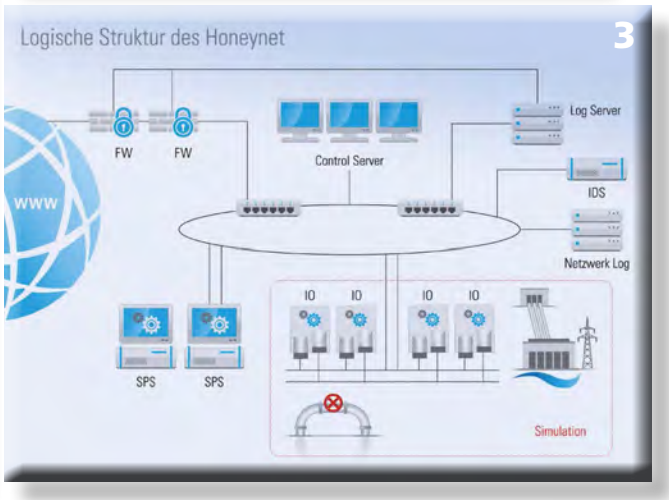
VDI technikforum

VDE

Gesellschaft und Technik in Nordbaden-Pfalz/Kurpfalz



Aus dem Inhalt:

- IT-Sicherheit
- MINT 2015

Mitgliederversammlungen 2016

- **VDI Nordbaden-Pfalz: 20. April**
- **VDE Kurpfalz: 22. April**

Nr. 3/2015

Editorial

Liebe Mitglieder, sehr geehrte Damen und Herren,

vielleicht fragen Sie sich, wie wir für diese Ausgabe des **technikforum** auf das Thema „IT-Sicherheit“ kamen? Es begann mit einem Scherz.

Ein Mitglied des Redaktionsteam kam von einer Dienstreise zurück und wurde gefragt, ob er anschließend die Bordkarte geschreddert habe? Wieso? Wenn man sich den Hintergrund der Frage anschaut, erkennt man, warum Vorsicht geboten ist. In 2014 wurden über 840 Millionen Fluggäste an europäischen Flughäfen gezählt. Folglich wurden mindestens ebenso viele Bordkarten entweder in gedruckter oder digitaler Form ausgegeben. Und die gedruckten Versionen erweisen sich als wahre Fundgrube, um Hackern persönliche Daten des Fluggastes zu liefern. Die Sicherheitslücke steckt im Barcode oder dem QR-Code. Denn beides lässt sich mit einer Scanner App relativ leicht auslesen. Also, so die Quintessenz: Die Bordkarte nicht achtlos liegen lassen, sondern schreddern.

Bei diesem Beispiel blieb es nicht. Jedes Redaktionsmitglied wusste aus dem beruflichen oder privaten Umfeld von Angriffen auf PC und Daten. Auch die Tageszeitungen berichten immer wieder von IT-Zwischenfällen. Dabei kommt heute niemand mehr an der Nutzung des Internets und der Übermittlung von Daten vorbei, egal ob es sich um im Personen oder Unternehmen handelt. Privat beispielsweise kauft man Online ein, bucht Reisen, bezahlt Mietwagen, erledigt Bankgeschäfte. Die Unternehmen sehen sich der Herausforderung von neuen IT-Standards bei Industrie 4.0 gegenüber. Versuche, Autos autonom fahren zu lassen, laufen bereits. Das Zuhause wird immer digitaler. Nicht von ungefähr hat die Bundesregierung ein IT-Sicherheitsgesetz auf den Weg gebracht.

Diese Überlegungen sind die Idee für das Thema des inhaltlichen Schwerpunktes, auf den wir in dieser Ausgabe den Fokus gelegt haben. Wie immer finden Sie, sehr geehrte Leserin, sehr geehrter Leser, zudem Berichte aus den Bezirksvereinen und über unsere verschiedenen Aktivitäten.

Da dies die letzte Ausgabe in Jahr 2015 ist, möchten wir Ihnen auf diesem Weg angenehme Feiertage und einen guten Beginn des Jahres 2016 wünschen.

Mit freundlichen Grüßen

Ihr Redaktionsbeirat

VDI Nordbadisch-Pfälzischer Bezirksverein

VDE Kurpfalz

Cover:

Foto 1: VDE Positionspapier „Smart Grid Security“; Abb.: VDE
Foto 2: MINT-Familientag 2015; Foto: Kunkel
Foto 3: „Honeynet“; Abb.: TÜV Süd
Foto 4: Delta Racing in Fahrt; Foto: Delta Racing
Foto 5: Führung durch die Produktion von HIMA; Foto: Plaga

Aus dem Inhalt:

Sie finden das aktuelle **technikforum** sowie vorangegangene Ausgaben auf den Homepages:
www.vdi-nordbaden-pfalz.de
www.vde-kurpfalz.de

Angriff auf das „schwächste Glied“ der IT Sicherheit – den Nutzer

Angriffe auf Daten privater Nutzer nehmen zu. Deshalb sind Misstrauen und Skepsis angesagt, wenn merkwürdige Anrufer sich am Telefon melden oder eigenartige E-Mails im Postfach auftauchen. Beim Social Hacking werden mit raffinierten Tricks persönliche Daten gestohlen.

Auch das gute, alte Telefon wird von Cyber-Kriminellen für Social Hacking benutzt, um an Nutzerdaten zu kommen.

Samstagnachmittag: Ich komme aus dem Garten, um mir eine Erfrischung aus dem Kühlschrank zu holen, da klingelt das Telefon. Rufnummer unbekannt, aber das kommt bei Anrufen aus unserem Bekanntenkreis immer noch vor. Denn nicht alle unsere Bekannten haben die digitale Telefonie angenommen, sondern nutzen teilweise ihre „altmodischen“ Apparate einfach nur zum Telefonieren.
Nicht so bei diesem Anruf – eine englischsprachige Frau mit eindeutig chinesischem Akzent gibt sich als Mitarbeiterin des Microsoft Support Center aus. Sie platziert eine erschreckende Botschaft: „Ihr Computer ist gehackt worden, was bei routinemäßigen Kontrollen bei Microsoft erkannt worden ist.“ Ich müsse unbedingt Abhilfemaßnahmen ergreifen, welche die freundliche Dame anbietet, sofort durchzuführen. Dazu soll ich meinen Computer einschalten, und sie würde dann diesen gemeinsam mit mir wieder in Ordnung bringen.

Nachdem ich den ersten Schock dieser Nachricht verdaut habe, klingeln, basierend auf den IT Sicherheitsschulungen, die ich bei meinem Arbeitgeber besucht habe, die Alarmglocken. In der Schulung haben wir gelernt: Bei allen nicht direkt bekannten Kontakten ist Misstrauen der beste Schutz vor Angriffen auf den Computer.

„Social Hacking“ oder „Social Engineering“ nennt man diese Art von Attacken, bei denen gezielt der Mensch als Schwachstelle im System „angegriffen“ wird. Eine geläufige Definition dieser Masche finden wir beispielsweise bei wikipedia: Social Engineering ist die zwischenmenschliche Beeinflussung mit dem Ziel, unberechtigt an Informationen oder technische Infrastrukturen zu gelangen.

Mit dem gebotenen Misstrauen sage ich der Dame, dass ich nicht bereit wäre, von ihr eine Fehlerkorrektur durchführen zu lassen, sondern dankbar für den Hinweis bin und mich lieber selbst um meinen Computer kümmern möchte. Die Antwort besagt, dass ich das nicht könne, denn die Hacker hätten schließlich meinen Computer schon gehackt. Aber die Spezialisten von Microsoft wären in der Lage, mir sofort zu helfen. Um dem ganzen Nachdruck zu verleihen, wird sofort der nächste Einschüchterungsversuch gestartet: Sie sagt mir, dass mein Computer bereits für kriminelle Handlungen missbraucht würde, und ich dringend handeln müsse, bevor die Polizei mich dafür verantwortlich mache. Diesem Versuch, Angst vor einer möglichen Strafverfolgung zu verbreiten, halte ich ebenfalls Stand.

Diese Vorgehensweise zeigt deutlich, wie systematisch und berechnend die Schwächen der Nutzer beeinflusst werden sollen. Doch gerade jetzt gilt es, misstrauisch und standhaft zu bleiben. Mit jeglicher Art von Aussagen und Informationen gegenüber Fremden, das sind alle Kontakte die nicht persönlich bekannt und vertrauenswürdig sind, muss man extrem zurückhaltend sein. Kann doch jeder Hinweis dazu genutzt werden, im Rahmen einer Attacke auf Sie bzw. Ihren Computer die mögliche Vertrauensbasis zu schaffen. Mit einem vermeintlich „vertrauenswürdigen Auftritt“ lässt sich der nächste Angriff, bei einem selbst oder im direkten Umfeld, leichter platzieren. Um diese vertrauensbildenden Informationen zu erhalten, wird das Social Engineering einfach, aber leider meist auch effektiv genutzt. Mit sehr wenig Hintergrundwissen wie dem Namen einiger Bekannten oder Kollegen oder auch mit Informationen zu aktuellen Projekten und Vorhaben lässt sich schnell ein vertrauenswürdiger Anschein schaffen. Leider bemerkt es der unerfahrene Anwender oft nicht, dass er gerade nutzbare Informationen preisgegeben hat.

Weiter geht’s: In der nächsten Angriffswelle sagt mir die Dame, dass sie, wie auch die Hacker, meine Daten bereits hätten. Auch hier ist Misstrauen der Schlüssel zur Abwehr, denn genau betrachtet waren quasi keine Daten von mir genannt worden, die dem Angreifer bekannt sind.

Analysiert man die Aussagen, so hat der Hacker lediglich die Telefonnummer. Mit dem Bezug auf Microsoft versucht man mit großer Wahrscheinlichkeit die Computersysteme seines Angriffsziels zu adressieren. Genaues Zuhören und Analyse des Gesagten hat mich hier davor bewahrt, dem Ansinnen des Angreifers nachzugeben.

In elektronischen Verzeichnissen sind häufig Telefonnummer und Mailadresse leicht zugänglich. Ist man auch in sozialen Netzwerken aktiv, so wird die Informationsbeschaffung noch leichter. Machen Sie den Selbstversuch und geben Ihren Namen in eine Suchmaschine ein. Es kann überraschend sein, was da an Daten frei verfügbar ist. Machen Sie sich diese Daten bewusst, denn werden diese Informationen zusammen mit einem Hacker-Angriff genutzt, ist dies keinesfalls als Vertrauensbeweis zu bewerten. Diese einfache Internetrecherche stellt für die Angreifer meist nur den ersten Schritt der Informationsbeschaffung dar, die dann mit Suchen in sozialen Netzwerken oder gezielten Anrufen weiter verfeinert werden. Das liefert dann meistens einen detaillierten „Steckbrief", um ein möglichst vertrauensvolles, authentisches Szenario aufzubauen.

Mit dem Bewusstsein, dass ich gerade Objekt eines „Social Hacking" war mit dem Ziel meinen Computer zu „erobern", beende ich bestimmt aber höflich das Gespräch. Zwei Tage später erhalten wir jedoch nochmal einen Anruf von Unbekannt, den wir, nachdem sich der angebliche Microsoft Support zu erkennen gegeben hat, durch Auflegen beenden. Das war anscheinend das Zeichen für die Hacker abzubrechen, denn weitere Anrufe blieben aus.

Dieses Beispiel einer Attacke zeigt sehr deutlich, wie dreist solche Handlungen durchgeführt werden, und wenn es nicht so ernst wäre, wäre es sehr interessant zu erfahren, was sich diese Hacker noch so alles einfallen lassen.

Virenscanner und Firewall sowie organisatorische Maßnahmen wie zyklischer Passwortwechsel und unterschiedliche Passwörter für unterschiedliche Anwendungen schützen den Computer und auch die dort gespeicherten Daten. Leider sind all diese Schutzmaßnahmen wirkungslos, wenn der Anwender einem Angriff nicht standhält.

Der Einfallsreichtum von Hackern ist unbegrenzt und hat nur ein Ziel: Auf möglichst viele Computer Zugriff zu erhalten. Mit dem Computer und den dort gespeicherten Daten lässt sich beliebig viel Schaden anrichten.

Da sich die Zahl der Attacken ständig erhöht, helfen das gesunde Misstrauen bei Anrufen, E-Mails oder Anfragen in sozialen Netzwerken sowie ein wachsamer Geist, sich in solchen Situationen richtig zu verhalten. Auch Beiträge im Internet informieren über die aktuelle Bedrohungslage. Bleiben Sie wachsam!

VDE
Ernst-Dieter Keller
VDE Kurpfalz

IT-Sicherheit – eine unendliche Geschichte mit ungewissem Ausgang?

Internet und Digitalisierung gehören heute zum Alltag, sei es im privaten oder beruflichen Kontext. Ohne deren Nutzung kommt heute kaum jemand mehr direkt oder indirekt aus. Sie sind schon lange nicht mehr „Neuland", sondern für unsere Gesellschaft, die Kommunikation, den Handel, die Produktion, die Forschung und Wissenschaft inzwischen unverzichtbar.

Aber bei der Fülle an Möglichkeiten der Informationstechnik gilt nach wie vor – oder besser gesagt: um so mehr – das altbekannte Sprichwort „Gelegenheit macht Diebe!" Es gibt Hackerangriffe, Cyberkriminelle begehen Datenklau, Viren und Trojaner machen sich breit – in den Medien findet sich tagtäglich die eine oder andere entsprechende Nachricht. Hier ein paar Ausschnitte aus der Themenvielfalt.

Achtung: Attacke auf PC (Abb.: wikicommons)

Wo Daten sind, gibt es Angreifer

Der Sicherheit der Daten und ihres Transfers vom Sender zum Empfänger kommt ein immer größer werdender Stellenwert zu. Wie groß das Interesse an dem Thema ist, zeigen beispielsweise die Einträge bei Google. Zum allgemeinen Stichwort „IT-Sicherheit" finden sich fast drei Millionen Beiträge. Gibt man als Suchbegriff „Trojaner" ein, erhält man die Auswahl von 1,3 Millionen Beiträgen, bei „phishing" stattliche 72 Millionen, und bei „Malware" sind es sogar 99 Millionen „hits".

Phishing

Diese englische Kunstwort setzt sich zusammen aus dem Jargon-Wort „phreaking", was so viel bedeutet wie Manipulation von Telefonen, sowie dem bildlichen Begriff „fishing". Eigentlich dürfte es heute kaum noch einen Internetuser geben, der nicht weiß, wie Phishing funktioniert.

Dennoch gibt es immer wieder erfolgreiche Phishings, auf die man hineinfallen kann. Ist es doch oft auch für geübte Internetbenutzer schwierig, gefälschte Webseiten beispielsweise einer Bank oder E-Mails von den echten Seiten zu unterscheiden. Gelangt man auf die oft täuschend echt gefälschten Seiten,

ist es für die Internetbetrüger nur noch ein kleiner Schritt, an persönliche Daten zu gelangen – sprich: Identitätsdiebstahl zu begehen. Die Folgen sind bekannt: Mit den Daten können Konten geplündert werden.

EC-Terminals

Ebenso wenig sicher kann man sich bei EC-Karten-Terminals fühlen. Sind Betrüger doch den Sicherheitsstandards oft den einen entscheidenden Schritt voraus. So ist die altbekannte Masche, die Daten der EC-Karten am Automaten durch ein kleines Vorsatzgerät am Kartenschlitz abzugreifen, schon seit geraumer Zeit erweitert worden. Nun reicht es nicht mehr aus, den Kartenschlitz auf verdächtige Aufsätze zu kontrollieren. Sind doch weitere Lesegeräte im Umlauf, die im Texteingabefeld des Geldautomaten die Persönliche Identifikationsnummer (PIN) erfassen und diese sofort an die Täter übermitteln. So lassen sich gefälschte EC-Karte mit richtigem PIN herstellen. Diese werden vorzugsweise im Ausland zur Abhebung von Bargeld eingesetzt.

Malware

Software, die malicious (engl.: bösartig) ist, wird heute meist unter dem englischen Kunstwort Malware zusammengefasst. Dahinter verbergen sich Menagerien wie Trojanische Pferde, Würmer oder Viren.

Wer den erfolgreichen Science-Fiction Film „Independence Day" des Regisseurs Roland Emmerich aus dem Jahr 1996 gesehen hat, weiß, wie es der Menschheit gelang, einer tödlichen Invasion von Aliens zu entgehen: Ein US-amerikanischer IT-Spezialist speist – dem Genre entsprechend natürlich auf spektakuläre Weise - in das System der angreifenden Außerirdischen einen Virus ein, womit die Schutzschilde der Invasionsschiffe deaktiviert werden. Der tödliche Angriff wird abgewehrt, da die Flugzeuge und Raketen der Menschheit nun die Operationsbasen der Aliens zerstören können. Im Film sieht man, wie dem Protagonisten die Idee dazu kam: Er hatte in den entscheidenden Stunden einen Schnupfen

Malware und Viren treiben ihr Unwesen im Internet. *(Abb.: wikicommons)*

und sich über die Viren geärgert, die diesen verursachten.

Er verteilt Gift, lateinisch: virus, und ist inzwischen ein in die Alltagssprache eingegangener Begriff: Der Computervirus. Es handelt sich dabei um ein Computerprogramm, das von außen, und wie Viren das so tun, vorhandene Programme infiziert und sich dann selbst reproduziert. Ein Virus kann nicht nur den Status der Hardware und/oder des Betriebssystems verändern, sondern auch den gesamten PC „übernehmen". Diese Art von Malware wird oft auch als „Computerwurm" bezeichnet.

Trojaner dagegen erscheinen zunächst als nützliche Computerprogramme, führen im Hintergrund aber ohne Wissen des Anwenders unerwünschterweise andere Funktionen aus.

Spyware

Kaum ein Internetuser, der sie noch nicht auf dem PC gehabt hat: Werbeeinblendungen und Werbebanner. Es scheint, als würde sich „jemand" merken, welche Internetseiten besucht wurden. In der Tat – genauso funktioniert eine Software, die sich als „Schnüffelsoftware" übersetzen lässt. Die Ernsthaftigkeit trifft jedoch besser die Übersetzung des englischen „Spyware" mit „Spähprogramm".

Die Rede ist von einer Software, die Daten eines Computernutzers an den Hersteller des Programms oder an Dritte sendet – und das ohne Zustimmung. Spyware wird eingesetzt, um das Surfverhalten im Internet zu analysieren. Die Erkenntnisse werden kommerziell genutzt beispielsweise um entsprechend Werbeeinblendungen vorzunehmen.

Angriffe auf IT-Systeme nehmen zu

Täglich sind in den Medien Berichte über Angriffe auf IT-Systeme von Unternehmen, Behörden, Forschungseinrichtungen und gar der Bundesregierung zu finden. Auch private PC-Nutzer bleiben natürlich davon nicht verschont. Ein paar Beispiele sollen die Vielfalt der Gefahren sowie die kriminelle Kreativität der Täter illustrieren.

- **Pikantes statt Fahrplan**

Eigentlich, so eine Pressemeldung im August, wollten die Fahrgäste eines Busterminals in der südbrasilianischen 2-Millionen Metropole Curitiba mit dem Blick auf die Bildschirme an den Bussteigen sich über die Ankunft- und Abfahrtzeiten der Überlandbusse informieren. Geboten wurde plötzlich aber ein besonderes Spektakel, das ihnen Hacker, die sich in das IT-System des Verkehrsbetreibers eingeschlichen hatten, bescherten: Statt Uhrzeiten gab es einen Film zu sehen, den die Zuschauer als „sehr pornografisch" beschrieben haben.

Die Idee war aber gar nicht so neu, wenn man einem Bericht der BILD-Zeitung glaubt. Schon im Sommer 2011 konnten Kunden eines Supermarktes in Dresden im Kassenbereich statt der Abfahrtszeiten der Straßenbahn einen Film

der ähnlichen Sorte wie in Sao Paulo sehen. Die Dresdener Verkehrsbetriebe entschuldigten sich und sprachen von einem Hacker-Angriff.

• Digitaler Patient?

Vor einiger Zeit meldete der „Chaos Computer Club" Bedenken an hinsichtlich des Datenschutzes bei Nutzung der neuen so genannten „Elektronischen Gesundheitskarte", kurz eGK. Ihre Einführung ist gesetzlich vorgeschrieben, und sie wird Nachfolgerin der bisherigen Chipkarte werden.

Die eGK enthält die üblichen Stammdaten des Versicherten wie Name, Geburtsdatum und Versicherungsstatus. Eine weitere, neue Funktion wird das elektronische Rezept sein. Statt ein Papierrezept auszustellen, schreibt der Arzt dies auf die Karte. Die Apotheke kann es dann auslesen.

Zusätzlich soll die eGK später auch eine „elektronische Patientenakte" beinhalten, zunächst jedoch noch auf freiwilliger Basis. In ihr werden Befunde und medizinische Informationen gespeichert. Die Idee ist, dass der Versicherte stets seine eigene medizinische Akte zur Verfügung hat. Die Daten werden vom behandelnden Arzt kryptisch verschlüsselt und auf den Servern eines privaten Unternehmens namens „gematik" gespeichert. Der Versicherte erhält einen Zugangscode.

Die Vortragsreihe **„forum mannheim"** widmet sich in 2015/2016 dem Thema **„Intelligente Assistenzsysteme: Zukunftsweisender Fortschritt oder Ende der Privatsphäre?"**

Als Ergänzung zum Schwerpunktthema dieses **technikforum** möchten wir Sie gerne auf folgenden Vortrag hinweisen:

Big Data: Datenschutz und Persönlichkeitsrechte im Netz
- Mittwoch, 9. März 2015, 18 Uhr
- Referent: Markus Morgenroth, Buchautor und Datenanalytiker
- Ort: Hochschule Mannheim, Gebäude C, Aula

Weitere Vorträge des **forum mannheim:** siehe Veranstaltungsübersicht

Die verschlüsselten Daten können in der Arztpraxis oder an einem speziellen Terminal mit der Versichertenkarte mittels dieses bestimmten Codes wieder aufgerufen und entschlüsselt werden.

Ob bei der Verwendung, dem Transfer und der Lagerung solch sensibler, persönlicher Daten der volle Datenschutz gewährleistet werden kann, wird von Kritikern angezweifelt. Denn der Patient habe nicht die alleinige Hoheit über den kryptographischen Schlüssel, moniert der Chaos Computer Club. Vielmehr habe naturgemäß auch die gematik die Möglichkeit, jederzeit den geheimen Schlüssel für die Patientendaten auszulesen, um beispielsweise bei Verlust des Codes dem Patienten erneut Zugang zu seinen Daten zu ermöglichen.

