IoT4 INDUSTRY & BUSINESS

Das Magazin für IoT, Big Data und Security

2 | 2020
Erscheinungstermin:
30. Oktober 2020
www.iot4industry.at

2 x jährlich

Interview mit Ing. Heinz Rechberger, Aucotec Österreich

BIG DATA ERFOLGREICH MANAGEN

Technik & Medien Verlagsges.m.b.H. • Traviatagasse 21-29/8/2, A-1230 Wien • Österr. Post AG, GZ 17Z041008 M • € 9,- • Maximale Zustelldauer: 5 Werktage

Im Fokus
LISTEN! SECURITY MUSS SEIN

Im Gespräch
ANGST VORM HACKER?

Im Fokus
IT-SA VERTRAUT AUFS WWW

TECHNIK & MEDIEN VERLAGSGMBH

SECURE REMOTE MAINTENANCE

Weltweit. Einfach. Sicher.

www.br-automation.com/remote-maintenance

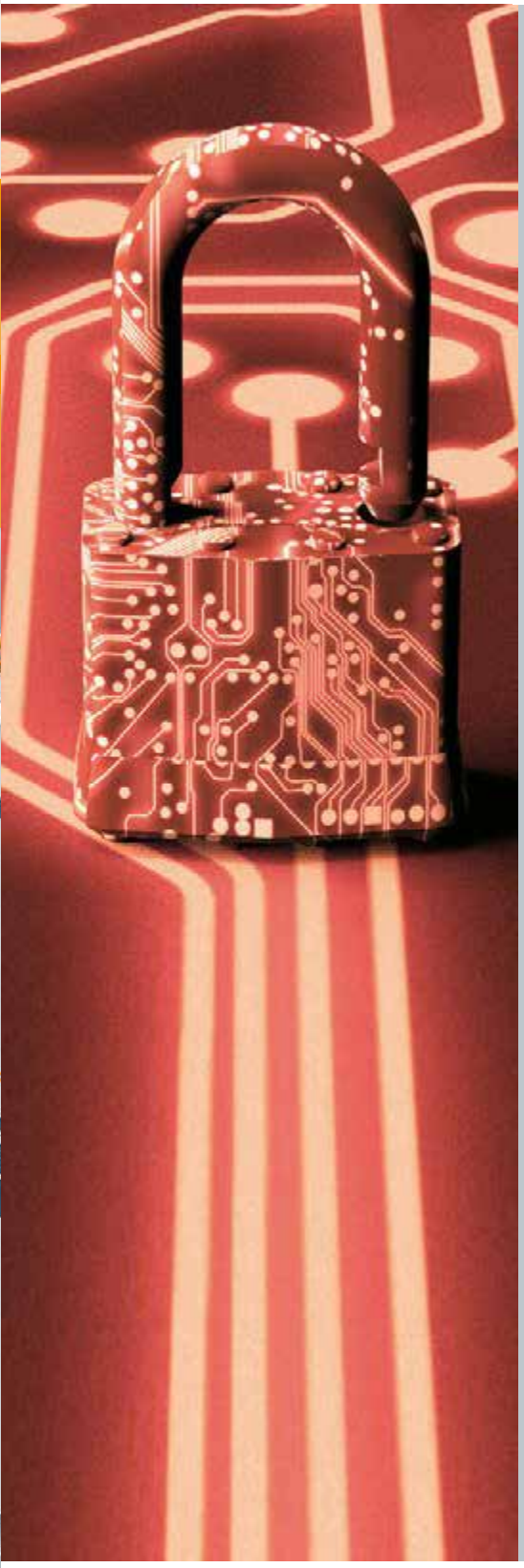
Weltweit zugreifen
Fernwartung vom Büro aus oder von unterwegs

Einfach implementieren
Integrierte Lösung aus einer Hand

Sicher verbinden
Jede Art Daten sicher übertragen

PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

IoT4 INDUSTRY&BUSINESS



DATENDIEBSTAHL – WAS SOLL DAS EIGENTLICH?

Wissen Sie, was ich ganz persönlich wirklich schwierig finde? Dem Thema Hacking etwas Positives abzugewinnen. Was treibt Menschen dazu an, anderen gezielt Schaden anzurichten und dann Lösegeld zu fordern? Sicher, man kann sich genauso gut fragen, was der Sinn von Banküberfällen oder Geiselnahmen ist. Aber es ist ja genau das Gleiche – nur der Zeit eben angemessen, sprich: modern.

Als im März 2020 die Covid-19-Pandemie zum Lockdown führte, waren viele Unternehmen vor den Kopf gestoßen. Telearbeit war die einzig machbare Lösung, den Betrieb einigermaßen in Gang zu halten. Fragile Infrastrukturen traten zu Tage und verdeutlichten einmal mehr, wie sehr am falschen Ende gespart wurde. Sergej Epp, CSO von Palo Alto Networks, brachte es in einem persönlichen Web-Gespräch (S. 18) auf den Punkt: „Security steht bei vielen einfach nicht auf der Agenda."

Und auch Reinhard Mayr vom Software-Experten Copa-Data aus Salzburg wies in einem Interview auf ein gravierendes Defizit bei den Unternehmen hin: „(…) die in die Jahre gekommenen, so genannten Legacy-Protokolle bzw. Infrastrukturen." Vielleicht hat diese gesundheitliche Krise doch in gewisser Hinsicht und mit viel Willenskraft auch etwas Gutes? Nämlich, dass der Schritt in Richtung Digitalisierung und allem, was hierzu benötigt wird (auch den Mitarbeiter von daheim aus arbeitend meine ich), endlich getätigt wurde. Man kann es sich für alle nur wünschen.

