaftler sind die Botschafter Bayerns weit über die Landesgrenzen hinaus. Ehrenamtliche machen unser Land im Stillen stark.“ Seit Gründung der Ehrung vor 62 Jahren, wurde der Bayerische Verdienstorden bisher insgesamt an 5661 Persönlichkeiten verliehen.

Als sein Nachfolger im Amt des VDI Landesvorsitzenden würdigte Prof. Dr.-Ing. Johannes Fottner die Verdienste von Prof. Dr. Reinhard Höpfl für den Aufbau der Hochschule Deggendorf, aber besonders seine Verdienste und sein Wirken und Handeln im VDI Landesverband Bayern. Es macht ihn stolz, dass Prof. Dr. Höpfl mit diesem Orden auch für sein ehrenamtliches Engagement beim VDI ausgezeichnet worden ist.

Günther Pfrogner

VDI-Gesellschaft Bauen und Gebäudetechnik

Ehrenurkunde des VDI

Professor Dipl.-Ing. Rasso Steinmann

erhält die Ehrenplakette des VDI mit Dank und in Anerkennung seiner langjährigen, umfassenden und unersetzlichen Mitarbeit im Fachbeirat sowie in Fach- und Richtlinienausschüssen der VDI-Gesellschaft Bauen und Gebäudetechnik. Rasso Steinmann hat insbesondere die Richtlinienreihe VDI 2552 „Building Information Modeling“ initiiert und entscheidend geprägt. Ohne seine Mithilfe wäre die Herausgabe dieser Richtlinie nicht möglich gewesen.

Dipl.-Ing. Andreas Wokittel
Vorsitzender der VDI-Gesellschaft Bauen und Gebäudetechnik

Prof. Dr.-Ing. Uwe Franzke
Vorsitzender des VDI-Fachbereichs TGA

VDIni Club München

Besuch beim Wasserkraftwerk „Isarwerk 2“

Am 29. Juli besuchte der VDIni-Club des VDI Süd das Isarwerk 2 in München Süd. Das Isarwerk 2 ist eines von mehreren Wasserkraftwerken, die von den SWM in ganz Deutschland betrieben werden. Mit einer elektrischen Leistung von 2,4 MW erzeugt das Laufwasserkraftwerk Strom für rund 6.000 Haushalte. Wie die Stromgewinnung mithilfe von Wasser im Isarwerk 2 funktioniert, konnten die Kleinsten unter den Ingenieursanwärtern in Begleitung ihrer Familien bei dieser Exkursion selbst miterleben.


Fotos: VDI

Mitglieder des VDIni-Clubs München besuchen das Wasserkraftwerk und die Ausstellung

Die Stadtwerke München

In einem aufschlussreichen Vortrag stellte Ina Oddoy, die im Veranstaltungsmanagement der SWM tätig ist und Betriebsbesichtigungen organisiert, zunächst die Tätigkeitsbereiche und Aufgaben der Stadtwerke München vor. Neben Stromerzeugung – wie im Isarwerk 2 durch Wasserkraft – sind die SWM auch für die Schwimm- und Freibäder sowie für die Mobilität verantwortlich. Auch die Förderung von Erdgas und die Wassergewinnung gehören zu den Tätigkeiten der Stadtwerke München.

Von Strom und Wasserkraft

Vor dem eigentlichen Rundgang durch das Laufwasserwerk ging Ina Oddoy näher auf die Stromerzeugung und die dabei stattfindenden physikalischen Vorgänge ein. Mithilfe eines Dynamos zeigte Sie den Teilnehmern anschaulich, wie ein Wasserkraftwerk funktioniert und aufgebaut ist.

Anschließend besichtigten die Teilnehmer gemeinsam das Kraftwerk, das mit vier Kaplan-Turbinen ausgestattet ist und in dem Wasser mit einer Fallhöhe von vier Metern hinunterfällt, um Energie zu gewinnen. Zum Abschluss der lehrreichen Exkursion wurde noch ein Film vorgeführt, um das im Rahmen der Exkursion erworbene Wissen zu vertiefen und zu festigen.

Über den VDIni-Club

Der VDIni-Club organisiert für Kinder ab vier Jahren verschiedene Aktivitäten rund um Technik und Naturwissenschaften. Spielerisch lernen so bereits die Jüngsten, technische Zusammenhänge und Gegenstände zu begreifen. Ob bei Exkursionen oder über das Internetangebot, der VDIni-Club vermittelt Wissen auf unterhaltsame und lehrreiche Weise.

Haben wir Ihr Interesse geweckt? Dann besuchen Sie den VDIni Club im Netz unter www.vdini-club.de.

Sarah Stingl

VDI-AK Normen und Richtlinien und Produktion und Logistik Nordost

VDI Richtlinien – wie geht das?

Wie entsteht eine VDI Richtlinie – Wer macht VDI Richtlinien – Wo finde ich VDI Richtlinien?

Die Arbeitskreise Normen und Richtlinien, sowie Produktion und Logistik hatten am 3.7.2019 gemeinsam zum Vortrag eingeladen, der von Dipl.-Ing. Jean Haeffs, Geschäftsführer bei der VDI Gesellschaft Produktion und Logistik gehalten wurde.

Eingangs ging Herr Haeffs auf die Standards im Alltag ein, die in der Regel als selbstverständlich angesehen werden, jedoch nationaler und vor allem internationaler Vereinbarungen bedürfen. So zeigte er als Beispiel auf einer Weltkarte, welcher Stecker und welche Steckdose wo verwendet wird.
Weitere Beispiele waren die verschiedenen USB Stecker, die seit 1996 standardisiert wurden. Mit einer Aufzählung von weiteren Alltagsstandards, wie z. B. dem bargeldlosen Bezahlen, Verkehrsschildern, Papierformaten, Treppen, Paletten, usw. leitete er über auf die Organisation im VDI, die die Basis für die Richtlinienarbeit ist.

Der Verein gliedert sich in 13 Fachgesellschaften, darunter die Gesellschaft für Produktion und Logistik, die sich wiederum in drei Fachbereiche untergliedert. Hier sind es die Fachbereiche Produktionstechnik und Fertigungsverfahren, Fabrikplanung und Betrieb, sowie Technische Logistik. Andere Fachgesellschaften sind in bis zu acht Fachbereiche untergliedert. Soweit dürfte die Organisation jedem VDI Mitglied bekannt sein, da er sich beim Eintreten in den Verein einer Fachgesellschaft oder einem oder mehreren Fachbereichen zugeordnet hat.
Der Anstoß für eine VDI-Richtlinie kann durch ein Problem oder auf Grund eines Themenvorschlags (von jedermann) gegeben werden. Ob die Richtlinienarbeit aufgenommen wird, entscheidet der Fachbeirat nach einer Bedarfs- und Ressourcenprüfung. In einer konstituierenden und weiteren vier bis sechs Richtlinien-Sitzungen wird ein Entwurf = Gründruck erstellt. In den folgenden drei bis neun Monaten besteht eine Einspruchsfrist, parallel wird die Übersetzung erstellt und die Richtlinie gegebenenfalls überarbeitet. Nach sieben bis neun Monaten steht dann die neue Richtlinie in deutscher und englischer Sprache im Weißdruck zur Verfügung. Die Arbeit der ehrenamtlichen Mitglieder wird dabei von der Hauptgeschäftsstelle unterstützt. Spätestens nach fünf Jahren wird die Aktualität der Richtlinie überprüft und weiter entweder unverändert gültig sein oder überarbeitet, eventuell zurückgezogen werden.
In seinem sehr ausführlichen Vortrag behandelte Herr Haeffs viele weitere Themen, wie z. B. die Verknüpfung hin zu den DIN Normen, die generellen Inhalte und Gremiumsmitglieder etc.
Bekannt ist, dass die Richtlinien über den Beuth Verlag Berlin bezogen werden können. Weniger bekannt ist, dass die Richtlinien in den Geschäftsstellen der Bezirksvereine vorhanden sind und dort eingesehen werden können.
Zum Abschluss verwies Herr Haeffs auf eine der ältesten Richtlinien, die VDI 2230 Systematische Berechnung hochbeanspruchter Schraubenverbindungen, die seit mehr als 40 Jahren angewendet wird, permanent erweitert und angepasst wurde und weltweites Standardwerk ist.
Eine Richtlinie, die häufig zu wenig Beachtung findet, ist die VDI 2700, Blatt 1 bis 31 Ladungssicherung. Die Fehler werden sowohl im professionellen Transportgewerbe, wie auch im privaten Bereich gemacht.

Hans-Peter Schobig

Sicherheitsrisiken bei der maschinellen Übersetzung

Die fortschreitende Digitalisierung und künstliche Intelligenz bieten heute ungeahnte Möglichkeiten. Was läge näher, als damit Geld zu sparen, etwa durch die maschinelle Übersetzung?


Foto: *REDPIXEL – stock.adobe.com.

Texte auf Knopfdruck in eine andere Sprache zu übertragen und dies zu geringen Kosten – das klingt sehr verlockend. Doch aufgepasst: Sie könnten sich erheblichen Risiken im Hinblick auf Datenschutz und Informationssicherheit aussetzen, was Sie teuer zu stehen käme.
Die maschinelle Übersetzung basiert auf großen digitalen Datenbeständen, in die Ihre Texte in der Regel einfließen. Was passiert dabei mit Ihren Daten oder gar vertraulichen Informationen? In welche Hände und Datenbanken gelangen sie? In welchen Ländern werden sie gespeichert und wie ist es dort um den Datenschutz bestellt? Dürfen Sie die verwendeten Dienste für Ihre Zwecke überhaupt gewerblich nutzen? Und sind sie vor Manipulation geschützt, damit entscheidende Aussagen nicht verfälscht werden können?

5 TIPPS ZUR VERGABE VON ÜBERSETZUNGEN

- **EXPERTENWISSEN**
  Achten Sie darauf, dass Ihr Übersetzer auf das jeweilige Fachgebiet spezialisiert ist.
- **ANGEBOTSANFORDERUNG**
  Geben Sie Ihrem Übersetzer vorab Einblick in den Text, damit ein verlässliches Angebot möglich wird.
- **BEI MEHREREN ANGEBOTEN**
  Noch wichtiger als der Preis ist das Fachwissen des Übersetzers, damit Sie Texte hoher Qualität erhalten.
- **FRÜHZEITIGE BEAUFTRAGUNG**
  Eilaufträge sind in der Regel deutlich teurer.
- **KOSTENEFFIZIENZ**
  Geben Sie möglichst nur Endfassungen von Texten in Auftrag, damit die Übersetzung günstig und effizient für Sie erfolgen kann.