(Abb.: wikicommons)

• Manipulation an medizinischen Apparaten

Gravierender als unbefugte Einsicht in Akten mit persönlichen, medizinischen Daten ist eine Gefahr, die Patienten im schlimmsten Fall das Leben kosten könnte: Falls es Hackern gelingt, medizinische Apparate zu kapern und deren Funktionen zu verändern.

Im SPIEGEL konnte man Anfang August nachlesen, dass dies offensichtlich bereits einmal gelungen sei.

Es wird berichtet, dass ein IT-Spezialist aus Heidelberg sich in ein Narkosegerät eines großen Herstellers gehackt hatte und mit Hilfe seines Laptops die Steuerung des Geräts übernahm. Er konnte die Beatmung stoppen und alle Funktionen blockieren.

Glücklicherweise handelte es sich um einen bewussten Test, bei dem keine Patienten zu Schaden kommen sollten. Vielmehr hatte ein Krankenhaus in Süddeutschland den Auftrag dazu erteilt, um so auf Sicherheitslücken aufmerksam zu machen. Denn eines steht fest: Hackerangriffe machen auch vor medizinischen Geräten keinen Halt.

• Hört der Fernseher mit?

Es wird immer schwieriger, sich gegen ungewollte Zugriffe auf die Privatsphäre zu schützen. Wer hätte aber vermutet, dass man selbst im heimischen Wohnzimmer nicht vor ungewollten Lauschattacken sicher ist? So sorgte Anfang Februar eine Pressemeldung im FOCUS für Aufregung um Smart-TVs des Herstellers Samsung, deren wunder Punkt die Spracherkennung ist.

Bei bestimmten Smart TVs kann die Bedienung der Funktionen statt über die Fernbedienung auch per Sprache erfolgen. Bevor man die Spracherkennung aktiviert, sollten jedoch die Nutzungsbedingungen des südkoreanischen Herstellers ernst genommen werden, warnte FOCUS.

Denn es heißt: „Bitte seien Sie sich bewusst, dass wenn Sie persönliche oder sensible Informationen sagen, diese zu den Inhalten zählen, die durch die Spracherkennung aufgezeichnet und an dritte Parteien weitergeleitet werden."

Nicht von ungefähr fühlen sich viele Nutzer von Smart TVs an Georges Orwells Roman „1984" erinnert: In der Tat hören die klugen Fernseher der neuen Generation allem zu, was in ihrer Nähe gesprochen wird – und zeichnen es auf. Samsung kann diese Daten dann offensichtlich Drittanbietern zur Weiterverwertung zur Verfügung stellen – wie aus den Nutzungsbedingungen hervorgeht.

- **Wenn das Auto fremdgesteuert wird**

Im Sommer kam aus den USA eine Meldung, die für Erschrecken sorgte: Zwei Sicherheitsexperten war es gelungen, ein fahrendes Auto eines Journalisten aus der Ferne zu manipulieren und von außen die Kontrolle über die Bremsen, Geschwindigkeit, Klimaanlage und das Radio des Jeep Cherokee zu übernehmen. Die beiden Hacker sagen, dass es durchaus möglich sei, auch andere Autos mit gleichem Unterhaltungs-System auf ähnliche Weise zu knacken. Ihren Hack auf den Jeep wollen sie insofern als Warnung verstanden wissen.

Der Zugang zum Fahrzeug erfolgte über eine Sicherheitslücke im Unterhaltungssystem. Dieses ist bei den US-Fahrzeugen des Herstellers mit dem Internet verbunden, damit die Fahrer Musik oder Radio aus dem Netz hören können. Die interne Steuerung wird somit jedoch von außen angreifbar. Genau von dort drangen dann auch die beiden Hacker in die Steuerungssoftware des Autos ein und programmierten das System so um, dass sie es kontrollieren konnten.

Allerdings war der Angriff auf das Steuerungssystem des Autos nicht so einfach, wie es klingt. Die beiden Hacker bedienten sich einer Schwachstelle bei dem Internetanbieter der Jeeps, mit Hilfe derer es gelang, die Internet-Adresse (IP-Adresse) ausfindig zu machen.

Der Vorfall schlug auch in Deutschland hohe Wellen. Der ADAC forderte entsprechend, dass Handlungsbedarf in diesen Bereich geboten sei, da die IT im Auto in ihrer Entwicklung schnell voranschreite. Es sei deshalb sinnvoll, IT-Systeme in Autos beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik (BSI) überprüfen zu lassen. Als Beispiel aus Deutschland wies der Automobilclub noch einmal darauf hin, dass er Anfang des Jahres eine Schwachstelle bei BMW entdeckt hätte. Damals war es Hackern gelungen, fremde Autotüren per Funk zu entriegeln. Die Lücke sei inzwischen gestopft, sagt dazu der bayrische Autobauer.

Ganz einfach per SMS war es Mitte August in den USA zwei IT-Experten gelungen, in das System eines Autos einzudringen. Sie konnten von ihrem Smartphone aus nicht nur die Scheibenwischer in Gang setzen, sondern das Gefährt auch abbremsen. Die Lücke im System, die sie sich zu Nutze machten, war ein so genanntes Telematik-Gerät einer Versicherung. In den USA kommen diese zum Einsatz, wenn die Versicherten ihre Versicherungstarife an die Fahrweise koppeln. Lassen sich mittels der Box doch sämtliche Manöver des Fahrers verfolgen – und leider offensichtlich auch von außen fremdsteuern.

Auch Smartphones haben Viren

Viele denken, es gäbe für Smartphones keine Viren. Verstärkt kam es aber in den letzten Jahren zu Angriffen auf die Systeme.

Denn für Smartphones, die auf Basis des Betriebssystems Android funktionieren, tauchte eine Art Schreckgespenst namens „Stagefright" auf.

Glaubt man den Medien, sind durch eine große Sicherheitslücke im System weltweit gut eine Milliarde Geräte in Gefahr. Angeblich soll es mit einer einfachen MMS möglich sein, ein fremdes Smartphone zu hacken und zu übernehmen. Dazu sagt Eric Bodden von der Technischen Universität Darmstadt: „Inzwischen sind die Ersteller von Schadsoftware auf Smartphones sogar aktiver als auf Desktop-Computern." Als Hauptquelle für Smartphone-Viren stehen inoffizielle App-Stores im Verdacht.

Cyber-Krieg zwischen Nationen?

Die US-amerikanische Öffentlichkeit zeigte sich geschockt, als im Juni die beunruhigende Nachricht über die Newsticker lief, dass chinesische Hacker Informationen von Millionen von Regierungsmitarbeitern, CIA-Agenten und Militärs gestohlen hätten. Washington sprach zunächst von 4,2 Millionen betroffenen Personen. Das FBI korrigierte bald die Zahl nach oben und gab bekannt, dass wohl mehr als 18 Millionen aktive und ehemalige Regierungs-Mitarbeiter von dem Cyber-Einbruch in die Datenbanken des Office of Personnel Management sowie des Heimatschutz-Ministeriums Homeland Security betroffen seien!

Auch der Deutsche Bundestag war bereits im Monat zuvor Ziel eines großangelegten Hackerangriffs. Bundestagssprecher Ernst Hebeker hatte damals zumindest bestätigt, dass bei dem Angriff E-Mail-Daten von Abgeordneten abgeflossen seien. Kritische Stimmen sprachen sogar von einem „Totalschaden" des so genannten Parlakom-Verbunds. Das konnten wohl auch die rund drei Milliarden Euro nicht verhindern, die der Bund jährlich für seine IT ausgibt.

Die Hintergründe für die Cyberattacke auf den Bundestag sind immer noch unklar, zumindest nicht öffentlich bekannt. Haben die USA chinesische Hacker im Verdacht, so verdichteten sich bald nach Bekanntwerden Hinweise, dass die Spur der Bundestagshacker nach Russland verfolgt werden könne. Ob die Spur im Sand verlief oder zu einem Ergebnis führte, ist nicht eindeutig kommuniziert.

Als Konsequenz aus dem groß angelegten Hackerangriff auf den Deutschen Bundestag musste in der Sommerpause das parlamentarische Computernetz Parlakom für mehrere Tage komplett abgeschaltet werden, während die Bundestagsverwaltung in Zusammenarbeit mit einem externen Dienstleister eine Neuinstallation von Teilen des IT-Systems vornahm. Auch wurden mehr als 100.000 Internetseiten dauerhaft gesperrt, die von Parlakom-Rechnern aus Sicherheitsgründen nicht mehr angewählt werden können.

IT-Sicherheitsgesetz des Bundes

Das Timing passte zum Hackerangriff: Der Deutsche Bundestag hat im Juni in 2. und 3. Lesung den Entwurf der Bundesregierung für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) beraten und mit großer Mehrheit angenommen. Am 25. Juli trat es in Kraft.

Worum geht es? Auf der einen Seite sind Betreiber kritischer Infrastrukturen aus den Bereichen Energie, Informationstechnik und Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen nun verpflichtet, einen Mindeststandard an IT-Sicherheit einzuhalten. Falls erhebliche IT-Sicherheitsvorfälle aufgetreten sind, müssen sie diese auch an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden.

Zur Steigerung der IT-Sicherheit im Internet werden zudem die Anforderungen an die Anbieter von Telekommunikations- und Telemediendiensten erhöht. Zusätzlich verstärken sich Kompetenzen des BSI und der Bundesnetzagentur sowie die Ermittlungszuständigkeiten des Bundeskriminalamtes.

Dazu erklärt Bundesinnenminister Thomas de Maizière am 12. Juni vor dem Deutschen Bundestag: „Mit der zunehmenden digitalen Durchdringung unseres Lebens wird Cyber-Sicherheit immer mehr zu einem zentralen Baustein der Inneren Sicherheit in unserem Land. Unser Ziel ist es daher, dass die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit gehören. Mit dem heute vom Deutschen Bundestag verabschiedeten IT-Sicherheitsgesetz kommen wir bei der Stärkung unserer IT-Systeme einen wichtigen Schritt voran. Heute ist ein guter Tag für mehr Sicherheit und Vertrauen im Internet."

Das IT-Sicherheitsgesetz hat mehrere Adressaten:

- Für Betreiber von Webangeboten wie zum Beispiel Online-Shops gelten mit Inkrafttreten ab sofort erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme.
- Telekommunikationsunternehmen sind ab sofort verpflichtet, ihre Kunden zu warnen, wenn sie bemerken, dass der Anschluss des Kunden - etwa als Teil eines Botnetzes - für IT-Angriffe missbraucht wird. Gleichzeitig sollen die Provider ihre Kunden auf mögliche Wege zur Beseitigung der Störung hinweisen.
- Mit Inkrafttreten des IT-Sicherheitsgesetzes werden die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Untersuchung der Sicherheit von IT-Produkten sowie die Kompetenzen des BSI im Bereich der IT-Sicherheit der Bundesverwaltung erweitert.
- Betreiber Kritischer Infrastrukturen (KRITIS) werden verpflichtet, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und – sofern nicht andere Spezialregelungen bestehen – diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen. Darüber hinaus müssen die Betreiber dem BSI erhebliche IT-Sicherheitsvorfälle melden. Die aus diesen Meldungen, aber auch aus diversen weiteren Informationen gewonnenen Erkenntnisse stellt das BSI allen KRITIS-Betreibern zur Verfügung, damit diese ihre IT angemessen schützen können. Die Meldepflicht von erheblichen IT-Sicherheitsvorfällen betrifft zunächst nur die Betreiber von Kernkraftwerken und Telekommunikationsunternehmen. Eine Meldepflicht erheblicher IT-Sicherheitsvorfälle für andere KRITIS-Betreiber tritt erst nach Verabschiedung der noch zu erstellenden Rechtsverordnung in Kraft. Diese wird festlegen, welche Unternehmen den Regelungen des Gesetzes unterliegen.

Quelle: https://www.bsi.bund.de

- Aktuelle Informationen zu Themen rund um die IT-Sicherheit: https://www.bsi.bund.de
- Sicherheitsportal des Bundesamts für Sicherheit in der Informationstechnik, das sich in erster Linie an unerfahrene Internet-Nutzer richtet: https://www.bsi-fuer-buerger.de
- Für die private Nutzung von PCs unter Windows und Ubuntu sowie Macs unter Apple OS X Mountain Lion hat das BSI konkrete Hilfestellungen: https://www.bsi-fuer-buerger.de/BSIFB/.../basisschutzComputer
- Eine so genannte „Schwachstellenampel" verdeutlicht die aktuelle Sicherheitslage in Bezug auf Sicherheitslücken in gängigen Softwareprodukten: https://www.cert-bund.de/schwachstellenampel

Nachdem die Vorteile der Digitalisierung und grenzenlosen Kommunikation sehr wohlwollend von den Nutzern aufgenommen wurden, ist es höchste Zeit, sich mehr Gedanken, um die Datensicherheit zu machen. Mit den Vorteilen sind speziell bei missbräuchlicher Nutzung auch Nachteile verbunden.

Wir müssen daher den Umgang mit diesen Daten und deren Sicherheit weiter verbessern und sicherer machen. Viel liegt an uns, den Betreibern und Nutzern dieser Technik. Sehen wir die möglichen Gefahren als Herausforderung, um die Systeme und die Datenwelt zu verbessern.

Anm. der Redaktion: Die kleine Übersicht über verschiedene Hackerangriffe haben den Stand Ende September. Bis zum Redaktionsschluss hätten wir noch viele weitere hinzufügen können …

Sybille Breunig

TÜV SÜD zum IT-Sicherheitsgesetz – Was auch KMU jetzt beachten sollten

Im Juli hat der Bundestag das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" beschlossen. Das sogenannte IT-Sicherheitsgesetz stellt an Unternehmen der kritischen Infrastruktur Mindestanforderungen für die IT-Sicherheit und verpflichtet sie zur Meldung von Datenpannen und Cyber-Attacken. Kleine und mittelständische Unternehmen (KMU) in diesem Bereich fallen durch das Gesetzesraster. Was das für sie bedeutet, wissen die Experten von TÜV SÜD.

Das neue IT-Sicherheitsgesetz fordert Absicherung der IT und Meldung von Datenpannen.

Zur kritischen Infrastruktur – KRITIS – zählen Unternehmen aus den Branchen Energieversorgung, Transport und Verkehr, Informationstechnik und Telekommunikation, Finanzwesen und Versicherungen sowie Gesundheit und Lebensmittel. Das IT-Sicherheitsgesetz ist eine Zusammenfassung von bereits bestehenden Gesetzen und legt nicht konkret fest, was Betreiber kritischer Infrastrukturen zur Absicherung ihrer IT realisieren müssen, was auf Grund der Schnelllebigkeit in diesem Bereich auch nicht zielführend wäre. Stattdessen schafft es einen Rahmen, der durch noch zu erlassende Rechtsverordnungen und abzustimmende Sicherheitsstandards konkretisiert werden muss.

KMU fallen zwar durch das Raster der Gesetzgebung und müssen demnach die Anforderungen an die IT-Sicherheit nicht zwingend erfüllen, doch häufig arbeiten sie als Zulieferer für größere Unternehmen, die sehr wohl das IT-Sicherheitsgesetz beachten müssen. Daher sollten KMU damit rechnen, dass ihre Auftraggeber die Einhaltung gewisser Standards von ihnen fordern.

„Eine gute Wahl ist dafür die ISO 27001*", erläutert Alexander Häußler, Produktmanager ISO 27001 bei TÜV SÜD. „Diese Norm ist aktuell der international anerkannteste Standard zum Thema Informationssicherheit. Außerdem lässt sie eine gewisse Flexibilität zu, durch die sich spezielle Gegebenheiten einzelner Unternehmen berücksichtigen lassen."

Grundsatz der Norm ist ein risikobasiertes Vorgehen, so dass die implementierenden Unternehmen je nach Geschäftsmodell entsprechend priorisiert vorgehen können. Denn für Betriebe mit hohen Verfügbarkeitsanforderungen sind andere Überlegungen wichtiger als für solche, bei denen das Thema Vertraulichkeit den höchsten Stellenwert hat.

„Unternehmen aus den im IT-Sicherheitsgesetz genannten Branchen sollten sich möglichst bald mit der Sicherheit ihrer Informationstechnik auseinandersetzen", ergänzt Alexander Häußler. „Denn sobald die Rechtsverordnung in Kraft tritt, haben sie nur sechs Monate Zeit, eine Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik zu benennen, und innerhalb von zwei Jahren müssen die definierten Mindeststandards umgesetzt sein."

Wer schon jetzt die Voraussetzungen für ein gesundes und nachhaltiges Management von Informationen schafft, kann den gesetzlichen Neuerungen gelassen entgegensehen. TÜV SÜD unterstützt Unternehmen dabei unter anderem mit Vor-Audits, durch die festgestellt werden kann, inwieweit die Anforderungen der ISO 27001 bereits umgesetzt sind oder welche Maßnahmen noch sinnvoll sind. Außerdem ist die Zertifizierung nach ISO 27001 möglich.

Weitere Informationen zu den Themen Datenschutz und Datensicherheit:
www.tuev-sued.de/ms/iso-27001

Carolin Eckert
www.tuev-sued.de

* *ISO/IEL 27001: Information technology – Security techniques – Information security management-systems – Requirements*

Vernetzte Medizinprodukte und IT-Sicherheit

Wer Medizingeräte entwickelt, die für den Datenaustausch mit anderen Geräten ausgelegt sind, muss neben den grundsätzlichen Anforderungen an Sicherheit und Funktion auch die regulatorischen und rechtlichen Anforderungen an den Datenaustausch und an IT-Netze an sich auf dem Schirm haben. TÜV SÜD hat die wichtigsten Informationen dazu in einer Med-Info zusammengefasst.

Sollen beispielsweise Röntgenbilder nach der Aufnahme direkt in eine digitale Patientenakte eingespielt werden, darf das in Deutschland nur nach Maßgabe des Datenschutzgesetzes und der Röntgenverordnung geschehen.

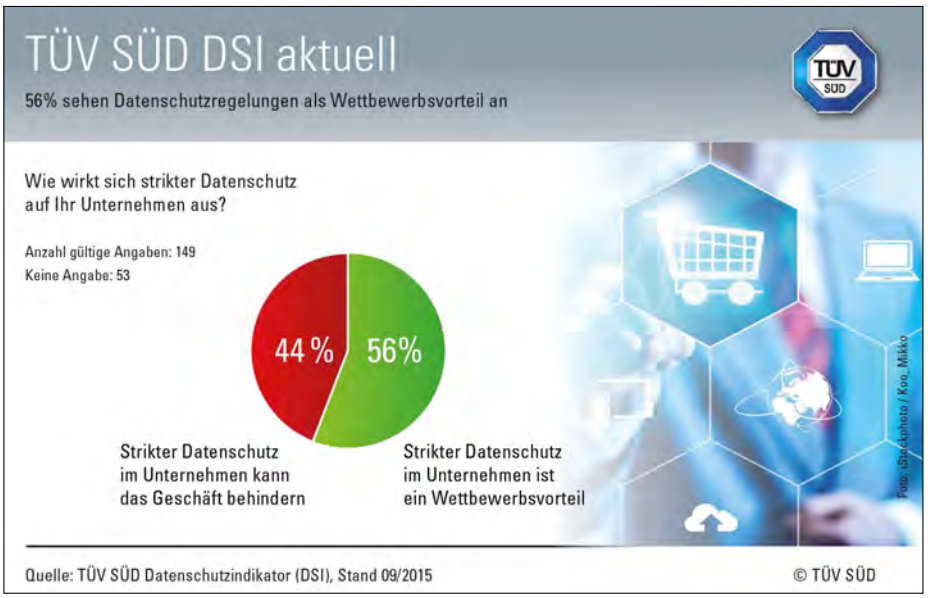
Solche und viele weitere Anforderungen an die IT-Sicherheit gehören von Anfang an als wesentlicher Bestandteil ins Risikomanagement für jedes Medizinprodukt, das mit einem programmierbaren elektrischen medizinischen System (PEMS) ausgestattet ist, das in das IT-Netzwerk Dritter integriert ist und dort von Dritten, also nicht vom Hersteller, bedient und kontrolliert wird.

Olaf Teichert
www.tuev-sued.de

TÜV SÜD DSI: Ein Großteil der Unternehmen setzt darauf, nicht kontrolliert zu werden

Ende Oktober kam eine interessante Pressemeldung aus München: Laut Paragraph 9 des Bundesdatenschutzgesetzes (BDSG) sind Unternehmen dazu verpflichtet, angemessene technische und organisatorische Maßnahmen zu treffen, um die gesetzlichen Vorschriften und Anforderungen zu gewährleisten. Dieses kann auch von der zuständigen Aufsichtsbehörde überprüft werden.

Doch der TÜV SÜD Datenschutzindikator (DSI) zeigte, dass ein Großteil der Befragten gar nicht damit rechnet, kontrolliert zu werden.



Die DSI-Ergebnisse zeigen, dass nur 25 Prozent der Befragten ihr Unternehmen in der Lage sehen, Anfragen von Aufsichtsbehörden zu Datenschutzmaßnahmen unmittelbar zu beantworten. „Wenn Unternehmen eine geforderte Auskunft aber nicht vollständig oder rechtzeitig erteilen, können Aufsichtsbehörden ein Bußgeld von bis zu 50.000 Euro verhängen“, erklärt Rainer Seidlitz von der TÜV SÜD Sec-IT GmbH.

Zudem geben fast 67 Prozent an, dass ein systematisches Vorgehen zum Umgang mit Datenschutzverletzungen in ihrem Unternehmen nicht näher definiert ist. Das BDSG verlangt jedoch, dass abhängig von der Art der Daten im Falle des Datenverlusts sowohl die Betroffenen, als auch die zuständige Aufsichtsbehörde unmittelbar zu informieren sind.

„Generell müssen Unternehmen bei Datenschutzverstößen schnell reagieren, um den Schaden wenigstens zu minimieren. Um die entsprechenden Maßnahmen unmittelbar in die Wege leiten zu können, ist es hilfreich, ein systematisches Vorgehen zu definieren, das verschiedene Stufen der Datenschutzverletzung berücksichtigt“, sagt Rainer Seidlitz. Findet eine solche Benachrichtigung nicht statt, und die Aufsichtsbehörde stößt bei einer Kontrolle auf dieses Versäumnis, müssen Unternehmen mit einem Bußgeld von bis zu 300.000 Euro rechnen.

