Ausgabe 02 | 2017

Z!

DAS ZUKUNFTSMAGAZIN

SCHWERPUNKTTHEMA SEITE 3 - 17:

IT-Sicherheit

AVG ASCHAFFENBURGER VERSORGUNGS GMBH
FrankfurtRheinMain GmbH International Marketing of the Region
OhmEx Industrielle Elektrowärme GmbH

Impressum

ZENTEC
Zentrum für Technologie, Existenzgründung
und Cooperation GmbH
Industriering 7
63868 Großwallstadt

Telefon: 06022 26-0
Telefax: 06022 26-1111

Die nächste Ausgabe von Z!
Redaktionsschluss: 18. Oktober 2017
Erscheinungstermin: Ende November 2017

ISSN-Nr.: 1862-1104
Auflage: 3000
Bezug kostenlos

E-Mail: redaktion@zukunftsmagazin.de
Internet: www.zukunftsmagazin.de

Redaktion & Anzeigenbetreuung:
Dr. Gerald Heimann

INHALT

I Inhalt 1

II Editorial 2

III Schwerpunktthema: 3
Datenschutz in Europa – Gleiches Recht für alle! ... 3
Wer schützt das Internet der Dinge? ... 5
Der Mensch im Fokus der IT-Sicherheit ... 6
Smart Industrial IT Security ... 8
IP-Schutz für CAD-Modelle: Innovative 3D-Technologie sichert sensible Konstruktionsdaten ... 9
Vorreiter in Sachen Informationssicherheit: die Stadtwerke Aschaffenburg ... 11
APOLI – die Fernwartung der Zukunft ... 12
IT Sicherheit: „nur die Spitze des Eisbergs“ ... 15
mainproject 2018 begleitet Industrie 4.0-Einführung in der Mainsite-Ausbildung ... 16

IV Z! Das Zukunftsmagazin im Interview mit Prof. Rainer Sieber 18

V Produkte, Projekte und Dienstleistungen 21
Migration zur neuen Netztechnologie ... 21
Virtuelle Telefonie – die Kommunikation der Zukunft ... 22
Digital Leadership ... 24
macooa - Von der Projektplanung bis zur Rechnung alles online ... 25
EU Datenschutz Grundverordnung (DSGVO), Bundesdatenschutzgesetz(neu) Jetzt wird es ernst! ... 26
Wie lernt ein Auto, Radfahrer zu verstehen ... 27
Fahrerloses Absperrfahrzeug für mehr Sicherheit an Tagesbaustellen ... 29

VI Stimmen und Maßnahmen aus Bundes- und Landespolitik 31
Politikansätze für mehr Sicherheit in der digitalen Gesellschaft ... 31
Für eine gerechte Arbeitswelt der Zukunft ... 32
In Bayern hat die digitale Zukunft schon begonnen ... 34
Standpunkte: WannaCry-Hackerangriff ... 36
Stark gefragt: IT-Experten in KMU ... 37
Schicht für Schicht: Neue Dimensionen in der Fertigung durch 3D-Druck ... 37

VII Kurzmeldungen 37
Hochautomatisiert unterwegs – Forschungsprojekt Ko-HAF zieht positive Zwischenbilanz ... 38
Anwendungspartner für Industrial-IT-Security-Projekt gesucht! ... 39
IHK-Unternehmerreise in die chinesische Provinz Shandong ... 40
InnovationsForum – Blockchains ... 40

VIII Kolumne z!um Schluss 41

EDITORIAL

Liebe Leserinnen und Leser,

„Daten sind das neue Gold“. So hört man es, so liest man es und alle nicken mit dem Kopf, was logisch ist: immerhin vernetzt sich unsere industrialisierte Wirtschaftswelt immer intensiver, digitalisiert sich und steigert den Wert von Daten immer weiter. Und außerdem erschrecken wir bei Cyber-Angriffen wie dem von „wannaCry“, sind froh, dass es uns nicht erwischt hat und gehen zur Tagesordnung über. Zumindest viele von uns.

Wenn Daten das neue Gold sind, schützen wir es eigentlich richtig? Wie schaut es aus mit Prozessen, mit den internen Kompetenzen und Prioritäten, der Investitionsbereitschaft, IT-Architektur und der Personalführung? Eines dürfte klar sein: das Gefahrenpotenzial steigt in einer sich digitalisierenden Welt, in der Maschinen mit Maschinen miteinander über Blockchains Geschäfte machen, in der in Echtzeit über Kontinente hinweg Standorte und Produktionsstätten miteinander kommunizieren und in der die berufliche mit der privaten Welt über Smartphones, Smartwachtes, Social Media etc. konvergiert.

Spannende Themen, für die Sie im vorliegenden Z! Zukunftsmagazin viele Informationen und Beiträge finden. Wie wichtig das Thema auch parteiübergreifend auf Bundes- und Landesebene diskutiert wird und welches umfangreiche Instrumentarium entwickelt wird, lesen Sie in einer eigenen Rubrik „Stimmen und Politikansätze aus Bund und Freistaat“. Besonders spannend ist auch das Interview mit Rainer Sieber, Geschäftsführer der Sapiens42 GmbH und Professor an der Hochschule der Bundeswehr.

Sicherheit in Bezug auf unsere Mobilität finden Sie in einem Artikel von „Hessen mobil“ sowie in einem Bericht der Hochschule Aschaffenburg - und in einem Artikel von uns, in dem wir Ihnen über die Zwischenpräsentation des Verbundprojekts „Ko-HAF Kooperatives hochautomatisiertes Fahren“ berichten, in dessen Rahmen u.a. eine Teststrecke auf den Autobahnen rund um Frankfurt eingerichtet wurde.

Viel Spaß beim Lesen wünscht Ihre Z! Redaktion

„Aktionstag Elektromobilität“

Elektronen statt Diesel – innovative Fahrzeugkonzepte auf unseren Straßen

Datum: 20. September 2017
Uhrzeit: 13:00 Uhr
Ort: ZENTEC GmbH – Industriering 7,63868 Großwallstadt

Weitere Informationen und Anmeldung unter:
http://kompetenznetze-untermain.de/aktionstag-elektromobilitaet

KUNZMANN Die neue Service-Dimension
Preissler Entdecken Fahren Freuen
RENAULT Passion for life
DIE WOLFERT GRUPPE zuverlässig - sympathisch - modern
Eichhorn
AUTOHAUS SEITZ
Elektro Braun www.elektro-braun.de

Datenschutz in Europa – Gleiches Recht für alle!

Ab dem 25. Mai 2018 gilt auch für Ihr Unternehmen die Europäische Datenschutz-Grundverordnung – Erfahren Sie die wichtigsten Neuerungen und wie Sie sich gut darauf vorbereiten

Als am 1. Januar 1978 das Bundesdatenschutzgesetz in Kraft trat, war es eines der ersten Datenschutzgesetze in Europa. Andere Länder zogen erst später nach und die Inhalte der jeweiligen Gesetze gingen weit auseinander. Erst als die EU 1995 eine Datenschutzrichtlinie verabschiedete, mit der Mindeststandards zum Schutz personenbezogener Daten innerhalb von 36 Monaten in nationales Recht umzusetzen waren, konnte man von einem einheitlichen Datenschutzniveau in Europa ausgehen. Allerdings gab es nur ein einheitliches Mindestniveau und die Länder begannen in den folgenden Jahren, bei den Anforderungen zum Schutz der Betroffenen, bzw. bei dem, was den Unternehmen bei der Verarbeitung dieser Daten erlaubt wird, wieder auseinander zu driften. Rechtsstreitigkeiten vor dem Europäischen Gerichtshof EuGH (z.B. Facebook-Urteil), Unternehmensverlagerungen in Länder mit weniger stringenter Datenschutzauslegung und uneinheitliche Beschwerdemöglichkeiten für Verbraucher waren die Auswirkung dieses Flickenteppichs an bestehenden Datenschutzregelungen.

Kernziele der neuen Datenschutz-Grundverordnung

Mit der neuen EU-Datenschutz-Grundverordnung (DSGVO) soll das **Datenschutzrecht innerhalb Europas** vereinheitlicht werden, um dem Einzelnen mehr Kontrolle über seine Daten zu verschaffen. Entsprechend gelten künftig in allen EU-Staaten die gleichen Standards in Sachen Datenschutz, datenschutzrechtliche „Rückzugsräume" innerhalb Europas wird es damit nicht mehr geben.

Gelten sollen die neuen Regeln nicht nur für in Europa ansässige Unternehmen. Alle globalen Unternehmen (z.B. US-Firmen) müssen sich fortan an die europäischen Vorgaben im Datenschutz halten, wollen sie ihre Dienste auch auf dem europäischen Markt anbieten. Das bislang immer gern vorgebrachte Argument, man sei nur an die US-amerikanischen Vorgaben gebunden, kann dann nicht mehr gelten.

Erstmals findet sich auch die Forderung **„Datenschutz durch Technik"** in einer gesetzlichen Regelung. Derzeit ergeben sich die Maßnahmen, welche zum Schutz der personenbezogenen Daten getroffen werden müssen, aus §9 Bundesdatenschutzgesetzes (BDSG) und werden dort als Oberbegriffe für technische und organisatorische Umsetzungen genannt. Weder die für ein Unternehmen zu berücksichtigenden Risiken noch die angemessenen Schutzmaßnahmen werden genannt. Die DSGVO ist hier deutlich konkreter. Es werden die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit aufgelistet. Die Unternehmen müssen dann den Schutzbedarf der bei ihnen vorhandenen Daten (Beschäftigtendaten, Kundendaten, Patientendaten usw.) ermitteln, diese mit der Eintrittswahrscheinlichkeit eines bestimmten Risikos sowie der Schwere der Auswirkung für die Rechte und Freiheit der betroffenen Person bei Eintritt des Risikos bewerten und daraus resultierend eine dem aktuellen Stand der Technik entsprechende Schutzmaßnahme etablieren.

Darüber hinaus gibt es nun auch die Anforderung „Privacy by Design", also „Datenschutz durch Technik" sowie „Privacy by default" / „Datenschutzfreundliche Voreinstellung", welche sicherstellen soll, dass der Datenschutz und die Privatsphäre bereits bei der Entwicklung von Technik beachtet werden. Diese soll so angelegt sein, dass nur die Daten erhoben und verarbeitet werden, die auch tatsächlich benötigt werden. Der Nutzer behält dabei die Kontrolle über die eigenen Daten.

Die **Stärkung der Betroffenen** bzw. **der Verbraucherechte** durch die Grundverordnung hat massive Auswirkungen auf die Art der Datenverarbeitung in den Unternehmen. Künftig sollen Betroffene leichteren Zugang zu ihren Daten haben. Dafür wurden zahlreiche neue Details bei den Betroffenenrechten ergänzt. Jeder hat z.B. ein Recht auf Auskunft und ein Recht auf Information, das Recht auf Löschung, Berechtigung, das Recht auf Vergessen werden und die Einschränkung der Verarbeitung. Und immer, wenn der Betroffene ein Recht hat, ergibt sich eine Pflicht für das Unternehmen.

Auf folgende Fragen sollten alle Unternehmen ab Mai 2018 Antworten geben können:
- Woher stammen die Daten eines Betroffenen,
- warum haben Sie die Daten,
- was machen Sie mit den Daten,
- geben Sie Daten an einen Dritten weiter,
- wann werden Sie die Daten löschen?

Auch Unternehmen, bei denen die Verarbeitung von personenbezogenen Daten nicht der eigentliche Geschäftszweck ist, können sich nicht entspannt zurücklehnen, denn Beschäftigte und Kunden sind auch hier sicher vorhanden.

Die größte Änderung und Auswirkung der neuen DSGVO hat aber die **Ausweitung der Verantwortlichkeit der Unternehmen**. Denn alle Unternehmen unterliegen nun der RECHENSCHAFTSPFLICHT! Das bedeutet, es ist für die Einhaltung der gesetzlichen Datenschutzgrundsätze (Rechtmäßigkeit, Treu und Glauben, Transparenz / Zweckbindung / Datenminimierung / Richtigkeit / Speicherbegrenzung / Integrität und Vertraulichkeit durch angemessene Sicherheit der Datenverarbeitung) verantwortlich UND muss die Einhaltung nachweisen.

Zukünftig muss also ein Betroffener oder eine Aufsichtsbehörde nicht mehr eine Verfehlung des Unternehmens nachweisen, sondern das Unternehmen muss zu jeder Zeit dokumentieren können, dass es rechtskonform arbeitet, Risiken bewertet, geeignete Schutzmaßnahmen etabliert und regelmäßig die Wirksamkeit dieser Schutzmaßnahmen und die Rechtmäßigkeit der Datenverarbeitung überprüft. Sollten Sie noch keine Dokumentation Ihrer Geschäftsprozesse besitzen sollten Sie zeitnah damit beginnen!

Nicht unerwähnt bleiben darf auch die neue Sanktionsmöglichkeit der DSGVO. Wo im alten BDSG Bußgelder bis max. 50 TSD € für einfache Verstöße und bis max. 300 TSD € für erhebliche Vergehen vorgesehen waren, orientiert sich die DSGVO am Kartellrecht und stößt in neue Dimensionen vor. Für einfache Vergehen können nun, je nach Schwere des Vergehens, Bußgelder mit bis zu 20 MIO € bzw. 4% des weltweit erzielten Vorjahresumsatzes fällig werden. Zusätzlich sind nun auch Versäumnisse mit einem Bußgeld belegbar, die bislang nur nachgebessert werden mussten.

Abschließend darf man sagen. dass sich viele Teile aus unserem alten Bundesdatenschutzgesetz in der neuen Europäischen Datenschutz-Grundverordnung wiederfinden. Vom Datenschutzbeauftragten, den es bislang nur in Deutschland verpflichtend gab, bis zu den verpflichtenden Datenschutzverträgen mit „Auftragnehmern“ bei der Überlassung von personenbezogenen Daten. Der „Kulturschock“ fällt für uns damit vergleichsweise moderat aus. In anderen Ländern ist der Umstieg von der bisherigen nationalen Regelung auf die neuen gemeinsamen Bestimmungen wesentlich arbeitsintensiver. Trotzdem müssen sich auch in Deutschland die Unternehmen für die neuen Herausforderungen fit machen und insbesondere die bekannten Defizite bei den Unternehmensdokumentationen abstellen.

Da die oben aufgeführten Neuerungen nur die Spitze des Eisberges der gesetzlichen Anforderungen darstellen, sollte man sich zeitnah bei Experten über die Auswirkungen welche die neue Grundverordnung für Ihr Unternehmen im Einzelnen hat informieren. Ab dem 25. Mai 2018 gilt nur noch die DSGVO und es gibt keine Übergangsfrist vom alten BDSG!

BE-protected
Die Experten für Datenschutz & Datensicherheit

Ansprechpartner

Jens Burkard - Geschäftsführer
BE-protected UG
Die Experten für Datenschutz und Datensicherheit
Telefon: 06182 829031
E-Mail: Jens.Burkard@be-protected.de
www.be-protected.de

Wer schützt das Internet der Dinge?

Mit „Industrie 4.0“ rückt auch das Thema IT-Sicherheit in den Fokus. Denn wenn alles miteinander vernetzt ist, eröffnen sich völlig neue Einfallstore. Die Verantwortung, das eigene Unternehmen zu schützen, liegt künftig auf vielen Schultern.

Der Vandale der Zukunft braucht kein geöffnetes Fenster, um in die Fabrik einzudringen. Er könnte sein zerstörerisches Werk vom Schreibtisch aus erledigen. Zumindest theoretisch, wenn Unternehmen, die mit vernetzten Produktionsabläufen arbeiten, ihr Netzwerk und ihre Produktionssysteme nicht angemessen schützen. „Wenn wir uns ausmalen, dass künftig immer mehr Fahrzeuge und Maschinen mit IT-Systemen gesteuert werden, dann entstehen da natürlich auch neue Einfallswege“, sagt Stefan Rieck, Chief Information Security Officer der KION Group. Das beträfe dann auch den vernetzten Stapler oder das vernetzte vollautomatische Hochregallager, die stillgelegt, zerstört oder gar als Vehikel für weitere Schäden zweckentfremdet werden könnten.

Zwei Welten wachsen zusammen

„Industrie 4.0“ ist ein Begriff, der im Kern immer damit zu tun hat, dass mehr und mehr Dinge miteinander vernetzt werden. Nun lassen sich Daten austauschen - zwischen Maschinen, Fahrzeugen und Mitarbeitern, zwischen Produzenten und Kunden. Der Kunde kann in Echtzeit verfolgen, wie sein Produkt gebaut wird, und in der Fabrik lässt sich detailgenau vorausplanen, wann Ersatzteile eintreffen. Neue Möglichkeiten, die allgemein begrüßt und sogar eingefordert werden. „Es wachsen zwei Welten zusammen“, sagt Rieck. Büro- und Produktions-Informationstechnologie, Computer und Werksmaschinen. Das aber führt auch zu wesentlich mehr beteiligten Partnern in einem einzigen Netzwerk. Plötzlich reicht es nicht mehr aus, die eigene Fabrik zu schützen – auch Kunden, Zulieferer oder Gebäudetechniker müssen ihre Zugänge sichern. „Die Verantwortung liegt nicht mehr bei einer einzigen Stelle, nicht mehr nur bei der IT“, fasst Rieck zusammen.

Dabei sind die Schutzmechanismen prinzipiell nicht neu, sondern bereits aus der traditionellen Büro-IT bekannt. Wie Virenschutz, verschlüsselte Datenübertragung, Firewalls oder Authentifizierung sowie die enge Zusammenarbeit mit zertifizierten, externen Partnern und Sicherheitsspezialisten, die Systeme und Netze regelmäßig auf Schwachstellen testen.

Also alle Maßnahmen, die davor schützen, dass jemand in das Netzwerk eindringt, und gleichzeitig die Garantie bieten, dass ein bestimmtes Datenpaket tatsächlich vom Gabelstapler gesendet wurde – und eben nicht von einem unerkannten Eindringling. In den kommenden Jahren wird es darauf ankommen, diese Werkzeuge sinnvoll aus dem Büroalltag auf die vielfältigen Einsatzmöglichkeiten in der Produktion zu übertragen.

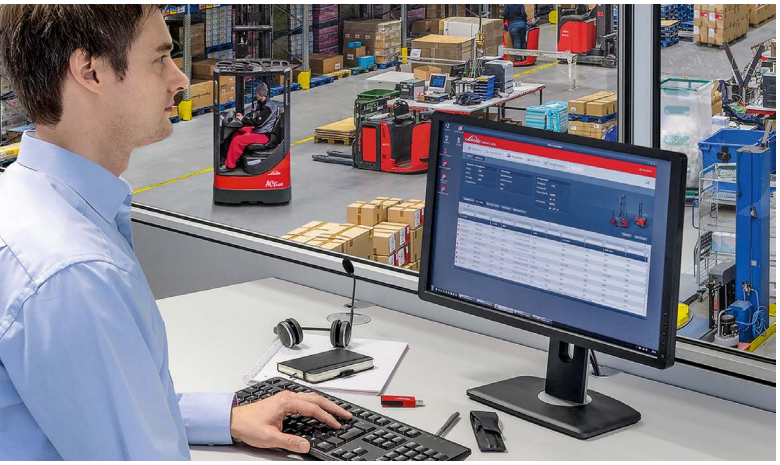
Kann Steuerungselektronik auch Angriffe abwehren?