Dolmetscher- und Übersetzerdatenbank Bayern: by-suche.bdue.de

Bundesverband der Dolmetscher und Übersetzer e. V. (BDÜ) Landesverband Bayern: by.bdue.de

Sprachprofis sorgen für mehr Sicherheit

Angesichts der erhöhten Sicherheits- und Datenschutzanforderungen von heute können frei verfügbare Tools für die automatisierte Übersetzung ein Risiko darstellen. Bei der Beauftragung qualifizierter Sprachdienstleister, die Mitglied in einem anerkannten Berufsverband sind, können Sie ruhiger schlafen, denn diese sind dazu verpflichtet, die Daten ihrer Kunden vertraulich zu behandeln und die geltenden Vorschriften (z. B. der DSGVO) zu beachten.
Neben dem Sicherheitsaspekt ist auch die Qualität ein kritischer Faktor. Maschinell produzierte Übersetzungen klingen auf den ersten Blick zwar manchmal erstaunlich gut, doch häufig verstecken sich darin unbemerkt gravierende Fehler, die fatale Folgen haben können – etwa durch fehlerhafte Gebrauchsanleitungen. Hier sind Sprachprofis gefragt, um gerade im technischen Bereich schwerwiegende und kostspielige Konsequenzen wie Personen-, Sach- oder auch Imageschäden zu vermeiden.
Solche Profis bieten nicht mehr nur komplette Sprachdienstleistungen an, sondern stehen Hand in Hand mit künstlicher Intelligenz auch für das Post-Editing, also die Nachbearbeitung von maschinellen Übersetzungen, oder als kompetente Berater für den Übersetzungsprozess zur Verfügung.

Qualifizierte Übersetzer und Dolmetscher finden

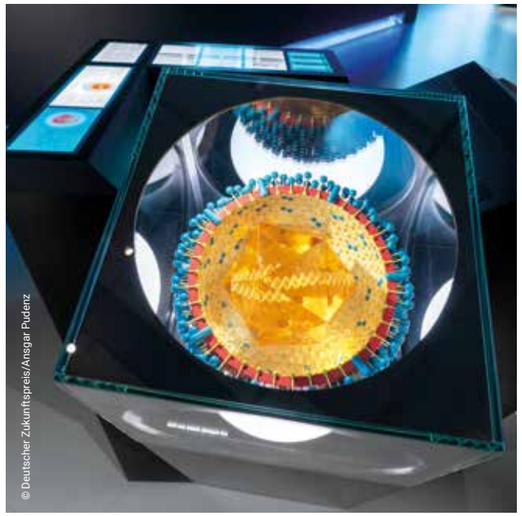
In jedem Fall erleichtert Ihnen der **Bundesverband der Dolmetscher und Übersetzer (BDÜ)** die Suche nach kompetenten Sprachprofis, denn in den größten deutschen Berufsverband der Branche wird nur aufgenommen, wer eine entsprechende fachliche Qualifikation nachweisen kann, etwa ein Übersetzer- bzw. Dolmetscherstudium oder eine staatliche Prüfung. Damit unterscheiden sie sich von unqualifizierten Anbietern auf dem Markt.
In der kostenlos nutzbaren Onlinedatenbank des BDÜ finden Sie allein in Bayern rund 1.500 professionelle Dolmetscher und Übersetzer für mehr als 40 Sprachen und zahlreiche Fachgebiete. Bundesweit sind es sogar mehr als 7.500 BDÜ-Mitglieder mit insgesamt 80 Sprachen, von denen viele auf Ihre Branche spezialisiert sind. Diese Profis unterstützen Sie durch vertrauenswürdige Dienstleistungen, mit denen Sie die Risiken im Bereich der Informationssicherheit verringern können.

Dipl.-Übers. Manuela Wilpert

Deutsches Museum München

Lebensretter für Schutzlose

Neues Modul in der Ausstellung zum Deutschen Zukunftspreis: Innovativer Wirkstoff gegen gefährliche Viren hilft Menschen mit geschwächtem Immunsystem


© Deutscher Zukunftspreis/Ansgar Pudenz

Das Schnittmodell des Virus im Maßstab 1.500.000:1. Das Virusmodell besteht aus 2.600 Teilen und wurde in 150 Stunden zusammengebaut. Im Inneren der Kugel schwebt ein kantiger Kern aus bernsteinfarbenem Glas in dessen Zentrum die DNA-Doppelhelix zu sehen ist

Die Angreifer sind winzig und zielen auf die Schwächsten: Humane Cytomegalie-Viren (HCMV) können bei Menschen mit geschwächtem Immunsystem schwerste Schäden verursachen und bis zum Tod führen. Helga Rübsamen-Schaeff und Holger Zimmermann haben einen neuen Wirkstoff dagegen gefunden. Für die „lebensrettende Innovation gegen gefährliche Viren" wurde das Team von der Wuppertaler AiCuris GmbH mit dem Deutschen Zukunftspreis 2018, dem Preis des Bundespräsidenten für Technik und Innovation, ausgezeichnet. Seit heute kann man in der zugehörigen Ausstellung im Deutschen Museum an einem neuen Modul sehen, wie der Lebensretter für Schutzlose funktioniert.

Das Virus ist ein echter Blickfang: Eine gelbe Hülle, gespickt mit blauen Noppen, im Inneren der Kugel schwebt ein kantiger Kern aus bernsteinfarbenem Glas in dessen Zentrum die DNA-Doppelhelix zu sehen ist. Das Schnittmodell im Maßstab 1.500.000:1 sticht im beleuchteten Glaskubus aus einer Flanke des neuen Moduls heraus. „Wir haben bei diesem Einfallstor das Virus ins Zentrum gestellt und bewusst auf zusätzliche Erklärungen verzichtet", sagt Sabine Gerber, die Kuratorin des Deutschen Zukunftspreises am Deutschen Museum.

Die Erläuterung zu dem Virusmodell gibt es dann auf der nächsten Modulseite. „Hier wird auch der Mechanismus beschrieben, wie so ein Virus in die menschliche Zelle eindringt, sich dort vermehrt und die Zelle letztlich schädigt oder gar tötet", sagt Gerber. Dort erfährt man dann auch, dass etwa jeder Zweite dieses Virus in sich trägt. „Für gesunde Menschen ist das kein Problem, da hält die eigene Körperabwehr den Erreger in Schach", erklärt die Kuratorin. „Aber wenn die Immunabwehr zum Beispiel für eine Transplantation ausgeschaltet werden muss, wird das HCM-Virus zu einer tödlichen Bedrohung."

Wie es dem Team von Helga Rübsamen-Schaeff und Holger Zimmermann gelungen ist, den neuen Wirkstoff zu finden und wie sie ihn bis zum marktreifen Medikament weiterentwickelt haben, wird auf einer weiteren Seite des neuen Moduls beschrieben. „Hier sieht man die einzelnen Schritte von den ersten Tests an Zellkulturen über die klinischen Versuche bis hin zur Zulassung", so Gerber.

Zum Abschluss des Rundgangs um das neue Modul kommen dann auch die Preisträger zu Wort. Auf Knopfdruck kann man die Köpfe hinter dem Projekt kennenlernen und in weiteren Filmsequenzen die Hintergründe erfahren. „Ohne den großen persönlichen Einsatz von Helga Rübsamen-Schaeff und Holger Zimmermann wäre dieses lebensrettende Mittel wahrscheinlich nie auf den Markt gekommen", sagt Sabine Gerber.

„Wir freuen uns sehr, dass dieses Engagement mit dem Deutschen Zukunftspreis 2018 belohnt wurde", sagt Wolfgang M. Heckl, der Generaldirektor des Deutschen Museums. „Mit dem neuen Modul zu diesem Lebensretter für Schutzlose zeigen wir hier einmal mehr, wie wichtig Forschung und Entwicklung für die Menschen sind."

Informationen

„Aus Ideen Erfolge machen. Für die Menschen. Für das Land." – Diesem Gedanken folgen die Arbeiten der Preisträger, die in der Dauerausstellung zum Deutschen Zukunftspreis seit Ende 2006 im Deutschen Museum in München zu sehen sind. Die Präsentation der jeweils zehn neuesten preisgekrönten Projekte zeigt die wissenschaftliche Exzellenz und nachhaltige Wirkung der jeweiligen Innovation. Die Ausstellung stellt die beteiligten Forscher und Entwickler als Persönlichkeiten und Vorbilder dar, deren Leistungen in der „Hall of Fame" gewürdigt werden.

VDI-AK FiB Nürnberg

Benimmt sich Ihr Chef wie die Axt im Wald?

Mit dieser Frage hat die Referentin des Miniworkshops zum 3-G-Kommunikationsmodell, Dipl.-Ing. Beate Kaspar, am 17.07.2019 die anwesenden Teilnehmer/innen begrüßt. „Dann liegt das vielleicht daran, dass er viele Rot-Anteile in seinem Kommunikationsverhalten aufweist."

An vielen anschaulichen Beispielen stellte Beate Kaspar die drei Grundtypen des Kommunikationsverhaltens des 3-G-Modells vor.

Die Farbe Blau repräsentiert den sachorientierten Typus, dem Details wichtig sind und der nach perfekten Lösungen strebt.

Schnelle Lösungen bevorzugt der handlungsorientierten Menschentyp mit stark ausgeprägter Rot-Komponente. Handeln statt reden, ist seine Devise.

Dazwischen gibt es noch den Grün-Typ, bei dem eine starke Beziehungskomponente vorherrscht. Das sind Menschen, die mehr auf gutes Betriebsklima und Beziehungen unter den Kollegen achten, statt schnelle Ergebnisse oder Perfektion der Ausarbeitung anzustreben.

Nach der ausgiebigen Vorstellung der verschiedenen Typen konnten die Teilnehmer selbst einen Kurztest durchführen und sich in des 3-G-Kommunikationsmodell einordnen. Die einzelnen Farbtypen sind nur modellhaft zu verstehen – bei jedem Menschen sind die prozentualen Anteile der Farben verschieden ausgeprägt. Neben der Möglichkeit, dass eine Komponente sehr stark ausgeprägt ist, finden sich meist Mischtypen, die z. B. sowohl Blau als auch Rot zugeordnet werden können. Schon in der Gruppe der Anwesenden hat sich ein buntes Bild ergeben.

Was kann ich nun damit anfangen, wenn ich um meinen Kommunikationstyp weiß und auch die Kommunikationsweise meines Chefs analysieren kann?

Beate Kaspar gab klare Beispiele, wie die neuen Erkenntnisse in der Praxis angewendet werden können.

Wenn ich selbst, z. B. mehr blau ausgeprägt, gerne in Sitzungen auf die Details meiner Berechnungen eingehen möchte, aber weiß, dass mein Chef eher der roten Kategorie zugeordnet werden muss, dann kann ich meinen Vortrag entsprechend auf den Punkt bringen und strapaziere die Geduld meines Gegenübers nicht.