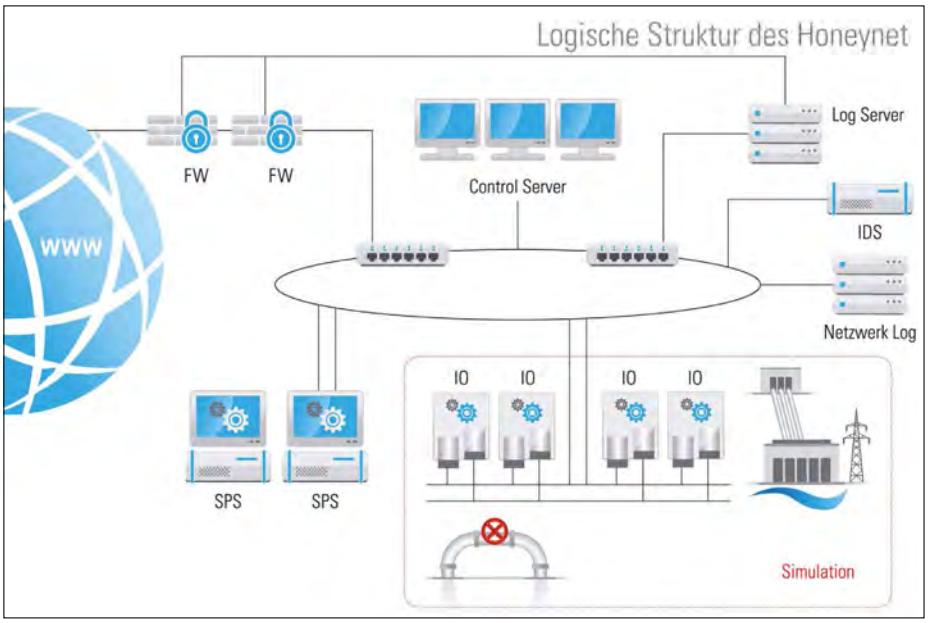
Immerhin sehen 56 Prozent der Teilnehmer an der Trendfrage strikte Datenschutzregelungen als Wettbewerbsvorteil an. Die Einsicht ist bei vielen Unternehmen also bereits da, nur an der Umsetzung muss noch gearbeitet werden.

Der TÜV SÜD DSI wurde im Juli 2014 von der TÜV SÜD Sec-IT GmbH, unterstützt durch die LMU München, vorgestellt. Unternehmen, die selbst prüfen möchten, wie gut sie in Sachen Datenschutz aufgestellt sind und an welchen Stellen Verbesserungspotenzial besteht, können am Test des TÜV SÜD DSI unter www.datenschutz-indikator.de teilnehmen.

Carolin Eckert
www.tuev-sued.de

Honeynet-Projekt – Potenzielle Angreifer lauern überall

Mehr als 60.000 Zugriffe auf eine virtuelle Infrastruktur verzeichnete TÜV SÜD in der achtmonatigen Laufzeit eines sogenannten Honeynet-Projekts, das reale Hardware und Software mit einer simulierten Umgebung eines kleineren Wasserwerks kombinierte. Die Zugriffe erfolgten von Servern aus der ganzen Welt und teilweise unter verschleierten IP-Adressen. Das Projekt zeigte, dass Infrastrukturen und Produktionsstätten gezielt ausgeforscht werden.



Lockvogel „Honeynet“

Die Industrie 4.0 stellt Unternehmen vor die Herausforderung, ihre Sicherheitsvorkehrungen grundsätzlich zu überdenken. Die zunehmende Digitalisierung und Vernetzung macht Infrastrukturen und Produktionsstätten anfälliger und schafft neue „Einfallstore“ für einen möglichen Missbrauch – von der Spionage bis zur Sabotage. Mit einem High-Interaction-Honeynet hat TÜV SÜD neue Erkenntnisse gewonnen, von denen Unternehmen aus unterschiedlichsten Branchen profitieren können.

Genaue Analyse von Zugriffs- und Angriffsaktionen

„Ein Honeynet ist ein System, das Angreifer anlocken und die Analyse der Zugriffs- und Angriffsaktionen ermöglichen soll“, sagt Dr. Armin Pfoh, Vice President im Bereich Strategie & Innovation von TÜV SÜD.

Für das aktuelle Projekt hatte TÜV SÜD ein Wasserwerk in einer deutschen Kleinstadt simuliert. „Zu diesem Zweck haben wir ein sogenanntes High-Interaction-Honeynet eingerichtet, das reale Hardware und Software mit einer simulierten Umgebung kombinierte“, erklärt Pfoh. Die Sicherheitsvorkehrungen entsprachen dem industrieüblichen Niveau.

Den praxisnahen Aufbau des Systems und die Sicherheitsvorkehrungen haben die TÜV SÜD-Experten zusammen mit Vertretern der Versorgungswirtschaft entwickelt und umgesetzt. Das Honeynet war insgesamt acht Monate im Netz. Der erste Zugriff erfolgte fast zeitgleich mit dem „Scharfschalten“. Während der Laufzeit verzeichnete der TÜV über 60.000 Zugriffe aus mehr als 150 Ländern (s. Grafik S. 12). „Damit konnten wir nachweisen, dass selbst eine relativ unbedeutende Infrastruktur im Netz wahrgenommen und ausgeforscht wird“, sagt Dr. Thomas Störtkuhl, Senior Security Experte und Teamleiter Industrial IT Security bei TÜV SÜD.

Die Top-3-Zugriffsländer nach IP-Adresse waren China, die USA und Südkorea, wobei die IP-Adressen allerdings keine belastungsfähige Aussage über den tatsächlichen Standort des Zugreifenden ermöglichen. Zudem erfolgten die Zugriffe zum Teil über verdeckte bzw. verschleierte IP-Adressen.

Interessant war auch die Erkenntnis, dass die Zugriffe nicht nur über Standardprotokolle der Büro-IT, sondern auch über Industrieprotokolle wie Modbus TCP oder S7Comm erfolgten.

„Die Zugriffe über Industrieprotokolle waren zwar deutlich seltener, kamen aber ebenfalls aus der ganzen Welt“, erklärt Störtkuhl. Damit ist für den Sicherheitsexperten klar, dass Lücken in der Sicherheitsarchitektur von Steuerungsanlagen entdeckt werden, und dass die Systeme für einen möglichen Angriff anfällig sind. Das kann entweder ein genereller Angriff auf bestimmte Strukturen und Devices oder ein gezielter Angriff auf ein ausgewähltes System sein.

Deutliches Warnsignal für Unternehmen

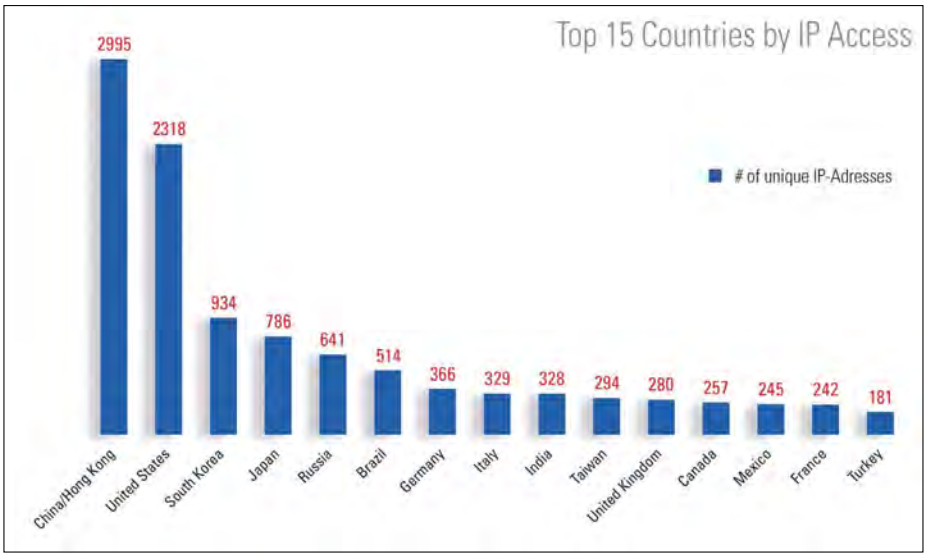
Die Ergebnisse des Honeynet-Projekts sind ein deutliches Warnsignal – nicht nur für die Betreiber von Infrastrukturen, sondern auch für produzierende Unternehmen. „Auch kleine oder unbekannte Firmen werden entdeckt oder gesehen, weil ständig Ausspäh-Aktionen im Internet laufen“, betont Störtkuhl.

Damit können diese Firmen zu Opfern einer Angriffswelle werden, auch wenn sie nicht gezielt ausgesucht wurden. Wenn Unternehmen durch Ausspäh-Aktionen erst einmal auf den Monitor von potenziellen Angreifern geraten sind, wird dadurch auch ein gezielter Angriff zu einem späteren Zeitpunkt erleichtert. Das zeigen auch die Angriffsversuche auf das TÜV SÜD-Honeynet, die über unterschiedliche Protokolle erfolgten. Dabei handelte es sich zum einen um eine weltweite Denial-of-Service-Attacke und zum anderen um zwei gezielte Angriffsversuche über zwei unterschiedliche Industrieprotokolle.

Monitoring ist Basis für Schutzmaßnahmen

Die wichtigsten Botschaften aus dem Honeynet-Projekt von TÜV SÜD: Infrastrukturen und Produktionsstätten werden kontinuierlich ausgeforscht. Das gilt selbst für ein relativ unbedeutendes Wasserwerk in einer deutschen Kleinstadt. Aus Zugriffen können Angriffe werden, die ein hohes Schadenspotenzial haben – von der Ausspähung von Betriebsgeheimnissen bis zur Sabotage einer kompletten Infrastruktur. Ohne die Anpassung ihrer Sicherheitsvorkehrungen fahren Unternehmen und Betreiber von Infrastrukturen ein hohes Risiko.

Ein gezieltes Monitoring ist Voraussetzung dafür, dass Unternehmen ihre Gefährdungslage realistisch einschätzen und wirkungsvolle Schutzmaßnahmen entwickeln können. Nach den Erfahrungen aus dem Honeynet-Projekt müsse das Monitoring zwingend auch Industrieprotokolle erfassen, weil potenzielle Angreifer diese Protokolle kennen und nutzen, sagt der TÜV SÜD.



Angriffe aufs Honeynet nach IP-Adressen

Dr. Thomas Oberst
www.tuev-sued.de

VDI Info: Statusreport „Regenerative Energien in Deutschland“

In seinem Statusreport „Statusreport 2015 Regenerative Energie in Deutschland“ von Ende Oktober zeigt der VDI den Stand der Technik und die sich abzeichnenden Tendenzen der regenerativen Energien auf.

Mit seinen Empfehlungen soll der Statusreport helfen, die politische Diskussion um das Für und Wider des regenerativen Energieangebots zu versachlichen und aus ingenieurtechnischer Sicht Hinweise zu geben, wo sich einerseits begrüßenswerte Entwicklungen abzeichnen und andererseits Tendenzen erkennen lassen, denen gegengesteuert werden muss.

Im Rahmen einer zukunftsfähigen Energieversorgung kommt den erneuerbaren Energien zwingend eine Schlüsselposition zu. Ihr Anteil im Wärmemarkt, bei der Stromerzeugung und im Verkehrsbereich wird steigen müssen, wenn die von der EU-Kommission und der Bundesregierung formulierten energie-, umwelt- und klimapolitischen Ziele – und damit die vielzitierte „Energiewende“ – erfolgreich erreicht werden sollen.

Die Nutzung regenerativer Energien hat in den letzten Jahren deutlich zugenommen. Die Strombereitstellung aus erneuerbaren Energien lag 2014 bei etwa 160,6 Terrawattstunden (TWh), das entspricht etwa 28 Prozent des Bruttostromverbrauchs. Dazu tragen die Windenergie 35 Prozent und die Bioenergie 31 Prozent bei. Die Fotovoltaik und die Wasserkraft haben einen Anteil von jeweils 22 Prozent.

Im Jahr 2014 wurden rund 471 Petajoule (PJ) an Wärme aus regenerativen Energien bereitgestellt, was 10 Prozent bezogen auf den Endenergieverbrauch (ohne Verkehr) an Brennstoffen entspricht. Dieser Beitrag wird nach wie vor überwiegend durch biogene Festbrennstoffe (87 Prozent) abgedeckt, gefolgt von Wärmepumpen und Solarthermie.

Der Fachausschuss „Regenerative Energien“ (FaRE) der VDI-Gesellschaft Energie und Umwelt (GEU) begleitet die Entwicklung der Nutzung des regenerativen Energieangebots in Deutschland und global seit vielen Jahren. Dazu behandelt er neben technischen, ökonomischen und ökologischen auch energie-, wirtschafts-, umwelt- und agrarpolitische sowie soziale Aspekte im Zusammenhang mit der Nutzung der erneuerbaren Energien als Teil des Energiesystems.

Der „Statusreport 2015 Regenerative Energien in Deutschland“ steht kostenfrei zum Download unter: www.vdi.de/fa-re.

Gegen eine Schutzgebühr von EUR 30,00 ist die gedruckte Version bei der VDI-Gesellschaft Energie und Umwelt erhältlich.
Telefon: +49 211 6214-415
Telefax: +49 211 6214-177
E-Mail: rufaut@vdi.de

Automation Security – Design, Implementierung und Betrieb sicherer Automatisierungssysteme

Moderne Automatisierungslösungen setzen in zunehmendem Maße offene und vernetzte Systemarchitekturen sowie Komponenten der Standard-IT ein – häufig sogar mit direkter oder indirekter Verbindung zum Internet. Solche Automatisierungslösungen sind dann den gleichen Bedrohungen durch Hacker und sogenannte Cyber Attacken ausgesetzt.

Die für die Standard-IT bekannten Angriffe, Fehler etc. wirken sich damit auch im Produktionsumfeld aus. Oft sind die Risiken für die Automatisierungstechnik sogar deutlich höher, da die typischen IT Security Maßnahmen aus der Office IT im produktionsnahen Umfeld in der Regel nicht umsetzbar sind. Zusätzlich sind mögliche Auswirkungen von Ereignissen meist weitreichender, da es neben dem wirtschaftlichen Schaden z. B. durch Datenverluste auch zu unmittelbaren in den Produktionsanlagen selbst bis hin zur Beeinträchtigung der funktionalen Sicherheit kommen kann.

Offensichtliche und zielgerichtete Angriffe auf Produktionsanlagen haben in den letzten Jahren zugenommen. Dies zeigen beispielsweise prominente Vorfälle wie „Stuxnet" oder der erfolgreiche Angriff auf ein Stahlwerk in Deutschland, die jeweils einen erheblichen Schaden, sowohl durch den Produktionsausfall, als auch durch mechanische Schäden in Anlagenteilen zur Folge hatten.

Damit wachsen die Bedeutung und die Anforderungen an Automation Security in den letzten Jahren in der Prozessautomatisierung kontinuierlich. Und auch das Bewusstsein, dass Schwachstellen und Angriffe aus der IT Auswirkungen auf die in der Produktion eingesetzten Anwendungen haben können, ist bei Betreibern von Produktionsanlagen mehr in den Mittelpunkt gerückt.

NAMUR* definiert Anforderungen an zukünftige Systeme und Lösungen

Bei Security Konzepten in der Office-IT stehen meist die Schutzziele Vertraulichkeit und Integrität im Mittelpunkt, um so Informationen und gegebenenfalls auch Systeme vor allem gegen unerlaubten Zugriff zu schützen. Im Gegensatz hierzu rücken im Umfeld der Produktion und Automatisierung jedoch die Verfügbarkeit der Produktionsanlage und vor allem die Zuverlässigkeit der eingesetzten automatisierungstechnischen Einrichtungen in den Vordergrund.

IT-Security spielt in der Prozessautomatisierung eine große Rolle.

Heute werden technische IT-Security-Maßnahmen in der Regel zusätzlich in automatisierungstechnische Systeme und Komponenten eingebaut. Dies erfordert weitreichendes Expertenwissen und führt zur Erhöhung der Komplexität von Automatisierungslösungen, die immer schwerer beherrschbar wird. Vor allem auch der wirkungsvolle Betrieb dieser Zusatzmaßnahmen wie Virenscanner, Firewalls etc. oder auch die Etablierung eines kontinuierlichen Patch-Managements ist im laufenden Betrieb nur mit erheblichen Aufwand und oft auch mit zusätzlichen Risiken möglich, da Automatisierungssysteme in der Prozessindustrie meist kontinuierlich und ohne den erforderlichen Neustart betrieben werden.

Die Anwender investieren derzeit sehr viel, um ihre Produktionsanlagen abzusichern. Dennoch sieht man, dass die verfügbaren Ansätze oft nicht ausreichen und viel zu aufwändig sind. Um dem langfristig zu begegnen, hat die NAMUR – gemeinsam mit dem Zentralverband Elektrotechnik und Elektroindustrie (ZVEI), dem Bundesamt für Informationssicherheit (BSI) und dem Institut für angewandte Informatik in Karlsruhe (IAI) – einige grundsätzliche Anforderungen für zukünftige Automatisierungslösungen in der neuen NAMUR Empfehlung NE 153 „Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme" definiert. Diese können im Kern wie folgt zusammengefasst werden: IT-Security Konzepte müssen zukünftig ein integraler Bestandteil im Funktionsumfang automationstechnischer Komponenten und Lösungen sein.

Innovative Sicherheitstechnologien

Von Seiten der Anwender besteht die Erwartungshaltung, dass innovative Sicherheitstechnologien und -konzepte frühzeitig auf ihre Anwendbarkeit in der Automatisierungstechnik geprüft und in neue Produkte integriert werden. Einige der Anforderungen sind schon heute umsetzbar. Andere spiegeln die Erwartungen an eine zukünftige Generation von Automatisierungslösungen wider und zeigen so neue oder erweiterte Handlungsfelder für Forschung und Entwicklung – auch in der konventionellen IT – auf.

Damit besteht die Chance, die Komplexität von Automatisierungslösungen erheblich zu reduzieren, da zukünftig die IT-Sicherheit ein grundlegendes Designziel beim Entwurf und der Entwicklung neuer Systeme und Lösungen wird. Dabei ist die enge Zusammenarbeit zwischen Herstellern, Anwendern, Forschung und Politik ein entscheidender Erfolgsfaktor.

Auch die mittlerweile langjährige und aktive Beteiligung in nationalen und internationalen Normungsgremien ist eine wichtige Grundlage für die breite Akzeptanz der Forderungen der NAMUR, denn IT Sicherheit in der Automation kann nur gelingen, wenn alle Beteiligten an einem Strang ziehen.

** Interessengemeinschaft Automatisierungstechnik und Prozessindustrie*

BASF
We create chemistry
Martin Schwibach
BASF SE Ludwigshafen
www.basf.com

Vulnerability Management – „Verwundbarkeitsmanagement“

Angriffe von Hackern, Computerbetrug, ausgespähte, gestohlene und abgefangene Daten gehören heute zum Alltag vieler Unternehmen, hinzu kommt der Verrat von Geschäfts- und Betriebsgeheimnissen. Diese und andere Ausprägungen von Computer-Kriminalität treffen Unternehmen aller Branchen. Informationen sowie Daten sind heute ein wesentlicher Erfolgsfaktor. Sie zu schützen, wird allerdings immer schwieriger aufgrund veränderter Infrastruktur, zum Beispiel durch Cloud- und Mobile Computing oder Transformationen wie die Vernetzung von Geschäftsprozessen.

Neben der Umsetzung von rechtlichen Anforderungen u. a. des Datenschutzes von Kunden, Lieferanten und Mitarbeitern, unternimmt Daimler Buses vielfältige Anstrengungen die „intellectual property“ wie zum Beispiel der Entwicklungsinnovationen und strategische Weiterentwicklung des Unternehmens zu schützen.

In Zeiten der zunehmenden Vernetzung wird auch die Bedrohung durch Hacker, die nicht nur Daten stehlen, sondern auch die Kontrolle über Geräte übernehmen, immer größer.

Eine der gängigen Methoden, um die Gefahr zu reduzieren, durch Malware angegriffen zu werden, sind regelmäßige Netzwerkaudits, um Verwundbarkeit zu identifizieren und die Schwächen zu korrigieren, bevor sie ausgenutzt werden können. Vulnerability Management erlaubt es dem Unternehmen, proaktiv potenziell gefährdete Geräte zu entdecken und sicherzustellen, dass Systeme in Übereinstimmung mit Richtlinien und spezifischen Vorgaben konfiguriert werden. Vulnerability Management ist ein Set von Prozessen und Technologien, die es Unternehmen ermöglichen, eine „Basislinie“ der Sicherheitskonfiguration zu definieren und aufrechtzuerhalten, Verwundbarkeiten zu priorisieren und zu lindern, Sicherheitssteuerungen zu implementieren, Einhaltung innerer und äußerlicher Voraussetzungen zu bewerten sowie die Quelle von Sicherheitsdrohungen zu identifizieren und das System zu härten.

Vulnerability Management ist viel mehr als einfach „scannen und berichten“. Um es als ein proaktives Mittel zur Senkung von Risiken erfolgreich zu verwenden, können Prozesse, die das Vulnerability Management Programm unterstützen so wichtig sein, wie die Technologie, die genutzt wird, um Sicherheitsdrohungen zu minimieren.

Lifecycle

Vorteile des Vulnerability Management

- Lieferanten- und produktunabhängige Bewertung von aktuellen IT-Risiken
- Vollständiges Überprüfen der IT-Landschaft und Entdeckung von unbekannten Geräten
- Basis für Vorschriften und für Entscheidungen in Notsituationen
- Einhaltung interner und externer Richtlinien und Vorschriften
- Bedrohungsverminderung durch frühes Aufdecken und Einleitung entsprechender Abhilfemaßnahmen
- Genaue und immer aktuelle Verwundbarkeitsaudits
- Umfassender Bericht, um die Effekte von Sicherheitsinvestitionen und Tätigkeiten zu messen und sich zu vergegenwärtigen
- Priorisierung der vorhandenen Verwundbarkeiten und erforderlichen Abhilfemaßnahmen
- Unterstützung und Überwachung von Patchprozessen
- Umfassende Wissensbasis, um Verwundbarkeit zu lindern
- Sichtbarer Nachweis der Wirksamkeit von Informationssicherheitsanstrengungen

Darüber hinaus werden eine Reihe von flankierenden Maßnahmen ergriffen. So wird zum Beispiel der Schutzbedarf der Daten über Informationsklassifizierungen dokumentiert. Die erforderlichen Schutzmaßnahmen werden entsprechend eines gestuften Sicherheitskonzeptes technisch und organisatorisch umgesetzt.