Für jemanden, der eindringt, um Schaden anzurichten, ist das Angriffsziel womöglich gar nicht der vernetzte Stapler selbst, sondern er dient nur als Schnittstelle zum nächsten Server und damit als Mittel zur Industriespionage. „Künftig müssen sich alle Produzenten bewusst sein, dass ihre Produkte

missbraucht werden könnten für etwas, das so nie geplant war“, sagt Rieck. Das erfordert bereits beim Entwurf und Design ein Umdenken. Die Steuerungselektronik eines Staplers etwa wurde früher allein dafür entworfen, um das Gerät zu bedienen – sie sollte nicht etwa auch die Rechenkraft für eine Abwehr von Hackerangriffen aus dem Internet besitzen. Müssen dazu weitere Komponenten eingebaut oder ganz individuelle Lösungen gefunden werden?

Die Ingenieure der KION Group berücksichtigen solche Themen bereits.

„Das Thema IT-Sicherheit wird auf jeden Fall ein spannendes Feld für kreative Köpfe", sagt Rieck. Das Spektrum sei breit, es werden viele Abteilungen und Experten zusammenarbeiten müssen. Was sicherlich einem Unternehmen wie der KION Group entgegen käme. Sie sei besonders breit aufgestellt ist, sowohl in der klassischen Flurförderzeug-Konstruktion als auch in Software und Vernetzung nach dem jüngsten Zukauf des Automatisierungsexperten Dematic. „Klar ist: Je mehr in Zukunft unter dem Label ‚Industrie 4.0' zusammenwächst, desto komplexer wird es." Sinnvoll wäre vermutlich, wenn sich in der Branche bald klare Standards herausbildeten und sie Akzeptanz fänden, damit alle an einem Strang ziehen könnten.



IT-Sicherheit wird zum Qualitätsmerkmal

Auch die Verantwortung, sein Unternehmen zu schützen, wird auf vielen Schultern verteilt sein. Denn was nützt, sinnbildlich, das bestgesicherte Haus, wenn der Mieter den Schlüssel unter die Fußmatte legt? Rieck sieht das Bewusstsein bei den Kunden allerdings längst angekommen: „Sehr viele Kunden fragen das Thema direkt an, zeigen sich sensibel und aufgeklärt." Immer häufiger verlangten auch gerade kleinere Unternehmen, die keine eigene Expertise aufbauen können, dass größere Produzenten wie die KION Group das Thema beherrschen. IT-Sicherheit werde in Zukunft ein Qualitätsmerkmal sein. Und „Industrie 4.0" bedeute eben nicht nur, alles zu machen und alles zu vernetzen, was möglich ist. „Es bedeutet auch Verantwortung", betont Rieck. „Und die nehmen wir sehr ernst."

Ansprechpartner

David Frogier de Ponlevoy
Profilwerkstatt GmbH
Telefon: 06151 599020
E-Mail: info@profilwerkstatt.de

Der Mensch im Fokus der IT-Sicherheit

In einer von PwC im Februar 2017 veröffentlichten Studie geben insgesamt 400 mittelständische Unternehmen Auskunft über ihren aktuellen Stand zur Informationssicherheit. Dabei führt knapp 1/5 der Befragten an, innerhalb des letzten Jahres mindestens einer erfolgreich durchgeführten Cyberattacke zum Opfer gefallen zu sein. Im Vergleich zur Vorjahresstudie hat sich somit die Anzahl der angegriffenen Unternehmen nahezu verdoppelt. Bei der Betrachtung der Schwachstellen in Bezug auf den Schutz informationeller Werte steht bei 76% der Studienteilnehmer nach wie vor der Mensch an erster Stelle.

WannaCry

Diese Einschätzung wird auch durch den jüngsten Fall von Cyberkriminalität rund um die Ransomware „WannaCry“ bestätigt. Versteckt im Anhang oder getarnt als unverfänglicher Link in einer harmlos anmutenden E-Mail bahnte sich der Schädling seinen Weg in die digitalen Postfächer dieser Welt. Auf der Gegenseite verhalf der nichtsahnende Mitarbeiter der Deutschen Bahn, bei Renault, FedEx und Co. dem Verschlüsselungstrojaner mit Wurm-Charakter per Mausklick in die Freiheit. Gepaart mit einem veralteten Betriebssystem oder versäumten Updates verschlüsselte WannaCry zunächst die vom infizierten Gerät aus erreichbaren Dateien auf Festplatten, Speichermedien und im Netzlaufwerk, um anschließend selbständig weitere Rechner im Netzwerk ausfindig zu machen und zu befallen.

Gefahrenquelle USB-Stick

Doch nicht nur per Mail gelangt immer wieder Malware in Systeme, auch ein böswillig umprogrammierter oder unfreiwillig infizierter USB-Stick in der Hand eines unbedarften PC-Nutzers kann ungeahnte Folgen haben. Ein Experiment der Firma Sophos aus dem Jahr 2011 macht deutlich, wie ernst diese Thematik genommen werden sollte. Sophos kaufte bei einer Fundsachen-Auktion der australischen Rail Corporation in Sydney insgesamt 50 intakte USB-Sticks auf. Anschließend durchgeführte Tests ergaben, dass ein beachtlicher Anteil von 66% der Sticks mit Schadsoftware verseucht war. Paul Ducklin, Senior Security Advisor bei Sophos, sagte damals, dass es ganz danach aussieht, als seien die betroffenen Speichermedien nicht vorsätzlich von Kriminellen mit Schadsoftware versehen und platziert worden, sondern dass die Analyse die weite Verbreitung schlechter PC-Hygiene offenlegt. Dies ist allerdings nicht minder gefährlich, da man nach dieser Erkenntnis wohl nicht einmal mehr USB-Sticks von Freunden mit gutem Gewissen in den eigenen PC stecken kann.

Menschliche Neugier

Dass gefundene USB-Speichermedien vom Finder häufig ohne Vorkehrungen mit einem PC verbunden werden, belegt eine Studie der Universitäten Illinois und Michigan aus 2016. Zakir Durumeric und sein Team verteilten 297 USB-Sticks auf dem Campus der University of Illinois, präpariert mit Dateien, nach deren Öffnen eine Rückmeldung an die Wissenschaftler gegeben wird. Bei 45% der Sticks wurde mindestens eine Datei geöffnet und in der anknüpfenden Befragung gab eine Mehrheit von über 2/3 an, keinerlei Vorsichtsmaßnahmen vor dem Einstecken des Mediums getroffen zu haben. Einige wenige äußerten sogar, sie haben bewusst einen Rechner der Universität verwendet, um ihren eigenen keiner Gefahr auszusetzen. Darüber, ob die restlichen Speichersticks, von denen keine Rückmeldung kam, nicht auch angesteckt worden waren, kann nur spekuliert werden.

Prävention

In Bezug auf die Gewährleistung der Informationssicherheit innerhalb eines Unternehmens wird deutlich, dass die Verantwortung bei jedem einzelnen Mitarbeiter beginnt. Hierzu ist die kontinuierliche Sensibilisierung des Personals unerlässlich, damit durch stetige Maßnahmen ein unternehmenskulturelles Bewusstsein zur IT-Sicherheit geschaffen werden kann. Für den Fall, dass doch einmal der PC eines Mitarbeiters von einem Schädling befallen wird, sollten Systeme so strukturiert sein, dass die Auswirkungen des Angriffs so gering wie möglich gehalten werden können. Neben der altbekannten Mahnung, stets flächendeckend die Aktualität eingesetzter Software und Betriebssysteme sicherzustellen, hätte im Kasus „WannaCry“ die strikte Trennung der Anwendergeräte von Datenbanken und Datei-Systemen vor der Datei-Verschlüsselung geschützt. Ein Dokumentenmanagementsystem beispielsweise, dessen Clients keine direkten Aktionen auf den zugeordneten internen Datenbank- und Datei-Servern ausführen, sondern nur definierte autorisierte Anfragen senden können, bietet gemeinsam mit einer vernünftigen Server-Backup-Strategie ein fundiertes Bollwerk gegen wurmgleiche Ransomware.

Dokuneo.
Dokumentenmanagement. Einfach gemacht.

Ansprechpartner

Frank Zimlich
Dokuneo Software GmbH

Telefon: 06021 13077-0
E-Mail: mail@dokuneo.de

Smart Industrial IT Security

Sicherheit im Netzwerk ist auch die Gewissheit, dass nichts schiefläuft. Insofern stellt die Analyse des Kommunikationsverhaltens ein probates Mittel dar, um Anomalien zu erkennen, und damit umzugehen. Die Möglichkeiten reichen von regelbasierten Ansätzen, über Advanced Analyses bis hin zu machine learning und werden am Beispiel von Automatisierungsnetzen grundlegend dargestellt.

Ausgangssituation

Automatisierungsnetze halten verschiedenste industrielle Prozesse in Gang - von einfachen Fertigungsabläufen bis zu komplexen kritischen Infrastrukturen. In der Regel ist ein solches Netz heterogen aufgebaut und setzt sich aus übergeordnetem Systembus(sen) (Ethernet), Feldbus (bspw. Profinet) und/oder Sensor-/Aktor-Bus(sen) zusammen. Unterschiedliche Protokolle kommen zur Anwendung, unterschiedliche Verbindungen und Netzübergänge, von kabelgebunden, bus-powered bis Industrial WLAN. Komplexere Netzwerke setzen sich aus mehreren Segmenten (und Controller) und ggf. mehreren Layern mit Switches und Servern zusammen. Hier gilt es also eine vielschichtige und sich durch hohe Diversität auszeichnende Systemlandschaft vor Angriffen zu schützen.

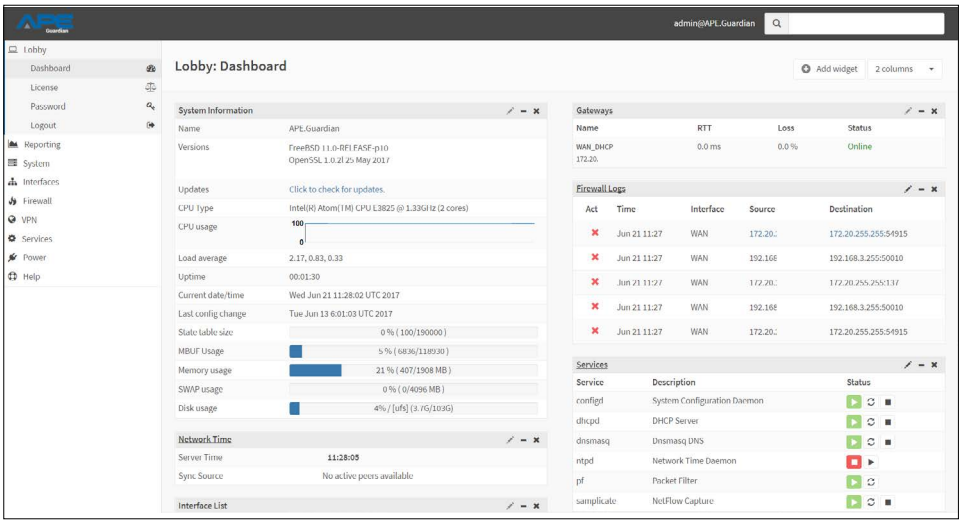
Das Automatisierungsnetzwerk selbst ist in der Regel nicht isoliert, sondern steht in reger Kommunikation mit unterschiedlichsten anderen Systemen und/oder Netzwerken, wie zum Beispiel einem ERP System oder der Office-Welt. Gerade im Zuge von Industrie 4.0 wird eine Anbindung an solche, übergeordnete Systeme angestrebt. Dies geschieht über eine Firewall und ggf. eine demilitarisierte Zone, was auch zu einer kontrollierten bzw. kontrollierbaren Kommunikation und Separierung der Netze beiträgt. Dennoch bleibt die Gefahr von Angriffen von Innen sowie von Lücken in der Abschottung. Dies geschieht insbesondere, wenn man die erforderliche Flexibilität gegenüber den Anforderungen der Industrie 4.0 Rechnung tragen möchte.

Verhaltensanalyse

Um Anomalien im Kommunikationsverhalten zu erkennen, müssen allerdings in kurzer Zeit große Datenmengen mittels komplexer Algorithmen bewerten werden. In Automatisierungsnetzen, insbesondere bei kritischen Infrastrukturen und großen Netzwerksegmenten mit verschiedensten Komponenten, ist die Echtzeitfähigkeit der Kommunikation ein ausschlaggebendes Kriterium. Das vollständige Monitoring unter Echtzeitbedingungen stellt eine der großen Herausforderungen dar. Zudem soll bzw. muss die Lösung aufgrund der Separation vom Unternehmensnetz in der Lage sein, diese Aufgaben auch ohne Anschluss an eine Cloud Infrastruktur

Die einfache SchaltschrankMontage und Vernetzung von Firewall Appliances wie dem APE Guardian ermöglichen den Einsatz modernster IT Security Techniken auch für Klein- und mittelständische Unternehmen.

Komplexe Netze lassen sich per Dashboard über Webclient intuitiv darstellen.



leisten zu können: Dies bringt hohe Anforderungen an die Performance der Software mit sich.

Aber wie wird anomales Verhalten erkannt? Zunächst wird das normale Verhalten initial angelernt (Regelkommunikation), was beispielsweise in der Inbetriebnahme-Phase passieren kann. Dazu wird ein kleiner Mini-PC im Schaltschrank montiert, der die Datenströme auf Paketebene direkt am Switch analysiert. Mit einer ausreichenden Datenmenge und Abdeckung der möglichen Kommunikation können so automatisch Regeln aufgestellt oder mittels machine learning Verfahren antrainiert werden. Später, im Standardbetrieb, können auf dem gleichen Mini-PC Abweichungen erkannt werden. Dieses Verfahren ist unabhängig vom Anwendungsbereich, welcher von der Maschinen- und Anlagensteuerung bis zur Verfahrenstechnik reichen kann.

Best Practice

Die zur Sicherung der individuellen Netzwerke erforderlichen Techniken sind vorhanden und werden beispielsweise von der APE Engineering GmbH bereits projektbezogen eingesetzt. Unter dem Namen APE Guardian filtert ein Mini-PC im Schaltschrank verdächtige Kommunikation und blockiert diese mit einer regelbasierten Firewall. Hierbei kommen die zuvor beschriebenen Ansätze zum Einsatz: Packet Capturing und Stateful Packet Inspection analysieren auf Basis von dynamischen Regeln den Datenverkehr auf Paket-Ebene. Netzwerkanomalien werden durch das Intrusion Detection System anhand der Signatur zuverlässig erkannt. Im Langzeittest erwies sich diese Lösung als stabil und performant.

Fazit

Systeme technisch auf dem neuesten Stand und software-technisch auf dem aktuellen Patch-Level zu halten ist eine wichtige Voraussetzung, um gegen Cyber-Angriffe gewappnet zu sein. Auch ist die Sensibilisierung der Mitarbeiter ein ebenso wichtiges Element. Darüber hinaus können aber, wie in diesem Beitrag gezeigt, auch intelligente Monitoring-Ansätze, wie die Analyse des Datenverkehrs auf Anomalien einen entscheidenden Beitrag leisten.

Ansprechpartner

Michael Kröhn
APE Engineering GmbH

Telefon: 06028 9915414
E-Mail: michael.kroehn@ape-engineering.de

IP-Schutz für CAD-Modelle: Innovative 3D-Technologie sichert sensible Konstruktionsdaten

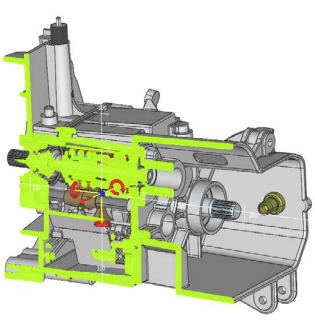
Der Schutz von geistigem Eigentum, Produkt- und Unternehmensgeheimnissen gewinnt im globalen Wettbewerb zunehmend an Bedeutung. Durch Software-Tools kann die Datenverfügbarkeit bei der Weitergabe von CAD-Modellen gezielt eingeschränkt werden und der Wissenstransfer findet selektiert und einsatzbezogen statt.

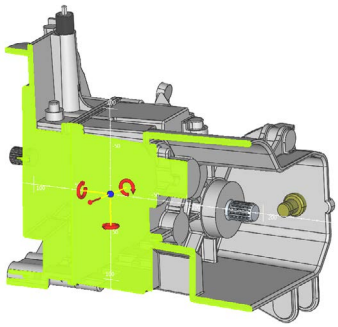
Der in Mömbris ansässige, deutsch/französische Softwarehersteller Core Technologie hat ein Programm zur automatisierten Erzeugung virtueller Hüllen für 3D-Modelle entwickelt. So werden im Entwicklungsprozess sensible Konstruktionsdaten bei Weitergabe an Entwicklungs-Partner, Kunden und Lieferanten vor unberechtigten Zugriffen geschützt.

Das Programm „3D Evolution Simplifier“ entfernt durch die automatische Erzeugung von Hüllgeometrie-Modellen sensibles Knowhow, welches durch die internen Geometriebereiche der CAD-Modellen dargestellt wird. Dabei können Daten aller gängigen CAD-Systeme und -Formate wie CATIA, Siemens

NX, Creo, Solidworks, STEP und JT verarbeitet und konvertiert werden.

Mit der Simplifier-Methode vereinfachte Daten entsprechen der Qualitätsnorm für Solid Modelle gemäß VDA 4955/2. Weiterhin können mit der Software verschiedene Abstufungen der Vereinfachung durchgeführt werden, je nachdem welche Informationstiefe die Entwicklungspartner benötigen. Die Simplifizierung geht hierbei von der gezielten

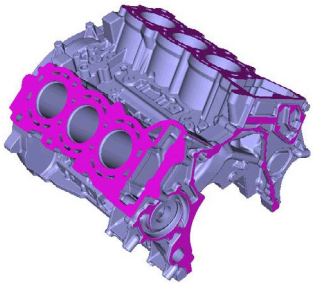


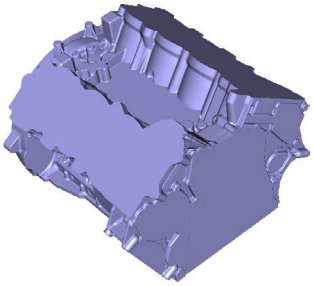


Entfernung der Konstruktionshistorie und Kinematik über die Löschung sensibler Metadaten wie Materialparameter und funktionalen Abhängigkeiten sogenannten Constraints bis hin zur Erzeugung einer reinen Hüllgeometrie, wobei die letzte Stufe den ultimativen Schutz von wertvollem Knowhow darstellt, da eine Wiederherstellung der Information ausgeschlossen ist.

Zudem werden durch die automatische Erzeugung der Hüllengeometrie wesentlich „leichtere“ Modelle erreicht, da bis zu 95% weniger Elemente dargestellt und verarbeitet werden müssen. Für zahlreiche Prozesse im Bereich der virtuellen Realität und Konstruktion birgt dies naturgemäß deutliche Vorteile in Sachen Performance. Insbesondere bei großen 3D-Modellen wie Zügen, Flugzeugen, Fahrzeugen sowie im Maschinen und Anlagenbau wird oft nur eine leichte Außengeometrie der Komponenten benötigt. Bislang geraten selbst moderne 3D-Systeme für die Konstruktion, Simulation und VR-Darstellung schnell an ihre Grenzen, wenn zu detailliert ausgeführte Konstruktionsdaten den Datenumfang unnötig anreichern. Mit dem „3D Evolution Simplifier“ komprimierte Daten sind somit nicht nur wirkungsvoll vor Produktpiraterie geschützt sondern können auch signifikant zügiger visualisiert und weiterverarbeitet werden.