Zum Thema Hacking gibt es übrigens noch etwas Spannendes: Auf S. 38 lesen Sie etwas über „die Guten" der sonst so verachteten Hackerwelt: White-Hat-Hacker. Sind diese Angreifer also die Batmans des WWW? Frei nach dem Motto: Ich bin zwar Spion und dringe in dein Unternehmen ein, aber zu einem guten Zweck? Was genau dahinter steckt, erfahren Sie in dem spannenden Gespräch mit Ulrich Fleck von SEC Consult.

Doch wie gehe ich nun mit dem Big Data-Schatz bei mir im Betrieb am besten um? Das zeigt Aucotec in der Coverstory ab S. 26 wieder einmal sehr eindeutig mit der Plattform EB. Neugierig? Dann lesen Sie los! Ich wünsche Ihnen mit der aktuellen Ausgabe spannende Einblicke und vielleicht sogar den einen oder anderen Aha-Moment, denn wer denkt, er oder sie wisse – nicht nur zum Thema Security – bereits alles, irrt.

Bleiben Sie gesund!

Stephanie Englert, Chefredakteurin

INHALT
NOVEMBER 2020

Big Data erfolgreich managen

Die Herausforderungen an das Maschinen- und Anlagen-Engineering sind vielfältig und enorm.

www.aucotec.at

Lesen Sie mehr ab Seite 26!

IM FOKUS

6 **Listen!**
8 **News Security**
12 **Angriff und Verteidigung** | Uwe Gries, Stormshield
16 **Willkommen im Netz** | Frank Venjakob, NürnbergMesse
18 **Security?** | Sergej Epp, Palo Alto Networks
20 **Bestens gerüstet** | Reinhard Mayr, Copa-Data
23 **Gastkommentar** | Strategische Infrastrukturen und Cyberresilienz
24 **Angriff aus dem Netz** | Torsten Wiedemeyer, Adaptiva

IM GESPRÄCH

26 **Coverstory** | Big Data erfolgreich managen
29 **Interview: So geht beeindruckend** | Ing. Heinz Rechberger, Aucotec
30 **„Vertrauen ist gut – Kontrolle und Nachweis sind besser“** | Hirsa Navid, Relicense AG und Jan Minartz, Deloitte
34 **„Jedes Unternehmen beschäftigt sich mit dem eigenen Optimierungspotenzial“** | Wolfgang Weidinger, Weidmüller
38 **Wer hat Angst vorm Hacker?** | Ulrich Fleck, SEC Consult
41 **„NoSQL bügelt die Schwächen relationaler Datenbanken aus“** | Steffen Schneider, Couchbase
42 **Ethisch korrekt** | Christoph Peylo, Bosch
44 **Vertrauen schaffen** | Jochen Kressin, floragunn
46 **Krise? Nein danke!** | Bastian Karweg, Echobot
47 **Gastkommentar** | 4. IoT-Fachkongress: Corona, Tracing und die Sache mit der Privatsphäre ...

SECURITY | BIG DATA | CLOUD COMPUTING

48 **Erfolgreich durch den Digitalisierungs-Dschungel**
50 **Fernwartung statt Flugticket**
51 **Kurzinterview: René Blaschke, B&R**
53 **Gastkommentar** | Cyberangriffe auf Unternehmensdaten – Datenschutzstrategie unerlässlich
54 **„Datenschutz ist eine Errungenschaft“**
59 **Gastkommentar** | Deutsche Unternehmen im Fokus von Hackern
60 **News**
64 **IIoT-Lösungen für intelligente Verbindungslösungen**

STÄNDIGE RUBRIKEN

65 **Veranstaltungen**
66 **Impressum** | **Vorschau**

IoT4 INDUSTRY&BUSINESS

12
Wie planen Unternehmen ihre digitale Zukunft? War ein Umdenken in Richtung Homeoffice längst überfällig? Dies sind einige Fragen, die sich durch die Covid-19-Pandemie relativ schnell von selber beantwortet haben. Doch gleichzeitig stieg auch die Gefahr von Cyberattacken. Wie man dem am geschicktesten begegnet und wo die Schwächen vieler liegen weiß Uwe Gries, Country Manager DACH bei Stormshield.

38
Hacken ist im Trend. Wer etwas auf sich hält, gibt sein Wissen insofern preis, als dass er die Gehackten im Anschluss des Feldversuches darauf hinweist, wo ihre Schwachstellen sind. Diesen Prozess würde man dann als White-Hat-Hack bezeichnen. Doch was genau verstehen wir unter diesem Begriff?

54
Das Kippen des Privacy Shields durch den europäischen Gerichtshof zeigt einmal mehr, in welcher unsicheren Rechtslage sich der internationale Datentransfer mit den USA befindet, denn dieses Land hat eine ganz eigene Vorgehensweise hinsichtlich Datenschutz, die nicht unbedingt mit den europäischen Standards im Einklang stehen, weiß auch Andreas Hajek von Rittal Österreich.

2 x jährlich


work
from
Home!