IT-Systeme werden unter Gesichtspunkten der Informationssicherheit konzipiert und konfiguriert. Vor Inbetriebnahme erfolgen Überprüfungen auf Schwachstellen bezüglich Informationssicherheit und Datenschutz.

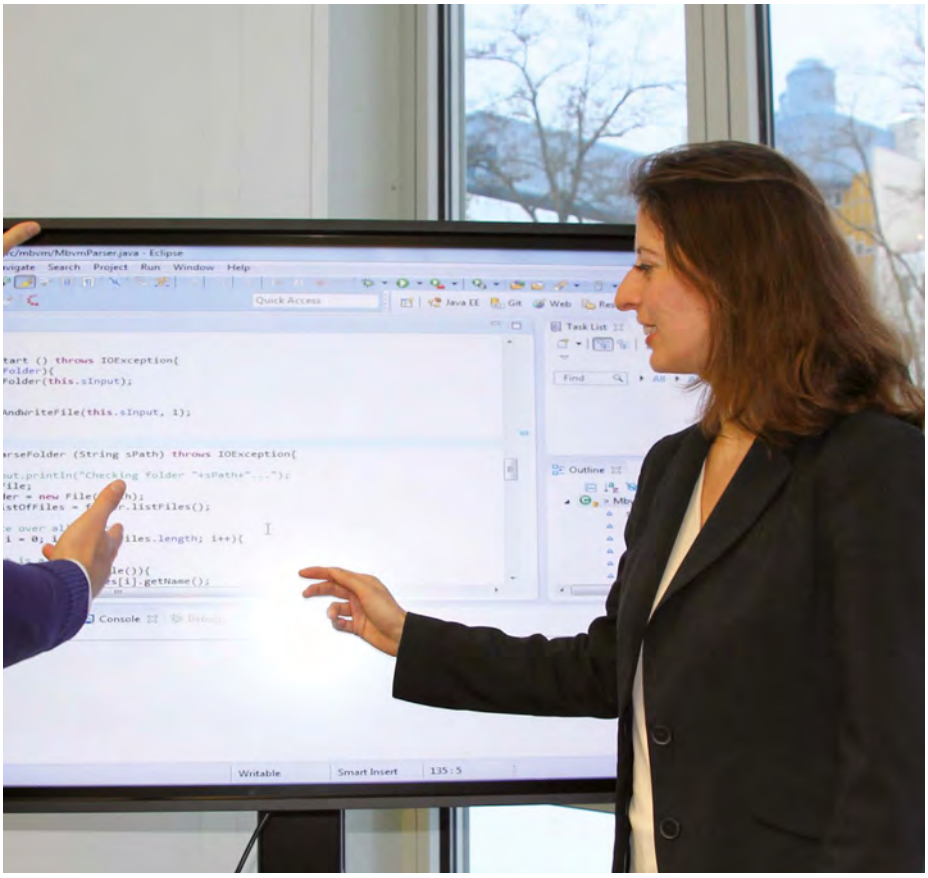
Unterstützt werden die vielfältigen Anstrengungen durch Security Audits gem. ISO/IEC 27001. Hierin sind die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation spezifiziert.

EvoBus
Bernhard Webersinn
EvoBus GmbH
www.evobus.com

Intelligente Datenanalytik mit garantierter Privatsphäre – Datenschutzregeln

Siemens entwickelt Werkzeuge, die in großen Datenmengen den Datenschutz gewährleisten. Der verlässliche Schutz der Privatsphäre in den Daten ist hier eine wichtige Voraussetzung, denn nur dann sind Menschen oder Institutionen bereit, ihre Daten solchen Anwendungen zur Verfügung zu stellen.

Zusammen mit dem Fraunhofer Institut für intelligente Analyse- und Informationssysteme (Fraunhofer IAIS) arbeiten Wissenschaftler der globalen Siemens-Forschung Corporate Technology (CT) an einem Werkzeugkasten, der den Nutzern von Smart Data hilft, die für ihre Anwendung definierten Datenschutz-Regeln umzusetzen. Zwar gibt es verschiedenste Algorithmen zur Anonymisierung von Daten, aber viele sind nicht auf die für Smart Data typischen Software-Umgebungen zugeschnitten. Die neue Toolbox soll eine Auswahl an Algorithmen für solche Umgebungen zur Verfügung stellen.



Keine Sicherheit ohne Datenanalyse

Smart Data-Analyse: Analyse großer Datensätze

Smart Data, also die intelligente Analyse riesiger Datensätze, stellt neue Anforderungen an den Datenschutz. Es geht nicht mehr nur um persönliche Daten aus einer Quelle. Man muss auch verhindern, dass Personen durch die Kombination von Datensätzen identifizierbar werden. Wie die Privatsphäre gewährleistet wird, hängt von der jeweiligen Anwendung ab. Im einfachsten Fall reicht es, einzelne Merkmale aus dem Datensatz zu entfernen. In anderen Fällen werden bestimmte Informationen generalisiert, also etwa das Alter von Personen in Bereiche zusammengefasst. Oder die Namen werden so verschlüsselt, dass sie nicht mehr als Klartext erkennbar, aber noch eindeutig sind. Es gibt auch Algorithmen, die garantieren, dass die Abfrage größerer Datensätze immer eine bestimmte Mindestanzahl an Treffern ergibt. So verhindert man zum Beispiel, dass bei der Analyse medizinischer Datensätze einzelne Personen und ihre Krankheit identifiziert werden können.

Die sogenannte Privacy Preserving Big Data Analytics Toolbox wird Algorithmen für verschiedenste Anonymisierungsverfahren enthalten. Eine wichtige Anforderung ist die schnelle Verarbeitung riesiger Datenmengen. Dafür müssen die Algorithmen die für Smart Data typischen Datenbankarchitekturen nutzen und große Datensätze parallel verarbeiten können. Um dies zu garantieren, adaptieren die Forscher die in der Toolbox enthaltenen Algorithmen an die gebräuchlichen Systeme wie Hadoop und massiv parallele Datenbanken.

Originaldaten nicht mehr rekonstruierbar

Die Toolbox wird entweder zum Einlesen von Daten eingesetzt, so dass die Informationen direkt anonymisiert abgespeichert werden. Oder man nutzt sie zur nachträglichen Verarbeitung bereits gespeicherter Daten. Die Originaldaten können nach der Anonymisierung nicht mehr rekonstruiert werden.

Siemens CT entwickelt die Toolbox in enger Verzahnung mit Konzern-Bereichen, die verstärkt auf Smart Data Anwendungen setzen. Dazu gehört zum Beispiel Siemens Healthcare, wo die Zusammenführung von Daten aus bildgebenden Verfahren wie Computer- oder Magnetresonanztomographie den technischen Service oder die Entwicklung von Diagnosesoftware unterstützt. Ein anderes Anwendungsfeld sind Smart Cities, also Städte mit intelligenten Steuerungssystemen beispielsweise für Verkehr oder Energieversorgung.

SIEMENS
Dr. Norbert Aschenbrenner
www.siemens.de

VDE-Positionspapier – Smart Grid Security

Im Dezember 2014 veröffentlichte der VDE das Positionspapier „Smart Grid Security Energieinformationsnetze und -systeme" und griff damit ein sehr aktuelles Thema auf. Die benötigte Funktionalität von Smart Grid ist ohne Informationsaustausch nicht möglich. Für diesen Informationsfluss werden vorhandene Kommunikationseinrichtungen wie das Internet genutzt. Diese Systeme bieten allein durch ihre Existenz schon gewaltige Vorteile. Bezüglich Datensicherheit der mit der Anwendung einhergehenden Verfügbarkeitsanforderungen für elektrische Energie erhält die IT-Sicherheit einen besonders hohen Stellenwert.

Nachfolgend sind Auszüge – Management Summary und die Einleitung – aus dem Positionspapier abgedruckt, die einen ersten Einblick in das Papier geben sollen und dieses als wertvolle Informationsquelle aufzeigen. Das Positionspapier ist im Internet für VDE-Mitglieder kostenlos downloadbar unter: https://www.vde.com/de/InfoCenter

Management Summary

Das elektrische Energieversorgungssystem durchläuft gegenwärtig eine Transformation zu einem Energiesystem mit dem Vorrang an erneuerbaren, volatilen Energien sowie den Trends zu einer lastfernen und im hohen Maße zunehmend dezentralen Erzeugung.

Hierdurch ergeben sich Veränderungen im Netz und in der Netztopologie, die u.a. dadurch gekennzeichnet sind, dass die Prozessdatenverarbeitung (PDV) und die Bürokommunikation (IT) schleichend mehr und mehr zusammenwachsen (auch als OT/IT-Integration bezeichnet). Des Weiteren sind Prozesssteuerungssysteme dezentraler Anlagen zunehmend über das Internet erreich- und konfigurierbar. Hierdurch ergeben sich neue Bedrohungsszenarien, die es bis dato nicht gab, auf die jedoch zukünftig reagiert werden muss.

Das Positionspapier beleuchtet zunächst neue Sicherheitsziele und Sicherheitsanforderungen, die sich in Folge der Markt- und Netzintegration und der zunehmenden OT/IT-Integration ergeben. Anschließend werden Angreifermodelle und Schutzmaßnahmen erläutert; ferner werden Test und Testverfahren vorgestellt, mittels denen man eine Sicherheitsevaluierung von Energieinformationsnetzen vornehmen kann. Aufbauend darauf werden die aktuell diskutierten Smart Grid Topologien betrachtet und Design-Empfehlungen für Sicherheitssysteme, einerseits für bestehende historisch gewachsene Architekturen, andererseits für den Entwurf neuer Architekturen, vorgestellt; denn Sicherheitsaspekte müssen beim Entwurf neuer Systeme essenzieller Bestandteil der Topologie sein.

Abschließend werden spezifische Handlungsempfehlungen für Politik, Standardisierung, Energieversorger, Hersteller und Wissenschaft/Forschung zum Aufbau sicherer IKT-Infrastrukturen (Informations- und Kommunikationstechniken) für die Energieversorgungssysteme vorgestellt.

Einleitung

Das bisherige fossile und nukleare Energiesystem wurde insbesondere durch die zentralisierte Energiegewinnung sowie zentralisierte Steuerungsmechanismen und Systemverantwortung bestimmt. Daraus resultierte die gute Planbarkeit der Erzeugung. Das Verteilungsnetz stellte die benötigte Energie den Kunden unidirektional bereit, wobei der Kunde selbst im System eine passive Rolle spielte.

Um die ökologischen und energiepolitischen Ziele erfolgreich umzusetzen, gilt es nun, die Säulen eines neuen Gesamtkonzeptes zu bestimmen. Ihre Tragkraft basiert auf dem Gedanken, dass die Energiewende nicht nur als Pflicht und unter Kostenaspekten betrachtet werden sollte, sondern sich aus diesem historischen Prozess neue Chancen für die zukünftige Wirtschaftskraft des Landes ergeben. Diese neuen Chancen für vielfältige Beteiligte werden durch die Erschließung von Energiepotenzialen aus zentralen Lagen sowie auch die Erschließung dezentraler Erzeugungs- und Speicherpotenziale bei Bürgern und Unternehmen sowie Kommunen und Regionen eröffnet.

Die Teilnehmer am Energienetz als Erzeuger sowie als Verbraucher und damit als sogenannte Prosumenten wachsen in eine aktive Rolle, womit die Wertschöpfung in den Regionen gestärkt wird. Ein daraus resultierender wachsender Grad an Partizipation am Energiesystem mit regionalen Ausgleich- und Austauschmechanismen wiederum führt zu einer zunehmenden Vielfalt von Energieflüssen unterschiedlichster Quellen und Energieträgerarten in der Verbindung von Strom, Wärme, Gas sowie den Treibstoffen des Verkehrs. Die zentrale Erzeugung wird zunehmend durch die dezentrale Erzeugung ergänzt, wodurch bidirektionale Energieflüsse entstehen, die neue Prozesse und Formen der Organisiertheit erfordern. Erneuerbare Energien bringen aber auch eine zunehmende Volatilität der Erzeugung in das Gesamtsystem, womit die Planbarkeit abnimmt und neue Prognosemethoden erforderlich sind.

Datenschutz bei Versorgungssicherheit

Dabei wird eine hohe Versorgungssicherheit weder allein durch ein zentralisiertes System, noch durch regionale Egoismen entstehen. Ein zellularer Ansatz unterstützt dabei, die zunehmende Komplexität der Systemführung zu beherrschen, Subsidiarität und globale Verbundenheit zu vereinen sowie Sicherheit und Datenschutz im Gesamtsystem zu erhöhen. Die Komplexitätsbeherrschung gelingt dabei insbesondere durch neue Markt- und Netzfunktionen zur Flexibilisierung des Gesamtsystems im Rahmen eines Ampelmodells. Dabei werden rein marktbasierte Funktionen dem Grünbereich, die Priorität von Netzfunktionen im Störungsfalle dem Rotbereich und Abstimmungen zwischen Markt und Netz dem Gelbbereich zugeordnet.

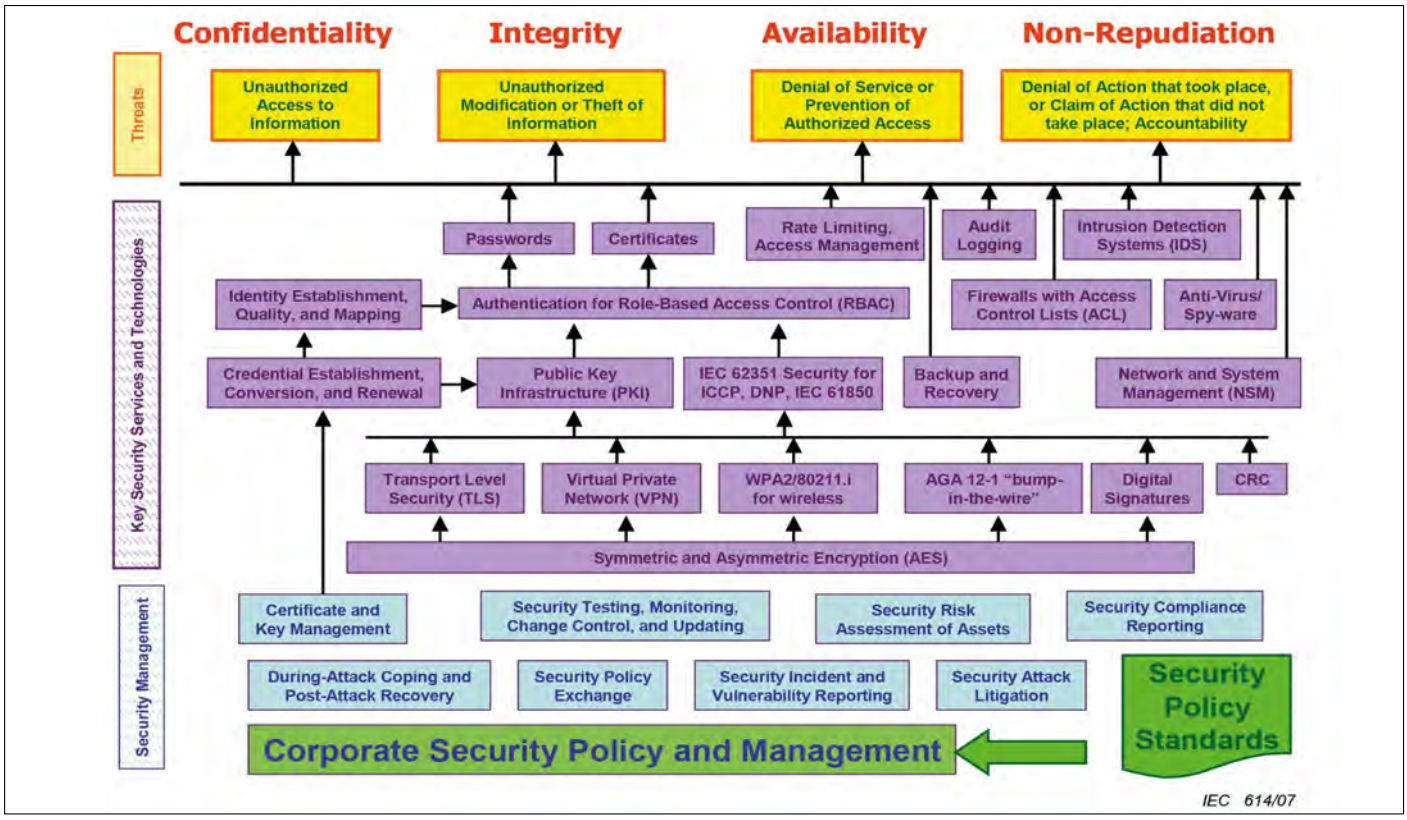


Abbildung 15 des Positionspapiers: „Sicherheitsanforderungen, Bedrohungen, Gegenmaßnahmen und Management" (Quelle: IEC 62351-1)

Neue Energieaggregationsfunktionen für Mengen von Kleinanlagen, neue Flexibilitäts- und Netzunterstützungsfunktionen umfassen dabei Demand-Response-Verfahren zur anreizbasierten Verbrauchssteuerung, die Marktintegration erneuerbarer, dezentraler Energien in virtuelle Kraftwerke, neue Systemdienstleistungen im Verteilungsnetz in Interaktion mit Liegenschaften, neue Formen der dezentralen, automatisierten Regelung im Verteilungsnetz sowie neue Energiedienstleistungen (smart Metering, Anlagen-Contracting usw.).

Informationssicherheit

Für Teile dieser Funktionen wird eine gemeinsame IKT-Infrastruktur im Smart Grid als Voraussetzung benötigt. Wer sollte die Erweiterung der notwendigen IKT-Infrastruktur für neue Markt- und Netzmechanismen vornehmen? Die Vielzahl der Ak-teure und der Komponenten in einem komplexen, vernetzten sowie zentral und dezentral verbundenen System erfordert das Vorantreiben einer standardisierten Kommunikation sowie die Gewährleistung von Informationssicherheit und Datenschutz. Die dafür notwendige IKT-Infrastruktur vernetzt eine kritische Infrastruktur. Um die Versorgungssicherheit in gewohnter Weise auch unter den neuen Bedingungen zu erhalten, sollte die IKT-Infrastruktur durch einen verantwortlichen Akteur, wie den Verteilungsnetzbetreiber (VnB) als Betreiber einer intelligenten Energieinfrastruktur, gestaltet werden, wobei dies Dienstleister für die VnBs umsetzen können. Gemeinsame, diskriminierungsfrei bereitgestellte Smart-Grid-Infrastrukturen aus elektrotechnischer und informationstechnischer Vernetzung verbessern dabei gleichzeitig die Wirtschaftlichkeit von Geschäftsmodellen verschiedener Marktakteure.

Vernetzung von Energiekomponenten

Zusätzlich sind die durch die Transformation des Energiesystems entstehenden neuen Möglichkeiten des Energiemarktes in Verbindung mit dem Einsatz von IKT-Technologien zur Vernetzung der Energiekomponenten (Erzeuger, Speicher, Verbraucher) von Marktakteuren im Smart Grid hochrelevant. Dafür wurde auch der Begriff „Smart Market" geprägt. Dies umfasst ebenso neue Marktmechanismen zur Aggregation der Energiemengen vielfältiger, dezentraler Energieanlagen sowie auch das Angebot von Leistungsflexibilitäten in der Erzeugung, in der Speicherung und in der Nutzung von Energie verschiedener Energieträger (Elektrizität, Gas, Wärme, Verkehr) sowie neuartige Dienstleistungen, die durch die Informationen und die Vernetzung im Smart Grid verfügbar werden. Ein Beispiel für eine mögliche Dienstleistung besteht darin, die Energieeffizienzpotenziale in Haushalten automatisiert ständig zu bewerten und diese wirtschaftlich zu nutzen.

Im Rahmen dieser Marktpotenziale entstehen somit auch völlig neue Fragestellungen und Herausforderungen bezüglich der Daten, die einerseits für die Schaffung von Marktchancen zur Verfügung gestellt werden, jedoch andererseits aufgrund ihres Personenbezugs oder ihrer Kritikalität eines besonderen Schutzniveaus bedürfen. Hier sind aktuell neben der Nutzerakzeptanz auch rechtliche Grundsätze zu betrachten, da diese eine Weitergabe von Nutzerdaten aufgrund von Paragraf 9 abs. 1 EnWG verbieten. Um die Weiterverarbeitung dieser Daten trotzdem zu ermöglichen, ist zunächst eine Bewertung der Daten in Bezug auf deren Kritikalität (Gefahr für die Energieinfrastruktur

an sich) und Personenbezug (Gefahr für den Datenschutz und rechtliche Konsequenzen) unerlässlich. Danach müssen neuartige Bewertungs- und Anonymisierungsmethoden untersucht werden, die als Ausgangspunkt die Offenlegung der Daten auf eine „nicht diskriminierende Weise“ (gemäß Paragraf 9 abs. 2 EnWG) ermöglichen.

Darüber hinaus stellt der Schutz der Privatsphäre eine wesentliche Voraussetzung für die Übertragung von energiebezogenen Daten dar. Mit Hilfe von Smart Metern können detaillierte Verbrauchsinformationen gesammelt und zu individuellen Verbrauchsprofilen zusammengesetzt werden. Die Erfassung und Verarbeitung dieser personenbezogenen Daten muss im Sinne der informationellen Selbstbestimmung für den Verbraucher transparent, durch ihn freizugeben und sperrbar sowie kontrollierbar sein.

Neuartige Bedrohungsszenarien

Durch die Einführung von Informations- und Kommunikationstechnologie in der Stromversorgung entstehen auch neuartige Bedrohungsszenarien. Die Kommunikation im Smart Grid, die in einem Energieinformationsnetz stattfindet, muss neben Dienstgüteanforderungen vor allem Anforderungen im Bereich der IT-Sicherheit und Widerstandsfähigkeit erfüllen. Da es sich bei Energienetzen um kritische Infrastrukturen handelt, werden auch Fragen der funktionalen Sicherheit aufgeworfen.