Weitere Informationen sind abrufbar unter





www.coretechnologie.com.

Ansprechpartner

Armin Brüning
CT CoreTechnologie GmbH
Telefon: 06029 9588210
E-Mail: a.bruening@de.coretechnologie.com

Hintergrundinformationen

Der Softwarehersteller CoreTechnologie mit Standorten in Deutschland, Frankreich, USA, Japan und Großbritannien wird seit seiner Gründung im Jahr 1998 von den Geschäftsführern Dominique Arnault und Armin Brüning geleitet. Mit innovativen Produkten hat das visionäre Unternehmen sein Produktportfolio konsequent optimiert und sich die Technologieführerschaft im Bereich der Konvertierungssoftware gesichert. Jedes Jahr investiert CoreTechnologie mehr als 30 Prozent des Umsatzes in die Erforschung und Umsetzung neuer Technologien und verfügt heute über die vollständigste Produktpalette auf diesem Gebiet.

Im Fokus der Technologie-Entwicklung steht die Produktlinie „3D Evolution“, die einen effizienten und verlustfreien Austausch komplexer Datenstrukturen zwischen unabhängigen und heterogenen CAX Softwarelösungen gewährleistet. Mit extrem leistungsstarken Nativschnittstellen für alle führenden CAD-Systeme und zur Umwandlung in alle gebräuchlichen 3D Formate sichert das Software-Modul die optimale Interoperabilität der unterschiedlichsten IT-Lösungen.

Neben der Bereitstellung der Visualisierungs- und Fertigungsdaten über unterschiedliche Systeme hinweg bietet CoreTechnologie herausragende Technologien für die automatische Datenkorrektur, Feature basierte Konvertierung, Geometrieoptimierung, Qualitätskontrolle und die Langzeitarchivierung, sowie zur Visualisierung komplexer 3D Modelle. Die Software-Komponenten für Softwarehersteller der unterschiedlichsten CAX-Anwendungen sind das zweite Standbein des Unternehmens.

Das Kundenportfolio von CoreTechnologie umfasst mehr als 400 Unternehmen aus Automobil-, Aerospace-, Maschinenbau- und Konsumgüterindustrie, vielfach die Qualitätsführer in ihrem jeweiligen Segment.

Vorreiter in Sachen Informationssicherheit: die Stadtwerke Aschaffenburg.

Mehr als 70.000 Personen in 26.000 Haushalten verlassen sich darauf: Strom und Gas stehen rund um die Uhr zur Verfügung, aus der Leitung kommt sauberes Wasser, öffentliche Busse bringen die Fahrgäste sicher ans Ziel, das Auto kann im Parkhaus günstig abgestellt werden, der Müll wird pünktlich abgeholt und für die Freizeit gibt es ein Freibad, ein Hallenbad und eine Eissporthalle.

Das alles leistet der Unternehmensverbund der Stadtwerke Aschaffenburg mit seinen Tochtergesellschaften. Im Vordergrund stehen bei den Stadtwerken die Kunden und Dienstleistungen in den Bereichen Energie, Wasser, Entsorgung, Verkehr, Parken, Service und Freizeit. Das Versorgungssystem der Stadt Aschaffenburg ist das, was man eine kritische Infrastruktur nennt.

Ein solch umfassendes Dienstleistungsangebot ist heutzutage nur noch auf Basis einer reibungslos funktionierenden IT zu Bewältigen. Störungen oder gar Ausfälle der IT könnten die Lebensadern aus Strom und Wasser der größten Stadt in der Region Bayerischer Untermain empfindlich treffen und sogar zum Versiegen bringen. Umso erfreulicher ist es, dass die Stadtwerke Aschaffenburg ganz weit vorne sind, was den Schutz ihrer IT-Infrastruktur gegen Hackerangriffe und andere Bedrohungen aus dem Cyberspace angeht. So weit vorne, dass die Unterfranken im Projekt CyberWiz als Pilotpartner fungierten.

EU fördert den Kampf gegen Cyber-Bedrohungen.

CyberWiz dient dem Schutz kritischer Infrastrukturen und wird von der EU im Rahmen des Programms Horizon 2020 gefördert.

Das Programm hat den Fokus, die Entwicklung bahnbrechender Technologien zu unterstützen, die insbesondere in den kreativen Köpfen kleiner und mittlerer Unternehmen entstehen. CyberWiz kombiniert das Know-how der Softwareentwickler und Risikoexperten des schwedischen Unternehmens foreseeti AB, einem Spin-off der Königlichen Technischen Hochschule Stockholm, und des deutschen Spezialisten für Informationssicherheit, der Applied Security GmbH (apsec) aus Groswallstadt. Wissenschaftlich unterstützt wird CyberWiz von den Forschern der KTH Stockholm und vom paluno Institut für Softwaretechnologie der Universität Duisburg-Essen.

Security Engineering in unterfränkischer Allianz.

Ziele von CyberWiz sind die Entwicklung und Erprobung der Software securiCADR, sowie eines zugehörigen Implementierungs- und Beratungskonzepts. securiCADR bietet die Möglichkeit, IT-Netzwerke zu modellieren und mittels ausgefeilter Simulationstechniken auf Schwachstellen zu testen.

Ein Ergebnis der Simulation liefert unter anderem eine Abschätzung, wie lange ein Angreifer benötigt, ein Netzwerk entscheidend zu kompromittieren. Was aber noch wichtiger ist: securiCADR gibt zu allen gefundenen Schwachstellen Hinweise, auf welchen Wegen potenzielle Angreifer die Schwachstelle ausnutzen und was dagegen unternommen werden kann. Ein solches Präzisionswerkzeug der Software-Ingenieurkunst passt hervorragend zum Qualitätsanspruch, den auch die Stadtwerke Aschaffenburg in ihrem Selbstbild formulieren. So war es sicher kein Zufall, dass es zu der Zusammenarbeit der beiden unterfränkischen Unternehmen kam.

In dem sieben Monate laufenden Pilotprojekt machten die Sicherheitsexperten von apsec eine Bestandsaufnahme eines Ausschnitts der IT-Infrastruktur der Stadtwerke Aschaffenburg und erstellten davon ein Modell mittels securiCADR. Es galt, hunderte von Clients, Servern, virtuellen Maschinen, Firewalls und die Datenflüsse zwischen den verschiedenen Netzwerkzonen mit den darin befindlichen IT-Komponenten zu modellieren und die vorhandenen Sicherheitsmechanismen einzupflegen. Darüber hinaus wurde von apsec auch ein Kurzcheck über die technischen und organisatorischen Maßnahmen zur Informationssicherheit nach dem Vorbild des ISIS12-Standards gemacht.

Spannend wurde es nach Abschluss der Modellierung, denn nun konnten die Angriffssimulationen starten. Dabei wählt securiCADR einen Ingenieur-Ansatz. Anders als beispielsweise bei einem Penetrationstest, bei dem ein Netzwerk von einem IT-Experten auf eine Reihe von möglichen Schwachstellen getestet wird und somit eine Momentaufnahme darstellt, spielt securiCADR, ausgestattet mit der Rechenpower moderner Computersysteme, in einer Simulation jede Menge Angriffsvektoren, die in der Software implementiert sind, durch. Dabei ermittelt securiCADR die Auswirkungen der simulierten Angriffe auf die angrenzenden Systeme und erstellt so ein „Wärmebild" der Verwundbarkeiten im Netzwerk. Ein Ergebnis, dass allein schon aufgrund der schieren Komplexität und der Menge der Abhängigkeiten und Wechselwirkungen der einzelnen IT-Komponenten untereinander von einer Person händisch nicht mehr leistbar ist. Und nicht nur die reine Ermittlung von Schwachstellen ist das Ergebnis. securiCADR liefert darüber hinaus auch eine Abschatzung, wie lange es dauert, bis ein Angriff erfolgreich sein Ziel erreicht hat.

Die Ergebnisse der Simulation wurden von den apsec-Beratern dem Pilotkunden aus Aschaffenburg vorgestellt und anhand der Ergebnisse Verbesserungspotenziale gemeinsam diskutiert. Auch hier kann securiCADR weitere wertvolle Dienste leisten, denn auch eine Veränderung der IT-Infrastruktur kann per Simulation getestet werden, bevor sie in die Tat umgesetzt wird. So können von verschiedenen Verbesserungsmöglichkeiten die wirtschaftlich sinnvollsten ausgewählt werden.

Überzeugende Ergebnisse.

Verantwortlich für das Pilotprojekt auf Seiten der Stadtwerke Aschaffenburg war IT-Leiter Dr. Michael Konik.

„Der Ansatz einer Angriffssimulation, die auf wissenschaftlichen Methoden beruht, hat mir als studiertem Mathematiker gleich gefallen. Daher waren wir auch gerne bereit, unser Netzwerk in dem Pilotprojekt von apsec untersuchen zu lassen. Natürlich kommt es bei solchen Piloten immer mal zu kleineren Stolperern. Dafür sind Pilotprojekte ja da, dass man gemeinsam die Verbesserungsmöglichkeiten identifiziert. Insgesamt sind wir sehr beeindruckt von dem Ergebnis. Es hat uns auf jeden Fall geholfen, die Sicherheit in unserer IT zu erhöhen. Besonders nützlich sind für uns das vollständige Lagebild und vor allem die Möglichkeit, künftige Änderungen an unserer Infrastruktur vorab darauf zu testen, wie sie sich auf die Sicherheit des Gesamtsystems auswirken. Die Zusammenarbeit mit apsec haben wir als sehr professionell und angenehm empfunden. Es wird sicher nicht das letzte gemeinsame Projekt gewesen sein."

Ansprechpartner

Steffen Gumbel
Werkstraße 2
63739 Aschaffenburg
Telefon: 06021 391401
E-Mail: steffen.gumbel@stwab.de

APOLI – die Fernwartung der Zukunft

Im F&E-Projekt APOLI wird die Zukunft der Fernwartung von Maschinen definiert.

IT in Produktionsunternehmen

Industrie 4.0 als Schlagwort ist in aller Munde. Sie führt auf der einen Seite zu effizienteren Prozessen, schnelleren Produktionen und neuen Geschäftsmodellen, auf der anderen Seite kommen viele Unsicherheiten auf die Unternehmen zu. Der klassische mittelständische Unternehmer begriff und begreift manchmal auch heute noch die Informationstechnologie nur als Mittel zum Zweck, als „notwendiges Übel". Investitionen in IT sind immer als Kosten gesehen worden – und Kosten sind niedrig zu halten, bestenfalls sogar zu senken.

Aus diesem Grund kann in vielen Unternehmen die IT nicht mit dem aktuellen Stand der Technik mit-

halten. Neben einem möglichen Verlust an Produktivität geht damit in vielen Fällen ein Verlust des Sicherheitsniveaus einher. Das zeigen die folgenden Beispiele:

- Der Einsatz veralteter Software: In vielen Unternehmen werden, oft aus Kostengründen, veraltete Softwareprodukte eingesetzt. Betriebssysteme wie Windows XP werden nicht mehr gewartet und sind damit anfällig für Attacken, die in neueren Betriebssystemversionen abgefangen werden. Hier sei exemplarisch der Virus WANNACRY genannt.
- In Produktionsnetzen wurden aus Einfachheitsgründen oft gleiche IP-Adressen für gleiche Maschinen verwendet. Damit kann zwar intern gearbeitet werden, eine Anbindung ans Internet (und damit die Industrie 4.0) scheidet damit aus bzw. öffnet Sicherheitslücken. Eine Separierung der Produktionsnetze in unterschiedliche Bereiche, z.B. nach Hersteller, findet sich nur in den wenigsten Unternehmen.
- Die Mitarbeiter sind in IT-Themen und den damit verbundenen Gefahren oftmals nicht geschult und nur unzureichend sensibilisiert. Der „Locky"-Virus, der auch am bayerischen Untermain mehr als die Hälfte aller Unternehmen befallen hat, zeigt dies deutlich.

Neben diesen eher IT-spezifischen Themen ändern sich aber auch die Nutzungszeiten von Maschinen. Waren früher oft 30 Jahre und mehr die Regel, so gehen die Hersteller heute eher von einer 15-jährigen Nutzungsdauer aus.

Industrie 4.0 auf einen Blick

In diesem Zusammenhang stehen mit der Industrie 4.0 grundlegende Veränderungen für alle Unternehmen ins Haus – ob es dem Einzelnen nun gefallen mag oder nicht. Was heißt aber Industrie 4.0 jetzt eigentlich? Wikipedia definiert verschiedene Aspekte dieses Begriffs.

- Vernetzung: Maschinen, Geräte, Sensoren und Menschen können sich miteinander vernetzen und über das Internet der Dinge oder das Internet der Menschen kommunizieren.
- Informationstransparenz: Sensordaten erweitern Informationssysteme digitaler Fabrikmodelle, um so ein virtuelles Abbild der realen Welt zu erstellen.
- Technische Assistenz: Assistenzsysteme unterstützen den Menschen mit Hilfe von aggregierten, visualisierten und verständlichen Informationen. So können fundierte Entscheidungen getroffen und auftretende Probleme schneller gelöst werden. Außerdem werden Menschen bei anstrengenden, unangenehmen oder gefährlichen Arbeiten physisch unterstützt.
- Dezentrale Entscheidungen: Cyberphysische Systeme sind in der Lage, eigenständige Entscheidungen zu treffen und Aufgaben möglichst autonom zu erledigen. Nur in Ausnahmefällen, zum Beispiel bei Störungen oder Zielkonflikten, überträgt es die Aufgaben an eine höhere Instanz.

Insgesamt werden sich das Arbeiten und die Arbeitswelt durch Industrie 4.0 einschneidend verändern. Einen Aspekt dieser Veränderung hat sich das Projekt APOLI (Aufgabenbezogene polymorphe Identifikation) herausgepickt, nämlich wie die Fernwartung von Maschinen in Zukunft aussehen wird. In APOLI arbeiten unter der Federführung der Fraunhofer ESK München die Software Factory GmbH Garching, die Felss Systems GmbH, Nesselwang, die Otto Biehler Maschinenfabrik GmbH & Co. KG, Halblech, und die Applied Security GmbH, Großwallstadt, an diesem Thema.

Fernwartung

Unter Fernwartung wird der Zugriff eines Servicetechnikers auf einen Maschinenpark, auf eine Maschine oder eine Komponente einer Maschine verstanden. Fernwartungen stellen alle Beteiligte vor Herausforderungen und vielfältige Diskussionen.

- Diskussion beim Verkauf von Produktionsanlagen mit der IT des Kunden über die ausreichende Sicherheit der eingesetzten Verfahren, die Ende-zu-Ende-Sicherheit der Verbindungen, die Freigabe und den Zugriff auf die jeweiligen zu wartenden Komponenten und vieles mehr
- Vorgaben durch jeden einzelnen Kunden, nach denen sich der Hersteller zu richten hat, z.B. unterschiedliche Kommunikationsverfahren, unterschiedliche Sicherheitsmechanismen, unterschiedliche Identifikationen des Servicetechnikers, unterschiedliche Token zur Identifikation etc.

Das Ziel des Projektes ist es, eine Strategie und Technologie zu entwerfen, mit deren Hilfe die Durchführung von AA(Authentisierung und Autorisierung)-Vorgängen grundlegend effizienter als heute üblich gestaltet werden kann. Der Nachweis der Praktikabilität wird durch die Implementierung eines Kunden-Modellfalls erbracht. Dieser bezieht sich auf die AA-Vorgänge im Rahmen von

Fernwartung mit zukünftiger Erweiterung auf neue Geschäftsmodelle.

Software-Defined Networks mit Authentisierung und Autorisierung

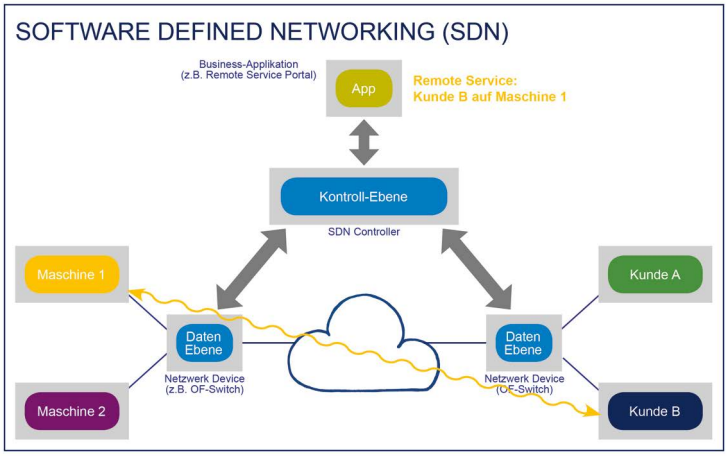
Zur Umsetzung wird die Technik von SDN (Software Defined Network) mit zentralen AA-Services verbunden. Ein SDN-Controller leitet – definiert durch die jeweils aktuell benötigte Fernwartungskonfiguration – den Datenverkehr zusammen mit sogenannten OF-Switches durch das eigene Netz des Unternehmens, ohne dass diese Routen manuell durch die IT konfiguriert worden wären. Sie sorgen automatisch an der richtigen Stelle für Sicherheit und berücksichtigen automatisch die zentralen Leitlinien, die vom Unternehmen vorgegeben werden. Damit können Zugriffe auf die internen Netze bzw. einzelne Teile daraus dynamisch gegeben werden, ohne Sicherheit oder Flexibilität zu verlieren.

Mittels der AA-Services werden die Zugriffe freigegeben und die dazugehörigen Regeln an zentraler Stelle erfasst und verwaltet. Der Servicemitarbeiter authentisiert sich nur an einer Stelle mit einer digitalen Identität (Single point of authentication) und einem Token. Der „Tokenzoo" wird damit abgeschafft. Der AA-Service kann die einzelne Maschine oder sogar Komponente identifizieren und genau darauf den Zugriff freigeben.

Mit der von APOLI entwickelten Architektur wird der Aufwand insgesamt spürbar reduziert und eine Infrastruktur geschaffen, die für weitere Einsatzmöglichkeiten verwendet werden kann.

- Aufhebung der Isolierung der Maschinennetze. Durch eine zielgerichtete Steuerung der Kommunikation wird die strikte Trennung von Maschinen-, Produktions- und Büronetzen überflüssig. Diese Kommunikation kann jetzt über die zentral überwachten Businessprozesse vorgenommen werden.
- Zentraler Leitstand. Durch die Bündelung der Kommunikationsbeziehungen im SDN-Controller ergibt sich die Möglichkeit, mit Hilfe eines zentralen Leitstandes die Hoheit über alle Verbindungen ins Unternehmen zurückzugewinnen.
- Condition Monitoring. Die in APOLI verwendete Technik kann nicht nur zur reaktiven Fernwartung eingesetzt, sondern auch auf ein „Condition Monitoring" ausgeweitet werden. Dabei werden durch die kontinuierliche Überwachung der Maschinen mit Sensoren zum einen mögliche Störfälle aktiv bereits vor dem Ausfall einer Komponente gemeldet, zum anderen ergeben sich durch die Verknüpfung von Daten verschiedener Maschinen Optimierungspotentiale in der Produktion. Das führt wiederum zu einer besseren Auslastung einzelner Komponenten und einer verbesserten Effizienz.