Security ist vor allem durch den plötzlichen Lockdown Mitte März wieder stärker in den Fokus gerückt. Das Homeoffice für ziemlich alle Mitarbeiter – und das weltweit – hat dieses komplexe Thema auf einen Schlag noch entscheidender für die Zukunftsfähigkeit des eigenen Betriebes gemacht. Von Stephanie Englert

Heutzutage stellt sich beim Thema Security die Frage: Wie finde ich die richtige Lösung im Dschungel der Anbieter? Beratung ist sicher entscheidend und je nach Unternehmensgröße gibt es andere Lösungen und Preisvorstellungen. Man darf jetzt auch nicht vergessen, dass das Defizit nicht auf der Entwicklungsseite der Lösungen liegt, sondern eher auf der Entscheiderseite. Zu lange wurde daraufhin gewartet, die eine, im Geheimen gehofft „billige" Lösung, entsprechend in den Betrieben zu implementieren. Sicherheit kostet Geld, doch auf lange Sicht weniger, als wenn man den abschreckenden Beispielen folgt und schlussendlich vor Zahlungsforderungen oder Notlösungen steht. Hacking ist ein Geschäft geworden, ein sehr lukratives leider sogar. Und man sollte nicht davon ausgehen, dass dieser Trend abschwächt.

Informieren – bleibt die Botschaft. Während der Recherche zum Thema Security stößt man unweigerlich auf ein Trendmedium der letzten Jahre – den Podcast. Und es gibt einige wenige Beispiele, die sich inhaltlich wirklich zu hören lohnen. Lohnen insofern, dass diese von Anfang bis Ende mit einem gewissen Mehrwert oder eben Lerneffekt hörbar sind. Ein Beispiel sind hier die Podcasts vom VDMA.
Mitte Juli wurde der Industrie-Podcast „Cybersecurity im Fokus, Angriffsziel Industrie" veröffentlicht. Im Gespräch waren Franz Köbinger, Siemens, und Dr. Thomas Nowey von der Krones AG. Beide Experten berichten hier detailliert über Angriffe und wie sie stattfinden und gegebenenfalls schon vorab vermieden werden können. Grund ehrlich gehen sie auf dieses Thema ein und warnen vor zu viel Nachlässigkeit auf einem Erfahrungslevel, der sich zu hören lohnt.

Auch von Lösungs-Anbieterseite gibt es gute Podcasts, so wie von Waterfall Security. Wie intelligent sind die Angriffe bereits geworden? Auf was zielen sie ab? Andrew Ginter von Waterfall Security spricht ganz konkrete Themen an wie „Ransomware goes Nuclear" (23.7.) oder auch „We can handle disruption – not destruction" (5.3.). Auf Englisch und sehr gut verständlich kann man hier das Eine oder Andere inhaltlich für seinen eigenen Erfahrungsschatz mitnehmen.
Und auch innerhalb der Gründerszene hat sich Joel Kaczmarek mit „Digital Kompakt" einen Namen gemacht. Eine Podcast-Folge mit Sven Weizenegger, Head of Cyber Innovation Hub der deutschen Bundeswehr vom 16.9. zum Thema „IT-Sicherheit für die Industrie 4.0" ist empfehlenswert. Szenarien wie Industrial Security und autonomes Fahren oder Echtzeitdaten werden unter anderem einsichtig beleuchtet und spannend diskutiert – nicht nur für die Nachwuchs-Spezialisten auf diesem Gebiet.

Berücksichtigen Sie Security. Unabhängig davon, auf welcher Erfahrungsebene man sich im eigenen Unternehmen beim Thema Security befindet, die Informationen hierzu werden nicht weniger und der Informationsbedarf ebenfalls nicht. Security ist nicht nur ein „Trend", es ist eine Notwendigkeit geworden. In der aktuellen Ausgabe des IoT4 Industry&Business sprechen Experten zu diesem Thema detailliert. Doch auch Podcasts dienen durchaus als Anregung zum Nachdenken. Das Angebot ist groß und das Reinhören lohnt sich.

www.vdma.de
www.digitalkompakt.de
www.waterfall-security.com

LAGE? BEDROHLICH!

Im Mai 2020 wurde für zirka 52.000 österreichische Unternehmen, die aufgeteilt nach Bundesland/Bezirk und Branche aus öffentlichen Quellen bezogen wurden, eine sogenannte OSINT-Studie durchgeführt. OSINT steht für Open Source Intelligence und bedeutet, dass Informationen aus frei verfügbaren, offenen Quellen verwendet werden. Ziel war es herauszufinden, wie Unternehmen mit bereits – teilweise länger – bekannten Sicherheitslücken in ihrer öffentlich erreichbaren IT-Infrastruktur umgehen und sich vor Hackerangriffen schützen.

Erste Ergebnisse dieser Studie zeigen, dass bei einem überraschend großen Anteil der Unternehmen (nicht gepatchte) und daher bekannte IT-Sicherheitsschwachstellen vorliegen, die nutzen können. „In Zeiten von Corona und Homeoffice sind das leider keine guten Nachrichten. Bekannte IT-Sicherheitsschwachstellen die älter als ein Jahr sind, sind verantwortlich für einen überwiegenden Großteil (90 Prozent) der erfolgreich durchgeführten Cyber-Angriffe auf IT-Infrastruktur", so Martin Herfurt (Bild), der Studienautor. Weitere Ergebnisse sind: 31,24 Prozent der Unternehmen in der Stadt Wien weisen kritische Schwachstellen in ihrer öffentlich erreichbaren Server-Infrastruktur auf. Die Klasse der mittelgroßen Unternehmen (6-15 öffentliche IP-Adressen) konnten zu 49 Prozent mit bekannten Schwachstellen auf ihrer öffentlichen Server-Infrastruktur in Verbindung gebracht werden.