Angriffe auf Energieinformationssysteme oder Ausfälle von Kommunikationssystemen und wesentlicher Systemfunktionen können zu Stromausfällen führen und stellen damit eine akute Gefahr für Unternehmen sowie öffentliche Einrichtungen dar. Längerfristige Störfälle können die gesamte Versorgungsinfrastruktur und in weiterer Konsequenz auch Leib und Leben bedrohen. Durch eine mögliche Verflechtung zwischen Energie- und IT-Systemen im Rahmen des Smart Grids entsteht eine gegenseitige Abhängigkeit dieser beiden Netze, die im Falle eines großflächigen Stromausfalls zu erheblichen Problemen führen kann.

Das Szenario einer Wiederinbetriebnahme dieses Systems, als Schwarzstart bezeichnet, ist allein aufgrund der komplexen Abhängigkeiten im heutigen Stromnetz schon eine Herausforderung. Im zukünftigen Energiesystem stellt sich durch die Durchdringung mit IT-Systemen bis in den Niederspannungsbereich und hin zu Millionen von Liegenschaften eine nochmals größere Herausforderung. Nicht zuletzt spielt natürlich auch die Akzeptanz seitens der Verbraucher eine wichtige Rolle, die von der Benutzbarkeit, der Zuverlässigkeit und der Sicherheit der Smart Grid Technologien abhängt. Ein zukünftiges Smart Grid muss all diesen Herausforderungen gerecht werden. Durch seine Rolle als kritische Infrastruktur spielt dabei die Sicherheit eine wesentliche Rolle. Es ist daher notwendig, einerseits geeignete Sicherheitsanforderungen zu formulieren und andererseits neue Konzepte und Schutzmaßnahmen zur Absicherung dieser Infrastruktur zu entwickeln.

Titelbild des VDE-Positionspapier „Smart Grid Security“
Siemens/Grafik: Markus Kellermann Graphik-Design, Schwielowsee-Caputh

VDE Positionspapier

Zur Betrachtung dieser Themen wurde das Positionspapier folgendermaßen gegliedert. In Kapitel 2 werden die Infrastruktur und die fachlichen Besonderheiten des erweiterten Energieinformationsnetzes und -systems detailliert beschrieben. Kapitel 3 beschäftigt sich mit den Sicherheitszielen und Sicherheitsanforderungen in Folge der Markt- und Netzintegration erneuerbarer Energien und schafft den Übergang zu den folgenden Kapiteln. Wichtige Aspekte, die bei den Sicherheitsanforderungen berücksichtigt werden müssen, stellen sowohl der Schutz der Prosumenten, der Marktakteure und ihrer Komponenten im Energiesystem sowie der Infrastruktur selbst dar. Kapitel 4 erläutert im Anschluss Sicherheitsmaßnahmen im erweiterten Energieinformationssystem. Dabei werden zunächst Sicherheitsziele und Angreifermodelle gegenübergestellt, bevor nachfolgend Schutzmaßnahmen erläutert werden. In Kapitel 5 werden die aktuell diskutierten Smart-Grid-Topologien betrachtet. Unterschieden wird zwischen zentral geführten und dezentralen/zellularen Systemen. Weitere in diesem Kapitel abgedeckte Themen beinhalten Kommunikationstechnologien sowie deren Sicherheits- und Zugriffsverfahren. Kapitel 6 entwickelt aus den zuvor diskutierten Technologien und Ansätzen aktuelle Empfehlungen und zieht das Fazit für ein sicheres Energieinformationsnetz und -system als gemeinsame Grundlage im Smart Grid.

VDE
Ernst-Dieter Keller
VDE Kurpfalz

Freudenberg investiert in Kaiserslautern – Vliesstoffspezialist weiht Versuchsanlage ein

Spinnvliesstoffe, die die Freudenberg Gruppe am Standort Kaiserslautern produziert, kommen in einer Vielzahl von Anwendungen und Märkten zum Einsatz: In Teppichen für den Autoinnenraum, in Teppichbahnen für Gebäude, in Innenraumfiltern für Kraftfahrzeuge oder in Allergiker geeigneten Encasings für Bettwaren. Freudenberg entwickelt seine Herstellverfahren für Spinnvlies am Standort Kaiserslautern ständig weiter. Das globale Kompetenzzentrum weihte Anfang September eine Versuchsanlage ein. Die Investition beträgt rund drei Millionen Euro.

Dr. Frank Heislitz, CTO Freudenberg Performance Materials (l.), und Dr. Volker Röhring, Manager Process Development Freudenberg Performance Materials, weihten die Versuchsanlage ein.

Neue Verfahren werden zunächst an Versuchsanlagen entwickelt und getestet, bevor sie auf Produktionsanlagen übertragen werden. Mit der jetzt eingeweihten Versuchsanlage führt Freudenberg ein aktuelles Innovationsprojekt in die nächste Entwicklungsstufe. „Wir stellen Spinnvliesstoff mit unserem selbst entwickelten und patentierten Verfahren her, das bedeutende Vorteile gegenüber Konkurrenztechnologien hat“, sagt Michael Ehret, Head of Operations Regional Business Unit Europe Freudenberg Performance Materials und Werksleiter Kaiserslautern. Zu den Vorteilen gehören maßgeschneiderte Produkte, gleichmäßige Qualität und hohe Produktivität.

„Die Inbetriebnahme der Versuchsanlage ermöglicht es uns, völlig neue Anwendungsfelder zu erschließen und weitere innovative Produkte für individuelle Kundenbedürfnisse herzustellen“, sagt Dr. Volker Röhring, Manager Process Development Freudenberg Performance Materials. Die Anlage wird mit der bestehenden Belegschaft betrieben.

Das Spinnvliesverfahren

Beim Spinnvliesverfahren werden Polymer-Granulate wie Polypropylen, Polyester, Polylactid und Polyethylen geschmolzen. Durch Spinndüsen hindurch wird die Polymermasse zu haarfeinen, aber sehr festen Endlosfasern gesponnen. Diese werden als Flächengebilde auf einem Transportband abgelegt und mithilfe von Druck und Wärme zu einem Spinnvliesstoff verfestigt. Schließlich wird der Spinnvliesstoff aufgerollt und kann für die unterschiedlichen Anwendungen weiter verarbeitet beziehungsweise veredelt werden.

Freudenberg Performance Materials produziert, entwickelt und vermarktet von Kaiserslautern aus Polyester, Polypropylen und Biko-Feinfilament Spinnvliesstoffe.

Der Standort Kaiserslautern

Am Standort Kaiserslautern produziert, entwickelt und vermarktet die Geschäftsgruppe Freudenberg Performance Materials Spinnvliesstoffe für die Automobil-, die Bau-, die Filter- und die Teppichindustrie. Der Standort Kaiserslautern wurde im Jahr 1970 gegründet. Neben Freudenberg Performance Materials sind auch die beiden Geschäftsgruppen Freudenberg Filtration Technologies und Freudenberg Medical vertreten. Zum 1. Januar 2015 beschäftigte Freudenberg in Kaiserslautern 630 Mitarbeiter.

FREUDENBERG
INNOVATING TOGETHER

Jens Zillmann
www.freudenberg.com
Fotos: Freudenberg

40 Jahre Duales Studium bei Mercedes Benz am Standort Mannheim

Dieses besondere Jubiläum würdigten Ende September Vertreter der Daimler AG, der Arbeitnehmer, der Dualen Hochschule Baden-Württemberg (DHBW) und der Stadt Mannheim. Dabei wurde eines klar: Das duale Studium ist ein echtes Erfolgsmodell.

„Das duale Studium bietet mit seiner Mischung aus Theorie und Praxis sowohl Studierenden als auch Unternehmen große Vorteile. Für Mercedes-Benz und Daimler ist diese Form der Ausbildung deshalb ein wichtiger Baustein bei der Sicherung des akademischen Nachwuchses", sagte Frithjof Punke, Leiter Personal bei Daimler Trucks.

Daimler-Werk Mannheim

Optimale Mischung von Theorie und Praxis

Vor allem die Praxisnähe ist einer der großen Vorteile des dualen Studiums. Die Verzahnung von theoretischem Wissen und praktischen Einblicken ist optimal. Denn die Studierenden sammeln während ihrer verschiedenen Einsätze im Unternehmen bereits viel Erfahrung. Durch diese Berufserfahrung sind sie nach dem Studium sehr schnell einsetzbar und benötigen im Vergleich zu externen Studienabgängern eine kürzere Einarbeitungszeit. Die Absolventen verfügen zudem über eine solide wissenschaftliche Qualifikation. Sie sind so für die Aufgaben bei Mercedes-Benz und im Daimler-Konzern gut vorbereitet.

Bruno Buschbacher, Betriebsrat im Mercedes-Benz Werk Mannheim, sagte: „Die duale Berufsausbildung ist der Grundstein des Erfolges der deutschen Wirtschaft, welcher auf dem Wissen und Können der Facharbeiter basiert. Die DHBW ist ein fester Bestandteil der dualen Berufsausbildung im Hause Daimler, der jungen und qualifizierten Menschen während des dualen Studienganges sowohl im Betrieb, als auch in der Hochschule viel abverlangt, aber auch einen optimalen Einstieg in das Berufsleben bietet. Die dual Studierenden bilden zusammen mit den Facharbeitern im Betrieb eine Gruppe, die für die Zukunftsfähigkeit und Wirtschaftlichkeit der Standorte der Daimler AG steht und somit für die Arbeitsplatzsicherung aller Beschäftigten. Vierzig Jahre duales Studium bei Mercedes-Benz Mannheim sind es wert, die Ausbildung der DHBW gebührend zu feiern."

Stärkung des Ausbildungsstandortes

„Ich freue mich sehr, dass so viele junge Talente sich für das Mercedes-Benz Werk Mannheim entscheiden", sagte Dr. Ulrike Freundlieb, Bürgermeisterin für Bildung, Jugend und Gesundheit der Stadt Mannheim. „Die Zahlen belegen, dass die Daimler AG damit nicht nur den Ausbildungsstandort Mannheim stärkt, sondern auch langfristig Fachkräfte an Stadt und Region bindet."

Im Dreimonatsrhythmus wechseln die Studierenden zwischen Hochschule und Partnerunternehmen und erwerben so gleichermaßen fundiertes theoretisches Wissen, als auch praktische Berufserfahrung. Das Studium dauert drei Jahre. Gruppen von ca. 30 Studierenden ermöglichen intensive individuelle Betreuung und den Einsatz modernster Lehr- und Lernmethoden. Rund 2.000 Ausbildungspartnerunternehmen vertrauen auf das Ausbildungskonzept und arbeiten mit der DHBW Mannheim zusammen.

„Wie das bestmögliche technische Hochschulwesen aufgestellt wird, ist eine Frage, die auch und gerade für Deutschland hochaktuell ist. Dabei ist das duale Hochschulstudium aus der Ingenieurausbildung Deutschlands nicht mehr wegzudenken", sagte Professor Dr. Georg Nagler.

Aktuell studieren aus dem Werk rund 35 Personen der Hochschuljahrgänge 2012 bis 2014 an der DHBW Mannheim. Belegt werden von ihnen folgende Studiengänge: Maschinenbau/Produktionstechnik, Mechatronik/Allgemeine Mechatronik, Mechatronik/Elektromobilität, Wirtschaftsingenieurwesen, Wirtschaftsinformatik/Software Engineering, Wirtschaftsinformatik/Sales und Consulting und Betriebswirtschaftslehre/Industrie.

Bernd Weber
www.daimler.com
Foto: Daimler

DHBW
Duale Hochschule
Baden-Württemberg
Mannheim

Was HIMA mit überlaufenden Tanks zu tun hat

Buncefield, England, 2005: Ein Treibstofflager in der Nähe von London läuft über. Ein Funke reicht aus, und die Anlage explodiert. Es gibt Schwerverletzte. 20.000 Beschäftigte verlieren ihren Arbeitsplatz. Der wirtschaftliche Schaden beläuft sich auf etwa 100 Millionen Pfund. Zehn Jahre später und 600 Kilometer weiter südöstlich erfahren Studierende der Hochschule Kaiserslautern bei einem von der VDE-Hochschulgruppe initiierten Besuch, was Unfälle wie dieser mit HIMA zu tun haben.

Steffen Philipp, Geschäftsführender Gesellschafter der HIMA, berichtet den Studierenden, wie seine Familie das Unternehmen aufbaute.

Peter Sieber, General Manager Global Sales von HIMA, erklärt den Studierenden, was die Tanklager von Buncefield in der Praxis davor bewahrt hätte. Schnell wird klar: Bei HIMA dreht sich alles um funktionale Sicherheit.

„Wie schützt man einen Tank vor dem Überlaufen?“

Wie das Unternehmen zum weltweit führenden Spezialisten für sicherheitsgerichtete Automatisierungslösungen wurde, erfahren die Studierenden aus erster Hand vom geschäftsführenden Gesellschafter Steffen Philipp, der zusammen mit CEO Sankar Ramakrishnan einen Einblick in die Geschichte, familiäre Leitkultur und internationale Aufstellung von HIMA gibt.

Nach einer Führung durch die Produktion können sich die Studierenden anschauen, wie eine Abnahme funktioniert. Dabei steht die wesentliche Erkenntnis des Tages im Mittelpunkt: Bei HIMA wird getestet, getestet und wieder getestet. Dazu Steffen Philipp: „Beim Thema Sicherheit gibt es keine Kompromisse.“ So ist es nur nachvollziehbar, dass die Kundenabnahme bei Großprojekten auch mal mehrere Wochen in Ansprung nehmen kann. Produkte und Lösungen verlassen HIMA erst, wenn 100 Prozent Sicherheit gewährleistet werden kann.

Als Highlight des Tages steht im hauseigenen Trainingscenter die Programmierung einer Sicherheitssteuerung mit HIMAs Engineering-Tool SILworX auf dem Programm.

Bei der Führung durch die Produktion bekommen die Studierenden ein genaues Bild über die Abläufe.

Wie wird man nun ein Sicherheitsspezialist?

Klaus D. Mittorp, Head of Human Resources, gibt zum Abschluss des Besuchs einen Einblick in die verschiedenen Einstiegsmöglichkeiten, die HIMA Studierenden und Absolventen bietet. Besonders Ingenieure und Absolventen der Elektrotechnik werden bei HIMA gesucht. Dabei legt der Personalchef vor allem Wert darauf, „dass Sie bei HIMA nicht nur an unsere Lösungen denken, sondern daran, dass wir unsere Werte als Familienunternehmen leben und dieses Versprechen jeden Tag neu einlösen.“

Sowohl für HIMA als auch für die Studierenden war der gegenseitige Austausch ein Erfolg. „Der heutige Ausflug in die funktionale Sicherheit war nicht nur überaus spannend, sondern zeigte den Studierenden auch gänzlich neue Möglichkeiten für ihre berufliche Zukunft auf“, sagte Prof. Sven Urschel von der Hochschule Kaiserslautern, Betreuer der Hochschulgruppe. „Mit HIMA haben wir einen sehr guten Partner gefunden und würden mit der Hochschulgruppe jederzeit wiederkommen“, ergänzte er.

SAFETY NONSTOP HIMA

HIMA Paul Hildebrandt GmbH
Daniel Plaga
Fotos: HIMA Paul Hildebrandt GmbH
www.hima.de

MINT Zukunft schaffen – nach wie vor aktuell

Eine gestiegene Nachfrage nach Arbeitskräften und im Wesentlichen konstante Arbeitslosenzahlen habe zu einem weiteren Anstieg der MINT-Arbeitskräftelücke auf inzwischen 156.200 geführt, wird Anfang September Dr. Oliver Koppel vom IW Köln auf der Homepage der „MINT-Initiative Zukunft schaffen" zitiert. Dies zeigt: Zurücklehnen geht noch lange nicht. Es gilt vielmehr, weiter für MINT aktiv zu sein. VDE und VDI haben dies mit dem MINT-Familientag 2015 und den Auszeichnungen für MINT-freundliche Schulen in der Region erneut getan.

Schon seit geraumer Zeit schlagen Wirtschaft und Politik Alarm: Ein Mangel an Nachwuchs in den MINT-Qualifikationen (Mathematik, Informatik, Naturwissenschaften und Technik) gefährde den Standort Deutschland, wirke als Wachstums- und Innovationsbremse und führe in der Folge zu einem Wertschöpfungsverlust.

MINT-Lücke

Die Zahlen, die „MINT Zukunft schaffen" veröffentlicht, sprechen eine deutliche Sprache: So war im Herbst 2015 die MINT-Arbeitskräftelücke höher als im August und deutlich größer als im August des Vorjahres. Zudem war im August bei den MINT-Ausbildungsberufen die Arbeitslosigkeit auf den niedrigsten Stand seit Beginn der Aufzeichnungen in der aktuellen Berufsklassifikation (Januar 2011) gesunken. Die Arbeitskräftenachfrage in diesem Segment hatte den zweithöchsten August-Stand erreicht.

Nicht von ungefähr also will die Initiative sich bundesweit weiter mit den verschiedenen Partnerorganisationen mit Nachdruck für eine Stärkung der MINT-Fächer einsetzen. Die Forderung lautet: Unterricht und Lehre in den MINT-Fächern sowie die Kenntnis mathematisch-naturwissenschaftlicher Zusammenhänge sowohl an Schulen, als auch in den Hochschulen quantitativ und qualitativ zu verbessern sowie alle frühen Talentquellen auszuschöpfen und Bildungsbarrieren abzubauen.

Im Rahmen ihres MINT-Familientages am 10. Oktober im TECHNOSEUM Mannheim konnten VDE und VDI über 1.100 Besucherlinnen begrüßen, ein unterhaltsames Programm anbieten sowie zahlreiche Ehrungen von MINT-freundlichen Schulen der Region vornehmen.

Der MINT-Familientag 2015 startete mit der Begrüßung der Gäste.

„Hier sind sie richtig, wenn es um Spaß am Lernen geht", begrüßte der Direktor des TECHNOSEUM, Professor Hartwig Lüdtke, die zahlreichen Gäste und freute sich, dass VDE und VDI die Mannheimer Institution wieder für ihren MINT-Familientag ausgewählt hatten.

Der Vorsitzende des VDE Kurpfalz, Professor Wolfram Wellßow, wies darauf hin, dass es nach wie vor einen Mangel an Ingenieuren und Ingenieurinnen gäbe und deshalb Werbung für MINT nicht an Wichtigkeit verloren habe. „Ohne die Innovationen aus den Naturwissenschaften und dem Ingenieurwesen gibt es keinen Fortschritt", lautete sein Credo. Die Handy-Technologie, die Mobilität oder die Fortschritte in der Medizintechnik seien nur drei Beispiele, die aus der modernen Gesellschaft nicht mehr wegzudenken seien.

Dr. Ditmar Flothmann zeigte sich erfreut, dass auch in diesem Jahr wieder zahlreiche Schulen neu mit dem Signet „MINT freundlich" geehrt werden. Hinzu kämen viele Schulen, die sich nach drei Jahren um einer Rezertifizierung beworben haben. „Wir haben alle Bewerbungen positiv bewertet", sagte der MINT-Repräsentant des VDI Nordbaden-Pfalz. Zudem sei das MINT-Netzwerk in der Region erfreulich gewachsen.

Durch das Programm führte Dr. Karlheinz Fischer, der im Vorstand des VDE-Kurpfalz für das Thema MINT verantwortlich ist.

Spannender Vortrag – Einfluss der Medien auf das Gehirn

„Das Gehirn im Multimedia-Zeitalter“, so lautete der Titel des lebendigen Vortrags von Professor Thomas Korff, Universität Heidelberg, der anregte zu Fragen und anschließender Diskussion.

Professor Thomas Korff

Worum ging es? Einfach gesagt: Darum, was unser Gehirn im Zeitalter von beispielsweise Smartphones, Computerspielen, Social Media und ständig auf den modernen Menschen einprasselnden Multimediaeinflüssen zu tun hat, um dies alles zu verstehen und zu verarbeiten.

Besonders betroffen von dem ständigen „Mediengewitter“ sind junge Menschen, die sich dem Angebot nicht entziehen wollen. In der Pubertät findet ein groß angelegter Gehirnumbau statt, unter anderem sind die Dopaminrezeptoren reduziert, die als eine Art Motivator für das Gehirn fungieren.
Auf der einen Seite führt dies dazu, dass Jugendliche oft in der Schule unmotiviert sind und Schwierigkeiten haben, Lerninhalte langfristig zu speichern. Auf der anderen Seite wird das Gehirn in dieser Zeit aber maßgeblich davon geprägt, für welche Denkleistung und Anregungen es genutzt wird. Medienkonsum kann dabei schnell zu Mediensucht werden.

Jeder Mensch lernt anders – das sei wahrlich keine neue Erkenntnis, sagte Kroff mit einem Augenzwinkern. Neu sei aber, dass der Lernprozess in zunehmendem Maße durch Einflüsse von außen gestört würde. Lernen bedeutet, Informationen zu dechiffrieren und sie über das Arbeitsgedächtnis im Langzeitgedächtnis zu deponieren. Wird dieser Verlauf gestört, kommt es zur Stressreaktion, die nicht nur den Lernprozess stört, sondern auch aggressiv machen kann und das Gehirn abstumpfen lässt.

Wird Medienkonsum ekzessiv betrieben, führt dies zu neuronalen Fehlentwicklungen – so lautet unterm Strich die Erkenntnis der Hirnforschung. Jugendliche sollten eigentlich nicht mehr als 90–100 Minuten pro Tag mit Handy oder PC verbringen. Keine guten Aussichten seien das, war die besorgte Reaktion der zahlreichen Zuhörerinnen und Zuhörer, viele selbst Eltern. Wie könne man bei Kindern und Jugendlichen gegensteuern, lautete entsprechend die Frage an den Fachmann. Es gibt ein paar einfache Regeln, zu denen ausreichend Schlaf und mindestens eine Stunde vor dem Schlafengehen Handy- und PC-Abstinenz ebenso gehören wie Sport. Auch sollte in der Schule kein Surfen in den Sozialen Netzen stattfinden und keine Computerspiele die Pausen füllen.