APOLI wird vom FuE-Programm „Informations- und Kommunikationstechnik" des Freistaats Bayern gefördert. Die bisherigen Ergebnisse des Projekts, das noch bis Jahresende läuft, zeigen, dass die gewünschten Potentiale gehoben werden und damit der bayerischen Wirtschaft die Möglichkeit geben, ihre Spitzenposition in der Welt beizubehalten bzw. weiter auszubauen.



apsec applied security

Ansprechpartner

Frank Schlottke
Applied Security GmbH
E-Mail: frank.schlottke@apsec.de

IT Sicherheit: „nur die Spitze des Eisbergs“

Es ist wie mit Eisbergen: Die wirkliche Gefahr lauert im Verborgenen und ist vermutlich größer als angenommen. Ohne Schutzmaßnahmen und Notfallplan können Unternehmen leicht an der Gefahr zerschellen.

Was wir derzeit an Bedrohungen für die Informationssicherheit sehen, ist nur die Spitze des Eisbergs. Anfang 2016 zählten Security Anbieter alle 2 Minuten eine Ransomware-Attacke auf Unternehmen. Gegen Ende des Jahres 2016 schrumpfte die Taktrate schon auf 40 Sekunden. Im Falle von WannaCry ist eine Taktrate schon nicht mehr messbar, da es sich praktisch um eine weltweite Malware Flut handelte. Erpressungen durch Verschlüsselungstrojaner erweisen sich für Kriminelle als äußerst lukrativ. So zahlte kürzlich der südkoreanische Webhoster Nayana die Rekordsumme von 1,14 Mio. US Dollar, um wieder an verschlüsselte Daten zu kommen. Für Ungeübte finden sich im Dark Web einfache Anleitungen und buchbare Services für derartige Angriffe. Das führt unter anderem dazu, dass Straftaten über das Internet immer weiter anwachsen. Das „Internet der Dinge“ wächst laut Gartner von aktuell 8,4 Milliarden vernetzten Objekten bis 2020 auf 20,4 Milliarden an – ob smarte Stromzähler, IP Kameras oder intelligente Messgeräte – die Möglichkeiten für neue Angriffsformen wachsen mit der Digitalisierung und den über IP erreichbaren Objekten exponentiell.

IT-Sicherheit wird auch für kleinere und mittelgroße Unternehmen ein immer wichtigeres Thema. Wer sich nicht ausreichend schützt, riskiert Ausfälle und Datenverluste, die für den Betrieb schnell verheerende Folgen haben können. Es ist eine weit verbreitete Fehleinschätzung, dass das eigene Unternehmen zu klein sei, um für einen Angriff interessant zu sein. Der „Cyber Readiness Report 2017“ von Forrester Consulting zeigt, dass 62 % aller deutschen Unternehmen sogenannte „Cyber-Anfänger“ seien – also unzureichend geschützt. Im Ländervergleich bildet Deutschland hier das Schlusslicht.

Was muss ich tun? – Die Basics:

Updates installieren: Betriebssystem und alle installierten Anwendungen auf Computern, Smartphones oder Tablets sollten kontinuierlich auf den aktuellen Stand gebracht und gehalten werden. Programme, die vom Hersteller nicht mehr mit Updates versorgt werden, sollten gelöscht oder durch neue Software ersetzt werden. Das gilt auch für die installierte Sicherheitslösung.

Daten sichern: Die massiven Angriffe durch Ransomware haben einmal mehr gezeigt, dass Daten dauerhaft verloren gehen können. Ein regelmäßiges Backup sichert ab und ist deshalb für alle wichtigen Datenbestände Pflicht.

Apps aus sicheren Quellen: Anwendungen nur aus vertrauenswürdigen App Stores der Hersteller und Provider herunterladen. Bei jeder Installation sollten die eingeforderten Rechte kritisch überprüft werden.

Sicherheitslösung einsetzen: Eine leistungsstarke

Security Soft-und Hardware gehört zur Grundausstattung bei PCs, Macs, Mobilgeräten und Netzwerken. Diese müssen einen umfassenden Schutz vor Schadprogrammen und anderen Cyberbedrohungen beinhalten.

Starke Passwörter nutzen: Passwörter sollten immer mindestens zehn Zeichen lang sein und eine Kombination aus Klein- und Großbuchstaben zusammen mit Ziffern und gegebenenfalls Sonderzeichen umfassen. Außerdem sollte dasselbe Passwort niemals für verschiedene Online-Portale genutzt werden.

Dokumentieren: Dokumentieren Sie kritische Systeme, die Verarbeitung sensibler Informationen, Rechte, Rollen, Verantwortlichkeiten und Änderungen. Ein Notfallplan hilft, im Schadensfall schnell wieder operativ zu werden.

IT-Security fängt im und am Kopf an:

Informationssicherheit ist Chefsache! Wirtschaftlich wie rechtlich bescheinigt ein zertifiziertes Informationssicherheitsmanagementsystem ein Qualitätsmerkmal, schafft Transparenz und Struktur in der IT Umgebung und deckt Optimierungspotenziale auf. Gleichermaßen werden Image- und Wettbewerbsfaktor erhöht. Im Hinblick auf die neue EU Datenschutzgrundverordnung ist es nahezu für jede Organisation notwendig, sich mit dem Thema auseinander zu setzen. Auf dem Gebiet der Cyber-Sicherheit mangelte es bisher an einem für kleine und mittelständische Unternehmen handhabbaren und angemessenen Standard. Abseits von BSI Grundschutz und ISO 27001 hat der VdS eine aufwärtskompatible Richtlinie erstellt. Mit der VdS 3473 wird Informationssicherheit für KMU machbar, bewertbar und zertifizierbar. Die VdS-Richtlinien bilden das Schutzniveau, das kleine und mittlere Unternehmen benötigen, ohne sie finanziell oder organisatorisch zu überfordern. Der VdS selbst nennt das Thema Cyber Security auch den „Brandschutz des 21. Jahrhunderts".

Und wenn jemand einfach die Tür öffnet?

Im Dezember 2016 setzten mehr als 99% aller infizierten E-Mail Anhänge auf Klicks der Benutzer statt auf automatisierte Exploits. Demnach sind logische Maßnahmen wie die Schulung der Benutzer zu aktuellen Bedrohungen ein weiteres Kernelement der IT Sicherheit.

Der physische Zugang zu IT Anlagen, Computersystemen und Netzwerkzugängen ist mit gleicher Bedeutung kritisch zu überprüfen, wie sämtliche digitalen und organisatorischen Maßnahmen. Denn was bringt die beste Firewall und der preisgekrönte Antivirenschutz, wenn man einfach direkt zu den Daten spazieren kann?

Ansprechpartner

Stefan Dyck
Gleich IT Service GmbH

Telefon: 06021 416686
E-Mail: stefan.dyck@gleich-IT.com

mainproject 2018 begleitet Industrie 4.0-Einführung in der Mainsite-Ausbildung

Für das mit Mitteln des europäischen Sozialfonds vom Bayerischen Wissenschaftsministerium geförderte Wissenstransferprojekt „mainproject 2018" der Hochschule Aschaffenburg und der Mainsite GmbH & Co.KG, Betreiber- und Industriedienstleistungsgesellschaft des Industrie Centers Obernburg, bildet „Industrie 4.0" einen zentralen thematischen Schwerpunkt. Denn die Digitalisierung vieler oft noch analog ablaufender Vorgänge und Prozesse hat gerade bei kleineren und mittleren Unternehmen noch

Nachholbedarf – sei es aus Kapazitätsgründen oder, weil man Nutzen und Vorteile für den eigenen Betrieb nicht abzuschätzen vermag.

Mainsite nutzt bei der Digitalisierung von Prozessen die Fachexpertise von mainproject 2018. Als einer der größten Ausbildungsbetriebe am bayerischen Untermain bildet das Mainsite-Ausbildungszentrum sowohl den betrieblichen Nachwuchs für die Unternehmen des Industrie Center Obernburg, als auch im Auftrag für namhafte Unternehmen der Region aus. Frühzeitig erkannten die Verantwortlichen, dass bereits in der Berufsausbildung - neben klassischen handwerklichen Fähigkeiten - auch der Umgang mit digitaler Technik erlernt und geübt werden muss. Daher hielt die Digitalisierung im Rahmen von Industrie 4.0 auch in der Ausbildung Einzug. Hans-Peter Rüth, Projektmitarbeiter von mainproject 2018 und SAP-Spezialist bei Mainsite, initiierte gemeinsam mit Mainsite-Ausbildungsleiter Ingo Bazalik ein Projekt, das den technischen Auszubildenden die Handhabung digitalisierter Prozesse an originalem Equipment möglichst hautnah ermöglicht. Materielle Unterstützung leistete hierbei die Mannheimer TechniData Biz Solutions GmbH, ein Unternehmen der TechniData IT-Gruppe und Innovationsführer im Bereich mobile Datenerfassung für papiergestützte Geschäftsprozesse.

Konkret geht es dabei um ein digitales Rückmeldesystem für geleistete Arbeitsstunden, das im Betrieb schon heute Anwendung findet. Für die jungen Kollegen der Zukunft wird es so selbstverständlich zum Arbeitsalltag gehören, wie früher der klassische Stundenzettel aus Papier. Bislang füllte ein Handwerker nach Abschluss eines Arbeitsauftrags von Hand einen Zettel aus, auf dem er neben den Stammdaten der Anlage oder Maschine, an der Arbeiten ausgeführt wurden, die Verbrauchsmaterialien und die geleisteten Stunden notierte. Dieser Zettel wurde dann im Büro in einem Verrechnungssystem erfasst, was sowohl aufwändig war, als auch eine Fehlerquelle darstellte.

Das neue System basiert auf einem Formular von PaperDynamix, das ein Koordinatensystem bildet und mithilfe eines normalen Druckers ausgedruckt wird. Bereits im Vorfeld wurden Datenfelder in diesem Koordinatensystem definiert. Vor Ort an der Arbeitsstätte trägt der ausführende Monteur mittels Digital-Pen in diese Datenfelder die verschiedenen Daten ein, z.B. die Anzahl der geleisteten Tätigkeiten bei Abarbeitung des Auftrags, Ort und Zeit, Bezugsdaten des Ausführenden oder die Anzahl der Ausführung geleisteten Arbeitsstunden. Der Digital-Pen fungiert dabei als Kugelschreiber, nur mit dem Unterschied, dass dieser auch eine Optic-Scan-Linse besitzt und die eingetragenen Daten in ein integriertes Speichermedium speichert. Das Papierexemplar kann der Kunde - wie einen klassischen Leistungserfassungszettel – unterschreiben und in Kopie erhalten.

Nach Erledigung des Arbeitsauftrags und Ausfüllen des Datenblatts steckt der Mitarbeiter den Digital-Pen auf die Dockingstation. Diese überträgt die Formularinhalte als Daten fehlerfrei und zeitaktuell über ein Webinterface an das SAP-System zur Weiterverarbeitung. Das Verfahren erleichtert die Datenverarbeitung enorm. Man spart sich die lästige und oft fehlerträchtige Übertragungsarbeit ins Verrechnungssystem und beschleunigt den gesamten Vorgang.

Dankenswerterweise stellte die Firma TechniData Biz Solutions GmbH, vertreten durch Geschäftsführer Detlev Homilius, der Mainsite-Ausbildung insgesamt 13 Digital-Pens nebst Dockingstation kostenfrei zu Verfügung und übergab diese an Mainsite-Ausbildungsleiter Ingo Bazalik. Auch das für die Datenübertragung zu SAP erforderliche Web-Interface gab es gratis, damit die angehenden Handwerker den Umgang mit den Geräten an den Schulungs-PCs in der Ausbildung live üben können. Auch für individuelle Handschriften ist der Digital-Pen geeignet, denn er ist lernfähig und kann Handschriften interpretieren.

Ansprechpartner

Thilo Berdami
Mainsite GmbH & Co. KG
Telefon: 06022 812565
E-Mail: thilo.berdami@mainsite.de

Z! DAS ZUKUNFTSMAGAZIN IM INTERVIEW MIT PROF. RAINER SIEBER

Prof. Rainer Sieber,

Geschäftsführer sapiens42 GmbH und Professor für Informatik an der Universität der Bundeswehr in München

Herr Sieber, Sie unterstützen viele namhafte Unternehmen bei der Strukturierung und dem Aufbau von IT-Security. Hand aufs Herz: ist unser Mittelstand im Bereich IT-Security gut aufgestellt?

Um es auf den Punkt zu bringen: Nein! Die meisten Unternehmen - und ich meine hiermit ca. 90% der Unternehmen - priorisieren das Thema nicht hoch genug, weil sie die Bedrohungen und Gefahren weder spüren noch sehen und Ausgaben für Prozesse, Personal und Investiti-onen in erster Linie als verzichtbare Ausgaben ansehen. Die meisten, die angegriffen wur-den, wissen das gar nicht, weil erst mal alles weiterläuft, bis man irgendwann ähnliche Pro-dukte im Markt findet, die mit den eigenen CAD-Daten, aber nicht von einem selber hergestellt wurden.

Welche Argumente würden Sie anführen, um für die Fragestellung zu sensibilisieren und zu motivieren?

Ich habe die Erfahrung gemacht, dass die Analogie zu einem „Hausbau“ am eingängigsten ist. Jeder, der ein Haus hat oder es wie die ZENTEC betreibt, macht sich Gedanken über Brandschutz und Einbruchschutz, ergreift entsprechende Schutzmaßnahmen und möchte und muss wissen, wer ein- und ausgeht. Natürlich möchte man wissen, wer vielleicht etwas aus dem Haus mitgenommen hat. Bei Unternehmen kann das existenzbedrohend sein, weil wertvolles Know-how bspw. in Form von CAD-Daten, Prozesswissen oder Kundeninformati-onen kopiert werden kann, ohne dass ich als Unternehmer das mitbekomme. Es gibt mehr als genug Beispiele dafür, sie gelangen aber meistens aus nachvollziehbaren Gründen nicht in die Öffentlichkeit.

Durch die Digitalisierung der Wirtschaft und durch Industrie 4.0 wird eine extrem hochgradige Vernetzung der Wirtschaft erwartet, die weitgehend automatisiert zwischen Unternehmen bzw. Maschinen stattfindet.

Das ist ein massiv wichtiges Thema, da vor allem für kleine und mittelständische Betriebe, die ihre

Marktposition vor allem durch ihr hochspezialisiertes Know-how haben, neue Gefahren erwachsen. KMU können nicht sicher sein, sicher zu sein, nicht jetzt und vor allem nicht in einer digitalisierten Wirtschaft. Die strukturellen Änderungen in der Wirtschaft, die wir er-warten und die gerade erst beginnen, sind vor allem eine Chance, aber auch ein Zwang, sich im Hinblick auf IT-Security fit zu machen und den Wandel zu nutzen, um eigene IT- Sicherheit zu erhöhen.

Ist das Instrumentarium, das Unternehmen nutzen können, vorhanden?

Das Problem ist, dass in Echtzeit ständig ohne Unterlass immer neue Bedrohungs-Ideen mit wechselnden aber auch neuen Akteuren auf dem Markt aktiv erscheinen, die immer wieder Schwachstellen und Einfallstore abtasten und finden. Das bedeutet auf der einen Seite, dass es vollständige Sicherheit nicht gibt und auf der anderen Seite, dass man die Anstrengungen ständig auf höchsten aktuellem Niveau halten muss. Das vorhandene Instrumentarium an Schutzmaßnahmen ist somit möglicherweise nicht ausreichend. Um es nochmal deutlich zu sagen: IT-Security ist eine Daueraufgabe und keine Aufgabe, die man nur gelegentlich an-nimmt und abarbeitet!

Ich ziehe die Analogie eines Hauses nochmal heran: jeder möchte wissen, wer in seinem Haus war und was ein Besucher dort gemacht oder gar mitgenommen hat. Man kann z.B. eine im eigenen Netzwerk installierte „Watch-Box“ implementieren, wie wir sie in unserem Unternehmen entwickelt haben, die laufend und in Echtzeit aufzeichnet, wer in das Haus wo hineingeht und welchen Türschlüssel benutzt, wer und wo herausgeht und was dort ge-schieht. Ungewöhnliches Verhalten fällt dann sehr schnell auf und bietet die Möglichkeit, der Ursache für diese Abweichung nachzugehen. Diese Box ist so eine Art „digitaler Hausmeis-ter“.

Welche Empfehlungen würden Sie einem mittelständischen Unternehmer geben?

IT-Security muss als zentrale und hoch priorisierte Aufgabe in der Unternehmensleitung auf-gehängt sein. Es hat überhaupt keinen Sinn, gelegentlich einen statischen Check wie ein Audit zu machen oder machen zu lassen. IT-Security richtig zu machen heißt, jemanden autark und fokussiert abzustellen, der sich um alle Facetten der IT-Security kümmert, der in alle unternehmerischen Entscheidungen eingebunden wird und der im Zweifelsfall auch die Ent-scheidung trifft für eine Überarbeitung der Investitionen in Bezug auf die mangelnde IT-Security. In Bezug auf den Datenschutz bspw. ist in der neuen „Europäische Datenschutz-Grundverordnung“ ab Mai 2018 festgeschrieben, dass ein Sicherheitsexperte gestellt sein muss und dass dieser Experte nicht in Teilzeit beschäftigt sein darf (ab 200 Beschäftigte).

Ganz wichtig ist, die Einhaltung der IT-Security Vorgaben regelmäßig zu prüfen und fertige Abläufe zu haben, was im Fall des Falles zu geschehen hat. Nur dann stellt man fest, wo es hakt und wo man nachbessern muss. Manchmal ist das ganz einfach, wie z.B. durch tägliche Backups oder Server vom Netzwerk abgekoppelt auf Standby zu haben.
Was sind erfahrungsgemäß die größten Schwachstellen?

Der Mensch. Nicht aus Absicht, sondern aufgrund von Nachlässigkeit oder Lässigkeit, die wiederum dadurch entsteht, dass die Unternehmensleitung das Thema nicht ausreichend priorisiert und kommuniziert, vor allem nicht die notwendige IT-(Security)-Architektur schafft und IT-Security nicht in die Personalführungs- und Personalentwicklungsstrategie einbaut.

Im Jahr 2012 kam der Thriller „BLACKOUT – Morgen ist es zu spät“ heraus und entfachte eine lebhafte Diskussion über die Verletzbarkeit unserer Gesellschaft. Was hat sich seit damals geändert?
Es hat sich nach wie vor nichts Wesentliches geändert, weder an der Eintrittswahrscheinlich-keit noch an der Priorität und der Priorisierung des Themas.
Was sind aus Ihrer Sicht die Hauptgründe für Angreifer?

Das Spektrum ist breit. Es reicht von finanziellen Motiven, die sich in Erpressung äußern wie bei wannacry, über fast schon sportliche Wettbewerbe von Hackern oder Hackergruppen gegeneinander bis hin zu staatlich gelenkten Angriffen und staatlich gelenkter Industriespio-nage. In meiner Funktion als Professor an der Hochschule der Bundeswehr in München und über zahlreiche Auslandseinsätze der Bundeswehr, bei denen ich in die Ausgestaltung der IT- und Kommunikationstechnik eingebunden bin, habe ich viele Einblicke und sehe, dass wir uns bereits in einer Vorphase der digitalen Kriegsführung befinden. Das Sammeln von Informationen über Personen, um sie später vielleicht unter Druck setzen zu können, ist hierfür nur ein Mosaik-Element der Bedrohung. Unsere Politik könnte hier durchaus mal aktiver werden. Viele der Gefahren sind

bekannt, werden aber nicht beseitigt, was vielleicht mit da-ran liegt, dass die eigenen Nachrichtendienste die Lücken im System kennen und selber nutzen.