Martin Herfurt , geschäftsführender Gesellschafter der toothR new media GmbH

Im Schnitt sind die Unternehmen in der Stadt Wien mit 10,22 Schwachstellen pro Unternehmen und 2,59 Schwachstellen pro betrachtetem Serversystem belastet. Hinter der Studie steht ein Salzburger Start-up, dass sich auf IT-Risikoabschätzungen und IT-Security spezialisiert hat (**toothR new media GmbH**).

www.it-wachdienst.com

ANGREIFER ERFOLGLOS

Sophos veröffentlichte jetzt seinen neuen Report „Maze Attackers Adopt Ragnar Locker Virtual Machine Technique". In diesem beschreiben die Security-Experten, wie Cyberkriminelle bei einem Angriff auf drei unterschiedliche Arten versuchten, die Ransomware Maze bei ihrem Opfer zu aktivieren. Als Lösegeld verlangten die Erpresser 15 Millionen USD. Maze ist eine der berüchtigtsten Ransomware-Familien und seit 2019 aktiv. Sie entwickelte sich aus der ChaCha-Ransomware und ist eine der ersten, die Datenverschlüsselung mit Informationsdiebstahl kombinierte.

Drei Angriffsvarianten. Die Cybergangster hinter Maze sind hartnäckig und versuchen die Ransomware auf unterschiedliche Arten im Unternehmen zu verbreiten. Forensische Untersuchungen ergaben, dass die Angreifer mindestens sechs Tage vor ihrem ersten Versuch, die Ransomware zu aktivieren, in das Netzwerk eingedrungen waren. Während dieser Zeit erkundeten sie die Netzinfrastruktur, starteten reguläre Tools von Drittanbietern, stellten Verbindungen her und leiteten Daten zu einem Cloud-Speicherdienst. Diese Schritte dienten der Vorbereitung für die eigentliche Ransomware.

Nach Aktivierung der Ransomware verlangten die Cyberkriminellen ein Lösegeld. Das Opfer zahlte die Summe jedoch nicht und als die Angreifer merkten, dass der erste Angriff fehlgeschlagen war, starteten sie einen zweiten, modifizierten Versuch. Dieser wurde von Security-Lösungen und dem Sophos Managed Threat Response (MTR)-Team, das für die Reaktion auf den Vorfall zuständig war, entdeckt und abgewehrt. Doch die Maze-Angreifer gaben noch nicht auf. Beim dritten Versuch verwendeten sie eine neu konfigurierte Version der Ragnar Locker VM-Technologie unter Einsatz von Windows 7 anstelle der Windows XP-VM. Zudem konzentrierten sie den Angriff nur auf einen Dateiserver. Auch dieser Versuch wurde erkannt und blockiert.

www.sophos.com

Der komplette Report steht zum Download bereit unter:
https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique

ANGEPASSTES KONZEPT

Schon sehr früh, parallel mit den ersten Profinet-Spezifikationen, veröffentlichte **PI** ein umfassendes Security-Konzept, das in mehreren Schritten weiter detailliert und angepasst wurde. Dabei reicht es nicht, Anlagennetze und Automatisierungskomponenten zu schützen, sondern die eingesetzten Schutzmechanismen und Konzepte dürfen den laufenden Produktionsbetrieb nicht stören. Zudem müssen Schutzkonzepte einfach umsetzbar und bezahlbar bleiben. Der wichtigste Aspekt ist jedoch, dass die Konzepte immer wieder an die aktuellen Entwicklungen angepasst werden müssen. PI hat nun sein IT-Sicherheitskonzept ergänzt.

Das IT-Sicherheitskonzept für Profinet geht von einem Defense-in-Depth-Ansatz aus. Dabei wird die Produktionsanlage durch einen mehrstufigen Perimeter (u. a. Firewalls) gegen Angriffe, insbesondere von außen, geschützt. Darüber hinaus ist innerhalb der Anlage eine weitere Absicherung durch Unterteilung in Zonen unter Einsatz von Firewalls möglich. Zusätzlich wird durch einen Security-Komponententest die Festigkeit der Profinet-Komponenten gegen Überlastung in einem definierten Umfang sichergestellt. Dieses Konzept wird durch organisatorische Maßnahmen in der Produktionsanlage im Rahmen eines Security-Management-Systems unterstützt. Allerdings ist Security ein Thema, das permanent an die aktuelle Entwicklung angepasst werden muss und daher nie abgeschlossen ist. Dies gilt insbesondere vor dem Hintergrund der zunehmenden Vernetzung von Produktionsanlagen.

https://de.profibus.com

ERHÖHTE IT-SICHERHEIT

Die **econ solutions GmbH** hat die neue Generation ihrer Energiemanagement-Software econ4 mit zahlreichen Neuheiten ausgestattet: Für höhere IT-Sicherheit läuft der Server nun auf dem Betriebssystem Debian 10, der neue und komplett überarbeitete Assistent zur ISO 50001 2018 leitet Nutzer Schritt für Schritt bis zur Zertifizierung und das Visualisierungsmodul verbessert durch zahlreiche Funktionen die User-Experience. Diese und weitere Optimierungen gehen auf das Feedback von Nutzern zurück und beantworten die steigenden Anforderungen an professionelle Energiemanagement-Software.

www.econ-solutions.de

CORONA BEEINFLUSST SICHERHEIT

Wo liegen derzeit die größten Hindernisse bei der raschen Umsetzung von Cybersicherheitsprojekten im industriellen Umfeld? Die aktuelle internationale **Kaspersky**-Studie namens „State of Industrial Cybersecurity in the Era of Digitalization" zeigt, das am häufigsten genannte Hindernis in Europa (40 Prozent) und weltweit (34 Prozent) ist die Notwendigkeit eines Produktionsstopps bei einer Security-Implementierung, den sich viele Unternehmen nicht leisten können. Gleich danach folgt die Einbindung zu vieler Entscheidungsträger (24 Prozent in Europa, weltweit 23 Prozent) und langwierige Freigabeprozesse, die von 21 Prozent der europäischen Industriefirmen (weltweit 31 Prozent) angeführt werden. Gerade im Kontext der Corona-Pandemie werden so viele neue Sicherheitsmaßnahmen im Bereich Betriebstechnologie (Operational Technology, OT) verzögert. (...)