Auf der anderen Seite kann sich ein schwieriger Kunde als eher „blau" ausgeprägter Typus herausstellen. So kann ich besser verstehen, dass seine genauen Nachfragen nur sein Weg sind, zu einem für ihn zufriedenstellenden Ziel zu kommen. Daraufhin kann ich meine Präsentation entsprechend ausrichten und seine Fragen antizipieren, damit auch ich mein Ziel erreiche.

Auch für die Team-Bildung sind Überlegungen zum Kommunikationstyp hilfreich. Ein Team, das nur aus roten und blauen Kommunikationstypen besteht, wird niemals gut zusammenarbeiten können.

Hier kann ein Anteil an Grünen hilfreich sein, um das Gesamtklima im Team zu heben.

Der Mini-Workshop gab einen erkenntnisreichen Einblick in die vielfältige Welt der menschlichen Kommunikation und hat unser Interesse auf mehr geweckt.

Marion Gieseler und Johanna Uhl


Mini-Workshop zum 3G-Kommunikationsmodell

Foto: VDI

VDI-AK FiB Nürnberg

Agiles Arbeiten

Dr.-Ing. Claudia Kostka

Anhand eigener Aufgabenstellungen üben wir agile Techniken und lernen die Begriffswelt kennen – empirisch, inkrementell und iterativ.

Inhalt: Agile Werte und Prinzipien; Agile Führung und ihre Events – Meetingkultur im selbstorganisierten Team.

Das Ganze und seine Teile – Vorhabenklärung am eigenen Beispiel; 3 Rollen, 4 Meetings (Events) und 3 Artefakte; Scrum Events: Sprint Planning, Daily Stand up, Sprint Review und Retrospektive; Agile Methoden: User Story, Kanban Board

17.11.2019, 10:00 – 17:00 Uhr
Training
Nachbarschaftshaus Gostenhof
Adam-Klein-Straße 6
90429 Nürnberg
Gebühr: 20,00 Euro
Online Anmeldung

Ausbildung

Technikcampus Stubai – lernen, wo andere Urlaub machen

Das Stubaital verbinden die meisten mit Urlaub, Wandern und Skifahren. Dass im Hauptort Fulpmes eine hochwertige Technikausbildung für 14- bis 19-Jährige an der Höheren Technischen Lehranstalt (HTL) Fulpmes angeboten wird, ist weniger bekannt.
Die Ausbildungsstätte in Fulpmes blickt auf eine über 120-jährige Geschichte zurück. AbsolventInnen der HTL Fulpmes findet man heute weltweit in Technik und Management. Der Maschinenbau-Schwerpunkt der HTL Fulpmes ist aus der Stubaier Tradition von Metallverarbeitung und Werkzeugbau gewachsen.
Die Schule bietet heute die Vertiefungsrichtungen Smart Engineering, Produktdesign, Fertigungstechnik und Kunststofftechnik in vier- und fünfjährigen Ausbildungsschienen an.

Foto: HTL Fulpmes

Der Technikcampus Stubai war die beste Wahl. Wir haben die richtige Entscheidung getroffen

Maschinenbau in Theorie und Praxis

Grundlagen des Maschinenbaus bilden den Schwerpunkt der ersten Ausbildungsjahre. Ein hoher Praxisanteil in den Werkstätten und Laboratorien ist dabei kennzeichnend: was in der Theorie erarbeitet wurde, wird in praktischen Tätigkeiten umgesetzt. „Die Ausbildung an der HTL Fulpmes ist darauf ausgerichtet, den AbsolventInnen einen direkten Berufseinstieg in Gewerbe und Industrie zu ermöglichen," erklärt Direktor Dr. Martin Schmidt-Baldassari, nicht ohne Stolz. Für die Ausbildung stehen Anlagen auf industriellem Niveau zur Verfügung, großteils finanziert durch den „Förderkreis der HTL Fulpmes", einer Verbindung namhafter Gewerbe- und Industriebetriebe.

Abschluss mit Studienberechtigung

Die Ausbildung wird mit einer in Teamarbeit erstellten Diplomarbeit abgeschlossen. Die SchülerInnen der HTL Fulpmes stellen dabei ihre fachlichen Kenntnisse und ihre soziale Kompetenz an einem praxisrelevanten Thema unter Beweis, fast immer in Zusammenarbeit mit einem Industriebetrieb. Der Abschluss der HTL Fulpmes ist auf Level 5 des europäischen Qualifikationsrahmens eingestuft. Nach drei Jahren Berufspraxis erfolgt eine Einstufung auf Level 6, gleichwertig zu einem Bachelorabschluss. Zusätzlich wird die österreichische Qualifikation „Ingenieur" verliehen.
Die Matura / das Abitur an der HTL Fulpmes berechtigt zum Studium an Fachhochschulen und Universitäten. Der ausgewogene Lehrplan, der Technik, Wirtschaft und Allgemeinbildung verbindet, ermöglicht den AbsolventInnen auch einen leichten Einstieg in komplementäre Studienfächer.

„daHeim" am Technikcampus Stubai

Zum Technikcampus wird die HTL zusammen mit dem Schülerheim Don Bosco, das rund zwei Drittel der SchülerInnen beherbergt. Fast alle PädagogInnen im Schülerheim sind selbst AbsolventInnen einer HTL oder der HTL Fulpmes. Sie sind AnsprechpartnerInnen in allen Lebenslagen und bieten eine intensive fachliche Lernbegleitung, die fast schon eine schulische Erfolgsgarantie bedeutet. Im renovierten Bau stehen unter der Leitung von P. Peter Rinderer Ein- und Zweibettzimmer, hervorragende Küche und zahlreiche Freizeitmöglichkeiten, mit Kraftraum, Musikproberaum, Billard usw. zur Verfügung.
Am Technikcampus Stubai ist ein besonderes Klima spürbar: familiär, offen, wertschätzend. In der kleinen Ausbildungsstätte mit lediglich 270 SchülerInnen wird jede Einzelne / jeder Einzelne individuell wahrgenommen und gefördert.

Dr. Martin Schmidt-Baldassari
Direktor HTL Fulpmes

Informationen

Technikcampus Stubai: 270 SchülerInnen, 36 Lehrpersonen, 282 Computer und jede Menge Zukunft
4- oder 5-jährige Ausbildung in Maschinenbau mit den Vertiefungsrichtungen Smart Engineering, Produktdesign, Fertigungstechnik und Kunststofftechnik.

HTL Fulpmes, www.htl-fulpmes.at,
htl-fulpmes@tsn.at
Schülerheim Don Bosco,
www.schuelerheim-donbosco.at,
schuelerheim.fulpmes@donbosco.at

Tage der offenen Tür: 8. und 9.11.2019
Schnuppertage und Schulführungen: jeweils Mittwochs ab 9:00 nach tel. Voranmeldung

Foto: AdobeStock_201012265-Von sdecoret

VDI BV München, Ober- und Niederbayern

VDI startet neuen Hochschulwettbewerb

Mit der VDI Autonomous Driving Challenge, dem neuen Wettbewerb für autonom fahrende Modellautos im Maßstab 1:8, können Studenten-Teams am 13. März 2020 an der Hochschule München erstmals zeigen, weches Potenzial sie mit autonomen Modellautos erreichen können.

Gefragt sind Programmierung und Konzepte für autonome Modellautos, die im Wettbewerb in verschiedenen Kategorien gegeneinander antreten. So müssen die Teams bei Klassikern wie Fahren auf Zeit und eigenständiges Ein- und Ausparken im laufenden Verkehr ihr Können beweisen. Ein Fokus liegt auf der Vernetzung der Fahrzeuge untereinander und deren Infrastruktur.

Studenten-Teams, die Spaß an der Entwicklung und Umsetzung von technischen Konzepten und Algorithmen für autonom fahrende Autos haben, können sich bereits jetzt über den VDI unter www.vdi-adc.de anmelden.

VDI Bayern Nordost und VDE Nordbayern

Der Zoll als Hüter geistigen Eigentums im grenzüberschreitenden Warenverkehr

Foto: AdobeStock_124295616-Von sittinan

Der grenzüberschreitende Warenverkehr nimmt beständig zu

Im Juli 2019 fand an der TH Nürnberg ein von VDI Bayern Nordost, VDE Nordbayern und VPP organisierter Vortrag der Generalzolldirektion Direktion VI zum Thema „Der Zoll als Hüter geistigen Eigentums im grenzüberschreitenden Warenverkehr" statt.
Inhalt dieses Vortrages von Roland Bittner waren verschiedenste Themen, wie zum Beispiel der Auftrag des Zolls oder auch die Struktur der Zollverwaltung.
Darüber hinaus wurden bestehende Verbote und Beschränkungen im grenzüberschreitenden Warenverkehr angesprochen. Es wurde das Ausmaß von Produktpiraterie auf Basis von Zahlen und Fakten verdeutlicht. Statistiken zeigten die Anzahl der Aufgriffe der letzten Jahre und die wichtigsten Herkunftsländer. Dies führte dann auch zur Darstellung einer Rolle des Zolls als strategischem Partner zum Schutz gewerblicher Schutzrechte. So konnte ein umfassender Einblick in die Arbeit des Zolls erlangt werden.

Matthias Barbian

VDI BG Erlangen + SuJ Erlangen

Frag doch mal den Ingenieur!*

Foto: Fotolia_74460599_M/Urheber Photographee.eu

Die BG Erlangen und die suj Erlangen möchten Studenten, berufstätige Ingenieure und Ingenieure im Ruhestand miteinander vernetzen.
Ziel ist eine Vernetzung von Studenten und Ingenieuren verschiedenen Alters. Die Ideen sollen dabei möglichst von den VDI- Mitgliedern selbst kommen. Eine aktive Beteiligung an der Vorbereitung von Veranstaltungen ist sehr willkommen.

- Ingenieure vermitteln einen Einblick in die heutige Arbeitssituation, oder
- Ingenieure im Ruhestand erzählen von den Herausforderungen in Studium und Beruf früherer Zeiten, oder
- Studenten berichten von Lehre und Forschung an der Universität.

Den Anfang machte die Führung durch den Siemens Campus am 23. Oktober 2019, die Studenten und Ingenieuren einen Einblick in die Büros der Zukunft gab. Weitere Veranstaltungen sollen folgen.
Um dafür Ideen und Mitstreiter zu gewinnen, ist eine Umfrage bei den Mitgliedern geplant.