Ein anderes Thema: durch private Smartwatches und Smartphones, die im Betrieb genutzt werden, durch vernetzte Fahrzeuge verwischt die Grenze zwischen privater und beruflicher Sphäre. Welche Rolle spielt IT-Security in diesem Kontext?

Wir werden eine Vielzahl von neuen Anwendungen und Angeboten sehen. Für ein Universi-tätsklinikum haben wir ein System entwickelt, bei dem man automatisiert durch das Kran-kenhaus gelenkt wird und zum Ort der Behandlung geleitet wird, ohne zuvor einen Menschen gesehen zu haben. Wartezeiten werden vermieden, Ansteckungsmöglichkeiten vermindert und Personal kann sinnvoller eingesetzt werden, als Patienten den Weg zeigen zu müssen. In der Bundeswehr z.B. tragen die Soldaten Chips unter der Haut, auf denen wichtige Informationen wie die Blutgruppe oder Arzneimittelunverträglichkeiten gespeichert sind, so dass im Fall von Verletzungen sofort richtig reagiert werden kann. Auch IKEA entwickelt solche Konzepte, bei denen man bei der Autobahn-Vorbeifahrt an einem Einrichtungshaus von IKEA in der Auto-Navigation eine Empfehlung erhält, dass ein bestimmtes Produkt, nach dem man seit Längerem sucht, in dieser Niederlassung vorhanden ist. Bestätigt man, bekommt man dann die Lieferung an einen vorreservierten Parkplatz des Möbelhauses geliefert, muss nicht mehr aussteigen und kann automatisiert bezahlen. Es muss aber jedem bewusst sein, dass diese Informationen für viele einsehbar und nutzbar sind. Diejenigen im Betrieb, die sich besonders interessieren, sollten den IT-Security-Verantwortlichen (vielleicht hat ja das Unternehmen einen CISO Chief Information Security Officer) einbeziehen und fragen. Wenn es den nicht gibt, wird es Zeit, ihn zu intern schaffen oder extern fallweise zu beauftragen.

Herr Sieber, ich danke Ihnen für das Gespräch.

Das Interview führte Dr. Gerald Heimann - ZENTEC GmbH

FrankfurtRheinMain GmbH | International Marketing of the Region

FrankfurtRheinMain
Become a part of it.

Jedes erfolgreiche Business beginnt mit einem ersten Funken, der in der richtigen Atmosphäre zur zündenden Idee wird. Hier in FrankfurtRheinMain sind wir Feuer und Flamme für kreative Innovationen und multikulturelle Vielseitigkeit – auch im Hinblick auf unser Freizeitangebot. Brennen Sie für Ihr Business? Dann werden Sie ein Teil von FrankfurtRheinMain.

Die **FrankfurtRheinMain GmbH International Marketing of the Region** ist der zentrale Ansprechpartner für alle Anfragen bei Ansiedlungen von Unternehmen aus dem Ausland.

Mehr Informationen unter www.frm-united.de

Migration zur neuen Netztechnologie

Festnetz, Mobilfunk und Datenverkehr rücken zusammen. Durch die „Digitale Transformation“ wird alles IP – ALL-IP! Was bedeutet das für die IT-Infrastruktur?

Die Entscheidung ist schon vor langer Zeit gefallen! Die bisherigen analogen und ISDN-Anschlüsse wird es in Zukunft nicht mehr geben. Weltweit werden die öffentlichen Kommunikationsnetze auf das Internetprotokoll (IP bzw. VoIP) umgestellt. Die Deutsche Telekom will ihr Netz bis 2018 komplett auf All-IP umrüsten.

All-IP „Quo vadis“

Klassische Sprachübertragung mittels ISDN erfolgt über separate Kupferleitungen. Bei All-IP wird das gesprochene Wort in Datenpaketen über die Datenautobahn des Internets versendet. Das Protokoll (IP – Internet Protocol) sorgt dafür, dass die Sprachpakete bei dem richtigen Empfänger ankommen. Telefongespräche, Faxe, Videos und Daten werden über die gleiche IP-basierte Netzwerktechnik übertragen – ein Netz für alles.

Vorteile überwiegen

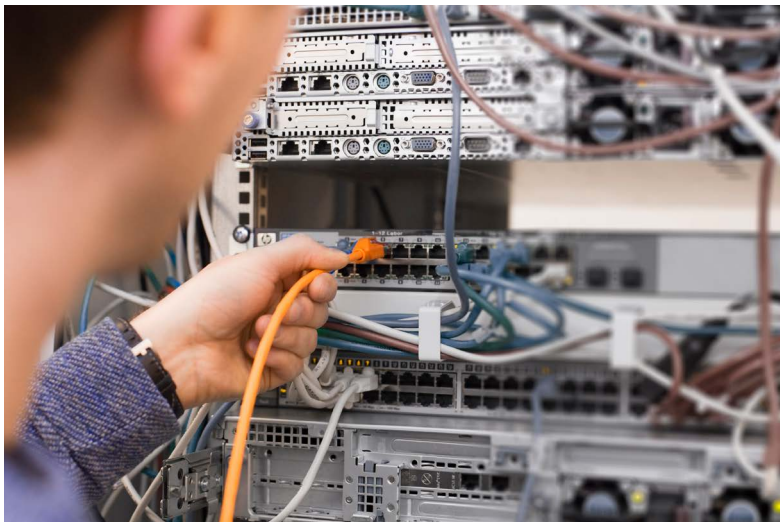
Die durchgängig IP-basierte Kommunikationstechnik eröffnet neue Möglichkeiten. Je nach Kommunikationssystem wird es zum Beispiel möglich, mit der Büronummer von unterwegs aus zu telefonieren. Anrufe können ganz individuell auf ein mobiles Telefon, eine Voicebox oder einen anderen Apparat umgeleitet werden. Das Steuern der eigenen Erreichbarkeit wird einfach und unkompliziert. Smartphones und Tablets können in die IT-Infrastruktur eingebunden werden. Zudem schaffen All-IP-Anschlüsse den Unternehmen Kostenvorteile im Betrieb und Service.

Hürden meistern

Die Umrüstung von ISDN auf IP-Technologie ist für jede Telefonanlage bzw. ITK-Infrastruktur individuell zu prüfen. Bei älteren Systemen ist ein Umstieg auf IP unter Umständen nicht ohne weiteres möglich. In diesen Fällen können IP-ISDN Gateways eingerichtet werden, die evtl. den Weiterbetrieb des Telefonsystems zulassen. Eine denkbare Alternative ist auch, auf ein eigenes, stationäres Kommunikationssystem gar komplett zu verzichten. Verschiedene Anbieter bieten bereits umfangreiche Cloud-Lösungen an, die über das Internet bezogen werden können. Dank All-IP ein möglicherweise lohnendes Modell.

Neue TK-Anlagen können in der Regel auch mit der neuen Anschlussart betrieben werden. Welche Strategie zu verfolgen ist und ob alle relevanten Komponenten IP-fähig sind, ist jeweils spezifisch auf die Gegebenheiten und Erfordernisse des Unternehmens zu prüfen.

Ob der bisherige Internetanschluss behalten werden kann oder ein neuer Internetprovider eingebunden werden sollte, ist von der garantierten Bandbreite abhängig. Zur VoIP Telefonie wird je Telefonat eine Bandbreite von ca. 100 kBit/s gleichzeitig sowohl im Up- als auch Downstream empfohlen.



ALL-IP - ein Netz für alles!
Die Umstellung benötigt eine gute Vorbereitung

Rufnummern behalten

Die bisherigen und bekannten Rufnummern bleiben zumeist erhalten. Dafür ist lediglich ein wenig Bürokratie erforderlich. Schwierig wird es, wenn in der

bisherigen TK-Anlage Rufnummern verlängert wurden, ohne die Bundesnetzagentur einzubeziehen. Mit dem Telekommunikationsanbieter sind diese Hindernisse zu diskutieren. Es sind diverse Anträge zu stellen und der Umstellungstermin ist genau abzustimmen. Zuverlässige Anbieter übernehmen diesen Service für Ihre Kunden.

Zeitpunkt der Umstellung auf All-IP

Generell gilt: So früh wie möglich! Wer ohne Ausfallzeiten oder Datenverlust zu ALL-IP migrieren möchte, benötigt Zeit. Zeit für Planung, zum Testen und dem Aufbau eines evtl. Parallelbetriebes vor einer kompletten Umschaltung. Sind Brandmeldeanlagen, Alarmanlagen, Aufzugnotrufsysteme etc. eingebunden, müssen auch diese sicher in die neue Infrastruktur eingebunden werden. Nur wer ohne Zeitdruck plant, kann einen reibungslosen Ablauf der Umstellung und einen zuverlässigen und sicheren Betrieb der neuen IP-Technik erwarten.

Fazit

Der Technologiewechsel ist ein Faktum, die Umstellung ist ein Muss. Gerade im Hinblick auf die Digitalisierung 4.0 ist es zwingend notwendig, dass alle Kommunikationseinrichtungen die gleiche Sprache sprechen.

Die gemeinsame Datensprache durch die IP-Technologie ist ein „Enabler" für eine Vielzahl neuer Kommunikationsservices. Telefonie, Internet, Mobilfunk - alles wird vernetzt und steht als einheitlicher Dienst zur Verfügung. Das bietet zahlreiche Vorteile für Unternehmen, die es aufzudecken gilt. Mit professioneller Hilfe kann ein reibungsloser Wechsel auf ALL-IP ohne Ausfallzeiten gelingen. Ein Umstieg der Chancen nutzt und Problemstellungen bereits bei der Planung erkennt.

CITEC
the IP Company

Ansprechpartner

Andreas Herget
C+ITEC AG
Telefon: 06021 4436-1100
E-Mail: vertrieb@citec-ag.de
www.citeg-ag.de

Virtuelle Telefonie – die Kommunikation der Zukunft

Die Digitalisierung der Arbeitswelt ist seit Jahren auf dem Vormarsch und hat, nach der Mobiltelefonie, nun ein weiteres Gebiet der sprachlichen Kommunikation erreicht: Virtuelle Telefonanlagen, „Hosted-PBX" (Private Branch Exchange), lösen ISDN-Anlagen zunehmend ab. Doch wie in allen Bereichen, die das Internet zur Datenübertragung nutzen, stellt sich dabei die Frage: Wie sicher ist diese Form der Kommunikation? Die Stichworte Georedundanz, Verschlüsselung und deutscher Datenschutz geben eine eindeutige Antwort.

Das Prinzip hinter einer „Telefonanlage im Netz" ist denkbar einfach: Alle Funktionen einer klassischen Telefonanlage werden in mehreren Rechenzentren eines Anbieters virtuell gehostet und über das Internet zur Verfügung gestellt. Entscheidet sich ein Unternehmen für eine Umstellung, muss es lediglich für das Vorhandensein eines Internetzugangs sowie eines SIP-Endgerätes sorgen – um Inbetriebnahme, Wartung und Updates kümmert sich der Anbieter der Cloud-Telefonanlage. Von dieser Auslagerung

profitieren Existenzgründer und Unternehmen jeder Größe: Eingesparte Kosten, Raum und Zeit sowie die gewonnene Flexibilität lassen sich für die Kernbereiche des Geschäfts nutzen.

Einmal installiert bietet Hosted-PBX alles, was eine zukunftsfähige, moderne Telefonanlage ausmacht: Sie ist beliebig erweiterbar, über ein Kundenportal einfach zu bedienen – und sicher. Denn ihr Betrieb ist, im Gegensatz zur bisherigen Geschäftstelefonie, nicht von Hardware abhängig, die veralten oder versagen kann und regelmäßig ausgetauscht werden muss. Die georedundante Verteilung auf mehrere Hochleistungsrechenzentren sorgt dafür, dass Telefonieren über das Netz ausfallsicher möglich ist – selbst bei einer Fehlfunktion in einem der Rechenzentren.

Doch wie sieht es mit der eigentlichen Sprachübertragung und potentiellen Sicherheitslücken aus? Im Prinzip funktioniert die virtuelle Übertragung folgendermaßen: Gesagtes wird als analoges Signal aufgenommen, anschließend digitalisiert und dabei in ein Audioformat umgewandelt. Über das Internet gelangen die Datenpakete zum Empfänger, wo sie wieder in ein analoges Signal umgewandelt werden. Die Verbindung erfolgt also nicht mehr über ein Telefonkabel, sondern über eine breitbandige Internetanbindung, die eine hohe Übertragungsqualität gewährleistet und Verständigungsschwierigkeiten ausschließt. Viele Dienstleister bieten zudem eine Verschlüsselung der Übertragung zwischen Telefon und Server an, sodass Gespräche unter abhörsicheren Bedingungen und ohne ungewollte Zuhörer stattfinden können.

Das Thema Datenspeicherung im Netz bereitet vielen Unternehmern Kopfzerbrechen. Aus Angst vor möglichen Hackerangriffen, Datenraub und -missbrauch scheuen sie sich davor, Cloud-Dienste trotz aller Vorteile in Anspruch zu nehmen. Diese Sorge ist bei einer virtuellen Telefonanlage unbegründet – denn Interessenten haben die Möglichkeit, auf eine deutsche Komplettlösung zu setzen und damit auf die Integrität eines deutschen Unternehmens. Die Dienstleistungen vieler Anbieter basieren auf Markentechnik „made in Germany“ und werden zumeist in nationalen Rechenzentren bereitgestellt, die den strengen deutschen Datenschutzbestimmungen unterliegen, ISO-27001-zertifiziert sind und regelmäßige Updates durchlaufen. Dabei fungiert der Dienstleister auch nach dem „go live“ als Ansprechpartner bei Fragen, Schwierigkeiten und Anpassungen jeglicher Art. Für den Kunden bleibt die Telefonanlage so trotz Auslagerung sehr transparent und kontrollierbar, und die Sorge, dass Firmeninterna in die falschen Hände geraten, unbegründet. Das gilt auch für Nutzer mobiler Endgeräte: Mit einer Einbindung in die virtuelle Telefonanlage lassen sich Smartphones wie Bürotelefone nutzen und obliegen dabei besagten Datenschutzrichtlinien, auch wenn sich der Anrufer im Ausland befindet.

Die Digitalisierung hat die Arbeitswelt zum Positiven gewandelt – Flexibilität, Zeit- und Kostenersparnis sind dabei die wichtigsten Stichwörter. Nun gilt es, diesen Prozess im Bereich der Telefonie voranzutreiben, denn auch hier profitieren Unternehmer von besagten Vorteilen. Setzt man zudem auf einen deutschen Anbieter, kann man nur gewinnen: Hinsichtlich Technik und Sicherheit sind Cloud-Telefonanlagen stets auf dem neuesten Stand – ein klarer Vorteil gegenüber klassischen Telefonanlagen, aber auch gegenüber ausländischen Dienstleistern. Die hohen Standards im Bereich Datenschutz machen die virtuelle Telefonie somit zu einer besonders sicheren Kommunikationsform, die, gerade in der Geschäftswelt, definitiv ihre Daseinsberechtigung hat.

Ansprechpartner

Franziska Genster
equada GmbH
Telefon: 06023 96741-24
E-Mail: info@equada.de

Digital Leadership

„Wer nicht digital denkt, ist raus!“ Diesen dramatischen Appell richtete der Springer-Chef Matthias Döpfner bereits 2013 an seine Mitarbeiter. Was zunächst der Produktinnovation und sodann der Produktion (Industrie 4.0) galt, erfasst nun auch die Digitalisierung von Führung in den Unternehmen.

Die Übertragung bzw. Delegation von Aufgaben an einen Mitarbeiter erfolgt bereits heute vielfach in digitaler Form von E-Mails, Outlook, SMS usw. Neu am „Digital Leadership“ ist nun die bewusste und systematische Delegation auf der Führungsebene mithilfe professioneller Delegationssoftware. Hierbei wird externes oder internes Expertenwissen in Form von Aufgaben digital zur Verfügung gestellt. So können Führungskräfte Routineaufgaben zentral und dabei gleichzeitig an mehrere und geeignete Funktionen, Rollen und/oder konkreten Personen zuordnen. Die Software meldet via Ampelfunktion die Umsetzung der Aufgaben an die Führungskraft zurück.

Merkmale funktionierenden Digital Leadership sind Schnelligkeit, Effektivität, Flexibilität und Transparenz innerhalb der Organisation. So setzen viele Unternehmen in der Region im Compliance-Bereich bei der Einhaltung externer und interner Vorschriften und Richtlinien den digital gelieferten Compliance-Service der Martin Mantz GmbH ein. Zu den Unternehmen zählen komplexe Produktionsunternehmen, Unternehmen mit vielen dezentralen Standorten, Logistikunternehmen, Servicegesellschaften mit ständig wechselnden Einsatzorten oder Mitarbeitern an Heimarbeitsplätzen.

Digital Leadership setzt einige wesentliche Elemente voraus:

1. **Digitale Unternehmenskultur**
   Digitalisierung braucht die Entwicklung einer entsprechenden Unternehmenskultur. Weit verbreitet ist der Anspruch der Mitarbeiter auf persönlicher Ansprache und Delegation der Aufgaben durch die Führungskräfte. Zukünftig muss allen Mitarbeitern bewusst sein, dass die digitale Führung ein wesentlicher Bestandteil moderner Unternehmensführung ist. Dies erfordert ein hohes Maß an digitaler Führungsverantwortung, von der Unternehmensführung bis zum Mitarbeiter.

2. **Digital orientierte Mitarbeiter**
   Bei der digitalen Orientierung geht es nicht allein nur darum, die digitalen Medien zu beherrschen. Selbst viele junge Menschen der sog. Y-Generation leben privat digital, handeln jedoch in der beruflichen Praxis analog. Hier setzt bereits ein Umdenken auf allen Unternehmensebenen ein. Die digitale Führung will von allen Beteiligten, den Führungskräften und Mitarbeitern, gelernt sein. Gefordert ist ein Verständnis für die Bedenken der Mitarbeiter und Geduld bei der Umsetzung. Das Statement der Geschäftsführung zur Digitalisierung muss jedoch klar sein und bleiben.

3. **Kommunikation**
   Während die persönliche Führungskommunikation abnimmt, steigt im gleichen Maße das Bedürfnis nach Teamkommunikation. Digital Leadership ermöglicht die flexible Zusammensetzung von Teams interner und externer Mitarbeiter. In den gut organisierten Teams tauschen sich die beteiligten Mitarbeiter über die Abteilungsgrenzen hinaus dann themenbezogen aus. In der Regel erfordert dies keine Führungskräfte um gute Ergebnisse zu erzielen.

4. **GEORG Compliance Manager®**
   Selbstverständlich braucht Digital Leadership eine gute und ausgereifte Software. Kriterien für eine gute Software sind Einfachheit, Funktionalität und Akzeptanz.