Weitere Details bzw. zur Studie geht es hier:

AUFGENOMMEN

Die **secunet Security Networks AG**, deutscher Anbieter von IT-Sicherheit und IT-Sicherheitspartner der Bundesrepublik Deutschland, wird in den SDAX aufgenommen. Wie die Deutsche Börse bekannt gegeben hat, erfolgte der SDAX-Aufstieg der secunet Security Networks AG mit Wirkung zum 21. September 2020. Der Auswahlindex SDAX umfasst die 70 nach Marktkapitalisierung und Börsenumsatz größten Unternehmen unterhalb der MDAX-Werte. Axel Deininger, Vorstandsvorsitzender der secunet Security Networks AG, kommentiert: „Wir freuen uns sehr über die Aufnahme in den SDAX. Der Aufstieg in den SDAX stellt einen wichtigen Meilenstein der Börsenstory unserer Gesellschaft dar."

www.secunet.com

ERNANNT

Veeam Software hat Gil Vega zum Chief Information Security Officer (CISO) ernannt. Vega verantwortet die Definition und Einhaltung der Veeam-Sicherheitsstrategie zum Schutz der eigenen Informationswerte und Lösungen. Zudem leistet Vega einen wesentlichen Beitrag zur Weiterentwicklung von Strategien, die Veeam-Kunden helfen, ihre geschäftskritischen Daten in unterschiedlichen Infrastrukturen zu schützen sowie die Einhaltung von gesetzlichen Vorschriften sicherzustellen. In der Vergangenheit war Vega in verschiedenen Führungspositionen im Bereich Cybersicherheit im US-Verteidigungsministerium (DoD) sowie im nachrichtendienstlichen Umfeld tätig. Zuletzt arbeitete er unter anderem als Managing Director und CISO bei der CME Group sowie als Associate Chief Information Officer & CISO für das US-Energieministerium und die US-Einwanderungs- und Zollbehörden.

www.veeam.com

ÜBERNAHME

Der weltweit agierende Sicherheitsspezialist **WatchGuard Technologies** mit Sitz in Seattle, USA, gab Anfang des Jahres die verbindliche Einigung zur Übernahme von Panda Security – seines Zeichens Experte für fortschrittlichen Endpoint-Schutz – bekannt. Die Lösungen des in Spanien ansässigen Unternehmens sollen nach Abschluss der Akquisition schnellstmöglich ins Produktangebot von WatchGuard integriert werden, um gegenüber Kunden wie Partnern volle Leistungsstärke ausspielen zu können. Ziel ist der Ausbau der bestehenden WatchGuard-Sicherheitsplattform. Juan Santamaria Uriarte, CEO von Panda Security (Bild), hierzu: „Wir sind begeistert, mit WatchGuard zu fusionieren, da dies unseren Kunden und Partnern ganz neue Möglichkeiten im Hinblick auf die Dimension und den Zugang zum Portfolio eröffnet. Jetzt gilt es, gemeinsam an einer Sicherheitsplattform zu arbeiten, die konsequent die Brücke zwischen Netzwerk und Endpunkt schlägt und bisher nie dagewesene Funktionalität bietet."

www.watchguard.de

NEUE RICHTLINIE

Die neue Richtlinie **VDI/VDE 2206** versetzt Anwender in die Lage, ein komplexes technisches System erfolgreich entwickeln zu können. Ganz konkret bedürfen cyber-physische mechatronische Systeme einer besonders sorgfältigen Planung und Ausrichtung. Ihre Entwicklung muss fachkundig und gewissenhaft vonstattengehen, um das Risiko späterer Ausfälle und Komplikationen gering zu halten. Die Richtlinie VDI/VDE 2206 wurde im Jahr 2004 ins Leben gerufen, um den Rahmen für ein systematisches Vorgehen bei der Entwicklung cyber-physischer mechatronischer Systeme zu schaffen.

Die seit ihrer ersten Veröffentlichung stattgefundenen Sprünge in Sachen Komplexität, Interdisziplinarität und Heterogenität machten eine gründliche Überarbeitung unabdingbar, sodass die vorliegende Aktualisierung erarbeitet wurde. Die Neuerungen in der VDI/VDE 2206 betreffen unter anderem das V-Modell und die Anwendung von Hilfsmitteln in der interdisziplinären Produktentwicklung.

Herausgeber der Richtlinie VDI/VDE 2206 „Entwicklung cyber-physischer mechatronischer Systeme (CPMS)" ist die **VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik** (GMA). Die Richtlinie ist im September 2020 als Entwurf erschienen und kann zum Preis ab EUR 89,79 beim Beuth Verlag bestellt werden.

www.vdi.de

FÜR DIE SICHERHEIT

In der Industrie ist nichts so wichtig, wie die Sicherheit der Daten. Eine wesentliche Komponente ist dabei der Speicher und speziell seine Fähigkeiten, auch bei widrigen Umständen die Daten sicher zu speichern. Deshalb ist bei der Zusammenstellung eines Industriecomputers essenziell, auf die Industrietauglichkeit der einzelnen Komponenten zu achten. Die neuen 2.5" SATA und mSATA SSD der T376-Serie von **Spectra** bieten umfangreiche Funktionen zur sicheren Datenspeicherung und zeichnen sich durch hohe Geschwindigkeit und große Kapazität aus.