Warten auf den Beginn: Auf großes Interesse der kleinen Gäste stieß die Einladung zur „Physikalischen Zauberschule mit der Hexe Exploralda und ihrem Zaubergehilfen“.

Die Zauberhexe und ihr Zaubergehilfe hatten auch einen Zauberlehrling mitgebracht.

Mitmachen war gewünscht – und der Wunsch der Zauberhexe wurde von den kleinen Zuschauern gerne erfüllt.

Ehrungen „MINT-freundliche Schule“

„Eine Maßnahme, um MINT zu fördern: Schulen, die ihr Profil „MINT-freundlich“ gestalten und einen Schwerpunkt auf die MINT-Bildung legen, für deren Engagement auszuzeichnen, zu ehren und dies in der Öffentlichkeit bekannt zu machen“, erläutern Dr. Karlheinz Fischer, VDE, und Dr. Ditmar Flothmann, VDI.

Unter der Federführung der beiden MINT-Beauftragten von VDE und VDI verleihen die Bezirksvereine seit 2012 jährlich das Signet „MINT-freundliche Schule“.

Laut „MINT Zukunft schaffen“ gibt es mindestens sechs Gründe, sich zu um die Auszeichnung „MINT-freundliche Schule“ bewerben:

- Profilbildung in den mathematisch-naturwissenschaftlichen Unterrichtsfächern
- Vernetzung mit Partnerunternehmen und MINT-Botschaftern
- Stärkung der MINT-Fächer
- Angebote der Schule regional und überregional darstellen
- Anerkennung für geleistete Arbeit im MINT-Bereich der Schule
- Qualitäts- und Werteprogramm für „MINT-freundliche Schulen“

Erstmals ehrten VDE Kurpfalz und VDI Nordbaden-Pfalz in 2012 Schulen mit diesem besonderen Signet. Da es für drei Jahre gültig ist, standen in diesem Jahr nicht nur neue Auszeichnungen, sondern auch Verlängerungen der Auszeichnung an.

Verlängerung 2015 der Ehrung „MINT-freundliche Schule“ für weitere drei Jahre

Albertine-Scherer-Grundschule, Birkenheide

Bunsen-Gymnasium, Heidelberg

Carl-Benz-Gymnasium, Ladenburg

Carl-Bosch-Schule, Heidelberg

Eleonoren-Gymnasium, Worms

Elisabeth-von-Thadden-Schule, Heidelberg

Friedrich-Grundschule, Weinheim

Grundschule, Zweibrücken-Mittelbach

Gymnasium am Rittersberg, Kaiserslautern

Hans-Freudenberg-Schule, Weinheim

IGS Ernst Bloch, Ludwigshafen

Internationale Gesamtschule, Heidelberg

Johann-Wolfgang-von-Goethe-Gymnasium, Germersheim

Käthe-Kollwitz-Gymnasium, Neustadt

Privatgymnasium, St. Leon-Rot

Privatgymnasium, Weinheim

Werner-Heisenberg-Gymnasium, Weinheim

Wilhelm-Erb-Gymnasium, Winnweiler

Wimpina Grundschule, Buchen

Neue Ehrungen 2015

Berufsbildende Schule Technik, Kaiserslautern

Carl-Orff-Schule Fehlheim, Bensheim

Erich-Kästner-Gymnasium, Bürstadt

Gauß-Gymnasium, Worms

Grundschule Pestalozzi, Zweibrücken

Karl-Kübel-Schule, Bensheim

Kurpfalz-Gymnasium, Schriesheim

Leonardo-da-Vinci-Gymnasium, Neckargemünd

Pfrimtal Realschule Plus, Worms

Privatgymnasium, Schwetzingen

Realschule, Lauterecken-Wolfstein










Das Mannheimer Partnerunternehmen Pepperl+Fuchs bot in bewährter Weise einen Lötkurs an. Auszubildende zeigten Kindern ab acht Jahren, wie es geht.

„Lernen kann tatsächlich Spaß machen", das bewies die Physikshow von „Stella Nova". Die beiden Akteure zeigten verschiedene Phänomene und erklärten diese humorvoll.

Thomas Wiessler vom Arbeitgeberverband Südwestmetall, einem Partner der Auszeichnungen, überbrachte Glückwünsche an die Schulen.

Mit von der Partie war die Mannheimer Eismanufaktur FONTANELLA, die die Besucherinnen und Besucher mit MINT-Eis versorgte.

Die MINT-Repräsentanten erhielten für Ihr Engagement symbolisch eine MINT-Pflanze. „Möge die Minze gedeihen wie die MINT-Idee", bedankten sich Professor Wolfram Wellßow und Sybille Breunig, VDE-VDI-Geschäftsstelle, bei Dr. Ditmar Flothmann (2.v.r.) und Dr. Karlheinz Fischer (2.v.l.).

VDE zeichnet hervorragende Abschlussarbeiten aus

Professor Wolfram Wellßow (r.) und Yvonne Kremer (l.) vom VDE Kurpfalz gratulierten zu herausragenden Abschlussarbeiten.

„An einem Ende von MINT steht der Abschluss eines Studiums", leitete Professor Wellßow die Ehrung für ausgezeichnete Abschlussarbeiten an Hochschulen der Region ein. Die Absolventin und die Absolventen wären gute Beispiele dafür, wie interessant und motivierend ein Studium in einem MINT-Fach sein kann.

Geehrt wurde	Hochschule	Titel der Abschlussarbeit	Laudator
Timm Harbarth	SRH Hochschule Heidelberg	Bachelorarbeit: Erarbeitung und Implementierung von Methoden zur automatisierten akustischen Kennfeldvermessung von Abgasturboladern am Heißgasprüfstand	Prof. Dr. Achim Gottscheber
Carl Christian Rheinländer	Hochschule Kaiserslautern	Masterarbeit: Conception and Development of a Flexible Multi Sensor Ultra Low Power Wireless Sensor Network Using Bluetooth Low Energy	Prof. Dr.-Ing. Günter Biehl
Lasse Schnepel	Technische Universität Kaiserslautern	Diplomarbeit: Entwurf einer modularen, konfigurierbaren und erweiterbaren Mikroprozessorplattform für firmware-basierten Entwurf von Eingebetteten Systemen	apl. Prof. Dr.-Ing. habil. Dominik Stoffel
Josef Vaas	Duale Hochschule Baden-Württemberg Mannheim	Bachelorarbeit: Analyse und Zustandsbewertung eines ländlich geprägten Versorgungsnetzes zur Ermittlung einer Erneuerungsstratgie	Prof. Kay Wilding
Johanna Schneider	Hochschule Mannheim	Bachelorarbeit: Energy Harvesting auf Mittelspannungs-Freileitungen am Beispiel von Breitband-Powerline-Netzen	Prof. Jörg Best

VDE ehrt Aktive der Digital Summerschool

Im Jahr 2008 wurde die „Digital Summerschool" zum ersten Mal angeboten, seinerzeit noch unter dem Namen „IT Summer School". Nach zwei Jahren wurde der Name in „Digital Summerschool" umgewandelt. Das gemeinsame Angebot von VDE Kurpfalz und dem IT-Forum Rhein-Neckar versteht sich als IT-Erlebnis in den Sommerferien für Kinder und Jugendliche in der Metropolregion Rhein-Neckar.

Im ersten Jahr gab es ein begrenztes Angebot an Kursen, die nur an der SRH Hochschule Heidelberg angeboten wurden. Inzwischen hat sich der Kreis der durchführenden Institutionen erweitert, und in acht Jahren Summerschools haben viele Kinder und Jugendliche sich in die Welt von beispielsweise Robotern, Lego Mindstorms, APPs oder Filmproduktionen begeben. Der Ausblick war einhellig: „Wir werden sicherlich auch in 2016 wieder eine Summerschool anbieten."

Beim VDE-Forum am MINT-Familientag bedankte sich der Vorsitzende Professor Wellßow (Fotos je links) im Namen des Bezirksvereins Kurpfalz bei den Akteurinnen und Akteuren. Der VDE würdigte deren besonderes Engagement im Bereich der Nachwuchsförderung mit einer Urkunde: „Dies ist Ausdruck unserer Wertschätzung für einen außergesellschaftlichen Beitrag, um junge Menschen für Informationstechnik zu begeistern und an den innovativen Umgang mit Technik heranzuführen."

An der „Digtial Summerschool 2015" waren beteiligt:

- DHBW Mannheim
- ExploHeidelberg
- Hochschule Mannheim
- SRH Hochschule Heidelberg
- TECHNOSEUM Mannheim

Die Palette der Angebote war vielfältig:

- APPs Programmieren
- Robotik, Lego Mindstorms
- Mikrocontroller programmieren wie die Profis mit Arduino
- Robotik Abenteuerparcours mit Lego Mindstorms EV 3
- Robotikworkshop mit Lego Minstorms EV 3
- Hier kommt Bewegung in die Legosteine
- Bewegte Welt – ein Programmierkurs für Einsteiger
- Stop Motion
- Zum Jahr des Lichtes: Lichteffekte
- Bau und Programmierung von Robotern mit Lego Mindstorms EV 3
- Programmieren in JAVA mittels Lego Mindstorms
- Robotik für Girls
- Erneuerbare Energien & Medizintechnik

VDE würdigt besonderes Engagement im Bereich der Nachwuchsförderung

Professor Dr. Achim Gottscheber, SRH Hochschule Heidelberg

Dr. Anke Neuhaus, TECHNOSEUM Mannheim

Ute Ihme, Hochschule Mannheim

Dipl.-Ing. Peter Wittlinger, ExploHeidelberg

Sybille Breunig
Fotos: B. Kunkel

Unendliche Weiten: Faszinierende Sternenabenteuer im Dynamikum

Unzählige Sterne gibt es im Weltall – aber wie schafft man es, die ungeheuren Dimensionen der Planeten allein schon unseres Sonnensystems fühl- und auch erlebbar zu machen? Das Dynamikum in Pirmasens zeigt es vom 5. Oktober 2015 bis 10. Januar 2016 mit der erfolgreichen Zusatzausstellung „Nach den Sternen greifen – Astronomie im Dunkelraum“.

In der Wiederauflage der Sonderschau, die 2011 bereits zahlreiche Gäste begeistert hatte, können die Besucher des Pirmasenser Science Centers in einem komplett lichtfreien Raum „abtauchen“. Dort erkunden sie unter fachkundiger Anleitung von Dynamikum-Mitarbeitern gemeinsam Größen- und Gravitationsverhältnisse sowie Entfernungen und erfahren auf diese Weise viel Wissenswertes über unser Planetensystem. Passend zum Thema wird es außerdem spannende Experimentvorführungen und Exponaterklärungen in der Dauerausstellung geben. Aha-Erlebnisse sind garantiert.

Lichtfreien Raum erfahren

Da der Dunkelraum nur von jeweils zwölf Personen gleichzeitig betreten werden kann, sind für Gruppen eine vorherige Anmeldung und Terminbuchung erforderlich; Einzelgäste können sich auch noch vor Ort anmelden. Der Eintritt kostet ohne Dynamikum-Besuch pro Person 3 Euro, in Kombination mit dem regulären Dynamikum-Eintrittspreis 2 Euro. Zur Vertiefung des Themas bietet der hauseigene Shop während der Ausstellungsdauer eine Vielzahl passender Artikel rund um die Astronomie.

Die in dieser Form einzigartige Schau wurde realisiert von Petra Mohr vom Science Center „ExploHeidelberg“ in Kooperation mit dem Fachbereich Didaktik/Physik und Chemie der Universität Bamberg.

Weltall erfahrbar machen

Die Wissenschaft der Astronomie birgt für viele Menschen etwas Mystisches und Abstraktes. Da der größte Teil der astronomischen Erkenntnisse aus der Analyse des Lichtes resultiert, basiert die Wissensvermittlung meist auf Bildern: Sie faszinieren und schaffen einen besonderen Zugang zu der Thematik, sehbehinderten Menschen jedoch bleibt dieser Zugang im Verborgenen.

Der Grundgedanke des Projektes „Nach den Sternen greifen“ entstand in der Motivation, auch diesen Menschen die Möglichkeit zu bieten, ihre Fragen zu beantworten und das Weltall erfahrbar zu machen. Letztendlich stellte sich jedoch heraus, dass es allen Menschen eine besondere Erfahrung vermitteln kann. „Wie viele Sterne existieren im Weltall? Wie weit sind die Planeten voneinander entfernt? Wie groß sind die Planeten und wie sehen sie aus?“ – all dies sind Fragen, die sich die Menschen stellen, unabhängig davon, ob sie ihren Sehsinn nutzen können oder nicht.

Die Bilder aus dem Weltall schaffen Interesse, jedoch sind sie auch abstrakt und unnahbar. Der Dunkelraum bietet die neuartige Fremderfahrung der absoluten Dunkelheit und somit den Verlust des Sehsinns. Geräusche und Gerüche werden intensiver wahrgenommen, auch der Tastsinn gewinnt eine neue Bedeutung. Die Relationen und Größenverhältnisse des Weltalls werden erfahrbar gemacht sowie Planeten und Strukturen nachmodelliert, um so ein Gefühl für astronomische Dimensionen zu schaffen.

Der Dunkelraum bietet für alle Besucher eine einzigartige Einführung in die astronomische Wissenschaft sowie in die Wunder des Weltalls und zugleich die Erfahrung der absoluten Dunkelheit.

DYNAMIKUM Science Center Pirmasens
Sabine Sturm
www.dynamikum.de

Erfolge für Mannheim in Europa – Delta Racing auf guten Plätzen bei der Formula Student

Bei den internationalen Wettbewerben der Formula Student in Tschechien und Italien konnte das Rennteam der Hochschule Mannheim beeindruckende Erfolge einfahren. Innerhalb eines Jahres entwickelten, konstruierten, bauten und vermarkteten die Studierenden eigenständig und in Zusammenarbeit der unterschiedlichsten Studiengänge Fahrzeuge made in Mannheim. Dabei entstanden seit Gründung des Teams acht Fahrzeuge nur durch Studierende. Zum zweiten Mal in Folge wurden gleich zwei Fahrzeuge entwickelt.

Das Elektrofahrzeug DR15-E auf der Rennstrecke in Tschechien

Noch bedeutender wird diese Leistung in Hinblick auf die Resultate der Wettbewerbe. Mit dem Elektrofahrzeug DR15-E erreichte das Team im tschechischen Most den 8. Platz im Gesamtklassement aller angetretenen Teams aus der ganzen Welt und sogar den 3. Platz in der Kategorie Beschleunigung. In Verano de'Melegari in Italien konnte das Team mit dem Verbrennerfahrzeug DR15-C auf den 12. Platz fahren und damit im Vergleich zur Teilnehmerzahl von fast 50 Fahrzeugen das beste Resultat des Teams seit Gründung einfahren. Besonders erwähnenswert ist außerdem der Sieg des Combustion Fahrzeugs in der Kategorie Effizienz, der die Studenten motiviert, im nächsten Jahr erneut ihr Bestes zu geben.

„Wir sind stolz auf all das, was wir gemeinsam erreicht haben. Somit kommen zwei erfolgreiche Fahrzeuge wieder aus der Metropolregion Rhein-Neckar," freut sich Marketingleiter Marcel Erné in der Rückschau.

DR15-C im italienischen Verana de'Melegari im Einsatz

Die Leistung ist auch schon deshalb bedeutend, weil sich das Team um alle Belange selbst kümmern muss, um Konstruktion und Bau aber auch um die Organisation, Finanzierung und Vermarktung des gesamten Projektes. „Dies ist der besondere Reiz. Studierende arbeiten neben ihrem Studium aktiv an einem realen Projekt mit, bringen sich mit ihrer Fachkompetenz ein. Dabei vertiefen und festigen sie ihr Wissen aus dem Studium und lernen viel Neues dazu. Man lernt eben nicht nur ein Auto zu bauen, sondern bekommt einen Eindruck davon, was es bedeutet, in einem Team zu arbeiten und ein kleines Unternehmen aufzubauen", so Erné.

Inzwischen ist Delta Racing von den Wettbewerben im europäischen Ausland zurückgekehrt. Die Vorbereitungen für die kommende Saison beginnen, damit die Mitglieder von Delta Racing auch 2016 wieder mit verbesserten und ausgereiften Fahrzeugen die Jagd auf die vorderen Plätze eröffnen wollen.

Delta Racing Mannheim e.V.
Hochschule Mannheim
Marcel Erné
www.delta-racing.de
Fotos: Delta Racing

Sonja die Astronautin

Die kleine Sonja lebt auf einen fernen Planeten und beobachtet Tag für Tag die wunderschöne Erde durch ihr Teleskop. Jeden Abend denkt sie daran, wie schön es wäre, diesen blauen Planeten einmal besuchen zu können. Sonja hat viele Bücher gelesen und auch im Internet nach Möglichkeiten gesucht, die lange Reise zu bewältigen. Sonja zeichnete, rechnete und entwickelte unterschiedlichste Lösungen für ihre Reise. Nach vielen Jahren der Forschung hat sie eine Lösung für die lange Reise gefunden. Mittels einer Rakete möchte sie zur Erde fliegen. Dafür hat sie sich eine Startrampe gebaut auf der ihre kleine Rakete steht.

➔ Stelle einen Teebeutel auf einen Teller.

SonjasBruder ist nicht sehr glücklich über die bevorstehende Reise und möchte sie mit allen Mitteln verhindern. So beschließt er, die Steuerung der Rakete zu entfernen, damit Sonja nicht starten kann.

➔ Entferne den Zettel am Teebeutel.

Als Sonja die beschädigte Rakete am nächsten Morgen auf der Startrampe sieht, ist sie sehr traurig. Viel Zeit hat hat sie dafür benötigt, die Lösung für ihre Reise zu finden und jetzt rückt ihre Reise wieder in weite Ferne. Sonja lässt sich aber nicht entmutigen und sucht nach einer neuen Lösung. Der Bruder ist sich nicht sicher, ob das Entfernen der Steuerung ausreicht und entfernt in der nächsten Nacht auch noch die Zündschnur.

➔ Entferne die Schnur vom Teebeutel.

Als Sonja dies sieht, wird sie zornig und sagt sich, auch das wird mich nicht abhalten, zur Erde zu fliegen. Ihr Bruder weiß um die Beharrlichkeit seiner Schwester und beschließt in der folgenden Nacht, den Treibstoff aus der Rakete zu nehmen: „Denn ohne Treibstoff kann keine Rakete starten und meine Schwester bleibt für immer bei mir“.

➔ Öffne den Teebeutel und entferne den Tee. Danach stelle den leeren Teebeutel wieder mit der offenen Seite als Röhre auf den Teller.

Am nächsten Morgen kommt Sonja mit ihrem Astronautenanzug zur Rakete und sieht, was in der Nacht geschehen ist. Sie betrachtet sich ihre Rakete von allen Seiten und überlegt lange, was sie jetzt machen soll. Da kommt ihr eine Idee: „Ich setze mich in die Rakete und beobachte, wer jede Nacht meine Rakete beschädigt.“

Am Abend bemerkt Sonjas Bruder nicht, dass sie in ihrer Rakete sitzt und beschließt, dem Spuk ein endgültiges Ende zu setzen: „Ich werde die Raketenhülle verbrennen und dann kann meine Schwester mich nicht mehr verlassen.“ Er nimmt ein Streichholz und zündet die Rakete an.

➔ Mit einem Streichholz den Teebeutel oben anzünden.

In diesem Augenblick erkennt er, dass Sonja in der Rakete sitzt, da ist es aber schon zu spät. Die Rakete hebt ab, und Sonja fliegt auf direktem Weg zur Erde. Dort landet sie wohlbehalten und zeigt den Menschenkindern wie wichtig es ist, nicht beim ersten Rückschlag aufzugeben, sondern immer nach einer neuen Lösung zu suchen. Wenige Tage später kommt auch Sonjas Bruder mit einer Rakete auf die Erde geflogen und beide leben glücklich mit den Menschenkindern zusammen und lösen jeden Tag neue Probleme.

Liebe VDInis, bitte dieses Experiment nur zusammen mit einem Erwachsenen durchführen!

VDI

Alexander Kling, VDI

Block 9 des GKM offiziell am Netz – eine Nachlese

Zehn Jahre Planungszeit, sechs Jahre Bauzeit und im September 2015 die offizielle Inbetriebnahme des Block 9 der Grosskraftwerk Mannheim AG (GKM): „Ein wichtiger Meilenstein in der über 90-jährigen Geschichte des Unternehmens“, so Dr. Karl-Heinz Czychon, Technischer Vorstand des GKM. Nicht nur in den Medien der Region wurde über die Kontroversen im Vorfeld, das Genehmigungsverfahren, die Klageverfahren, die Grundsteinlegung, die Probleme beim Bau und schließlich die feierliche Inbetriebnahme ausführlich berichtet.

Auch das technikforum hat den Bau des Block 9 redaktionell begleitet. Zum Abschluss eine kleine Nachlese.

Der neue Block gilt als hocheffiziente Kraft-Wärme-Kopplungsanlage (KWK), in die RWE, ENBW und MVV Energie nach deren eigenem Bekunden 1,3 Milliarden Euro investiert haben. Das ist kein Pappenstiel, und so wird vom neuen Block einiges erwartet. Nicht von ungefähr halten zahlreiche Fachleute das GKM für das modernste Steinkohlekraftwerk weltweit.

Das GKM verfügt nun über eine installierte Gesamtleistung von rund 2.150MW. Mannheim hat sich damit zum größten Kraftwerkstandort Baden-Württembergs entwickelt und versorgt mittlerweile 120.000 Haushalte in der Rhein-Neckar-Region.

Blick ins Innere von Block 9 beim Tag der offenen Tür

Topmodernes Steinkohlekraftwerk

Laut GKM weist die neue Anlage eine Leistung von 911 MW auf, eine Fernwärmeauskopplung von 500 MW, einen elektrischen Wirkungsgrad von über 46 Prozent und eine Brennstoffausnutzung von bis zu 70 Prozent. Dies seien „neue Maßstäbe für Steinkohlekraftwerke“, sagt das GKM. Zudem trüge der Block 9 dazu bei, das KWK-Ausbauziel der Bundesregierung zu erreichen. Gemeint ist das Gesetz für die Erhaltung, die Modernisierung und den Ausbau der Kraft-Wärme-Kopplung, das seit April 2002 in Kraft ist.