MARTINMANTZ
COMPLIANCE SOLUTIONS

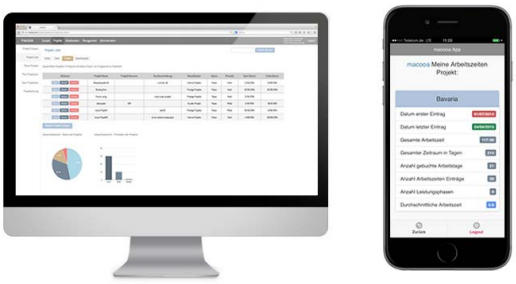
Ansprechpartner

Martin Mantz
Martin Mantz GmbH
Telefon: 06022 20827124
E-Mail: m.mantz@martin-mantz.de
www.martin-mantz.de

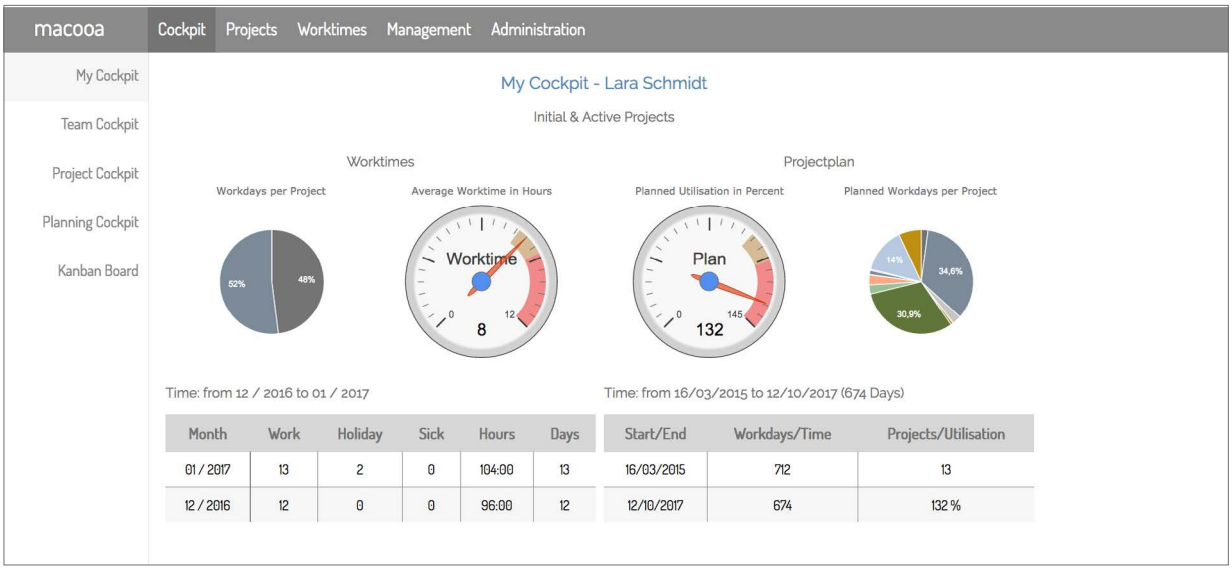
macooa - Von der Projektplanung bis zur Rechnung alles online

Die macooa GmbH hat eine Online-Software speziell für kleine und mittelständige Firmen entwickelt, die projektorientiert arbeiten, etwa Beratungsunternehmen, Marketingagenturen oder Architektur- und Ingenieurbüros.

„macooa“ stellt eine mehrsprachige Komplettlösung dar, mit der diese Unternehmen ihre Arbeitsprozesse ganzheitlich gestalten können, von Projektplanung und -controlling über Budgetplanung und -kontrolle, Rechnungstellung, Urlaubs- und Arbeitszeitplanung /-erfassung und vieles mehr.



Dank interaktiver Grafiken kann man beispielsweise Soll und Ist-Zustände vergleichen und als Unternehmer entsprechend reagieren. Dass sich „macooa“



speziell an kleine und mittlere Unternehmen richtet, begründet Geschäftsführer Ralf Behnstedt damit, dass gerade bei dieser Unternehmensgruppe der Einsatz entsprechender Software Planungs- und Kontrollinstrumente bisher eher „stiefmütterlich behandelt wurde, der Bedarf jedoch immens ist“.

„macooa“ ist in drei Versionen verfügbar, in der BASE (für sieben € im Monat/Benutzer), in der PRO (11 € Monat/Benutzer) und in der ENTERPRISE Version (pauschal 330 € im Monat). Bei allen drei Möglichkeiten steht selbstverständlich auch eine App für Smartphones zur Verfügung, die es erlaubt, die Projekte auch von unterwegs einzusehen und zu bearbeiten.

macooa

Ansprechpartner

Ralf Behnstedt Geschäftsführung
macooa GmbH
Telefon: 06023 503967
E-Mail: ralf.behnstedt@macooa.com
www.macooa.com

EU Datenschutz Grundverordnung (DSGVO), Bundesdatenschutzgesetz(neu) Jetzt wird es ernst!

Achtung: Bis zum 25. Mai 2018 muss jedes Unternehmen Datenschutz nach der neuen EU Richtlinie DSGVO garantieren. Passen rechtliche Erwartung und betriebliche Realität nicht zusammen kann es sehr teuer werden!

Die EU DS-GVO schreibt vor, Daten vor Diebstahl sowie vor unberechtigtem Zugriff zu schützen:

- Die Daten müssen verfügbar, absolut korrekt und aktuell sein.
- IT-Security muss sicherstellen, dass
  - von außen kein unberechtigter Zugriff auf Daten besteht (Hacker-Angriffe, Trojaner)
  - keine Daten von innen gewollt oder ungewollt nach draußen dringen (Disclosure, Data Loss Prevention).
- weiter fordert die EU DSGVO von der hoffentlich vorhandenen Abteilung IT-Sicherheit, Sicherheitsbarrieren, s.g. Controls, einzusetzen.
- Fast jedes Unternehmen hat einen Datenschutzbeauftragten (interner oder externer DSB) zu benennen. Dies dürfen nicht der IT-Verantwortliche und nicht der Geschäftsführer sein.

Für jeden Unternehmer ist nun zu entscheiden - trifft diese Verordnung auf mich überhaupt zu? Falls Sie personenbezogene Daten verarbeiten, können Sie dies als starken Indikator verwenden – und dies ist den meisten Unternehmen der Fall!

In einem solchen Fall werden Sie nicht vermeiden können, bestimmte Maßnahmen in angemessenem Umfang durchzuführen – hier eine kleine Beispielsammlung:

- Überprüfung / Einführung / Erweiterung von technischen und prozessualen Maßnahmen
  - ISMS – speziell auf das Unternehmen zugeschnitten
  - Review bestehender Verfahren zur Compliance mit EU DSGVO
- Schwachstellen und Sicherheitsüberprüfung der Technik sowie „Notfallübungen“ von Mitarbeitern mit Werkzeugen wie z.B. einer „TOOL-BOX42“ (vergleichbar einem digitalen Hausmeister)
- Audits der aktiven IT- Infrastrukturen, die personenbezogene Daten halten / verarbeiten / weitergeben / empfangen
- Überprüfung ausgelagerter Verarbeitung von Daten (Outsourcing, Outtasking), z.B. bei Lohnabrechnungen durch einen Steuerberater oder DATEV
- Prüfung der Notwendigkeit des Einsatzes eines internen oder externen Datenschutzbeauftragten (Vollzeit /Teilzeit, Skill und aktueller Ausbildungsstand)
- Etablierung zyklischer Datenschutz-Überprüfungen – Datenschutz nach EU DSGVO ist keine Einmalübung, sondern eine dauerhafte Etablierung von Überprüfungen
- Durchführung und Dokumentation zyklischer Notfallübungen auf allen Ebenen für jeden Mitarbeiter sowie der implementierten Technik und der prozessualen Abläufe
- Bei neu eingesetzter Software/Hardware und bei Aktualisierungen (Programmversionen / Upgrades / Updates) auf den Standard „Datenschutz nach EU DSGVO“ achten (Stichwort: privacy by default / privacy by design)

Aus den oben aufgeführten Maßnahmen entstehen in der Regel viele nachfolgenden weiteren Aufgaben und Aktionen auf allen Ebenen und Bereichen des Unternehmen – dies betrifft nicht nur die IT-Spezialisten, sondern auch den Rechtsberater sowie den Prozessgestalter und externe IT-Dienstleister.
Holen Sie sich erfahrene effektive Unterstützung bei der Umsetzung und Einhaltung der DSGVO - mittlerweile werden diese Dienstleistungen von Unternehmen, auch für den Mittelstand und kleinere Unternehmen, aus der Region angeboten!

Fazit:

Jedes Unternehmen ist gefordert, schnell zu handeln!

Die EU DSGVO inklusive der Konkretisierung durch das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU“ („BDSG neu“) lösen das bisherigen Bundesdatenschutzgesetz zum Mai 2018 ab. Damit ist der Datenschutz auf europäischer

Ebene harmonisiert. In den sehr hohen Bußgeldern und den möglichen Schadensersatzforderungen zeigt sich der Wille des Gesetzgebers nach einem konsequenten Datenschutz.

Informative Web-Links:

Bayrisches Landesamt für den Datenschutz:
Interessante, leicht verständliche Kurz-Papiere zum DSGVO:
https://www.lda.bayern.de/de/datenschutz_eu.html

Bundesamt für die Sicherheit in der Informationsverarbeitung (BSI):
Alles zum Thema IT-Grundschutz:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Die durchzuführenden Maßnahmen aus den unterschiedlichsten Bereichen machen es sinnvoll und notwendig, externe Spezialisten hinzuzuziehen.

Ansprechpartner

Andreas Schmidtke
Sapiens42 GmbH
Telefon: 06022 6692290
E-Mail: aschmidtke@sapiens42.de

Wie lernt ein Auto, Radfahrer zu verstehen

Mobilitätskonzepte der Zukunft setzen vermehrt auf eine Fortbewegung, bei denen der Mensch während der Fahrt nicht mehr selbst eingreifen muss. Die Vision ist im Grunde schon alt. Bereits in den 1980ern wurde das erste selbstfahrende Fahrzeug unter Leitung von Prof. Ernst Dickmanns der Universität der Bundeswehr in München entwickelt.

Bereits damals konnte man erfolgreich Spuren folgen und bekannten Hindernissen ausweichen. Bis heute haben sich selbstfahrende Autos deutlich weiterentwickelt. Das hochautomatisierte Fahren auf Autobahnen wird mit Forschungsfahrzeugen derzeit intensiv erprobt. In der Stadt hingegen ist das automatisierte Fahren wesentlich komplexer. Hier sind noch einige ungelöste Herausforderungen zu bewältigen. Dazu gehört das Erkennen und Verstehen des Fahrzeugumfelds. Im Gegensatz zu Autobahnen gibt es in der Stadt verletzliche Verkehrsteilnehmer wie z. B. Radfahrer, die schnell gefährliche Situationen hervorrufen können. Folgende Fragen stellen sich beispielsweise:

Fährt der Radfahrer vor das Auto? Kann der Radfahrer sicher überholt werden? Verhält sich der Radfahrer wie erwartet?
Als menschliche Autofahrer liegt die Aufgabe bei uns, einen Radfahrer wahrzunehmen und dessen Verhalten abzuschätzen. Dies fällt uns in der Regel relativ einfach, da wir gelernt haben und verstehen, wie sich Radfahrer verhalten. Wir können durch deren Handlungsweise auf Absichten schließen und so mögliche Gefahren frühzeitig erkennen.
Fällt der Fahrer weg, muss das Auto diese Aufgabe übernehmen. Mit genau dieser Aufgabe beschäftigt sich das Labor für Kooperative automatisierte Verkehrssysteme an der Hochschule Aschaffenburg. Das Projekt wird durch die Deutsche Forschungsgemeinschaft (DFG) gefördert. Mit Hilfe von verschiedenen Sensordaten (z. B. Kamera) sollen die Absichten und das Verhalten von Radfahrern vorausgesagt werden, um anschließend verhältnismäßig reagie-

Abgebildet ist eine Pfadschätzung eines Radfahrers. Eingezeichnet sind gepunktet die bisherigen Positionen des Kopfs, des Pedals und des Rads vom Start bis zur aktuellen Position und in Grün die vorhergesagten Kopfpositionen in einem zeitlichen Abstand von jeweils 0.2 s.

ren zu können.

Doch wie lernt ein Auto, Radfahrer zu verstehen? Dazu sind zwei Dinge ganz entscheidend. Erstens: Wie „sieht" das Auto einen Radfahrer, sprich wie nimmt ein Auto einen Radfahrer wahr? Zweitens: Wie verhalten sich Radfahrer? Dazu muss unser intuitives Verständnis vom Radfahrerverhalten in konkrete Formeln gefasst werden, man spricht hierbei von Modellbildung.

Der zweite Punkt schließt eine ausführliche Analyse von Radfahrerverhalten unter realen Bedingungen ein. Um das Verhalten von Radfahrern zu modellieren, wurde ein bestehendes Sensorsystem an einer Kreuzung in Aschaffenburg verwendet. An dieser Kreuzung können mit Hilfe von hochauflösenden Kameras verschiedenste Konstellationen nachgestellt und erfasst werden. Aus den gewonnenen Informationen lassen sich konkrete Werte für Beschleunigungs- und Geschwindigkeitsverläufe von Radfahrern bestimmen. Daneben werden typische Verhaltensweisen, beispielsweise vor einer Startbewegung, untersucht, um eine solche früher erkennen zu können.

Bereits heute lassen sich zukünftige Bewegungspfade an der Kreuzung mit einer Genauigkeit von 40 cm innerhalb eines Zeithorizonts von 1s vorhersagen. In der Zukunft soll die Genauigkeit der bestehenden Systeme weiter verbessert werden, um somit für mehr Sicherheit für Radfahrer zu sorgen und um damit auch dem Ziel des automatisierten Fahrens in der Stadt näherzukommen.

Ansprechpartner

Prof. Dr. Konrad Doll
Hochschule Aschaffenburg
Telefon: 06021 4206720
E-Mail: konrad.doll@h-ab.de

Fahrerloses Absperrfahrzeug für mehr Sicherheit an Tagesbaustellen

Noch vor ein, zwei Jahrzenten war es kaum vorstellbar, nun wird es immer wahrscheinlicher: selbstfahrende Fahrzeuge. Nach der kontinuierlichen Einführung verschiedener Assistenzsysteme ist das hoch- und vollautomatisierte Fahren der nächste bedeutsame Schritt in der technologischen Entwicklung auf dem Automobilsektor – die rechtlichen Voraussetzungen dazu wurden in Deutschland inzwischen geschaffen, es muss aber immer noch eine Person hinter dem Steuer sitzen. Das fahrerlose Fahren ist dann der nächste Entwicklungsschritt und das Projekt „aFAS – Automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Autobahnen" befasst sich bereits damit. Ziel ist die Entwicklung und Erprobung eines selbstfahrenden Absperrfahrzeugs für Tagesbaustellen.

Hessen Mobil setzt mit diesem zukunftsweisenden Projekt den konsequenten Weg zur Erhöhung der Sicherheit an Baustellen fort, der seit vielen Jahren mit richtungsweisenden innovativen Maßnahmen beschritten wird. Dazu zählen unter anderem die dynamische Ortung aller Tagesbaustellen (DORA), die Anwendung von Phasenplänen für den Auf- bzw. Abbau von Baustellenverkehrsführungen und die Einführung der kooperativen Baustellenwarnung im Rahmen des C-ITS Korridors Rotterdam – Frankfurt am Main – Wien.

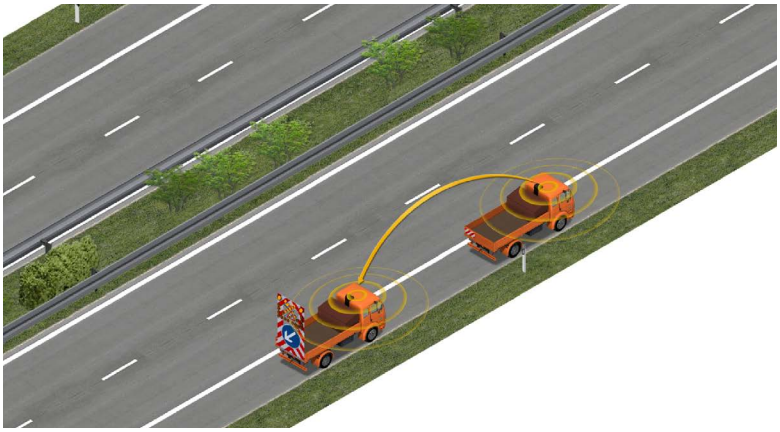
Absicherung eines Arbeitsfahrzeugs bei Mäharbeiten
Quelle: Hessen Mobil – Straßen- und Verkehrsmanagement

An Tagesbaustellen werden zur Sicherung des eingesetzten Personals und zur Minimierung der Gefährdungen für den fließenden Verkehr im Wesentlichen fahrbare Absperrtafeln, separate Absperrfahrzeuge und Vorwarneinrichtungen eingesetzt. Trotz des hiermit verbundenen erheblichen personellen und technischen Aufwands, der vielfach höher als der Aufwand für die Durchführung der eigentlichen Tätigkeit ist, bleibt das Gefährdungspotential für Mitarbeiter/-innen der Autobahnmeistereien sowie beauftragter Firmen hoch. Unfalluntersuchungen zeigen, dass von schweren Unfällen häufig Arbeitsfahrzeuge, die sich selbst absichern, und Absperrfahrzeuge auf dem Seitenstreifen betroffen sind. Vielfach werden die Unfälle durch Lkw aus dem fließenden Verkehr heraus verursacht, wodurch auch die überdurchschnittliche Unfallschwere begründet ist. Die wirkungsvollste Maßnahme im Hinblick auf die Sicherheit des eingesetzten Personals besteht darin, dessen Aufenthalt sowohl neben als auch in Fahrzeugen, die einer unmittelbaren Gefährdung im Längsverkehr, beispielsweise durch auffahrende Fahrzeuge, ausgesetzt sind, ganz zu vermeiden.

Diesem Ansatz trägt das Projekt aFAS Rechnung. Mit dem fahrerlosen Absicherungsfahrzeug, das einem Arbeitsfahrzeug auf dem Seitenstreifen automatisch folgt, können zum einen die Arbeitsstellen auf dem Seitenstreifen, die ein sehr hohes Gefährdungspotential beinhalten, abgesichert werden. Zum anderen wird im Rahmen des Projekts die Komplexität des Entwicklungsaufwandes überschaubar gehalten, da das automatisch fahrende Absperrfahrzeug in einer ersten Entwicklungsstufe nur außerhalb der regulär befahrenen Fahrstreifen eingesetzt wird, keine Fahrstreifenwechselvorgänge erforderlich sind und im fahrerlosen Betrieb nur geringe Geschwindigkeiten gefahren werden.

Es ist vorgesehen, den Prototyp des automatischen Absicherungsfahrzeugs auf ausgewählten Strecken-

abschnitten im DRIVE-Testfeld Hessen unter regulären Verkehrsbedingungen zu erproben. Dabei wird sich das Absicherungsfahrzeug während der Dauer der Tagesbaustelle fahrerlos bewegen. An- und Abfahrt zum Einsatzort erfolgen noch mit einem Fahrer am Steuer. Der Prototyp erfasst die Umgebung mit Hilfe seriennaher Kamera- und Radarsystemen. Die eingebaute Sensorik gewährleistet u.a. eine Objekt-, Fahrstreifen- und Freiflächenerkennung. Zudem erfolgt die Übertragung relevanter Informationen zwischen Absicherungsfahrzeug und vorausfahrendem Arbeitsfahrzeug per WLAN 802.11 p [ETSI ITS G5].