Die Steigerung von Geschwindigkeit und Kapazität wird durch die eingesetzte 3D NAND-Technologie erreicht. Damit sind bei der T376-Serie Speicherkapazitäten bis 2 TB möglich. Zusätzlich werden schnelle Schreibvorgänge durch die intelligente SLC Caching-Funktion unterstützt. Eine wesentliche Besonderheit ist die Powergard-Funktion, die vor Datenverlust bei einem plötzlichen Stromausfall schützt, indem die Boot-Dateien vom Controller im Flash-Speicher gespeichert werden. Dieser Speicher wiederum ist mit Tantal-Kondensatoren bestückt, die während des Betriebs zusätzliche Ladungen speichern und so einen „Notbetrieb" bereitstellen. Für zusätzliche Datensicherheit sorgt eine ausgefeilte End-to-End Data Protection-Funktion, die mögliche Fehler im Datenpfad erkennt und sofort korrigiert.

www.spectra-austria.at

ANGRIFF UND VERTEIDIGUNG

Wie planen Unternehmen ihre digitale Zukunft? War ein Umdenken in Richtung Homeoffice bzw. Fernwartung längst überfällig? Dies sind Fragen, die sich durch die Covid-19-Pandemie relativ schnell von selber beantwortet haben. Doch gleichzeitig stieg auch die Gefahr von Cyberattacken. Wie man dem am geschicktesten begegnet und wo die Schwächen vieler liegen weiß Uwe Gries, Country Manager DACH bei Stormshield im Gespräch mit Stephanie Englert.

IoT 4 Industry & Business: Wie sieht Stormshield den, auch durch Corona, angestoßenen Entwicklungsschub in Richtung Digitalisierung?

Uwe Gries: Die Gesundheitskrise hat von einem Tag auf den anderen Millionen Beschäftigte zur Telearbeit gedrängt, mit einer explosionsartigen Zunahme der Nachfrage nach Fernzugang und VPN. Die Reaktion der Organisationen war nicht einheitlich und zweifellos kein Ergebnis einer durchdachten digitalen Entwicklungsstrategie der Unternehmen, sondern eine Handlung aus einer Notsituation heraus, und als solche ist sie auch zu werten.

IoT: Inwiefern?

Gries: Zum Teil wurden hausinterne Sicherheitsrichtlinien abgebaut oder verändert, um schnellstmöglich für mehr Fernzugriffe zu sorgen, ohne übliche IT-Sicherheitsverfahren zu befolgen und ohne davor eine Risikoanalyse durchführen zu können. Allein in den letzten beiden Märzwochen verzeichnete etwa unser technischer Support einen 30-prozentigen Anstieg der Anfragen von Netzwerk- und Systemadministratoren, die über Nacht Fernzugriffe einrichten mussten.
Zum Teil vergingen hingegen Wochen, bis die Mitarbeiter überhaupt auf die Unternehmensressourcen von zu Hause aus zurückgreifen konnten, was vermehrt zum Einsatz von nicht per Sicherheitsrichtlinie genehmigten Plattformen für den Informationsaustausch führte.
Doch dem anfänglichen Chaos zum Trotz sind wir der Meinung, der vermehrte Rückgriff auf Telearbeit und Fernwartung könnte den Weg für einen Paradigmenwechsel geebnet haben. Es bleibt allerdings noch abzuwarten, ob sich die vielerorts zögerlich eingeführte neue Arbeitspraxis etablieren wird.

IoT: Sind bei Unternehmen, die vielleicht unvorbereiteter und einhergehend auch unvorsichtiger in die Telearbeit gestoßen wurden, denn wirklich mehr Zwischenfälle zu verzeichnen?

Gries: Die geringere Wachsamkeit und digitale Verunsicherung kamen bekanntermaßen Cyberkriminellen zugute, besonders bei Organisationen, in denen Telearbeit noch nie oder nur selten durchgeführt wurde. Sowohl in der öffentlichen Verwaltung, im Gesundheitswesen wie auch im Industrieumfeld wurden die IT-Systeme auf eine besonders harte Probe gestellt. Und ihre digitale Anfälligkeit zeigte sich deutlich, hierzulande wie international mit bedeutsamen Cybersicherheitsvorfällen: Die Covid-

19-Pandemie hat branchenübergreifend infrastrukturelle Mängel ans Tageslicht treten lassen, schließlich wurden die Sicherheitslücken der Unternehmen in die Wohnungen der einzelnen Mitarbeiter getragen – und umgekehrt.
Zudem wurden „Versprechen" von Seiten der Cyberkriminellen, in der Covid-19-Zeit auf Attacken zu verzichten, nicht eingehalten. Es gab daher abertausende Phishing-Mails mit Corona als Hauptthema und etliche Angriffe, die sich Schlupflöcher ins Unternehmensnetz aufgrund der unbedachten Öffnung von Ports zunutze machten.