Auch der Umwelt- und Klimaschutz ist im Fokus: Man gehe von einer möglichen CO2 Vermeidung von bis zu 1,3 Mio Tonnen pro Jahr aus, verlautet es aus dem Unternehmen.

BLOCK 9 – Die wichtigsten Daten

Bruttoleistung	*911 MW*
Elektrischer Wirkungsgrad	*46,4 %*
Fernwärmeerzeugung mit KWK	*Max. 500 MWth*
Brennstoffausnutzung bei KWK	*max. 70 %*
Bahnstromleistung	*ca. 100 MW*
Rauchgasreinigung	
– Stickoxidminderung	*SCR mit Ammoniakwasser*
– Entstaubung	*Elektrofilter*
– Entschwefelung	*Kalkstein-Gips-Nasswäsche*

Quelle: GKM

GKM macht Schlagzeilen

Dass kritische Stimmen bei einem solchen Großprojekt nicht ausbleiben, hat niemanden verwundert. Wie zu erwarten war, begleiteten in der vergangenen Dekade Bürgerproteste und Klagen, die übrigens alle abgewiesen wurden, das Bauprojekt.

Der BUND spitzte zur offiziellen Inbetriebnahme im vergangenen September die Kritik mit den Worten zu: „Kampfansage an den Klimaschutz“. Aber ohne Kohlekraft gäbe es in den nächsten Dekaden keine Versorgungssicherheit, mahnen die Verantwortlichen der drei Betreiberunternehmen. Das musste auch der baden-württembergische Umweltminister Franz Untersteller, Grüne, bei der Eröffnungsfeierlichkeit einräumen: „Kohle ist nicht der Brennstoff der Zukunft. Aber noch brauchen wir sie für eine sichere Energieversorgung.“

Zumindest bis zum Jahr 2050 kommt man zur Sicherstellung der zukünftigen Stromversorgung nicht ohne Ersatzbedarf an Kraftwerksleistung aus. In diese Richtung widmete Faz.net dem neuen Block 9 einen Artikel und titelte, dass das GKM „ein neuer Kohlegigant im Windradbiotop“ sei.

Die derzeitigen Fakten sprechen für das GKM. Zwar erzeugen schon 25.000 Windräder in der Bundesrepublik Strom. Problematisch sind jedoch nach wie vor die Transporttrassen von Nord nach Süd. Bis zur endgültigen Umsetzung der Energiewende werde der Mannheimer Block 9 in großem Maße zur Versorgungssicherheit beitragen, beruhigt das GKM.

Sybille Breunig
Foto: GKM

3D-Drucker für EXPLOHeidelberg

Ende Juli fand im ExploHeidelberg eine etwas andere Veranstaltung als sonst üblich statt. Wo sich sonst Schulklassen tummeln und Kinder in Technikworkshops tüfteln, fanden sich trotz herrlichen Sommerwetters viele Interessierte in den Ausstellungsräumen des kleinen Science Centers ein, um sich die neueste Anschaffung, die durch die Unterstützung des VDE Kurpfalz ermöglicht wurde, anzusehen und in Aktion zu erleben. Fasziniert standen die Besucher vor dem „Ultimaker2", einem 3D-Drucker, der nach dem FDM-Prinzip (Fused Deposition Modeling), d.h. dem Schmelzschichtungsverfahren, arbeitet und Büroklammern mit „explo"-Schriftzug ausdruckte.

Der 3D-Drucker wird ab den Herbstferien 2015 in Workshops eingesetzt, in denen Kindern und Jugendlichen unter fachkundiger Betreuung die Grundlagen des faszinierenden Verfahrens vermittelt werden.

3D-Workshops

Angefangen bei der Modellierung am PC, über die Prüfung des Modells auf Druckfähigkeit, bis hin zur Beachtung der Materialeigenschaften – und natürlich den abschließenden Druck – werden sie alle Schritte kennenlernen. „Dabei ist nicht nur räumliches Vorstellungsvermögen gefragt, sondern es werden alle Fähigkeiten aus dem MINT-Bereich geschult", erklärte Dr. Karlheinz Fischer vom VDE Kurpfalz, warum der Bezirksverein die Anschaffung für sinnvoll hielt.

Ernst-Dieter Keller (l.) und Dr. Karlheinz Fischer (M.) vom Vorstand des VDE Kurpfalz sowie Sybille Breunig (VDE-VDI-Geschäftsstelle) ließen sich im ExploHeidelberg den 3D-Drucker erklären.

In der Industrie findet das Verfahren in immer mehr Bereichen Einsatz, da schnell und unkompliziert Prototypen entworfen und günstig hergestellt werden können. Teilweise werden auch für Kleinserien Teile direkt gefertigt beispielsweise in der Fahrradproduktion. Ein großer Vorteil dabei ist, dass so gut wie kein Abfall produziert wird, da das Objekt direkt aus dem Material ohne Verschnitt gefertigt wird.

Funktionsweise des 3D-Druckers

Beim Druck wird Kunststoff bei einer Temperatur von ca. 210°C aus einer 0,4 mm dünnen Düse extrudiert und aufeinander geschichtet. Beim Abkühlen erstarrt der Kunststoff und bildet ein stabiles Gerüst. So entsteht Schicht für Schicht quasi aus dem Nichts das fertige Objekt. PLA (Polylactide), das eingesetzte Material, ist ein auf Milchsäure basierender Kunststoff, den es in vielen verschiedenen Farben gibt. Aufgrund seiner Zusammensetzung kann er in industriellen Kompostieranlagen biologisch abgebaut oder durch Aufschmelzen recycelt und wiederaufbereitet werden.

Ob ein Objekt druckfähig ist, liegt an mehreren Faktoren. Jede neue Schicht kann nur auf eine bereits existierende Schicht aufgesetzt werden. Die Basis bildet eine höhenverfahrbare Grundplatte aus Glas. „Man kann sonst nicht drucken", erklärte Peter Wittlinger vom Explo Heidelberg, der sichtlich Freude an dem neuen technischen Gerät hatte, die Funktionsweise. Der Leiter Techniklabor führte das Gerät den Gästen vor und erläuterte, dass Querverbindungen über Lücken hinweg nicht beliebig breit sein dürfen, da das Material sonst direkt aus der Düse nach unten in die Lücke fallen würde. Außerdem seien nicht unbegrenzt flache Steigungen möglich, da sonst die Verbindungsfläche zwischen existierender Schicht und neuer Schicht zu gering ist, und das Material abrutscht.

Weiterhin muss auf eine möglichst flache und große Auflagefläche geachtet werden, da sonst das gesamte Objekt verrutschen kann und

Peter Wittlinger, Leiter Techniklabor, erläuterte die Funktionsweise des neuen 3D-Druckers und ließ ihn probeweise ein kleines Objekt drucken.

der komplette Druck verworfen werden muss. Denn ist das Material einmal zu stark abgekühlt, verbindet sich die neue Schicht nicht mehr ausreichend gut. Außerdem wäre eine erneute Ausrichtung in der Praxis nur schwer möglich, da der Druckkopf bis auf wenige hundertstel Millimeter genau positioniert werden kann – in allen drei Raumrichtungen.

Die Höhenkoordinate werden dabei über die höhenverstellbare Grundplatte eingestellt. Der Druckkopf bewegt sich auf einer festen Ebene in den beiden anderen Raumrichtungen. So kann jeder Punkt im Druckraum genau angesteuert werden, der ca. 20 cm in jeder Richtung beträgt.

Alle diese Faktoren werden von den Teilnehmern der neuen Workshops zu beachten sein, um zu guten Ergebnisse zu kommen. „Sonst sind der Fantasie keine Grenzen gesetzt", freute sich Wittlinger. Entworfen werden können beispielsweise Schlüsselanhänger, Schmuck und Accessoires, Gehäuse, Stiftehalter, kleine Figuren, Kunstobjekte, Logos in 3D und vieles mehr. In längeren Projekten sind auch aufwändigere Dinge wie Schutzhüllen für Smartphones, Lampenschirme oder Ersatzteile für defekte Gegenstände möglich.

VDE
Peter Wittlinger / Sybille Breunig
VDE Kurpfalz
Fotos: Fischer

Hochschule Mannheim

hochschule mannheim

Hochschultag 2015

Ende November konnte der Rektor der Hochschule Mannheim, Prof. Dr.-Ing. Dieter Leonhard, rund 250 Gäste zum Hochschultag 2015 begrüßen.

Leitmotiv Innovation

In seiner Ansprache führte der Rektor aus, dass der Begriff „Innovation" in vielfältiger Weise ein Leitmotiv für die Hochschule Mannheim darstellt. Zum einen bereitet die Hochschule ihre Bachelor- und Masterabsolventen im Studium darauf vor, im späteren Berufsleben Innovationsprozesse in Wirtschaft und Gesellschaft anzuregen und zu gestalten. Gleichzeitig trägt sie durch ihre Forschungstätigkeit zum Innovationsgeschehen der Metropolregion bei und bringt sich in regionale Netzwerke ein. Zum andern müssen Hochschulen sich ständig erneuern und weiterentwickeln, um den Herausforderungen einer sich ständig wandelnden Welt gerecht zu werden. An Beispielen, wie der Promotion von Fachhochschulabsolventen und dem Bologna-Prozess, aber auch aus dem Bereich der Internationalisierung und der Digitalisierung skizzierte der Rektor, wie solche Veränderungsprozesse konkret aussehen.

Die Festansprache hielt Dr. Ursula Redeker, Sprecherin des Vorstandes Roche Diagnostics GmbH, zum Thema „Von Tradition, Wissen und Inspiration: Was Innovationen brauchen".

Preisverleihungen

Für das Studienjahr 2014/15 konnten zwölf Preise von Unternehmen, Institutionen und Persönlichkeiten an 19 Studierende und Absolventinnen und Absolventen der Hochschule verliehen werden, die sich im letzten Jahr durch hervorragende Studienleistungen, aber auch durch außerfachliches und gesellschaftliches Engagement ausgezeichnet haben. Das Preisgeld hierfür betrug insgesamt 24.500 Euro.

Außerdem konnten 30 ein- bzw. zweijährige Deutschlandstipendien im Gesamtwert von 122.400 Euro an Studierende der Hochschule Mannheim vergeben werden, die in ihrem Studium hervorragende Leistungen vorweisen können. Stifter sind die Unternehmen BASF SE, AbbVie Deutschland GmbH & Co. KG, Roche Diagnostics GmbH und Roche Diabetis Care, gempex GmbH, John Deere GmbH, Joseph Vögele AG sowie die Albert-und-Anneliese-Konanz-Stiftung und die Handwerkskammer Mannheim.

Den zum zweiten Mal vergebenen Albert-und-Anneliese-Konanz-Lehrpreis erhielt Prof. Dr. Chirly dos Santos-Stubbe, Fakultät für Sozialwesen. Die Stadt Mannheim stellt zwei einjährige Mannheim-Stipendien in Höhe von jeweils 1.800 Euro zur Verfügung.

hochschule mannheim
Bernd Vogelsang,
www.hs-mannheim.de

Technische Universität Kaiserslautern

Technische Universität Kaiserslautern

Sonderforschungsbereich gefördert

Die Deutsche Forschungsgemeinschaft (DFG) richtet 15 neue Sonderforschungsbereiche (SFB) ein. Vier der 15 eingerichteten Verbünde sind SFB/Transregio (TRR), die sich auf mehrere antragstellende Hochschulen verteilen. Einen davon konnte sich die TU Kaiserslautern, in Zusammenarbeit mit der Johannes-Gutenberg-Universität Mainz (JGU), sichern.

Mit insgesamt 12 Millionen Euro wird der Sonderforschungsbereich/Transregio „Spin+X: Spin in seiner kollektiven Umgebung", unter der Koordination von Physik-Professor Dr. Martin Aeschlimann der TU Kaiserslautern, gefördert. In diesem Rahmen befassen sich Wissenschaftler/Innen aus der Physik, der Chemie, dem Maschinenbau und der Verfahrenstechnik mit grundlegenden magnetischen Eigenschaften, Phänomenen und Prozessen. Diese sind, wenn auch noch nicht umfassend verstanden, bereits heute von zentraler Bedeutung für moderne technologische Anwendungen wie die Datenspeicherung oder die magnetische Sensorik.

Der Sonderforschungsbereich/Transregio widmet sich speziell sogenannten Spin-Phänomenen, die auf atomarer Skala den Ursprung für allgemein bekannte magnetische Eigenschaften bilden.

„Wir wollen hier an der TU Kaiserslautern international sichtbare Spitzenforschung betreiben.Uns interessieren grundlegende Aspekte wie auch funktionale magnetische Effekte mit dem mittel- und langfristigen Ziel praktischer Anwendungen", erläutert Professor Aeschlimann. „Zusammen mit 30 Wissenschaftler/Innen sind wir genau das richtige interdisziplinäre Team, um dieses anspruchsvolle Forschungsgebiet anzugehen", fährt er fort.

TU-Präsident Professor Helmut J. Schmidt zeigt sich sehr erfreut über die Entscheidung der DFG: „Mit der dynamischen und erfolgreichen Entwicklung unserer koordinierten Forschung sind wir somit auf dem richtigen Weg."

Technische Universität Kaiserslautern
Dipl.-Volkswirt Thomas Jung
www.uni-kl.de

VDI AK Technikgeschichte

Bundesweites Treffen in Naumburg/Saale

Mitte Juni lud der Hallesche Bezirksverein des VDI (BV) zum Jahrestreffen der Arbeitskreisleiter Technikgeschichte nach Naumburg an der Saale ein. Als Ergänzung zum umfangreichen Erfahrungsaustausch hatte Gerhard Brüsehaber vom dortigen BV ein attraktives Rahmenprogramm ausgearbeitet.

Ein historischer Straßenbahn-Triebwagen aus dem Depot der Naumburger Straßenbahn GmbH fuhr die Gruppe an die Peripherie der Stadt zur Firma Gehring, einem kleineren mittelständischen Unternehmen für die Herstellung von Honmaschinen (engl.: to hone – urspr. Wetzen auf einem Stein). Gehring Technologies wurde 1926 in Naumburg gegründet und fertigt heute Honmaschinen zur Bearbeitung von Bohrungen im Bereich von 0,8 bis 2.000 mm bei Bohrungslängen von bis zu 24 m.

Ziel des Honens ist die weitere Verbesserung der Maß- und Formgenauigkeit. Im Unterschied zum Schleifverfahren richtet sich jedoch das Werkstück selbst aus, beim Rundhonen entsprechend selbstzentrierend. Nach eigenen Angaben ist Gehring Technologies Weltmarktführer für Honmaschinen mit Standorten in den USA, Frankreich, Brasilien, Indien und China.

Ein weiterer Schwerpunkt des Treffens fand in Wettelrode im Mansfelder Land statt. Nach der friedlichen Revolution in der Ex-DDR wurde der Kupferabbau im Röhrigschacht Anfang der 1990er Jahre eingestellt. Die Flöze waren mittlerweile zu dünn und lagen zu tief, um seinerzeit mit den Weltmarktpreisen erfolgreich mithalten zu können. Die Fläche und der Schacht wurden Besucherbergwerk und Museum, wo die Besucher in 300 m Tiefe verschiedene Schiefer-Abbautechniken und die historischen Arbeitsbedingungen unter Tage hautnah noch einmal miterleben durften.

Unter Tage

VDI AK TG bei Fa. Gehring Technologies in Naumburg

Neben dem Maschinendenkmal in Hettstedt wurde das Humboldt-Schloss mit dem Nachbau der ersten Niederdruck-Dampfmaschine gewürdigt – siehe auch nebenstehenden Artikel „125 Jahre Maschinendenkmal in Hettstedt“.

Im Park des Humboldt-Schlosses

VDI AK Technikgeschichte

125 Jahre Maschinendenkmal in Hettstedt – und mehr!

Leonardo da Vinci trug seine Pläne, Zeichnungen und Entwürfe immer bei sich – bei Reisen sogar direkt an der Kleidung. Im frühindustriellen stationären Großmaschinenbau während des letzten Drittels des 18. Jahrhunderts galt es, handgezeichnete Konstruktionspläne und Stücklisten der Baugruppen unter Verschluss zu halten, um auf diese Weise eine unerlaubte Weitergabe der technischen Entwicklung und Erfahrungen zu vermeiden.

Rückblickend betrachtet ging es bei der 125-Jahr-Feier auch um eine der ersten Industriespionagen zugunsten Preußens bzw. Deutschlands.

Bereits in den 1780er Jahren hatten sich die Niederdruck-Dampfmaschinen der Firma Boulton & Watt aus Birmingham zum Abpumpen des Grubenwassers in den englischen Kohlegruben mehr oder weniger bewährt.

Da auch in Preußen und Sachsen die Bergwerksbetreiber Probleme mit der Wasserwirtschaft in ihren Schächten hatten, entstand eine Nachfrage – Nährboden für Technologieimport – nach Produkten aus der Wattschen Fertigungsstätte. Seit 1778 lag ein Angebot aus Birmingham zur Lieferung von Dampfmaschinen vor; Boulton & Watt knüpften jedoch ein 14-jähriges Liefermonopol daran. Dies führte zum Plan eines Eigenbaus im Mansfelder Land.

Die Fotografie war noch nicht erfunden, und so mussten fachinteressierte Gesandte aus Preußen in England vor Ort das Gesehene und Gehörte niederschreiben und skizzenhafte Aufzeichnungen vornehmen. Denn theoretisches Wissen und praktische Erfahrungen im Bergbau- und Hüttenwesen gepaart mit fundierten Erkenntnissen in Metallurgie und Werkstoffkunde waren durch die bereits bestehenden frühen technologischen Bildungseinrichtungen auch hierzulande vorhanden.

1783 erhielt der junge Bergmaschinenmann Carl Friedrich Bückling nach einer Studienreise in England, wo seine Gespräche allmählich zu Misstrauen bei James Watt führten, den Auftrag zum Bau einer Dampfmaschine nach ihm bekannten englischen Vorbildern. So gelang es, 1785 die erste in Deutschland gebaute Wattsche Balancier-Niederdruckdampfmaschine mit Kondensator in Betrieb zu nehmen. Sie wurde zum Auspumpen des König-Friedrich-Schachtes in Burgörner bei Hettstedt im Mansfelder Land errichtet. Ihr Erfolg führte zur Ausbreitung des Dampfmaschinenbaus für die Bergbaugebiete in Sachsen, Schlesien und Westfalen.

Zum Gedenken an diese technisch-innovative Pionierleistung stiftete 1890 der VDI auf der kegelförmigen Abraumhalte des König-Friedrich-Schachtes das Maschinendenkmal.

Das Maschinendenkmal in Hettstedt

Seine Ertüchtigung und teilweise Erneuerung bewirkten die Bürger von Hettstedt im Jahre 1985 – also zum 200 jährigen Jubiläum der Inbetriebnahme der ersten Dampfmaschine in Deutschland.

Der ebenfalls 1985 erfolgte originalgetreue Nachbau dieser Arbeitsmaschine ist auch ein Beleg für die Einstellung der DDR zu ihrem technikkulturellen Erbe, denn die DDR-Technikgeschichtsschreibung spricht von der Entfaltung der Produktivkräfte und damit grundsätzlich von einem positiv zu sehenden eigentümlich technischen Prinzip.

Die 125-Jahr-Feier des Maschinendenkmals wurde Mitte September in einem ansprechenden Rahmen auf der Parkanlage am Fuße des Denkmalsockels begangen. Unter den Gästen waren der sachsen-anhaltinische Ministerpräsident Reiner Haseloff sowie der VDI Direktor Ralph Appel. Sie würdigten in ihren Worten die Leistungen des Ingenieurstandes in Deutschland.

Appel erinnerte zudem daran, dass nicht nur das Jubiläum des Maschinendenkmals zu feiern sei, sondern auch die 25-jährige Wiederkehr der Vereinigung des Ingenieurstandes in Ost und West.

Dr. Hartmut Knittel VDI
Fotos: Dr. Horst Gudat VDI

VDI Studierende kamen Sternen zum Greifen nah

Mitglieder des Arbeitskreises Studenten und Jungingenieure (suj) des VDI Nordbaden-Pfalz hatten vor Kurzem die Gelegenheit das „Haus der Astronomie" auf dem Heidelberger Königstuhl zu besuchen.

Das Haus der Astronomie . Die Architektur ist fast maßstabsgetreu einer Galaxie nachempfunden.

Pengxiang Cao, der gemeinsam mit Eugen Stein die suj leitet, hatte die Initiative für die Exkursion zu dieser besonderen Institution und holte auch die suj der TU Darmstadt mit ins Boot.

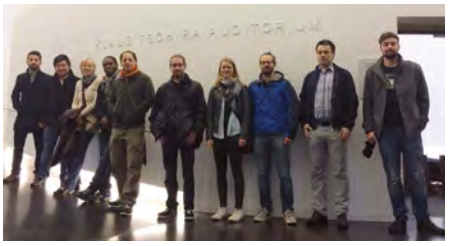
Das Haus der Astronomie beeindruckte die Mitglieder des suj nicht nur durch die exzeptionelle Architektur, sondern auch durch besondere Angebote unter dem Motto „Astronomie für die Öffentlichkeit". Nach eigenen Aussagen versteht sich die Ende 2008 von der Max-Planck-Gesellschaft zur Förderung der Wissenschaften und der Klaus Tschira Stiftung gegründete Einrichtung als „ein einzigartiges Zentrum für Öffentlichkeitsarbeit und Didaktik der Astronomie." Bauherrin war die Klaus Tschira Stiftung. Die Max-Planck-Gesellschaft und das Max-Planck-Institut für Astronomie haben die Leitung inne.

Beheimatet ist das Haus der Astronomie auf dem Heidelberger Königstuhl. Dort wurde Ende 2011 ein eigenes Gebäude bezogen. Die attraktive äußere Architektur sei passenderweise fast maßstabsgetreu der „Galaxie M 51" nachempfunden, erklärte Andreas Schreiber. Er ist Doktorand am benachbarten Max-Planck-Institut für Astronomie und betreute die Gruppe. Nur in der Höhe konnte die Maßstabstreue nicht eingehalten werden, sonst wäre das Gebäude nur ein paar Zentimeter hoch geworden. Warum dies so ist, erklärte er den erstaunten suj-Mitgliedern mit einer beeindruckenden Präsentation über u.a. Galaxien, das Weltall und die Struktur des Universums im Hörsaal.