WLAN-Kommunikation zwischen Arbeitsfahrzeug und fahrerlosem Absicherungsfahrzeug
Quelle: MAN Truck & Bus AG

Langfristige Zielsetzung in Hessen ist der Einsatz autonomer Sicherungsfahrzeuge bei allen Tagesbaustellen. Daher wird das automatische Absicherungsfahrzeug als Prototyp so entwickelt, dass eine nachfolgende serienmäßige Umsetzung möglich ist. Trotz des Forschungscharakters findet die Norm ISO 26262 zur funktionalen Sicherheit von Serien-Straßenfahrzeugen Anwendung, und es sollen - soweit möglich - bereits verfügbare seriennahe Komponenten eingesetzt werden.

Das Projekt aFAS soll nicht nur die Sicherheit an Tagesbaustellen erhöhen, sondern auch neue Impulse und wichtige Erkenntnisse für die Entwicklung hoch- und vollautomatisierter Fahrzeuge und ihren Einsatz im öffentlichen Straßenverkehr setzen.

Der Projektstart war im August 2014 – die Laufzeit ist auf vier Jahre angelegt. Das Bundesministerium für Wirtschaft und Technologie (BMWi) fördert das Vorhaben mit insgesamt rund 3,4 Mio. Euro.

Es beteiligen sich folgende Unternehmen und Institutionen: BASt – Bundesanstalt für Straßenwesen, Hessen Mobil – Straßen- und Verkehrsmanagement, Hochschule Karlsruhe – Technik und Wirtschaft, MAN Truck & Bus AG, Technische Universität Braunschweig – Institut für Regelungstechnik, ZF TRW, WABCO sowie Robert Bosch Automotive Steering GmbH.

Ansprechpartner

Gerd Riegelhuth
Hessen Mobil – Straßen- und Verkehrsmanagement
Abteilungsleiter Verkehr
Telefon: 0611 3663030
E-Mail: gerd.riegelhuth@mobil.hessen.de
www.mobil.hessen.de und www.afas-online.de

Politikansätze für mehr Sicherheit in der digitalen Gesellschaft

Die Digitalisierung hat längst alle Bereiche unserer modernen Gesellschaft erfasst. Das weltweite Datenvolumen wächst kontinuierlich und verdoppelt sich nahezu alle zwei Jahre. Der technische Fortschritt schafft für Bürger, Wirtschaft und Politik aber nicht nur Chancen, sondern auch erhebliche neue Risiken.

Wachsende Bedrohungen

Laut dem Branchenverband BitKom wird heute jeder zweite Internetnutzer Opfer von Cyberkriminalität, z. B. durch Schadsoftware oder Online-Betrug. Weltweit richtete der Diebstahl von Firmendaten im Jahr 2016 einen Schaden von rund 416 Milliarden Euro an. Bis 2019 könnte dieser Schaden um weitere 2,4 Billionen Euro ansteigen, schätzt eine Samsung-Studie, die auf der diesjährigen Fachmesse CeBIT vorgestellt wurde. In den USA und in Frankreich wurde versucht, demokratische Wahlen durch Diebstahl, Manipulation und Veröffentlichung vertraulicher Daten und die gezielte Verbreitung von Falschnachrichten im Internet zu beeinflussen. Mit Blick auf die Bundestagswahl am 24. September besteht auch in Deutschland die Gefahr der Wahlmanipulation. Sogar lebensbedrohlich können IT-Angriffe werden, wenn kritische Infrastruktur Ziel der Attacken wird. Fest steht: IT-Sicherheit ist längst ein gesamtgesellschaftliches Megathema.

Möglichkeiten der Politik

Natürlich lässt sich die Digitalisierung nicht aufhalten oder zurückdrehen. Außerdem sind der nationalen Politik räumliche Grenzen und hohe datenschutzrechtliche Hürden gesetzt. Deswegen ist das vereinte Europa auch beim Thema Digitalisierung von unschätzbarem Wert. Die Kooperation der EU-Staaten z.B. via Europol oder über die Gewährleistung gemeinsamer IT-Sicherheits- und Datenschutzstandards über die NIS-Richtlinie oder die Datenschutzgrundverordnung, machen das Netz in ganz Europa sicherer. Allerdings kann es aufgrund der technischen, rechtlichen und politischen Grenzenlosigkeit des Cyberraums keine absolute Sicherheit geben. Ziel einer verantwortungsvollen rechtsstaatlichen IT-Sicherheitspolitik muss daher sein, die Risiken der Digitalisierung beherrschbar zu machen, damit Bürger und Unternehmen die Chancen der digitalen Revolution möglichst gefahrlos nutzen können.

Maßnahmen der Politik

In dieser Legislaturperiode haben wir im Bund vieles beschlossen und umgesetzt, um Deutschland zu einem der sichersten Cyber-Räume weltweit zu machen. Im Juli 2015 trat das IT-Sicherheitsgesetz in Kraft, das private Betreiber von kritischer Infrastruktur (aus den Bereichen Energie, Gesundheit, Wasser, Ernährung, Telekommunikation, Verkehr, Staat, Finanzen, Medien) gesetzlich verpflichtet, relevante Sicherheitsvorfälle zu melden und bestimmte IT-Sicherheitsstandards einzuhalten. Aktuell wird das 2011 gegründete Nationale Cyberabwehrzentrum (NCAZ) zu einem Krisenabwehrzentrum ausgebaut, das über ein umfassendes Lagebild zur Cybersicherheit in Deutschland verfügt. Im NCAZ bilden die Sicherheitsbehörden des Bundes (BKA, Zoll, Bundespolizei, Katastrophenschutz, Nachrichtendienste) eine Einheit und teilen ihre Fähigkeiten. Zudem wird in München derzeit mit der „Zentralen Stelle für Sicherheit in der Informationstechnik“ (ZITiS) ein neues Forschungs- und Entwicklungszentrum aufgebaut, das die Sicherheitsbehörden mit Know-how und technischen Lösungen unterstützen soll. Im November 2016 hat die Bundesregierung außerdem die neue IT-Sicherheitsstrategie beschlossen und darin 30 konkrete Ziele definiert, um die IT-Sicherheit in Deutschland systematisch und in Kooperation mit der Wirtschaft zu verbessern. Eines der Ziele ist z.B. die Einführung eines IT-Gütesiegels, damit IT-Sicherheit bereits bei der Entwicklung und dem Kauf neuer Geräte mitgedacht wird. Ein weiteres Ziel ist

der Aufbau mobiler Teams von IT-Experten, um im Ernstfall schnell vor Ort Gegenmaßnahmen umsetzen zu können. Ziel all dieser Ansätze ist es, die IT-Sicherheitsarchitektur in Deutschland konsequent fortzuentwickeln und die Widerstandskraft systematisch auf allen Ebenen zu verbessern. IT-Sicherheit wird ein zentrales Arbeitsfeld der deutschen Innenpolitik in den kommenden Jahrzehnten bleiben.

Was tun im Notfall

Extra für die Wirtschaft haben die Polizeien von Bund und Ländern die „Zentrale Ansprechstelle Cybercrime“ (ZAC) geschaffen. Dort können gerade kleinere und mittelständische Unternehmen ohne eigene IT-Sicherheitsabteilung im Notfall Hilfe gegen Cyber-Angriffe finden Ein weiterer kompetenter Ansprechpartner ist in Bayern das bundesweit einzigartige Cyber-Allianz-Zentrum beim Landesamt für Verfassungsschutz Dort hilft man nicht nur im Notfall, sondern unterstützt auch mit einem umfangreichen Informationsangebot die Prävention. Denn am besten ist es, wenn man es gar nicht erst zum Notfall kommen lässt.

Prävention lohnt sich

Das effektivste Mittel für mehr IT-Sicherheit besteht aus dem Dreiklang: Eigenverantwortung-Wissen-Prävention. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf www.bsi.bund.de Bürgern und Wirtschaft kostenlose Informationen, Beratung und Schulungen an. Ziel des BSI ist es, Bürger und Unternehmen für die Bedeutung und Möglichkeiten der IT-Sicherheit zu sensibilisieren. In jedem Fall gilt: Prävention lohnt sich. Denn in der digitalen Welt hat der Verteidiger immer einen großen strukturellen Vorteil gegenüber dem Angreifer. Bereits ein einfacher Grundschutz macht Angriffe um ein Vielfaches schwieriger. Entscheidend bleibt dabei der Faktor Mensch. Der Cyber Security Intelligence Index von IBM zeigt, dass 60 Prozent der Cyberattacken auf Unternehmen im Jahr 2015 von Angestellten und ehemaligen Mitarbeitern mit Systemzugriff stammten. Dem kann präventiv vorgebeugt werden. Gleichzeitig müssen Staat und Gesellschaft noch deutlich mehr in Forschung und Ausbildung investieren. Der Bedarf an IT-Sicherheitsexperten wächst mit dem Datenvolumen mit. IT-Sicherheit berührt heute die Fundamente unserer hochtechnologischen freiheitlichen Gesellschaft. Das müssen wir uns das immer wieder bewusst machen und IT-Sicherheit konsequent mitdenken und weiterentwickeln.

Ob der bisherige Internetanschluss behalten werden kann oder ein neuer Internetprovider eingebunden werden sollte, ist von der garantierten Bandbreite abhängig. Zur VoIP Telefonie wird je Telefonat eine Bandbreite von ca. 100 kBit/s gleichzeitig sowohl im Up- als auch Downstream empfohlen.

Ansprechpartner

Andrea Lindholz, MdB
Deutscher Bundestag
Telefon: 030 22777399
E-Mail: andrea.lindholz.ma01@bundestag.de

weitere Informationen

Zentrale Ansprechstelle Cybercrime (ZAC)
Telefon: 089 1212-3300
E-Mail: zac@polizei.bayern.de
Cyber-Allianz-Zentrum beim
Landesamt für Verfassungsschutz
Telefon: 089 31201-222
E-Mail: caz@lfv.bayern.de

Für eine gerechte Arbeitswelt der Zukunft

Offensiv und optimistisch reagieren und soziale Antworten auf den Wandel finden

Als Leserinnen und Leser des Zukunftsmagazin erzähle ich Ihnen nichts Neues, wenn ich sage: Die Technik wandelt sich rasant. Ganze Volkswirtschaften stehen im Zeitalter der Digitalisierung und Vernet-

zung vor großen Herausforderungen. Es geht um Informatisierung, Ressourceneffizienz, intelligente Fabriken und Individualisierung von Produkten. Kurz: eine vierte industrielle Revolution nach der Dampfmaschine, den Fließbändern und der Automatisierung.

Damit wandelt sich auch die Arbeitswelt – und das birgt neben Chancen auch Risiken. Die Digitalisierung und die Industrie 4.0 werden viele Rahmenbedingungen Guter Arbeit verändern. Darauf müssen wir vorbereitet sein – als Politikerinnen und Politiker, als Unternehmerinnen und Unternehmer und natürlich als Arbeitsnehmerinnen und Arbeitnehmer. Dialogprozess der Arbeitsministerin

Im April 2015 hat Bundesarbeitsministerin Andrea Nahles dazu einen Dialogprozess zu Arbeitsformen und Arbeitsverhältnissen der Zukunft angestoßen. 18 Monate später hatten wir mit dem Weißbuch „Arbeiten 4.0“ das Ergebnis vorliegen.

Die Digitalisierung bietet enorme Chancen für mehr Souveränität über Ort und Zeit von Arbeit und neue Geschäftsmodelle. Gleichzeitig muss der Sozialstaat die Beschäftigten in diesem Wandel unterstützen: Berufsbilder und Anforderungen an Qualifizierung werden sich ändern, neue digitale Märkte entstehen, der Arbeits- und Datenschutz von Beschäftigten wird vor neue Herausforderungen gestellt.

Altersvorsorge für Selbstständige

Mit dem Wandel der Arbeitswelt durch die Digitalisierung werden Erwerbsbiografien voraussichtlich häufiger als früher Wechsel zwischen Zeiten der Selbstständigkeit und der abhängigen Beschäftigung aufweisen. Bereits heute haben wir circa drei Millionen Selbstständige in Deutschland, die keine obligatorische Altersvorsorge haben. Durch die im Gesamtkonzept zur Alterssicherung vorgeschlagene Einbeziehung von Selbstständigen in die gesetzliche Rentenversicherung kann eine durchgängige Absicherung für das Alter gewährleistet werden.
Selbstbestimmte Arbeitswelt

Arbeitszeitpolitik ist immer auch Arbeitsschutz – etwa vor Überforderung und Entgrenzung. Hinzu kommt aber das wachsende Bedürfnis nach Selbstbestimmung und Zeitsouveränität. Früher nach Hause gehen, um einen Nachmittag mit den Kindern zu verbringen und abends noch mal arbeiten, wenn die Kinder im Bett sind, ist nur ein – nach jetzigem Recht vielfach nicht mögliches – Beispiel. Deshalb wurde im Rahmen des Weißbuches das Modell der Wahlarbeitszeit entwickelt, das mehr Wahloptionen für Beschäftigte bei Arbeitszeit und -ort mit einer Möglichkeit der Abweichung von bestimmten Regelungen des Arbeitszeitgesetzes kombiniert. Mittelfristig könnte dies in einem neuen Wahlarbeitszeitgesetz verankert werden.

Für bestimmte Lebensphasen sollte es den Beschäftigten ermöglicht werden, die Arbeitszeit zu reduzieren, ohne dabei in die „Teilzeitfalle“ zu geraten. Deshalb setzt sich die SPD für ein Recht auf befristete Teilzeit ein.

Gut qualifiziert durch die Arbeitsversicherung

Die Umbrüche der Arbeitswelt 4.0 erfordern es, frühzeitig in die Stärkung der Qualifikation und die Verbesserung von Aufstiegsperspektiven zu investieren. Nur damit stellen wir sicher, dass das Angebot an Fachkräften zu der Nachfrage von morgen passen wird. Deshalb muss die Unterstützung präventiv ausgerichtet sein und darf nicht nur bei geringer Qualifikation oder bei unmittelbar drohendem Arbeitsplatzverlust greifen.

Wir haben bereits damit begonnen, Qualifizierungsberatung als Modellprojekt einzuführen. Langfristiges Ziel ist es, die Arbeitslosenversicherung zu einer Arbeitsversicherung weiterzuentwickeln, die auch Leistungen für Beschäftigte anbietet. Ein wichtiges Element ist hierbei das Recht auf eine unabhängige Berufs- und Weiterbildungsberatung; perspektivisch sogar ein Recht auf Weiterbildung.

Wir als SPD-Bundestagsfraktion wollen den digitalen Wandel unserer Wirtschaft im Allgemeinen und der Industrie im Besonderen aktiv begleiten und gemeinsam mit Gewerkschaften, Unternehmen und Verbänden daran arbeiten, Industrie 4.0 zu einem Erfolgsmodell für Deutschland zu machen.
Jetzt ist die Zeit, dass wir miteinander über die Zukunft der Arbeitswelt sprechen. Gesellschaft und Politik können diesen Weg selbst gestalten!

Ansprechpartner

Bernd Rützel, MdB
Deutscher Bundestag
Telefon: 030 22773434
E-Mail: bernd.ruetzel@bundestag.de

In Bayern hat die digitale Zukunft schon begonnen

Neuer 10-Punkte-Masterplan für Bayerns digitale Zukunft mit 3 Milliarden Euro

Der Schriftsteller Daniel Kehlmann hat in seinem Erfolgsroman „Die Vermessung der Welt“ das Leben des Mathematikers und Geodäten Carl Friedrich Gauß und des Naturforschers Alexander von Humboldt porträtiert. Beide haben sich in der ersten Hälfte des 19. Jahrhun-derts in ganz unterschiedlichen Bereichen um die „Vermessung der Welt“ verdient gemacht und dabei Neuland betreten. Von ihren Erkenntnissen profitieren wir noch heute.

Auch wir Menschen des 21. Jahrhunderts müssen unsere Welt wieder neu „vermessen“: Im Bereich der Digitalisierung, im Bereich des Breitbandausbaus und in vielen anderen Berei-chen. Denn der Fortschritt eines Landes und der Wohlstand seiner Menschen ist eng mit dieser „Vermessung“ verbunden!

Digitalisierung erfasst alle Bereiche unseres Lebens

Von welch überragender Bedeutung jetzt und in Zukunft die Digitalisierung ist, hat John Chambers, Präsident von Cisco, des weltweit führenden Anbieters im IT-Bereich, am Rande des Weltwirtschaftsforums 2017 in Davos betont. Auf die Frage, welche Branchen „der Wandel besonders hart treffen“ werde, sagte er: „Alle, denn alle werden digitalisiert. Da gibt es keine Unterschiede“.

Bayern fördert Ausbau des schnellen Internet mit 1,5 Milliarden Euro

Das haben wir in Bayern seit langem erkannt und setzen daher auch seit langem auf den Breitbandausbau und die Digitalisierung. Wir haben uns das ehrgeizige Ziel gesetzt, bis 2018 flächendeckend ein digitales Hochgeschwindigkeitsinternet zu schaffen. Dieser Ausbau ist das wichtigste Infrastrukturprojekt der Bayerischen Staatsregierung, die dafür in ihrem eigenen Förderverfahren 1,5 Milliarden Euro zur Verfügung stellt - eine bundesweit einzigartige Summe. Ziel sind hochleistungsfähige Breitbandnetze mit Übertragungsraten von mindestens 50 Mbit/s.

Bereits über 96 Prozent aller Kommunen im bayerischen Förderverfahren

Bayernweit sind bereits über 96 Prozent aller Kommunen in das bayerische Förderverfahren eingestiegen. 1.525 Kommunen starten mit einer Gesamtfördersumme von rund 612 Millionen Euro in den Breitbandausbau. Viele Gemeinden gehen mehrfach in das Verfahren, um schrittweise eine hohe Flächendeckung und besonders zukunftssichere Glasfasernetze bis in die Gebäude zu erreichen. Diese enorm hohe Beteiligung der Kommunen belegt den Erfolg unserer bayerischen Breit-bandstrategie nach dem Motto: Verfahren vereinfachen, Förderung verdoppeln und Bera-tung verbessern! Allein bei den bisher im Ausbau befindlichen Projekten werden über 29.000 km Glasfaser-leitungen verlegt. Damit können künftig weitere 625.000 Haushalte mit schnellem Internet versorgt werden, vor allem im ländlichen Raum. Wichtige Hilfe für die Kommunen ist die Beratung durch die Breitbandmanager an den Ämtern für Digitalisierung, Breitband und Vermessung. In über 7.500 persönlichen Gesprächen wurde jede Gemeinde beraten.

„Gigabit-Initiative“ in ausgewählten Gewerbegebieten

Mit der neuen „Gigabit-Initiative“ will der Freistaat zudem eine pilothafte „Gigabit-Förderung“ in ausgewählten Gewerbegebieten angehen. Unternehmen benötigen jetzt schon direkte Glasfaseranschlüsse und höhere Bandbreiten als 30 Mbit/s, damit sie im globalen Wettbewerb nicht den Anschluss verlieren. Nach EU-Vorgaben ist eine Förderung aber bisher nicht zulässig, wenn ein Gebiet bereits mit 30 Mbit/s erschlossen ist, weil diese Geschwindigkeit laut EU als „schnelles Internet“ gilt. Daher soll in Gesprächen mit der EU-Kommission das weitere Vorgehen hin zu einer Gigabit-Förderung in Bayern abgestimmt werden.