IoT: Welche „Lehren" werden hieraus nun gezogen?
Gries: Wir haben nicht den Eindruck gewinnen können, dass bislang die Unternehmen so richtig verstanden hätten, welche Chance zur Erneuerung obsoleter Infrastrukturen und zur Verstärkung der eigenen Cyberresilienz diese Situation geboten hat. Ebenso wenig glauben wir, dass diese Chance zur Weiterentwicklung überhaupt wahrgenommen wird.
Jüngste Studien bestätigen, dass in etwa 40 % der europäischen Unternehmen IT- und Cybersicherheitsinvestitionen kurz bis mittelfristig eingefroren hätten, um zumindest teilweise die Verluste durch Corona zu kompensieren. Andere Erhebungen zeigen jedoch, dass Zusatzinvestitionen im Bereich VPN und Datenverschlüsselung getätigt würden. Wir wollen hoffen, dass man ab sofort die Absicherung der Unternehmensinfrastruktur wie der Daten als ganzheitlichen Wachstumsprozess betrachtet und ggf. neue Maßnahmen nach dem Prinzip der „Security by Design" ergriffen werden.

IoT: Seit Kurzem sprechen Unternehmen und vereinzelt ganze Länder von einer Rückkehr der Mitarbeiter an den Arbeitsplatz im Office. Hat die Pandemie nun doch keinen Change in der Arbeitsdenkweise hervorgerufen oder reichen die infrastrukturellen Kapazitäten und Sicherheitsvorkehrungen für eine derart große Summe an Telearbeitsplätzen einfach nicht aus?
Gries: Die rosigen Erwartungen aus dem Sommer haben sich leider in der Form nicht bewahrheitet, die Zahlen steigen überall erneut. Doch haben sich viele Unternehmen in ganz Europa branchenübergreifend von der vermeintlichen „Ruhephase" nicht beirren lassen und auf unbefristete Zeit Schichten unter den Mitarbeitern eingeführt, damit – wenn überhaupt – deutlich weniger als 50 % der Belegschaft gleichzeitig in der Firma anwesend sind.
Zu diesem Zweck wurden die (fast überall) anfangs knappen infrastrukturellen Kapazitäten erweitert und entsprechende Sicherheitsrichtlinien vorgesehen. Dort, wo die Präsenzkultur am Arbeitsplatz hingegen am stärksten ist, nehmen die Organisationen das Risiko von gezielten Schließungen und Einzelquarantänen in Kauf. Der Rückgriff auf Telearbeit (falls überhaupt möglich) wird immer noch als „Notmaßnahme" und nicht als Garant für die Geschäftskontinuität gesehen. Die Unterschiede zwischen beiden Ansätzen sind sehr markant und führen auch zu einer unterschiedlichen Auffassung der einzuleitenden Cybersecurity-Maßnahmen.

IoT: Was müssen Telearbeiter/Unternehmen in Bezug auf Datenverschlüsselungen besonders beachten?
Gries: Je minimaler die Auswirkung jeder eingeführten Cybersecurity-Maßnahme für den Mitarbeiter, desto erfolgreicher deren Implementierung. Das gilt auch für die Datenverschlüsselung. Diese darf keineswegs Arbeitsprozesse belasten, muss für den Mitarbeiter transparent, schnell und zuverlässig sowie unabhängig vom Dokumenttyp, vom Gerät (Tablet, Smartphone, Laptop, Desktop-PC) oder vom Anbieter des eingesetzten Cloud-Services erfolgen und eine vertrauensvolle Zusammenarbeit unter Projektmitarbeitern gestatten. Zusätzliche Funktionen wie die Anzeige von Alarmen bei kritischen Ereignissen und die Möglichkeit, die – von den Daten getrennt gespeicherten – privaten Schlüssel über einen Zwangsabruf in Echtzeit zurückzurufen und die entschlüsselte Anzeige der Daten je nach Aufenthaltsort des Mitarbeiters zu unterbinden, runden den zu evaluierenden Leistungsumfang der Verschlüsselungslösung ab. >>

Uwe Gries,
Country Manager DACH Stormshield
„Die Covid-19-Pandemie hat branchenübergreifend infrastrukturelle Mängel ans Tageslicht treten lassen."

IoT: Punkto Datensicherheit: Was ist besonders zu beachten, auch in Hinblick darauf, dass mehrere, verschiedene Geräte gleichzeitig benutzt werden?

Gries: Wir bei Stormshield halten es für unangebracht, Mitarbeiter mit Geräten auszustatten, die ihre Aktivitäten auf invasive Weise überwachen, wo deren Zeitkarte nach dem Login ins Unternehmensnetz gestempelt und deren Produktivität an Serverlogs gemessen wird. Aufgrund der Vielzahl der (auch privaten) Geräte, die Mitarbeiter zu Hause einsetzen, ist es notwendig, Zero-Trust-Modelle in Erwägung zu ziehen. Darunter fallen sowohl eine transparente Ende-zu-Ende-Verschlüsselung der Daten unabhängig von der verwendeten Speicherplattform und der Verwendung von VPN als auch der eingeschränkte Zugriff auf Netzwerkressourcen, der für einen bestimmten Benutzer aufgrund seiner Rolle, des verwendeten Gerätes, des Arbeitsortes und der eingesetzten Anwendung zu festgelegten Zeiten autorisiert werden sollte.
Diese Faktoren würden es ermöglichen, den Zugriff, die Verarbeitung und die Weiterleitung sensibler Daten sowie die Privatsphäre der Benutzer zu schützen, indem Arbeitszeiten klar abgegrenzt und die Nutzung von Privatgeräten und -plattformen eingeschränkt werden, die nicht durch die hausinterne Sicherheitspolitik abgedeckt sind. Die Legitimität des gesamten Datenflusses sollte zudem gründlich überprüft und der Datenverkehr im Fall von Anomalien in Echtzeit unterbunden werden. Mit diesem Modell kann jede Organisation bestimmen, wer genau worauf, wie und wann Zugriff hat, und Daten sowie die gesamte Infrastruktur absichern.