Ihre Meinung ist gefragt! Beteiligen Sie sich an der Befragung auf der Homepage der BG Erlangen oder der suj Erlangen:

BG Erlangen: www.vdi-bno.de/bezirksverein-bayern-nordost/bezirksgruppen/erlangen/index.html

Suj Erlangen: www.vdi-bno.de/bezirksverein-bayern-nordost/studenten-u-jungingenieure/suj-erlangen/index.html

Zu einem gemeinsammen Treffen zur Ideenfindung und zur Auswertung der Befragung laden wir alle Interessierte ein:

Wann: im Januar 2020 in Erlangen
Details dazu siehe Veranstaltungskalender und TiB Ausgabe Jan/Feb 2020
Machen Sie mit!
Der VDI ist eine Gemeinschaft über Generationen hinweg.

BG Erlangen und suj Erlangen

* Der Artikel wendet sich an Ingenieurinnen und Ingenieure

Hochschule München

Wann wird Stahl müde?

Forschungsprojekt ermittelt, wie besondere Belastungen Material langsam zermürben

Ermüdungsversagen nennt man es, wenn zum Beispiel eine Büroklammer nach zehnmaligem Biegen an der kritischen Stelle bricht. Was bei einer Büroklammer harmlos ist, ist eine der häufigsten und gefährlichsten Schadensursachen bei Maschinen, Fahrzeugen und Bauwerken durch Belastungen während des Betriebs.
Bauteilermüdung ist somit wirtschaftlich und hinsichtlich möglicher Produktrisiken ausgesprochen relevant. Oft tritt Ermüdungsversagen scheinbar plötzlich ein, wie beispielsweise beim schweren ICE-Unfall von Eschede: Ein Teil eines Rades brach, brachte den Zug teilweise zum Entgleisen und führte zu einem für viele Menschen tödlichen Crash. Entstehende Ermüdungsrisse sind zunächst mit bloßem Auge nicht erkennbar, wachsen dann aber mit jedem Lastzyklus, bis ein sogenannter „Restgewaltbruch“ das versagende Bauteil abrupt teilt.

Um einzuschätzen, wie oft ein Material beziehungsweise Bauteil welche Belastung ertragen kann, arbeiten Konstrukteure mit sogenannten „Belastungskollektiven“. Anhand dieser Lastannahmen zum Verlauf der zu erwartenden Belastung der Struktur lässt sich die Lebensdauer zumindest abschätzen, wobei ingenieurmäßige Ansätze oder auch werkstoffmechanische Modelle zum Einsatz kommen. Bei geschweißten Verbindungen liegen hierzu hauptsächlich Ansätze vor, die mindestens 10.000 Lastzyklen (also auftretende Belastungswechsel) voraussetzen, was für viele Fälle auch zutrifft.
Zu selten auftretenden Sonderlasten, zudenen es z. B. bei zu stark beladenen Fahrzeugen kommt oder bei Extremereignissen wie Erdbeben, gibt es dagegen kaum Basisdaten zum Verformungs- und Versagensverhalten sowie der Abschätzung der Lebensdauer von Schweißverbindungen. Diese fallen in die sogenannte „nieder-zyklische Ermüdung“ (low cycle fatigue).

Solide Daten ermöglichen bessere Vorberechnungen für Konstruktionen

Im Forschungsprojekt LCF-Weld erforscht Prof. Dr. Klemens Rother von der Hochschule München am Institut für Material- und Bauforschung mit seinem Mitarbeiter Josef Neuhäusler anhand von zwei ausgewählten Werkstoffen dieses Gebiet. Gemeinsam mit Prof. Dr. Michael Vormwald von der Technischen Universität Darmstadt, Institut für Stahlbau und Werkstoffmechanik, ergründet er die Lebensdauer geschweißter Verbindungen und entwickelt anhand der im Projekt gewonnenen Versuchsergebnisse neue Verfahren zur rechnerischen Beurteilung niederzyklischer Ermüdung.
Im Prüfstand im Labor für Stahl- und Leichtmetallbau am Standort Kissing belasten die Wissenschaftler dazu geschweißte Bleche in verschiedenen Materialstärken mit unterschiedlichen Kräften. Dabei prüfen sie Schweißverbindungen aus dem austenitischen Stahlwerkstoff X6CrNiTi18-10 (1.4541) sowie dem hochfesten Baustahl S960M – zwei Werkstoffe mit sehr unterschiedlichem Verhalten und Eigenschaften.
Die Ergebnisse dieses Projekts sollen in Zukunft dazu beitragen, die Sicherheit geschweißter Strukturen zu verbessern. Gleichzeitig erlaubt eine verbesserte Kenntnis des Strukturversagens den Bau leichterer Strukturen, die trotzdem hinreichend lange haltbar sind.

Cathrin Cailliau

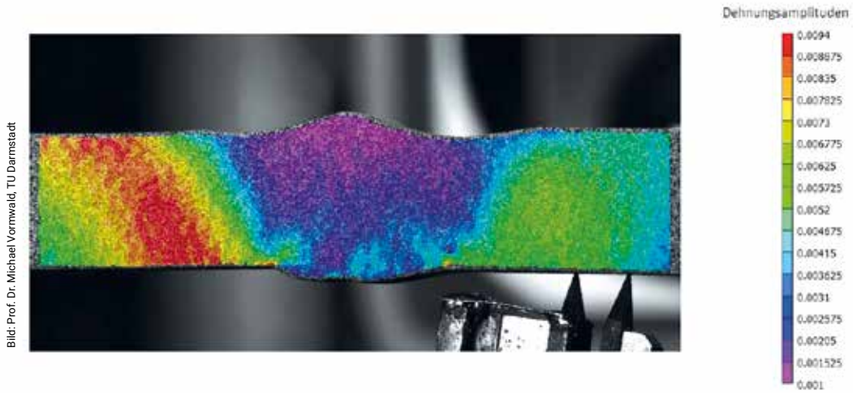


Bild: Prof. Dr. Michael Vormwald, TU Darmstadt

Dehnungen bei Belastung einer Schweißverbindung fallen je nach Position aufgrund der örtlich veränderlichen Werkstoffeigenschaften sehr unterschiedlich aus

VDI BV Bayern Nordost + VDE Nordbayern

ENGINEERING 2050 success story

„Technology & Art: Perfect.Ambivalence“ @ Nürnberg Digital Festival

Hinter dem ENGINEERING 2050-Team, der Bewegung aus VDI Bayern Nordost, VDE Nordbayern und Zentrifuge e. V., liegen neun wundervolle und interessante Tage auf dem Nürnberg Digital Festival – jeden Tag mindestens eine Veranstaltung im Admiral Filmpalast.

Die höchsten Teilnehmerzahlen mit jeweils weit über 100 Teilnehmern erzielten die Veranstaltungen „Digitalisierung und Nachhaltigkeit“ mit Dr. Dina Barbian (Institut für Nachhaltigkeit, https://nachhaltigkeit2050.de/) sowie „Mindset 2050“ mit dem Zukunftsforscher Ronald Zehmeister!

Matthias Barbian

Foto: VDI

VDI-AK Produkt- und Prozessgestaltung Nordost

Feedback 4.0: Wertschätzendes Feedback – Wirkungsvolles Führen

Seminarleitung: Hans-Joachim Scheler, Morphologisches Institut Scheler, Weitramsdorf, Dipl.-Ing. (FH) Günter Schmid

Regelmäßiges, wertschätzendes Feedback kann die Motivation und Leistung von Mitarbeitern um bis zu 10 % steigern, wie Untersuchungen belegen. Jedoch fühlen sich ca. 37 % der Vorgesetzten unsicher, Mitarbeitern Rückmeldungen zu deren Arbeitsleistungen zu geben oder Kritik auszusprechen.

Dies verwundert nicht, denn ungeschickt vorgetragenes Feedback kann beim Feedback-Nehmer demotivierend wirken. Wenn beim Feedback-Geben die Prinzipien wertschätzender Kommunikation beachtet werden, kann es so zum gegenseitigen Verständnis beitragen, die Zusammenarbeit verbessern und sogar Konflikten vorbeugen.

Dabei steht mit dem einfach handhabbaren Feedback-Prozess eine nützliche Richtlinie zur Verfügung. Der Nutzen ist, mehr Sicherheit beim Feedback-Geben zu gewinnen, Führungsaufgaben leichter zu bewältigen, Zeit zu sparen und Reibungsverluste zu vermeiden. Des Weiteren ist „Feedback-Geben“ ein wichtiges Führungs- und Motivationsinstrument, wenn es in einer wertschätzenden Art und Weise durchgeführt wird, und das fallbezogen, spontan zwischen Vorgesetztem und Mitarbeiter oder zwischen Kollegen eingesetzt werden kann.

In dem Seminar erfahren Sie mehr über

- Morphologische Grundsätze wertschätzender Kommunikation
- Feedback-Geben und -Empfangen als kommunikativer Regelkreis
- Relevante Ergebnisse der Gehirnforschung
- Wie gebe und wie empfange ich Feedback richtig und wertschätzend
- Der Feedback-Prozess
- Die „Hamburger“-Methode

Übungen auf Basis berufsspezifischer Situationen aus der Praxis runden das Seminar ab.

16.11.2019, 10:00 – 16:30 Uhr
Seminar mit Übungen
Technische Hochschule Nürnberg
Kesslerplatz 12, Seminarraum KA.404a

Organisation und Anmeldungen
Geschäftsstelle VDI-Bezirksverein Bayern Nordost e.V.
VDI-AK Produkt- u. Prozessgestaltung
Telefon 0911 / 55 40 30
Email: vdi@th-nuernberg.de
Teilnahmegebühr: EUR 80,00 (für Leitung, Catering, Material und Seminarunterlagen)
Bankverbindung:
IBAN DE53760700240644000200, VDI-Bezirksverein Bayern Nordost e. V.
Verwendungszweck bitte angeben: Seminar Feedback 4.0
Die Teilnehmerzahl ist auf 12 begrenzt Berücksichtigung in der Reihenfolge des Anmeldeeinganges.
Anmeldeschluss: 08. November 2019

Nicht verpassen!

Treffs, Vorträge und Exkursionen des VDI München/VDE Südbayern

04. November 2019 / Montag

16:30 Vortrag
Copernicus and the Arabs: Thoughts on Originality in the Practice of Mathematical Astronomy

Veranstalter: Deutsches Museum München
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Richard L. Kremer, Dartmouth College, Hanover, NH, USA

18:00 Vortrag
Autonome e-Kleinbusse (Shuttles) – Entwicklungsstand und Zulassung

Veranstalter: VDI-AK Aktuelles Forum Technik
Ort: München
Adresse: Brienner Str. 39, 80333 München, Hansahaus, Rahnstüberl
Referent: Prof. Dipl.-Ing. Manfred Plechaty
Anmeldung: Online Anmeldung

19:00 Treff
VDE YoungProfessionals Stammtisch mit Hochschulgruppe

Veranstalter: VDE YoungProfessionals
Ort: München
Adresse: Milchstraße 1, 81667 München, Lollo Rosso Bar(varian) Grill
Info: Terminänderungen unter www.vde-suedbayern.de
Anmeldung: per Mail: stammtisch@vde-muenchen.de

05. November 2019 / Dienstag

17:30 Vortrag
Erfahrungen mit dem additiven Fertigen von INVAR-, INCO- und Ti6Al4V-Halbzeugen bei Airbus

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dipl.-Ing. Jürgen Silvanus, AIRBUS Defence and Space GmbH, München
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

18:15 Vortrag
Medizinelektronik von Maxim Integrated

Veranstalter: VDE-AK ML
Ort: München
Adresse: Haidenauplatz 1, 81667 München, MDK Bayern, Nymphenburg, 6. OG
Referent: Tobias Hübner, Executive Director, Central Europe Sales Maxim Integrated Products, Inc.