Bayern wird das erste Bundesland mit einem eigenen WLAN-Netz

Darüber hinaus wird Bayern das erste deutsche Land mit einem eigenen WLAN-Netz. Bis 2020 wollen wir das kostenfreie BayernWLAN mit 20.000 Hotspots aufrüsten. Weitere 20.000 Hotspots sollen an den bayerischen Schulen entstehen. Ausgestattet werden insbe-sondere Kommunen, Hochschulen, Schulen, Behörden und Tourismusziele. Im öffent-

lichen Nahverkehr sollen Pilotprojekte zum BayernWLAN starten. Seit Start der Initiative Anfang 2015 wurden bereits rund 7.000 Zugangspunkte ins BayernWLAN realisiert. An über 1.100 kommunalen Standorten befindet sich das BayernWLAN bereits in der Umsetzung.

Das BayernWLAN bietet für jedermann ein offenes und kostenfreies WLAN-Angebot. Es sind keine Passwörter und keine Anmeldedaten erforderlich, eine Registrierung ist nicht nötig, der Jugendschutz ist durch Filter garantiert. Mit einem dichten Netz von kostenlosen Hotspots über ganz Bayern schaffen wir die digitale Chancengleichheit auch für den ländli-chen Raum. Das WLAN Zentrum Straubing unterstützt die Kommunen und koordiniert den Ausbau des BayernWLAN.

Kabinett beschließt neuen Masterplan für Bayerns digitale Zukunft:
Investitionsprogramm mit 3 Milliarden Euro und 2.000 neuen Stellen geplant

Mit einem neuen, breit angelegten 10-Punkte-Masterplan zur Digitalisierung hat die Staats-regierung am 30. Mai 2017 die zweite Stufe von BAYERN DIGITAL gestartet. Sein Ziel ist es, Bayern zur Leitregion für die Digitalisierung zu machen.

Ziel: Bayern zur Leitregion für die Digitalisierung machen

Dabei geht es in technologischer und wirtschaftlicher Hinsicht vor allem darum, den Mittel-stand bei der digitalen Transformation zu unterstützen. Darüber hinaus setzt die Staatsre-gierung bei den Maßnahmen zur Digitalisierung auch Impulse bei Themen wie Weiterbildung, Verbraucherschutz, Klimawandel oder Barrierefreiheit in der digitalen Welt. Denn nur wenn wir das Thema digitaler Wandel von allen Seiten beleuchten und nicht allein auf Technik und Wirtschaft begrenzen, erreichen wir eine echte Breite in der Diskussion und Akzeptanz in allen Gesellschaftsschichten.

Masterplan BAYERN DIGITAL II

Der Masterplan BAYERN DIGITAL II wird voraussichtlich ein Volumen von 3 Milliarden Euro haben und über 2.000 Stellen im Zeitraum von 2018 bis 2022 schaffen. Er gibt vor, in welchen Bereichen die Staatsregierung konkret ihre Investitionsschwerpunkte im Bereich Digitalisierung in den nächsten fünf Jahren setzen wird.

Masterplan stellt Weichen für Bayerns digitale Zukunft

Ich bin davon überzeugt, dass wir damit die Weichen für Bayerns digitale Zukunft gestellt haben. Unser Ziel ist es, dass Bayern und seine Menschen mit dem Masterplan zu Gewin-nern der digitalen Revolution werden. Wir reden nicht nur über Zukunftsinvestitionen, son-dern handeln ganz konkret!

Weitere Informationen zum Masterplan BAYERN DIGITAL II finden Sie im Internet unter http://q.bayern.de/bayern-digital-investitionsprogramm

Ansprechpartner

Berthold Rüth, MdL
Vorsitzender der Enquete-Kommission
„Gleichwertige Lebensverhältnisse in ganz Bayern“
Bayerischer Landtag
Telefon: 089 41263650
E-Mail: berthold.rueht@csu-landtag.de

Standpunkte: WannaCry-Hackerangriff: Wie können wichtige Infrastrukturen vor Cybercrime besser geschützt werden?

Hackerangriffe mit Erpressungstrojanern auf die IT-Infrastrukturen von deutschen Unterneh-men und Krankenhäusern sind schon länger an der Tagesordnung. Aber mit der weltweit geführten Wanna Cry-Attacke erreicht die Cyberkriminalität eine neue Dimension. Die Lehre aus diesen Angriffen muss lauten: Die IT-Sicherheit braucht deutlich mehr politische Auf-merksamkeit. Wir müssen gewappnet sein, wenn die Hacker wieder zuschlagen.

Auch bei uns in Deutschland und in Bayern liegt Einiges im Argen. Das Thema Cybersicherheit wurde viel zu lange der Wirtschaft überlassen. Aber gegen systematisch geführte Cyber-Attacken sind die betroffenen Unternehmen schutzlos. Bundesregierung und CSU-Regierung fehlt es bislang einer übergreifenden Strategie zur IT-Sicherheit, um unser digitalisiertes Leben wirksam zu schützen.

Die Politik muss hier den Rahmen setzen. Um die IT-Infrastrukturen zu härten, braucht es einheitliche Sicherheitsstandards für die Unternehmen. Das IT-Sicherheitsgesetz muss endlich auch auf den Gesundheitsbereich angewandt werden. Zudem sollte die Politik den Aufbau sicherer IT-Infrastruktur fördern, insbesondere über das Vergabewesen. Herstellern und Dienstleistern darf es juristisch nicht zu leichtgemacht werden, sich der Haftung zu entziehen. Und IT-Anbieter müssen den Nutzern regelmäßige Sicherheits-Updates zur Verfügung stellen.

Wir GRÜNE wollen uns aber auch der digitalen Aufrüstung seitens des Staates entgegen-stellen. Die staatlichen Sicherheitsbehörden befeuern derzeit die IT-Unsicherheit. Zwar soll der Staat einerseits IT-Angriffe abwehren; gleichzeitig sammeln oder kaufen vor allem die Geheimdienste Informationen zu Sicherheitslücken (Zero Days) und nutzen diese auch aus. Wir fordern, dass staatlichen Stellen künftig sämtliche Sicherheitslücken melden. Darüber hinaus sollten die Zuständigkeiten aus dem Innenressort gelöst, entwirrt werden und ein unabhängiges und vertrauenswürdiges (Bundes-)Amt für IT-Sicherheit geschaffen werden. Auch in Bayern braucht es eine Neuordnung. Mit dem neuen Landesamt für IT-Sicherheit sind heuer in Bayern schon drei Behörden in diesem Bereich tätig.

Ansprechpartner

Thomas Mütze, MdL, B90/Die Grünen
Finanz- und wirtschaftspolitischer Sprecher
Telefon: 06021 4510450
E-Mail: Muetze-wkbuero@t-online.de

Stark gefragt: IT-Experten in KMU

In der Wirtschaft 4.0 wird das Thema IT-Sicherheit zum beherrschenden Faktor. Laut dem „IHK-Unternehmensbarometer Digitalisierung“ fürchten 72 Prozent der Unternehmen wachsende Sicherheitsrisiken und 85 Prozent sehen die Notwendigkeit von mehr Weiterbildung, um der zunehmenden Komplexität im Digitalisierungszeitalter gerecht werden zu können. Die Gründe hierin liegen unteranderem in der Implementierung von „Mensch-Maschine-Schnittstellen“ bzw. Automatisierungsprozessen durch IT-Lösungen.
Damit die mainfränkische Wirtschaft im Umgang mit digitalen Herausforderungen unterstützt wird, startet die Weiterbildungsoffensive „Mainfranken 4.0“ ab Herbst in die nächste Runde.

Ein umfassend konzipiertes Seminarprogramm setzt topaktuelle Themenschwerpunkte aus den Bereichen IT-Sicherheit, neue Medien, Energieeffizienz sowie Unternehmenskommunikation und macht Teilnehmende zu echten Experten, sodass deren Fähig- und Fertigkeiten vor dem Hintergrund der Digitalisierung und Informationstechnologien nachhaltig verbessert werden.

Im Zertifikatslehrgang „IT Security Coordinator (IHK)“ beschäftigt sich die Zielgruppe intensiv mit dem systematischen Verständnisaufbau zum Thema IT-Security, um in der Folge die aktuelle Gefährdungslage und die Schwachstellen in Informationssystemen noch besser bewerten und einschätzen zu können. Darüber hinaus werden die Teilnehmenden zum souveränen Umgang mit Sicherheits- und Analysetools befähigt. Anhand konkreter Beispiele wird neben dem Fachwissen auch die Handlungsfähigkeit in IT-Sicherheitsfragen intensiviert, sodass der Transfer in das eigene Unternehmen gelingt.

Ab Oktober 2017 kann an zahlreichen weiteren Kursen teilgenommen werden, die dank der Förderung der Europäischen Union und des Freistaats Bayern besonders attraktiv sind:

- Netzwerkadministrator/in (IHK)
- IT Sicherheit und IT Risikomanagement
- Cloud Computing Coordinator/in (IHK)
- und viele mehr

Ansprechpartner

Julia Ruffert I Lisa Maria Köhler
Technologie- und Gründerzentrum Würzburg
Telefon: 0931 467909-0
E-Mail: info@tgz-wuerzburg.de
www.tgz-wuerzburg.de

Schicht für Schicht: Neue Dimensionen in der Fertigung durch 3D-Druck

Dem Markt für additive Fertigungsverfahren – umgangssprachlich 3D-Druck benannt – wird in den kommenden Jahren ein rasantes Wachstum vorausgesagt: Experten schätzen, dass dieser bis 2020 alleine in Deutschland von gegenwärtig ca. 3 Milliarden auf rund 21 Milliarden US-Dollar wachsen wird. Dabei gehen Experten davon aus, dass 3D-Druck-Verfahren in fast allen Bereichen Einzug halten werden: Sei es bei der schnellen Erstellung von Prototypen oder beim Nachdruck einzelner Ersatzteile, ob in Forschung und Medizin oder in der Unterhaltungselektronik in heimischen Wohnzimmern.

Das Thema 3D-Druck als Zukunftstechnologie bietet gerade auch für den Bayerischen Untermain mit seiner Vielzahl an produzierenden Unternehmen

große Chancen. Offen dabei ist, welche neuen Anforderungen bspw. im Bereich Urheberrecht und Datenschutz, aber auch an die berufliche und akademische Ausbildung der Konstrukteure gestellt werden.
Das Kompetenznetz Mechatronik & Automation Bayerischer Untermain veranstaltet am 13. September 2017 eine Veranstaltung zum Thema „Schicht für Schicht: Neue Dimensionen in der Fertigung durch 3D-Druck". Im Rahmen dieser Vortragsveranstaltung berichtet unter anderem Herr Günter Hofmann von der Concept Laser GmbH in Lichtenfels, einem der Marktführer in diesem Bereich, wie additive Fertigungsverfahren die nächste Stufe der Automation und Digitalisierung im Maschinen- und Werkzeugbau einleiten. v

Ansprechpartner / Anmeldung an Herrn Thorsten Stürmer (stuermer@zentec.de)

Ansprechpartner

Thorsten Stürmer
ZENTEC GmbH
Telefon: 06022 261115
E-Mail: stuermer@zentec.de

Hochautomatisiert unterwegs – Forschungsprojekt Ko-HAF zieht positive Zwischenbilanz

„Alles im Plan!" fasste Projektkoordinator Dr. Andree Hohm von Continental den Zwischenstand zur Halbzeitpräsentation des Forschungsprojekts „Ko-HAF – Kooperatives Hochautomatisiertes Fahren" kurz und knapp zusammen. Er kann zufrieden sein mit der Projektarbeit der 16 Partner aus Industrie, Wissenschaft und öffentlicher Hand: Zahlreiche Fachvorträge, Rollups, Videopräsentationen und Exponate zeigten den über 250 Fachexperten am 18. Mai 2017 im Schloss Johannisburg in Aschaffenburg anschaulich die Vielzahl an Fragestellungen, mit denen sich das Projektteam bisher befasst hat und welche Ergebnisse bereits erzielt wurden.

In der ersten Projekthälfte standen vor allem die Konzeption und Entwicklung des Safety Servers sowie die Kommunikation zwischen Fahrzeugen und Safety Server im Mittelpunkt. Hier ist zur Zwischenpräsentation die komplette Kommunikationskette „Safety Server > Fahrzeuge > Safety Server" prototypisch umgesetzt. Die Fahrzeuge erhalten auf Anfrage eine hochgenaue digitale Karte und können umgekehrt ihre Umfeldwahrnehmungen, das heißt statische Verkehrsobjekte wie Schilder, Markierungen, Leitplanken etc. hochladen. Aggregationsverfahren, mit denen die zahlreichen Meldungen aus den Fahrzeugen im Server sinnvoll fusioniert werden können, werden derzeit entwickelt.

Zur Abschlusspräsentation im September 2018 solle dann das hochautomatisierte Fahren im realen Verkehr auf der öffentlichen Teststrecke rund um Frankfurt demonstriert werden, gibt Ko-HAF-Koordinator Hohm einen Ausblick: „Die neue Technik liefert extrem effektive Werkzeuge zur Vermeidung von Verkehrsunfällen, die heute meistens von Menschen verursacht werden." Als weiteren Vorteil sieht er die Zeitersparnis: „Wer im dichten Autobahnverkehr Zeitung lesen, Nachrichten empfangen und schicken oder ein Fußballspiel anschauen kann, gewinnt enorm an Lebensqualität hinzu."

Ansprechpartner

Thorsten Stürmer und Sebastian Krug
Telefon: 06022 26-2050
E-Mail: ko-haf@zentec.de

Anwendungspartner für Industrial-IT-Security-Projekt gesucht!

Für ein Forschungsprojekt, in dem eine Appliance entstehen soll, die Anomalien im Kommunikationsverhalten erkennt, und Identitätsschätzungen der beteiligten Komponenten vornehmen kann wird ein Anwendungspartner gesucht. Basis ist eine Open Source Next-Gen Firewall, die um eine Machine Learning Komponente ergänzt wird. Der Anwendungspartner soll für den Entwicklungs- und Einlernprozess Daten aus seinem Netzwerk bereitstellen.

Ansprechpartner

Sebastian Krug
ZENTEC GmbH
Telefon: 06022 262050
E-Mail: krug@zentec.de

IHK-Unternehmerreise in die chinesische Provinz Shandong

Die IHK Aschaffenburg bietet vom 6. bis 11. November 2017 eine Unternehmerreise nach China mit den Schwerpunkten Industrie, Maschinenbau und Automotive an. Die Provinz Shandong ist die Partnerprovinz des Freistaates Bayern. Die Partnerschaft feiert in diesem Jahr ihr 30-jähriges Jubiläum.

Ziel der Reise ist es, direkt vor Ort Eindrücke vom chinesischen Markt und von relevanten Akteuren zu gewinnen. Die Reise führt in die Provinzhauptstadt Jinan sowie nach Weifang und Qingdao. Neben Unternehmensbesuchen sind Treffen mit der bayerischen Repräsentanz in Qingdao, Vertretern der deutschen Auslandshandelskammer in China, der Besuch des Sino German Ecoparks, die Besichtigung eines Ausbildungszentrums für die duale Ausbildung und der Besuch des neuen VW Werkes in Qingdao geplant. Ebenso wird die Teilnahme am German Business Community Meeting in Qingdao ermöglicht. Dieses größte Meeting deutscher Unternehmer in Qingdao organisiert die AHK alle zwei Monate.

Ansprechpartner

Ursula Müller
IHK Aschaffenburg
Telefon 06021 880113
E-Mail: mueller@aschaffenburg.ihk.de

InnovationsForum – Blockchains

Am 28. Juni referierte Prof. Dr. Philipp Sandner vom Blockchain Center der Frankfurt School of Finance & Management vor den Mitgliedern und Gästen des InnovationsForums in Groß-wallstadt über Blockchains. Er erläuterte, dass diese Technologie, die hinter Crypto-Währungen wie bspw. Bitcoin steht, auf dem Sprung ist, in der Wirtschaft breite Anwendung zu finden.

Pay-per-use-Anwendungen, micro-payments zwischen vernetzten Maschinen, intelligente Verträge, digitale Geschäftsmodelle u.v.m. vermindern Investitionsbedarfe, setzen Marktein-trittshürden herab und führen zu anderen Personalbedarfen.

Blockchains bieten fälschungssichere und transparente Prozesse und sind durch verteilte dezentrale Speicherung gerade für instabile Regionen dieser Erde ein optimales Werkzeug. Sandner führte aus, dass sich nahezu alle großen Unternehmen mit dem Einsatz von Blockchains befassen. Der Umsatz aller Crypto-Währungen zusammen sei bereits ungefähr auf dem Niveau von Dax-Konzernen, Start-Ups in diesem Bereich hätten bislang über 320 Mio. USD Wagniskapital gesammelt.

Ansprechpartner

Sebastian Krug
ZENTEC GmbH
Telefon: 06022 262050
E-Mail: krug@zentec.de

Hochschulstandort Miltenberg

Von Landrat Jens Marco Scherf

Eine besondere Stärke unserer Region Bayerischer Untermain und des Landkreises Miltenberg ist die Vielzahl kleiner und mittlerer hochspezialisierter Unternehmen, die sich erfolgreich im internationalen Wettbewerb behaupten und nah an ihren Kunden agieren. In Zeiten, in denen die Unternehmen dringend Fachkräfte benötigen und in denen der Trend zu immer größeren Unternehmen und Konzernen ungebrochen ist, müssen wir insbesondere als Landkreis Miltenberg dafür sorgen, dass unsere Unternehmen optimale Rahmenbedingungen vorfinden.

Ein wichtiger Schritt ist die Einrichtung eines Bachelor-Studiengangs „Betriebswirtschaft für kleine und mittlere Unternehmen", den die Hochschule Aschaffenburg in den Räumen der Berufsschule Miltenberg-Obernburg einrichtet. Der Studiengang ist auf den Bedarf kleiner und mittlerer Unternehmen ausgerichtet und bietet mit „Blended Learning" neue Formen des Studierens an. Eine maximale Flexibilität wird durch zwei Präsenztage und drei Tage, die im Selbststudium zugebracht werden, geboten. Dadurch, dass das Studium berufsbegleitend möglich ist, braucht ein Unternehmen auf seinen Mitarbeiter oder seine Mitarbeiterin während des Studiums nicht zu verzichten und der Praxiskontakt bleibt erhalten.

Der Studiengang ist in Bayern einmalig und nicht kostenpflichtig. Er ermöglicht Menschen, denen ein Präsenzstudium z.B. aufgrund von Eltern- oder Pflegezeit nicht möglich ist, ein Studium aufzunehmen. Damit leistet er einen Beitrag für eine familienfreundliche Region, in der nicht nur die Vereinbarkeit von Familie und Beruf, sondern zunehmend auch die Vereinbarkeit von Pflege und Beruf wichtig werden. Der Landkreis Miltenberg unterstützt die Einrichtung dieses Studiengangs, indem er die Kosten für den Umbau der Räumlichkeiten getragen hat. Er hat dies entschieden, da er der festen Überzeugung ist, damit eine wichtige Weichenstellung für die Menschen und die Betriebe zu machen.

Ich bitte daher die Unternehmerinnen und Unternehmern in unserer Region und im Landkreis Miltenberg, potenzialträchtige Mitarbeiterinnen und Mitarbeiter auf diesen Bachelor-Studiengang hinzuweisen und die Teilnahme zu unterstützen.

Ansprechpartner

Susanne Seidel
Telefon: 09371 501401
E-Mail: susanne.seidel@lra-mil.de