Dieses Auditorium in Form eines Kuppelsaals ist mit Technik vom Feinsten bestückt. Statt der meist in Planetarien eingesetzten Kugelprojektion sind fünf separate Projektoren in die Decke eingelassen. Ihre Bilder werden per Datenverarbeitung synchronisiert und erzeugen ein täuschend echtes Raumgefühl.

Die ausgefeilte Technik des Kuppelsaales lässt eine Galaxie vor den Augen schweben.

Astronomie erfreut sich in der Öffentlichkeit eines breiten Interesses. Die Forschungsarbeiten und die Erkenntnisse auch für Laien verständlich aufzubereiten und zu kommunizieren, sei ein Ziel des Hauses, erläuterte Schreiber dem VDI. Dabei richten sich die Angebote sowohl an Erwachsene, als auch an Schulen und Kindergärten.



Studierende Mitglieder des VDI Nordbaden-Pfalz hatten die Gelegenheit, einen Blick in die Weiten des Alls zu werfen.

Die Visualisierung astronomischer Phänomene ist ein wichtiger Faktor. Vorträge bieten die Möglichkeit, astronomische Forschung aus erster Hand zu erfahren. Wichtig sei auch, die Medien mit fachlichen Informationen zu versorgen, wenn es um Berichterstattung über astronomische Inhalte gehe. Hinzu kommt, dass man den Austausch von Fachleuten untereinander fördern möchte.

„Wissenschaft in die Schulen!" heißt ein besonderes Projekt, das gemeinsam mit dem Verlag Spektrum der Wissenschaft und der Landesakademie für Fortbildung und Personalentwicklung an Schulen vor einigen Jahren ins Leben gerufen wurde. Zum Thema Sterne und Weltraum werden didaktische Materialien kostenlos zur Verfügung gestellt. So können aktuelle Forschungsthemen direkt in den Unterricht eingebaut werden.

Informationen über Veranstaltungen im Haus der Astronomie: http://www.haus-der-astronomie.de

Sybille Breunig
Fotos: Haus der Astronomie/Cao

Das Angebot von Workshops für Schüler und Kindergartenkinder kommt auch den Mitgliedern des **VDIni-Clubs Nordbaden-Pfalz** zu Gute. Im Juni und Juli 2016 wird je ein Club-Treff für VDInis im Alter von 4–5 Jahren und 6–7 Jahren im **Haus der Astronomie** stattfinden.

Industrie 4.0 – Neue Jobs und Arbeitsprofile

Anfang November sprach der VDI mit dem Leiter des Stuttgarter Fraunhofer-Instituts für Arbeitswirtschaft und Organisation IAO, Prof. Dr.-Ing. Wilhelm Bauer zum Thema Industrie 4.0.

Bauer ist Vorsitzender des VDI Landesverbandes Baden-Württemberg und des WIV. Er gilt als renommierter Arbeitswissenschaftler und forscht unter anderem zum Thema Digitalisierung der Arbeit.

VDI: Wie wird sich die Arbeitswelt in den kommenden Jahren durch Industrie 4.0 verändern?

Unter dem Begriff „Industrie 4.0" wird aktuell die zunehmende Digitalisierung des Produktionsumfelds diskutiert. Neben einer erwarteten Produktivitätssteigerung steht für die Unternehmen in Deutschland allem voran die Möglichkeit im Vordergrund, Produktions- und Unternehmensprozesse flexibel und reaktionsfähig zu gestalten. Durch die Nutzung von Internettechnologien, Social Media und mobilen Endgeräten wird es zukünftig wie niemals zuvor möglich, die Mitarbeiter mit den richtigen Informationen zum richtigen Zeitpunkt zu versorgen, bessere Entscheidungen sicherzustellen, aber auch individuelle Bedürfnisse zu berücksichtigen. In einer zunehmend digitalisierten Welt wird vor allem der Umgang mit dem Thema flexible Arbeitszeitgestaltung eine entscheidende Rolle spielen.

VDI: Was müssen Bundesregierung und Unternehmen aus Ihrer Sicht noch tun, damit Industrie 4.0 in Deutschland erfolgreich umgesetzt werden kann?

Viele Unternehmen in Deutschland treten dem Thema Industrie 4.0 sehr abwartend gegenüber. Ein Grund hierfür ist, dass heutige Produktionsprozesse den Marktanforderungen meist gerecht werden und gleichzeitig der initiale Aufwand hin zu einer „Fabrik der Zukunft" für viele Unternehmen eine Hürde darstellt. Hier müssen die Unternehmen aus meiner Sicht umdenken. Sie müssen schneller werden, eigene Erfahrungen mit Industrie 4.0 sammeln und mehr Ideen von außen (z.B. von Hochschulen oder Start-ups) aufnehmen.

Die Bundesregierung zeigt durch das Interesse und die Förderung gerade auch des Mittelstands in dieser Themenstellung bereits eine hohe Unterstützung. Vor allem ist es wichtig, die Diskussionen weiterhin zu führen und auf die Umsetzungsebene zu kommen. Wenn weitere Anreize zur Erforschung und Erprobung von Industrie 4.0 geschaffen werden, können auch Unternehmen ohne Erfahrungen und Verständnis an dieses Themenfeld herangeführt werden.

VDI: Welche Rolle haben die Ingenieurinnen und Ingenieuren beim digitalen Wandel? Brauchen Ingenieure neue Qualifikationen?

Die Ingenieurinnen und Ingenieure leisten mit den MINT-Berufen einen wichtigen Beitrag bei der Entwicklung von passenden Ansätzen und der Umsetzung von Industrie 4.0-Lösungen in den Unternehmen. Ich erwarte, dass der Trend der Interdisziplinarität anhält. Damit meine ich, dass alle Ingenieure sich zukünftig neben ihrer Kernspezialisierung mit anderen Technologien und fachgebietsübergreifend mit Themen beschäftigen müssen. Denn nur wenn alle Fachbereiche gut zusammenarbeiten und sich verstehen, ist der Nutzen von Industrie 4.0 maximal.

VDI: Müssen Teile der Beschäftigten befürchten, in Zukunft durch Maschinen ersetzt zu werden?

Industrie 4.0 ist ein Zukunftsthema mit dem Ziel, durch mehr Produktivität und Flexibilität den Produktionsstandort Deutschland zu sichern und auszubauen. Einfache oder unergonomische Tätigkeiten mit einem hohen Wiederholungsgrad werden daher zukünftig zunehmend automatisiert werden, so es technologisch und wirtschaftlich möglich ist. Diese Entwicklung ist nicht neu, sondern zieht sich durch alle industriellen Entwicklungen wie ein roter Faden. Was die Geschichte auch zeigt: Jede Stufe der Optimierung hat ein Wachstum und in der Folge weitere Arbeitsplätze mit sich gebracht. Ich bin daher davon überzeugt, dass die Arbeitsmarktbilanz durch Industrie 4.0 positiv aussehen wird und neue Jobs und Arbeitsprofile entstehen werden. Die Frage für mich ist vielmehr, wie sieht gute Arbeit überhaupt aus? Wo werden wir zukünftig Bedarf haben und wie können wir unsere Mitarbeiter und die Menschen in der Ausbildung hierfür qualifizieren? Dieser Aufgabe müssen wir uns gemeinsam mit Politik, Wirtschaft, Ausbildung und Forschung widmen.

Quelle: VDI
Das Interview führte Stephan Berends

VDI Personalia

Im Jahr 1980 trat **Dr.-Ing. Karl-Heinz Czychon** in den VDI ein.

In die Metropolregion führte ihn sein Berufsweg, als er Technischer Vorstand der Mannheimer Großkraftwerk AG wurde.

Im Januar 2003 konnte der nordbadisch-pfälzische Bezirksverein (BV) ihn zum ersten Mal offiziell in seiner Runde im Engeren Beirat begrüßen. In den folgenden über zwölf Jahren hat er sich für den BV engagiert. Im Jahr 2006 übernahm Czychon die Funktion des Vorsitzenden – ein Amt, das er zwei Wahlperioden mit viel Einsatz, Kreativität und Überzeugung ausgefüllt hat. Nach dem Stabwechsel blieb er im Engeren Beirat aktiv.

Zum Jahresende geht Czychon in den Ruhestand. Der BV dankt ihm für seine Verbundenheit und wünscht alles Gute für die kommende Zeit.

Sybille Breunig
Foto: VDI

VDE-VDI-Veranstaltungen

Wir bitten zu beachten, dass dieser Überblick auf dem Stand **Mitte November** beruht.
Neue Veranstaltungen und Änderungen können nach Redaktionsschluss nicht mehr berücksichtigt werden.
Details zu den Veranstaltungen dieser Auflistungen, Änderungen sowie neu eingestellte Angebote finden Sie tagesaktuell im Internet: www.vde-kurpfalz.de + www.vdi-nordbaden-pfalz.de

	Datum / Zeit	Thema	Ort
VDI	**13.01.2016 18:00 Uhr**	**forum mannheim, Vortrag:** Mobilität der Zukunft – Autonomes Fahrzeug	**Mannheim TECHNOSEUM**
VDE	**20.01.2016 14:00 Uhr**	**Exkursion:** VDE-Institut	**Offenbach**
VDInis im Alter von 6–7 Jahren	**23.01.2016 10:00 Uhr und 12.00 Uhr**	**Abheben und Fliegen**	**Mannheim TECHNOSEUM**
VDI VDE	**10.02.2016 17:30 Uhr**	**AK Leitsysteme, Vortrag:** Erfolgreiche IT-gestützte Umsetzung der Risiko basierten Instandhaltung	**Mannheim TECHNOSEUM**
VDInis im Alter von 4–5 Jahren	**27.02.2016 10:00 Uhr und 12.00 Uhr**	**Wackelclown**	**Mannheim TECHNOSEUM**
VDI	**09.03.2016 18:00 Uhr**	**forum mannheim, Vortrag:** Big Data: Datenschutz und Persönlichkeitsrechte im Netz	**Mannheim Hochschule**
VDI	**07.04.2016 18:00 Uhr**	**AK Technikgeschichte, Vortrag:** 100 Jahre Skagerrak-Schlacht – Moderner Technikeinsatz oder Technikanachronismus in der größten Seeschlacht des Ersten Weltkrieges	**Mannheim TECHNOSEUM**
VDInis im Alter von 4–5 Jahren	**09.04.2016 10.00 Uhr**	**Licht und Schatten**	**Heidelberg EXPLO**
VDI	**13.04.2016 18:00 Uhr**	**forum mannheim, Vortrag:** Der gläserne Mensch – Ethik im digitalen Zeitalter	**Mannheim Abendakademie**
VDInis im Alter von 6–7 Jahren	**16.04.2016 10:00 Uhr**	**Papierschaltkreise**	**Heidelberg EXPLO**
VDI	**20.04.2016**	**JAHRESMITGLIEDERVERSAMMLUNG**	**Ludwigshafen AbbVie**
VDE	**22.04.2016**	**JAHRESMITGLIEDERVERSAMMLUNG**	**Mannheim Duale Hochschule**
VDInis im Alter von 6–7 Jahren	**23.04.2016 10:00 Uhr und 12.00 Uhr**	**Museumsdetektive**	**Mannheim TECHNOSEUM**
VDE	**01. – 05.02.2016**	**Seminar:** Zertifizierungslehrgang Power Quality Sachkundiger	**Mannheim Hochschule**
VDE	**09.05.2016**	**Seminar:** Power Quality Sachkundiger, Prüfung	**Mannheim Hochschule**
VDInis im Alter von 4–5 Jahren	**18.06.2016 11.00 Uhr**	**Blick ins All**	**Heidelberg Haus der Astronomie**
VDInis im Alter von 6–7 Jahren	**16.07.2016 11.00 Uhr**	**Blick ins All**	**Heidelberg Haus der Astronomie**

Datenhinweis: Es kann erforderlich sein, Ihre Daten zum Zweck der Organisation und Durchführung für die oben genannten Veranstaltungen zu erheben und an die Veranstaltungskooperationspartner weiterzugeben. Bei Veranstaltungen entstandene Fotos und Aufnahmen können im Rahmen von Berichten, in Zeitschriften und im Internet veröffentlicht werden.

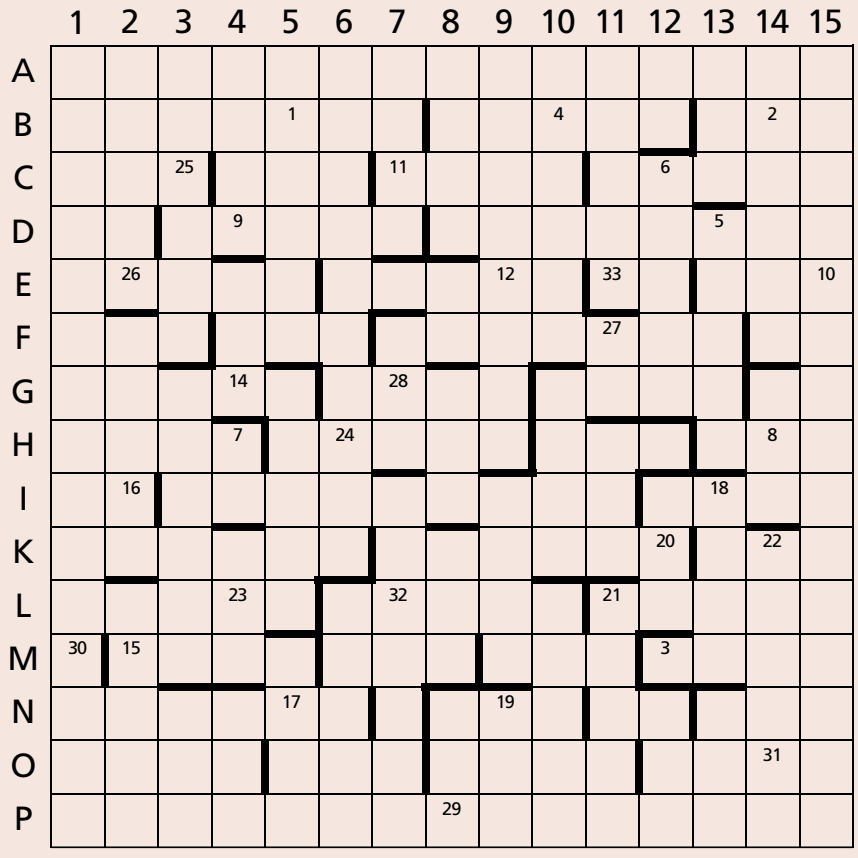
Gehirngymnastik: Preisrätsel

Entwurf: Prof. Dr. Hans Kahlen

Unser Rätsel enthält heute über 12 Begriffe, die sich auf Ende und Beenden beziehen oder in Verbindung damit angewendet werden können.

Waagerecht:
A1: Schreiben beim Verlassen; B1: etwas Unbekanntes vor sich; B8: Halbedelstein; B13: Fluss aus der Eifel; C1: Bewertung; C4: in die Jahre gekommen; C7: Widerhall; C11: Quittung für Zahlung; D1: Kurzf. für einen Fachbereich; D3: männl. Vorname; D8: chronische Veränderung der Leberzellen; E1: Fluss in Westfalen; E6: marok. Frauenname; E11: Beratungsstelle für Lebensfragen, Abk.; E13: Energieversorger in Bayern, Abk.; F1: Lebensbund; F4: Startdatei, Abk.; F7: Adverb; Wunsch vor dem Eintreten; F14: Kennzeichen für europ. Norm; G1: Bewegen; G6: Schluss, Aus; G10: Pilzbakterien; G14: Tierprodukt; H1: besitzanz. Fürwort; H5: Edelgas; H10: Schluss; H13: Halbton unter d; I1: Teil der Bibel; I3: Festlegung einer Größe; I12: unfein; K1: Wehklagen; K7: früh. ital. Tenor; K13: Abschiedsgruß; L1: glatt machen; L6: Vorname eines amerik. Popmusikers; L11: Funkortungssystem; M2: russ. männl. Vorname; M6: Weideland auf einem Berg; M9: ungebraucht; M12: ital.: Ende; N1: betrübl. Gemütsstimmung; N8: amerik. Militärrundfunkdienste; N11: hinw. Fürwort; N13: franz.: See; O1: weibl. Vorname; O5: vor Vergleich; O8: nicht fest; Teilabschnitte; O12: gebundene Schrift; P1: Behörde für Erbangelegenheiten.

Senkrecht:
1A: Sachzustände; 2A: Errungenes oder Gestohlenes; 2F: Tag nach gestern; 2L: früh. Name von Myanmar; 3A: langes Priestergewand; 3G: geol. Vertikalbewegung; 3N: amerik. Fernsehsender; 4A: größere Familiengruppe; 4E: überhaupt nicht; 4H: Erwiderung beim Skat; 4K: männl. Vorname; 5A: nicht abgeben; 5G: persönl. Kennzeichnung; 5M: wirklich vorhanden; 6A: Feinabstimmung von Tonhöhen; 6L: weibl. Vorname; 7A: paradis. Garten; 7F: nicht weit; 7I: absol. Ende; 8A: Hausabdeckung; 8E: Kennzeichen für Düren; 8G: Rechner Betriebssystem; 8K: dt. Schriftsteller und Maler, Museum in Rolandseck; 8N: wie O5; 9A: Trennen, Abschied nehmen; 9I: Harnflüssigkeit; 9N: engl.: dichter Nebel; 10A: indische Stadt; Hauptst. Madhya Pradesh; 10G: kleines Boot; 10L: salopp für Beenden; 11A: Hauptstadt von Marokko; 11F: salopp: Eselprokura; 11H: Abk. für umgangssprachlich; 11L: Einrichtung zur Richtungsänderung; 12A: neue Abk. für Datenverarbeitung; 12C: Fluss in Südtirol; 12I: kleinster indischer Bundesstaat; 12N: Abschluss am Gymnasium, Abk.; 13A: Passionsort in Tirol; 13D: Nachmahd, zweiter Grasschnitt; 13I: Rettich; 13N: franz. Vorname; 14A: Körperteile; 14K: später; 15A: Niederschrift einer abgeschlossenen Sache.



Lösung:

1	2	3	4	5	6	7	8	9		10	11	12		Z	14	15	16
17	18	19	20	21	22	23	24	25		26	27	28	29	30	31	32	33

Lösung des Preisrätsels aus Heft 2/2015

Die richtige Lösung lautet:

MIT MUSIK GEHT MANCHMAL, ALLES BESSER

Gewonnen hat
Dr. Erich Weippert

Wir gratulieren Herrn Dr. Weippert und wünschen ihm viel Spaß mit dem Präsent. Allen übrigen Einsendern danken wir für die rege Beteiligung, über die wir uns sehr gefreut haben.

... und in diesem Sinne ist dies das letzte Rätsel aus der Feder von Professor Kahlen. Er zieht sich nach vielen Jahren aus der aktiven Mitarbeit zurück, und der Redaktionsbeirat sagt: „Herzlichen Dank für Ihr Engagement und alles Gute!“

Die Buchstaben ergeben in der zahlenmäßig vorgegebenen Reihenfolge einen Lösungsspruch, der zum heutigen Thema passt.

Senden Sie den Lösungsspruch bis zum 1.2.2016 an die VDI/VDE Geschäftsstelle, Julius-Hatry-Straße 1, 68163 Mannheim, mit dem Kennwort: **technikforum** 2015-3, oder per E-Mail an: mail@vdi-nordbaden-pfalz.de. Die Einsender mit der richtigen Lösung nehmen an der Verlosung eines Präsentes teil.

VDI Nordbadisch-Pfälzischer Bezirksverein e.V.

VDI-Mitgliederversammlung 2016

Datum: Mittwoch, den 20. April 2016
Uhrzeit: 17:30 Uhr
Ort: AbbVie Ludwigshafen

Vorgesehene Tagesordnungspunkte

- Begrüßung
- Vorstellung – Präsentation AbbVie
- Geschäftsbericht 2015
- Kassenbericht 2015 und Haushaltsplan 2016
- Bericht der Rechnungsprüfer
- Entlastung des Vorstandes
- Wahlen
- Anträge
- Verschiedenes

Im Anschluss an die Versammlung laden wir Sie gerne zu einem Imbiss ein.

Gez. Prof. Dr.-Ing. Dieter Leonhard
Vorsitzender VDI Nordbadisch-Pfälzischer Bezirksverein e.V.

Vorankündigung

Die Jahresmitgliederversammlung 2016 findet statt

am: Freitag, den 22. April
in der: Dualen Hochschule Baden-Württemberg, Mannheim

Die Tagesordnung erhalten die Mitglieder rechtzeitig.

Gez. Prof. Dr.-Ing. Wolfram Wellßow
Vorsitzender VDE Kurpfalz

Die nächsten Ausgaben des technikforum

01/2016:
März / April

02/2016:
Juli / August

03/2016:
November / Dezember

Sie finden das aktuelle technikforum sowie vorangegangene Ausgaben auf den Homepages:
www.vdi-nordbaden-pfalz.de
www.vde-kurpfalz.de

Impressum

Herausgeber
VDI Verein Deutscher Ingenieure,
Nordbadisch-Pfälzischer Bezirksverein e.V.
Vorsitzender: Prof. Dr.-Ing. Dieter Leonhard

VDE Verband der Elektrotechnik Elektronik Informationstechnik, Bezirk Kurpfalz
Vorsitzender: Prof. Dr.-Ing. Wolfram Wellßow

VDE / VDI-Geschäftsstelle
Leitung: Sybille Breunig AdL
Mafinex-Technologiezentrum
Julius-Hatry-Str. 1
68163 Mannheim
Tel. 0621-22657
Fax 0621-20285

E-Mail
VDI: mail@vdi-nordbaden-pfalz.de
VDE: vde-kurpfalz@vde-online.de

Redaktion
Sybille **Breunig** AdL, VDE/VDI
Dipl.-Ing. Winfried **Eberbach,** GKM AG
Dipl.-Ing. Ernst-Dieter **Keller,** Siemens AG
Dipl.-Ing. Alexander **Kling,** VDI
Dr. Hartmut **Knittel,** TECHNOSEUM
Dr. Rainer **Kuntz,** Freudenberg Gruppe
Prof. Dr. Ralph **Urbansky,** TU Kaiserslautern
Alexander **Vogler** M. A., ABB AG

Endredaktion: Sybille Breunig AdL

Druck:
Chroma Druck & Verlag GmbH
Werkstraße 25, 67354 Römerberg-Berghausen
info@chroma-druck.de