05. November 2019 / Dienstag

19:00 Vortrag
JETZT ist sie da: Die neue DIN 1946-6: Lüftung von Wohnungen

Veranstalter: VDI TGA/ IDV
Ort: München
Adresse: Lothstraße 34, 80335 München, Hochschule München, G-1.27
Referent: Stephan Schreck, Vallox GmbH, Dießen
Info: kostenlose Parkplätze in der Tiefgarage

06. November 2019 / Mittwoch

18:00 Treff
Stammtisch der BG Rosenheim

Veranstalter: VDI, VDE, SuJ
Ort: Rosenheim
Adresse: Samerstr. 17, 83022 Rosenheim, Flötzinger Bräustüberl
Info: Auch interessierte neue Gesichter sind uns jederzeit herzlich willkommen

07. November 2019 / Donnerstag

19:00 Vortrag
Astrovortrag: Ein nicht nur astronomischer Blick auf den Stern von Bethlehem

Veranstalter: VDI, VDE, SuJ, TH-Rosenheim
Ort: Rosenheim
Adresse: Hochschulstr. 1, 83024 Rosenheim, TH Rosenheim, B023
Referent: Dr. Christian Theis

11. November 2019 / Montag

13:30 Exkursion
Klinikum Großhadern

Veranstalter: VDI-AK Bio-, Medizin- und Umwelttechnik
Ort: München
Adresse: Marchioninistr. 15, 81377 München, Klinikum Großhadern
Referent: N.N. Klinikum (Techn.Betrieb)
Anmeldung: Liepsch@hm.edu

17:00 Vortrag
Thermische Energiespeicher

Veranstalter: VDI-AK Energietechnik in Zusammenarbeit mit dem Lehrstuhl für Energiesysteme der TU München
Ort: Garching
Adresse: Lichtenbergstraße 2a, 85748 Garching, Institute for Advanced Study, IAS Auditorium
Referent: Dr.-Ing. Dan Bauer, Deutsches Zentrum für Luft- und Raumfahrt
Info: Sektorenkopplung Strom/Wärme – Forschung, Entwicklung und Systemintegration anhand ausgewählter Beispiele

11. November 2019 / Montag

19:00 Treff

Stammtisch der SuJ München

Veranstalter: VDI-AK SuJ München
Ort: München
Adresse: 80687 München
Info: Der genaue Veranstaltungsort wird über unseren E-Mail- und Whatsapp-Newsletter, sowie via Facebook, bekannt gegeben.

---

12. November 2019 / Dienstag

17:30 Vortrag

Crashversuche an mobilen Fahrzeugsperren (sog. Anti-Terrorbarrieren)

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dipl.-Ing. Peter Rücker, DEKRA Automobil GmbH, München
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

18:00 Forum

VDI Forum 2019 „Automatisiertes und autonomes Fahren – Mobilität der Zukunft“

Veranstalter: VDI Landesverband Bayern / VDI-BV Nordost e.V.
Ort: Nürnberg
Adresse: Bankgasse 9, 90402 Nürnberg, Bayerisches Staatsministerium der Finanzen und für Heimat, Atrium
Anmeldung: Online Anmeldung

19:00 Treff

VDI/VDE Treff

Veranstalter: VDI BG Landshut
Ort: Landshut
Adresse: 84028 Landshut, Gasthaus „Zur Insel”
Info: Dr. Helmut Strasser, Tel. 0871/74197

---

14. November 2019 / Donnerstag

18:00 Vortrag

Private Netzkopplung: Eigenerzeugten PV-Strom direkt mit den Nachbarn teilen

Veranstalter: VDE-AK Energie
Ort: München
Adresse: Lothstraße 64, 80335 München, Hochschule München, Raum R 2.004
Referent: Andreas Eberhardt, M.Sc.

19:00 Vortrag

Hochpräzise Navigation mit oder ohne Galileo? Herausforderungen an die Satellitennavigation

Veranstalter: VDE/VDI-AK Informationstechnik
Ort: München
Adresse: Werinherstraße 91, 81541 München, Nokia Solutions and Networks GmbH & Co. KG, Gebäude 41, Konferenzzone
Referent: Prof. Dr. Thomas Pany
Info: aki@vde-suedbayern.de

---

18. November 2019 / Montag

16:00 Vortrag

3D-Drucken mit Beton – Neue Möglichkeiten für Design und Konstruktion

Veranstalter: Aktuelles Forum Technik
Ort: München
Adresse: Brienner Str 39, 80333 München, Hansahaus, Rahnstüberl
Referent: Daniel Weger, M.Sc., Leiter Projektgruppe Additive Fertigung, TUM
Gebühr: 5,00
Anmeldung: Online Anmeldung

16:30 Vortrag

„Einsamkeit” und „Trieb zur Arbeit” Alexander von Humboldt als biographische Herausforderung

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Andreas W. Daum, University of Buffalo, NY, USA

16:30 Exkursion

Brandschutz im Krankenhaus

Veranstalter: VDI-AK Bio-, Medizin- und Umwelttechnik
Ort: München
Adresse: Lothstr. 34, 80335 München, Hochschule München, G 3.30
Referent: Dipl.-Ing. Reinhard Mermi
Anmeldung: Liepsch@hm.edu

18:00 Forum

Technischer Vertrieb im Zeitalter der Digitalisierung

Veranstalter: VDI-AK Technischer Vertrieb und Produktmanagement
Ort: Garching
Adresse: Boltzmannstr. 15, 85748 Garching, TU München, Gebäude 5 MW 1051
Referent: N.N.
Anmeldung: Online Anmeldung

---

19. November 2019 / Dienstag

17:30 Vortrag

Einzug der Additiven Fertigung in die Serienproduktion

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dipl.-Ing. Sebastian Edelhäuser, EOS GmbH, Krailling/Munich
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

23. November 2019 / Samstag

14:00 Exkursion

Besichtigung der militärgeschichtlichen Sammlung (MGS) Lechfeld

Veranstalter: VDI-AK Technikgeschichte
Ort: Lagerlechfeld
Adresse: Parkplatz an der Hauptwache der Kaserne Lechfeld 86836 Lagerlechfeld, Kaserne Lechfeld
Referent: Harald Knobloch
Info: Anreise individuell auf eigene Kosten, Tel. 08105 4261
Anmeldung: unbedingt erforderlich, Online Anmeldung

---

26. November 2019 / Dienstag

17:30 Vortrag

Entwicklung eines Full-Flight Simulators

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dr. Matthias Weinzierl, Firma RS Flight Systems GmbH, Berg/Germany
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

18:00 Treff

Stammtisch Cross Cultural Group

Veranstalter: Project Cross Cultural Group
Ort: München
Adresse: Bergmannstr. 46, 80339 München, Griechisches Haus, Café Philoxenos
Info: Um Anmeldung wird gebeten. Weitere Informationen unter: ccg@verein-der-ingenieure.de
Anmeldung: Online Anmeldung

18:15 Vortrag

Rundfunkhören macht gesund

Veranstalter: VDE-AK ML
Ort: München
Adresse: Haidenauplatz 1, 81667 München, MDK Bayern, Raum Nymphenburg, 6. OG
Referent: Dr. Marianne Koch, Ulrike Ostner, Klaus Schneider, Bayerischer Rundfunk, bekannt durch „Gesundheitsgespräch im Notizbuch“, Bayern 2

---

27. November 2019 / Mittwoch

15:00 Exkursion

Besuch der Schiffsmotorenfertigung bei MAN Diesel SE

Veranstalter: VDI-AK Schiffbau und Schiffstechnik
Ort: Augsburg
Adresse: Stadtbachstraße 1, 86153 Augsburg, MAN Diesel SE
Info: Dipl.-Ing. Klaus Kormann, klaus.kormann@vdi-sued.de
Anmeldung: klaus.kormann@vdi-sued.de

15:30 Treff

VDE Senioren-Stammtisch

Veranstalter: VDE Seniorenkreis
Ort: München
Adresse: Kaufingerstraße 5, 80331 München, Café Guglhupf, Obergeschoss
Info: Direkt neben dem Kaufhof am Marienplatz

19:00 Vortrag

Currency Technology – Umgang mit Geld als Physikerin und Mutter & Treffen zum Jahresabschluss

Veranstalter: VDI fib - Frauen im Ingenieurberuf
Ort: München
Adresse: Genaue Adresse folgt rechtzeitig mit der Einladung
Referent: Dr. Friederike Lichtenegger
Info: Adresse folgt rechtzeitig mit der Einladung
Anmeldung: Online Anmeldung

19:00 Vortrag

Karriere(n) machen – Bewerbung und Bewerbersuche

Veranstalter: VDI-AK Unternehmer und Führungskräfte
Ort: München
Adresse: Genaue Adresse folgt
Referent: Carmen Kraushaar, Personalberaterin
Anmeldung: Online Anmeldung

---

28. November 2019 / Donnerstag

18:00 Vortrag

Darf der Mensch alles machen, was er kann? – Satellitendaten zeigen den Klimawandel

Veranstalter: VDI-AK Technikgeschichte
Ort: München
Adresse: Ledererstraße 5, 2. Stock (Lift), 80331 München, Akad. Gesangvereins (AGV), Max-Planck-Saal 2. Stock (Lift)
Referent: Dipl. Ing. Martin Häusler, Deutsches Zentrum für Luft- und Raumfahrt
Info: Tel. 08105 4261
Gebühr: 5 Euro, Studenten, Schüler, VDI-Mitglieder und AGVer frei

---

02. Dezember 2019 / Montag

16:30 Vortrag

How special were the Mathematicians? Their Depictions in Ancient Greece and Rome

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Liba Taub, University of Cambridge, UK

---

02. Dezember 2019 / Montag

17:00 Vortrag

Hochtemperatur-Wärmepumpen zur Dekarbonisierung industrieller Prozesswärme und als wesentliches Bindeglied in der Sektorkopplung

Veranstalter: VDI-AK Energie in Zusammenarbeit mit dem Lehrstuhl für Energiesysteme der TU München
Ort: Garching
Adresse: Lichtenbergstraße 2a, 85748 Garching, Institute for Advanced Study, IAS Auditorium
Referent: Manfred Fricke, Ochsner Wärmepumpen GmbH

18:00 Event

FiB Ingolstadt Stammtisch

Veranstalter: VDI-AK FIB Ingolstadt
Ort: Ingolstadt
Adresse: 85049 Ingolstadt, Christkindlmarkt Ingolstadt, Haupteingang des Stadttheaters

---

19:00 Treff

VDE YoungProfessionals Stammtisch mit Hochschulgruppe

Veranstalter: VDE YoungProfessionals
Ort: München
Adresse: Milchstraße 1, 81667 München, Lollo Rosso Bar(varian) Grill
Info: Terminänderungen unter www.vde-suedbayern.de
Anmeldung: per Mail: stammtisch@vde-muenchen.de

---

03. Dezember 2019 / Dienstag

17:30 Vortrag

Automatisierungs- und Assistenzfunktionen im Test

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Andreas Rigling, ADAC e.V.
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

19:00 Vortrag

Stülpmembranspeicher für den Strom- und Wärmesektor

Veranstalter: VDI-AK TGA / IDV
Ort: München
Adresse: Lothstraße 34, kostenloses Parken i.d. Tiefgarage, 80335 München, Hochschule München, G-1.27
Referent: Prof. Dr.- Ing. Matthias Popp, Techn. Hochschule Georg Simon Ohm, Nürnberg
Info: Bernhard.fritzsche@vdi-sued.de

---

04. Dezember 2019 / Mittwoch

18:45 Exkursion

Renovierung St. Anna Kircherl, anschließend musisch-kulinarischer Abend

Veranstalter: VDI-AK Unternehmer und Führungskräfte
Ort: München
Adresse: Karolingerallee 34, 81545 München, Harlachinger Einkehr, Treffen am Parkplatz
Info: Anmeldeschluss 02.12.2019; Die Mini-Exkursion startet pktl. um 18:45 Uhr am Parkplatz Harlachinger Einkehr
Gebühr: 5,00 Euro pro Person
Anmeldung: Online Anmeldung

---

09. Dezember 2019 / Montag

19:00 Treff

Dezember Stammtisch der SuJ München

Veranstalter: VDI-AK SuJ München
Ort: München
Adresse: 80687 München
Info: Ort wird noch bekanntgegeben

---

10. Dezember 2019 / Dienstag

17:30 Vortrag

Ein neues Airtaxi-Konzept

Veranstalter: VDI-AK Fahrzeugtechnik
Ort: München
Adresse: Lothstr. 64, 80335 München, Hochschule München, R 1.049
Referent: Dr.-Ing. Matthias Bitter, AutoFlightX GmbH, Gilching
Info: Parken in der Tiefgarage, bei Rückfragen: gutmann@hm.edu

---

19:00 Treff

VDI/VDE Treff

Veranstalter: VDI BG Landshut
Ort: Landshut
Adresse: 84028 Landshut, Gasthaus „Zur Insel“
Info: Dr. Helmut Strasser, Tel. 0871/74197

---

11. Dezember 2019 / Mittwoch

18:00 Treff

Kapitänsdinner

Veranstalter: VDI-AK Schiffbau und Schiffstechnik
Ort: München
Adresse: Lagerhausstraße 15, 81371 München, Restaurant „Alte Utting“
Info: Dipl.-Ing. Klaus Kormann, klaus.kormann@vdi-sued.de
Anmeldung: klaus.kormann@vdi-sued.de

---

14. Dezember 2019 / Samstag

11:30 Exkursion

Magistrat, Monachia und Meisterfeier – Ein Rundgang durch das Neue Rathaus

Veranstalter: VDI-AK Aktuelles Forum Technik
Ort: München
Adresse: Marienplatz, 80331 München, Rathaus, Vor der Tourist Information
Anmeldung: Online Anmeldung

---

16. Dezember 2019 / Montag

16:30 Vortrag

Alexander von Humboldt: Die ganze Welt in tausend Schriften

Veranstalter: Münchner Zentrum für Wissenschafts- und Technikgeschichte
Ort: München
Adresse: Museumsinsel 1, 80538 München, Deutsches Museum, Bibliotheksbau, Alter Seminarraum (1402)
Referent: Prof. Oliver Lubrich, Universität Bern, Schweiz

---

16. Dezember 2019 / Montag

18:00 Forum

Produktmanagement in Kleinunternehmen: Aufgabe des Vertriebs?

Veranstalter: VDI-AK Technischer Vertrieb und Produktmanagement
Ort: Garching
Adresse: Boltzmannstraße 15, 85748 Garching, TU München, Gebäude 5 MW 1051
Referent: N.N.
Anmeldung: Online Anmeldung

---

19. Dezember 2019 / Donnerstag

18:00 Vortrag

„Blütenpracht und Nektartracht“ – Über die ökologische und volkskundliche Bedeutung

Veranstalter: VDI-AK Technikgeschichte
Ort: München
Adresse: Ledererstraße 5, 2. Stock (Lift), 80331 München, Akad. Gesangvereins (AGV), Max-Planck-Saal 2. Stock (Lift)
Referent: Thomas Janscheck, Dipl.-Ing. (FH) Gartenbau
Info: Tel. 08105 4261
Gebühr: 5 Euro, Studenten, Schüler, VDI-Mitglieder und AGVer frei

---

Die tagesaktuelle Veranstaltungsliste finden Sie unter www.technik-in-bayern.de

---

Die Musikfreunde des VDI und VDE laden zum

„Festlichen Konzert zur Weihnachtszeit“ mit dem Bamberger Streichquartett

in die **Kaiserburg Nürnberg am 7.12.19, 19:00 Uhr** mit Werken von Mozart, Vivaldi u. a. sowie adventlichen Weisen


Foto: Bamberger Streichquartett

Bamberger Streichquartett – Raùl Teo Arias, Andreas Lucke, Branko Kabadaic, Karlheinz Busch (Mitglieder der Bamberger Symphoniker – Bayerische Staatsphilharmonie)

Kartenkategorie
30,- Euro (VDI/VDE-Mitglieder, max. 2 Karten)
40,- Euro (Nichtmitglieder)

Kartenbestellung
VDI@th-nuernberg.de oder
Tel. (09 11) 55 40 30

Beginn: 19.00 Uhr **Einlass:** 18.00 Uhr

Nicht verpassen!

Treffs, Vorträge und Exkursionen des VDI BV Bayern Nordost

07. November 2019 / Donnerstag

16:00 Exkursion

Brauereibesichtigung Lammsbräu

Veranstalter: VDI-AK Technischer Vertrieb und Produktmanagement
Ort: Neumarkt i. d. Opf.
Adresse: Amberger Strasse 1, 92318 Neumarkt i. d. Opf., Neumarkter Lammsbräu, Innenhof
Referent: Herr Brechelnacher
Info: Brauereibesichtigung mit Vertriebsgespräch – Vertriebsstrategie und Vertriebsprozess
Gebühr: 8,00 Euro
Anmeldung: Online Anmeldung

---

12. November 2019 / Dienstag

17:00 Treff

Treffen für technische Gespräche

Veranstalter: VDI BG Erlangen
Ort: Erlangen
Adresse: Dorfstr. 14, 91054 Erlangen-Büchenbach, Gaststätte „Zur Einkehr"
Info: Dr. Hans Buerhop, Tel. (0 91 31) 4 49 54

18:00 Forum

VDI-Forum „Automatisiertes und Autonomes Fahren – Mobilität der Zukunft"

Veranstalter: VDI-BV Bayern Nordost e.V. / VDI Landesverband Bayern
Ort: Nürnberg
Adresse: Bankgasse 9, 90402 Nürnberg, Heimatministerium Nürnberg, Saal „Atrium"
Anmeldung: Online-Anmeldung

19:00 Vortrag

Additive Fertigung

Veranstalter: VDI BG Coburg
Ort: Coburg
Adresse: Friedrich-Streib-Strasse, 96450 Coburg, Hochschule Coburg
Referent: Eberhard Kübel

---

13. November 2019 / Mittwoch

14:00 Exkursion

Kunststofffertigung – Formenbau – Qualität – Logistik Präzision in Bestform

Veranstalter: VDI-AK Produktion und Logistik + AK Kunststofftechnik
Ort: Fürth
Adresse: Futuriastraße 1, 90763 Fürth, Höfer & Sohn GmbH
Info: Werksbesichtigung
Anmeldung: Online Anmeldung

---

13. November 2019 / Mittwoch

18:00 Vortrag

Zwischen Aufklärung und Provokation – der Wandel des politischen Diskurses im digitalen Zeitalter

Veranstalter: VDI BG Ansbach
Ort: Ansbach
Adresse: Residenzstr., 91522 Ansbach, Hochschule Ansbach, Hans-Maurer-Auditorium
Referent: Prof. Dr. Christian Schicha, FAU ER-NBG

19:00 Treff

Netzwerktreffen für SuJ Nürnberg

Veranstalter: VDI-AK SuJ Nürnberg
Ort: Nürnberg
Adresse: Weintraubengasse 2, 90403 Nürnberg, Kuhmuhne

---

14. November 2019 / Donnerstag

19:00 Treff

Treffpunkt Technikgeschichte

Veranstalter: VDI-AK Technikgeschichte
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: Dipl.-Ing. Klaus Jantsch,Tel. (09 11) 59 13 44

---

16. November 2019 / Samstag

10:00 Seminar

Feedback 4.0: Wertschätzendes Feedback – Wirkungsvolles Führen

Veranstalter: VDI-AK Produkt- und Prozessgestaltung
Ort: Nürnberg
Adresse: Kesslerplatz 12, 90489 Nürnberg, Technische Hochschule Nürnberg, KA.440a
Referent: Hans-Joachim Scheler, Dipl.-Ing. (FH) Günter Schmid
Info: siehe Ankündigung S. 38
Gebühr: 80,00 EUR
Anmeldung: Online Anmeldung bis 08. November 2019

---

17. November 2019 / Sonntag

10:00 Seminar

FIB Nürnberg Training: Agiles Arbeiten

Veranstalter: VDI-AK FIB Nürnberg
Ort: Nürnberg
Adresse: Adam-Klein-Straße 6, 90429 Nürnberg, Nachbarschaftshaus Gostenhof, Bitte schwarze Tafel am Eingang beachten
Referent: Dr.-Ing. Claudia Kostka
Info: 1-tägiges Training , siehe S. 33
Gebühr: 20,00 Euro
Anmeldung: Online Anmeldung

---

19. November 2019 / Dienstag

19:00 Treff

Gesprächsrunde Netzwerk Nürnberg

Veranstalter: VDI-AK Netzwerk Nürnberg
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: M.Eng Herbert Gaida, Tel. (01 77) 7 23 17 41

---

20. November 2019 / Mittwoch

14:30 Vortrag

Flammschutzmechanismen in der Kunststofftechnik

Veranstalter: VDI-AK Kunststofftechnik
Ort: Erlangen-Tennenlohe
Adresse: Am Weichselgarten 8, 91058 Erlangen-Tennenlohe, Lehrstuhl für Kunststofftechnik, Seminarraum
Referent: Priv.-Doz. Dr. rer. nat. habil. Bernhard Schartel
Anmeldung: Online Anmeldung

---

28. November 2019 / Donnerstag

16:30 Treff

Treffen zum Thema Systems Engineering

Veranstalter: VDI-AK Systems Engineering
Ort: Erlangen
Adresse: Wetterkreuz 19a, 91058 Erlangen, Method Park Holding AG
Anmeldung: XING

---

30. November 2019 / Samstag

14:00 Führung

Tag der Modelleisenbahn im 1. Märklin-Club Nürnberg e.V.

Veranstalter: VDI-AK Technikgeschichte
Ort: Nürnberg
Adresse: Am Wegfeld 41, 90409 Nürnberg, Vereinsheim TSV-Buch
Referent: Peter Reinwald, Vorsitzender 1. Märklin Club Nürnberg e.V.
Info: Anlagenvorführung „Betrieb auf Schienen und Straßen", Dipl.-Ing. Klaus Jantsch, dipl.ing.jantsch@gmx.de
Anmeldung: Online Anmeldung bis 20. November 2019 erforderlich!

---

10. Dezember 2019 / Dienstag

17:00 Treff

Treffen für technische Gespräche

Veranstalter: VDI BG Erlangen
Ort: Erlangen
Adresse: Dorfstr. 14, 91054 Erlangen-Büchenbach, Gaststätte „Zur Einkehr"
Info: Dr. Hans Buerhop, Tel. (0 91 31) 4 49 54

---

10. Dezember 2019 / Dienstag

19:00 Sonstiges

Adventsabend mit Vortrag

Veranstalter: VDI BG Coburg
Ort: Coburg
Adresse: Lossaustraße 12, 96450 Coburg, Hotel Stadt Coburg

---

11. Dezember 2019 / Mittwoch

19:00 Treff

Netzwerktreffen für SuJ Nürnberg

Veranstalter: VDI-AK SuJ Nürnberg
Ort: Nürnberg
Adresse: Bayernstraße 150, 90478 Nürnberg, Gutmann am Dutzendteich

---

12. Dezember 2019 / Donnerstag

19:00 Treff

Treffpunkt Technikgeschichte

Veranstalter: VDI-AK Technikgeschichte
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: Dipl.-Ing. Klaus Jantsch, Tel. (09 11) 59 13 44

---

17. Dezember 2019 / Dienstag

18:30 Treff

FIB Nürnberg Stammtisch

Veranstalter: VDI-AK FIB Nürnberg
Ort: Nürnberg
Adresse: 90489 Nürnberg
Info: ak-fib-nuernberg@bv-bayern-nordost.vdi.de
Anmeldung: ak-fib-nuernberg@bv-bayern-nordost.vdi.de

---

18. Dezember 2019 / Mittwoch

19:00 Treff

Gesprächsrunde Netzwerk Nürnberg

Veranstalter: VDI-AK Netzwerk Nürnberg
Ort: Nürnberg
Adresse: Wollentorstr. 3, 90489 Nürnberg, Restaurant „KIM CHUNG"
Info: M.Eng Herbert Gaida, Tel. (01 77) 7 23 17 41

Die tagesaktuelle Veranstaltungsliste finden Sie unter www.technik-in-bayern.de

VDI-AK Bio-, Medizin- und Umwelttechnik München

Umweltforschungsstation Schneefernerhaus

Am 27. Mai 2019 fuhren eine Reihe von Studenten und VDI-Mitglieder zum Schneefernerhaus auf die Zugspitze zum Schneefernerhaus.

Mit der Seilbahn ging es von der Eibsee-Talstation zur Zugspitze, wo wir in eine Gondel-Seilbahn wechselten, die uns zum Schneefernerhaus brachte.
Das Wetter spielte zwar nicht ganz mit. Wir hatten keine Fernsicht, aber es war möglich, die nähere Umgebung zu sehen wie den Gletscher und Garmisch im Tal. Es lag noch über 5 m Schnee, sodass wir nicht durch die Eingangstür der Forschungsstation gehen konnten, sondern über die Terrasse, die vom Schnee freigeschaufelt war.
Nach einer kurzen Einführung und einem Überblick über die Forschungsstation besichtigten wir die verschiedenen Mess-Stationen.

Die Besuchergruppe des VDI im Schneefernerhaus

Die Umweltforschungsstation ist ein international vernetztes Kompetenzzentrum für Höhen- und Klimaforschung mit zehn Konsortialpartnern. In weltweiter Zusammenarbeit werden die Auswirkungen des Klimawandels untersucht. Zahlreiche hochempfindliche Mess-Geräte und Mess-Stationen zeichnen kleinste Veränderungen der Umweltfaktoren wie z. B. Luftqualität, Feinstaub, Spurengase, Temperatur und Feuchtigkeit auf. Welche Rolle spielen Vulkanausbrüche, Waldbrände, atmosphärischer Wasserdampf etc.? Umwelt und Höhenmedizin sowie Auswirkungen des Klimawandels auf die Gesundheit sind weitere Forschungsgebiete.
Neben einer regelmäßigen Wartung muss vor allem darauf geachtet werden, dass es zu keinerlei Fehlmessungen durch unmittelbare Störungen in der näheren Umgebung kommt, wie z. B. Besuchergruppen, die bereits die Umgebungsluft beeinflussen. So wird auch der Schneepflug nicht mit einem Verbrennungsmotor betrieben, sondern elektrisch.
Neben den zahlreichen hochinteressanten Projekten besichtigten wir auch die unterirdischen Gänge und Tunnel. So herrscht Permafrost in den unterirdischen Gängen. Taut das Eis auf, kann es zu weitreichenden Folgen kommen.
Die Versorgung der Station ist durch die Zahnradbahn gewährleistet, da dieser Tunnel weitgehend wetterunabhängig ist. Die Entsorgung der Station erfolgt über eine Abwasserleitung, die durch den Stollen ins Tal führt.

Nach der Besichtigung fuhren wir noch zum Zugspitzgipfelrestaurant, wo wir uns stärkten und das Gesehene noch diskutierten.
Viele Interessenten fragten nach, ob eine solche Exkursion nochmal stattfindet. Sie ist für Juni 2020 geplant.

Prof. Dieter Liepsch

Weiterführende Literatur

Umweltforschungsstation
Schneefernerhaus/Zugspitze

Herausgeber:
Betriebsgesellschaft
Umweltforschungsstation
Schneefernerhaus GmbH
Zugspitze 5
82475 Zugspitze

Leserbrief zu TiB 04/2019 zum Leitartikel von Dr. Kefer

Hat die Eisenbahn eine Chance?

Ja, digitale Leit- und Sicherungstechnik oder Elektrifizierung weiterer Bahnstrecken bringen mehr Züge aufs Gleis. Ja, massiver Ausbau der Infrastruktur hilft unserem Klima.
Nein, kostspielige Messestände (Hannover Messe, Kirchentag) bringen weder neue Bahnreisende noch neue Fracht. Aber der Ausbau der Eisenbahn stockt. Gerade die selbsternannten Klimaschützer tragen ein gerüttelt Maß dazu bei. Sollen Strecken leistungsfähiger werden klagen sie gegen zusätzliche Züge, Lärm, Flächenverbrauch und Gefährdung von Sumpfpflanzen. Soll elektrifiziert werden wird Elektrosmog bejammert. Sollen Güterzüge über die Alpen LKW-Kolonnen ersetzen werden Rheintalbahn und Brennerzulaufstrecke bekämpft. Sollen Züge zwischen Stuttgart und Ulm schneller fahren erstreiten sie rund € 8.000,- pro Heuschrecke für „Umsiedlung“, „Fütterung“ und „Pflege“, um ihr ungeliebtes Bahnprojekt finanziell abzuwürgen.
Diese Gemengelage aus technischer Unkenntnis der Bevölkerung und religiösem Welterrettungswahn der Klimaaktivisten schreit nach öffentlich vorgetragenem technischem Sachverstand.

Möge der VDI unter Herrn Dr. Kefer die Kraft haben, dies wirksam anzustoßen und die Zweigleisigkeit der Ingenieurvereine VDI und VDE zugunsten eines gemeinsamen schlagkräftigen Auftritts in der Öffentlichkeit beenden helfen.

Unterbleibt der Ausbau der Eisenbahn, drohen Verfall der Infrastruktur und damit einhergehend wirtschaftlicher Niedergang und große Arbeitslosigkeit.

Hanno Röscheisen
München

Technische Hochschule Deggendorf

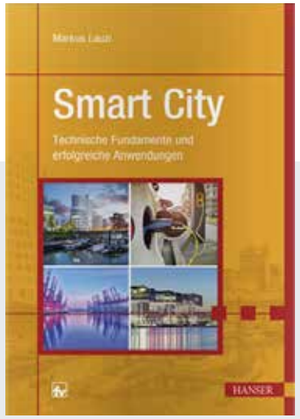
Unternehmen brauchen Kompetenz in KI

An der Technischen Hochschule Deggendorf (THD) wird ab dem Wintersemester 2019/2020 der Studiengang Künstliche Intelligenz angeboten. Zum Start des Studienbetriebs haben nicht nur Abiturienten die Chance, den Studiengang zu belegen, sondern einmalig auch Berufstätige mit Vorkenntnissen und entsprechend verkürzter Studienzeit.

Ingenieuren, Informatikern, Wirtschaftsinformatikern und allen anderen einschlägigen Berufsgruppen mit Diplom- oder Bachelorabschluss bietet die THD die Möglichkeit, sich ab Oktober in nur zwei Jahren im Bereich Künstliche Intelligenz (KI) weiter zu qualifizieren. „In Unternehmen ist jetzt KI-Wissen gefragt. Das Angebot der THD ist die perfekte Chance für einen Quereinstieg in die Thematik. Und das erworbene Wissen kann sofort am Arbeitsplatz eingebracht werden“, wirbt Prof. Heribert Popp, Leiter des Studiengangs Künstliche Intelligenz. Quereinsteiger können vorhandene Qualifikationen an das Studium anrechnen lassen.
Die Vorlesungen für die verkürzte Variante des Bachelors Künstliche Intelligenz finden donnerstags und freitags statt. Theoretisch ist es möglich, an drei Tagen pro Woche der bisherigen beruflichen Tätigkeit nachzugehen.

Der Studiengang Künstliche Intelligenz für Quereinsteiger startet bei einer Mindestteilnehmerzahl von 15 Studierenden und kostet nur 52 Euro Studentenwerksbeitrag.

Bei Fragen steht
Prof. Dr. Dr. Heribert Popp
E-Mail: heribert.popp@th-deg.de
als Ansprechpartner zur Verfügung.



Smart City
Technische Fundamente und erfolgreiche Anwendungen
Markus Lauzi
Carl Hanser Verlag
München 2018
ISBN 978-3-44645-496-5
19,00 Euro

Weltweit leben immer mehr Menschen in Städten. Es ist eine Herkulesaufgabe, diese optimal zu organisieren. Die Werkzeuge der Smart City (Digitalisierung, Automatisierung, Vernetzung) sollen die Städte der Zukunft effizienter, umweltfreundlicher und lebenswerter gestalten als die derzeitigen Megastädte.
Mit „Smart City" will der Autor sowohl ein Lehrbuch für Studenten als auch eine Einführung für interessierte Laien vorlegen. Er beschreibt zunächst die historischen und globalen Treiber der Siedlungsentwicklung. Ein gutes Viertel der nur 140 Seiten des knappen Buches widmet der Autor dann den technischen Grundlagen der Digitalisierung. Das ist für Studenten etwas wenig, für den Laien mit zu vielen Details nicht immer relevant. Als digitale Anwendungen werden eine vernetzte Zahnbürste (!) und der allseits beliebte „intelligente" Kühlschrank beschrieben. Interessantere Geschäftsmodelle werden nur aufgelistet. Schließlich erfahren wir etwas über Digitale Anwendungen (Verwaltung, Mobilität, Umwelt etc.). Hier würde es interessant werden, aber mangels Raum wird alles nur angetippt.

Systemrelevante Themen wie Ressourcenverbrauch, gesellschaftliche Bedürfnisse und Auswirkungen, Ethik der Digitalisierung werden nur sehr kurz angesprochen. Der Autor selbst ist auch durchaus skeptisch. Er mahnt: „Nicht der Einsatz neuer Technologie löst die Probleme der Stadtentwicklung, vielmehr muss die Technik von den gesellschaftlichen Akteuren zur Problemlösung eingesetzt werden".

Gerhard Grosch

Die Energiewende in Europa
Eine Fortschrittsvision
Peter Hennicke, Jana Rasch, Judith Schröder, Daniel Lorberg
Oekom
München 2019
ISBN 978-3-96238-144-8
20,00 Euro

Die Autorinnen und Autoren sind Politologen am Wuppertal Institut bzw. an der Bergischen Universität Wuppertal. Demzufolge ist ihre Argumentationsführung eher wenig technikbasiert. Das Buch taucht vielmehr mit professoral gedrechselter, wissenschaftlich exakter Sprache, tief und facettenreich in den europäischen Energieverordnungsdschungel und seine nationalen und regionalen Ausblühungen ein. Neben vielen anderen Aspekten werden aktuell die Empfehlungen der Deutschen Kohlekommisssion, sowie die verschiedenen Modelle einer CO_2-Bepreisung dargestellt und diskutiert. Im Fokus steht dabei die Einhaltung der vereinbarten Klimaziele (Paris 2015).
Die Kernaussage ist, dass man bei richtiger Steuerung des Ausstiegs aus den fossilen Energieträgern die Wende auch unabhängig vom Klimaeffekt zu einem wirtschaftlich erfolgreichen Selbstläufermodell gestalten kann, das ein Leuchtturmprojekt für Europa und ein Beispiel für andere Länder werden könnte. Auf dem Weg dahin taucht aber leider ein technisches Problem auf, nämlich dass der immer größere Anteil von erneuerbaren Energien die Stromnetze instabil machen kann. Speicher sind teuer oder unrealisierbar, doch hier hilft Emmanuel Macron, der den Franzosen ja ehrgeizige Wendepläne verschrieben hat. Die Kernkraftwerke sollen zwar weniger werden, aber nicht ganz verschwinden, die Stromnetze zum Nachbarn Deutschland dagegen ausgebaut werden. Da hätten wir ja dann die benötigte Pufferleistung für unsere dunklen und windstillen Tage. Aus französischen Kernkraftwerken. Na also.

Fritz Münzel

Verkehrszentrum München

Der bewegte Mensch

Fotos des Münchner Fotografen Roger Fritz

Fotos und Bewegung – ein Widerspruch in sich: Das Medium per se steht still, die Motive sind in zwei Dimensionen fixiert.
Und doch kann man das mobile Leben mit der Kamera einfangen und damit nicht zuletzt die Gemüter der Betrachter bewegen. Das beweist der bekannte Münchner Fotograf Roger Fritz mit „Der bewegte Mensch".
Die Bilderreihe ist als Sonderausstellung bis 9. Februar 2020 im Verkehrszentrum des Deutschen Museums zu sehen.

Weitere Informationen

11. Oktober 2019 bis 9. Februar 2020
Deutsches Museum
Verkehrszentrum
Am Bavariapark 5
80339 München

Die Sonderausstellung mit Fotos des bekannten Münchner Fotografen Roger Fritz präsentiert Porträts von alltäglichen und weniger alltäglichen Situationen mobilen Lebens aus drei Jahrzehnten. Der immer freundliche Blick des Fotografen richtet sich auf Menschen, die unterwegs sind, fahren, laufen, sportlich agieren – oder auch im Verkehrsbetrieb innehalten und warten. In ihrer Summe veranschaulichen sie, wie grundständig Mobilität unser gesamtes Leben prägt. Roger Fritz porträtiert nicht nur Menschen, die unterwegs sind, fahren, laufen oder auch im Verkehrsbetrieb innehalten und warten. Er hält das Besondere im Alltäglichen fest. Und in der Summe veranschaulichen seine Bilder aus drei Jahrzehnten, wie grundlegend Mobilität unser gesamtes Leben prägt.
„Diese Bilderreihe passt ganz hervorragend ins Verkehrszentrum", findet Bettina Gundler, Leiterin des Zweigmuseums am Bavariapark.
„Unsere Autos, Züge, Räder, Kutschen und Co. repräsentieren ja, was uns bewegt. Roger Fritz' Fotos ergänzen das Was durch ein Wie – oder besser gesagt: durch ein So!"

Wie ein Wimmelbild: das Sonnendeck eines Kreuzfahrschiffes

TECHNIK IN BAYERN

Impressum

Herausgeber:
Verein Deutscher Ingenieure (VDI),
Bezirksverein München, Obb. u. Ndb. e.V.
Anschrift der Redaktion:
„Technik in Bayern", Westendstr. 199 (TÜV)
80686 München

Chefredakteur: Dipl.-Ing. Friedrich Münzel (verantw.)
Tel. (0 89) 57 91 22 00, Fax (0 89) 57 91 21 61

Chefin vom Dienst: Silvia Stettmayer
Tel. (0 89) 57 91 24 56, Fax (0 89) 57 91 21 61
E-Mail: tib@bv-muenchen.vdi.de

Redaktion:
Hermann Auer Ing. (grad.); Dipl.-Ing. Wolfgang Berger; Dr. Frank Dittmann; Christina Kaufmann M.A.; Bernhard Kramer M.Sc.; Dipl.-Ing. Jochen Lösch; Dipl.-Phys. Susanne Moses; Dipl.-Ing. Harold Plesch

Verlag:
MuP Verlag GmbH
Nymphenburger Str. 20b, 80335 München
Tel. (089) 1 39 28 42-0, Fax: (089) 1 39 28 42-28
Geschäftsführer: Christoph Mattes

Anzeigenleitung: Christoph Mattes
Tel. (089) 1 39 28 42-20, Fax: (089) 1 39 28 42-28
E-Mail: christoph.mattes@mup-verlag.de

Anzeigenverkauf: Regine Urban-Falkowski
Tel. (0 89) 1 39 28 42-31, Fax: (0 89) 1 39 28 42-28
E-Mail: regine.urban@mup-verlag.de
Es gilt die Anzeigenpreisliste Nr. 22 von 01.01.2019

Vertriebsleitung: Philip Esser
Tel. (0 89) 1 39 28 42-33, Fax: (0 89) 1 39 28 42-28
E-Mail: philip.esser@mup-verlag.de

Layout und Grafik: Ines Fischer

Internet-Service: SpaceNet AG

22. Jahrgang 2019
Technik in Bayern erscheint zweimonatlich.
Der Bezugspreis ist bei VDI- und VDE-Mitgliedern der Bezirksvereine in Bayern sowie dem IDV in der Mitgliedschaft enthalten.

Jahresabonnement 36,– Euro / 72,– SFr, Einzelheft 8,– Euro / 16,– SFr. Jahresabonnement für Studenten gegen Einsendung einer entsprechenden Bestätigung 27,– Euro/ 54,– SFr. Der Euro-Preis beinhaltet die Versandkosten für Deutschland und Österreich, der SFr-Preis die Versandkosten für die Schweiz. Bei Versand in das übrige Ausland werden die Porto-Mehrkosten berechnet. Die Abodauer beträgt ein Jahr. Das Abo verlängert sich um ein weiteres Jahr, wenn es nicht zwei Monate vor Ablauf schriftlich gekündigt wird.

Druck: Mayr/Miesbach GmbH
Am Windfeld 15, 83714 Miesbach

Technik in Bayern ISSN1610-6563

Nächster Redaktionsschluss: 11.11.2019

CARTOON

Cartoon: Cornelis Jettke

VORSCHAU

Ausgabe 01/2020 erscheint am 24. Dezember 2019
mit dem Schwerpunktthema

Technisches Facility Management

In der nächsten Ausgabe beschäftigen wir uns mit Planung, Betrieb und Instandhaltung der technischen Infrastruktur einer Immobilie. Building Information Modelling (BIM) und der digitale Zwilling spielen auch im technischen Gebäudemanagement mittlerweile eine große Rolle.

Anzeigenschluss: 02. Dezember 2019

Foto: photlook - Fotolia

Schwerpunktthema der Ausgabe 02/2020
Autonomes Fahren im Wettbewerb

Anzeigenschluss: 07. Februar 2020

Schwerpunktthema der Ausgabe 03/2020
Energiekonzepte

Anzeigenschluss: 08. April 2020

Fraunhofer
ACADEMY

FIT IN IT-SICHERHEIT

WEITERBILDUNG IM LERNLABOR CYBERSICHERHEIT

Sichern Sie sich Ihren Wissensvorsprung:
- Aktuellstes Forschungswissen von Experten praxisnah aufbereitet
- Passgenaue Lösungsstrategien in hochwertigen Lernlaboren erproben
- Mit Fraunhofer Know-how den Hackern einen Schritt voraus

www.cybersicherheit.fraunhofer.de