IoT: Bieten denn Cloud-Lösungen die Sicherheit, die Unternehmen benötigen?

Gries: Cloud-Lösungen waren in der akuten Lockdown-Phase eines der am meisten genutzten Werkzeuge für die Gewährleistung der Geschäftskontinuität. Doch allgemein besteht ein großer Unterschied zwischen privaten Cloud-Diensten und öffentlichen SaaS-Anwendungen und Cloud-Plattformen. Erstere sind meistens mit unternehmenseigenen Cybersecurity-Lösungen geschützt. Bei Cloud-Plattformen muss man eine weitere Unterteilung vornehmen: Es gibt solche, die Unternehmen gewidmet und deshalb durch Service-Level-Agreements und vom Provider gestellte Sicherheitslösungen abgesichert sind, und solche für den privaten Gebrauch. Da letztere leicht und schnell zugänglich und bedienbar sind, wurde sehr oft in der Not darauf zugegriffen, ohne Rücksicht auf die Sicherheitsrichtlinien des Unternehmens.
Firmen, die von den Vorteilen einer flexiblen IT-Infrastruktur mittels Cloud-Lösungen profitieren möchten, sollten zum Schutz der eigenen Daten das Schatten-IT-Phänomen weitestgehend unterbinden. Ein weiteres Element muss zudem berücksichtigt werden: Durch die Abschaffung des Privacy-Shield-Abkommens zwischen der EU und den USA ist die Nutzung von Cloud-Services aus Übersee besonders kritisch, auch im Hinblick auf die mögliche Verhängung von Geldstrafen durch die zuständigen Behörden.

IoT: Auch Deep Fakes sind rasant angestiegen. Wie begegnen Sie dem?

Gries: In Verbindung mit Corona sind zahlreiche schwerwiegende Fälle von Betrug bekannt, die auf Deep Fakes basieren. Doch meistens entsteht der Schaden im Unternehmen aus einer unglücklichen Kombination aus Menschenversagen und unzulänglicher Technik. Genau darauf bauen die Cyberkriminellen, und der Anstieg dieses Phänomens bezeugt, wie sehr Menschen für trickreiche Maschen anfällig sind.

IoT: Ist die Schadenssumme aufgrund von Phishing-Angriffen/Deep Fakes auch auf die im Unternehmen nicht getätigten Investitionen in neuere Techniken zurückzuführen oder besteht kein Zusammenhang?

Gries: Der Zusammenhang besteht natürlich, denn das Vorhandensein von infrastrukturellen Schwachstellen und unangemessener Technik ist – wie erwähnt – eines der Elemente, worauf

Uwe Gries
Country Manager DACH Stormshield

„Cloud-Lösungen waren in der akuten Lockdown-Phase eines der am meisten genutzten Werkzeuge für die Gewährleistung der Geschäftskontinuität."

Ob Mitarbeiter besser von daheim aus arbeiten oder eben doch im Unternehmen, ist grundsätzlich auch eine Frage der sicheren Infrastruktur.

Cyberkriminelle aufbauen. In diesem Zusammenhang ist die relevantere Frage eine andere: Was ist „angemessen"? Spätestens seit Einführung der DSGVO haben Firmen in ein für sie angemessenes Sicherheitsniveau investiert, ohne jedoch genau zu verstehen, dass jegliche Cybersicherheitssysteme keine Plugin-and-forget-Gegenstände sind, sondern gepflegt werden müssen.
Auch die Fehlbarkeit der Mitarbeiter als mögliches Risiko in der eigenen Strategie zur Absicherung der Unternehmensinfrastruktur wurde nicht berücksichtigt. Ohne digitale Hygiene und ständige Anpassung der Sicherheitsmaßnahmen an eine sich ständig verändernde Bedrohungslage erweist sich selbst die Investition in modernste Technik als unzulänglich.

IoT: Haben versäumte Mitarbeiterschulungen ebenfalls einen Einfluss auf die Angriffsempfindlichkeit eines Unternehmens?
Gries: Davon sind wir überzeugt: Der Mitarbeiter ist in jedem Unternehmen die erste Verteidigungslinie. Ein gutes Maß an Wachsamkeit und Wahrnehmung cybersicherheitsrelevanter Themen hat bereits oft den Unterschied bei Angriffsversuchen gemacht.

IoT: Abschließend haben Sie einen Wunsch frei. Was wäre das in Hinblick auf Security?
Gries: Die unter normalen Umständen gewährte Möglichkeit der Telearbeit kann branchenübergreifend tatsächlich für ein höheres Maß an Flexibilität sorgen. Wir haben nun die einmalige Gelegenheit, Modelle und Werkzeuge zu evaluieren, die geeignet sind, die Art und Weise, wie man bislang arbeitete, langfristig zu verändern – und diesmal, so hoffen wir, nach den besten Vorsätzen der „Security by Design".

www.stormshield.com

Zum ausführlichen Interview:

Was 2021 geschehen wird und wie das zusätzliche neue digitale Format angenommen wird, zeigt sich in den kommenden Monaten.

WILLKOMMEN IM NETZ

Die Security-Fachmesse it-sa wird wie viele andere Formate erst 2021 wieder als Präsenzveranstaltung über die Bühne gehen (12. bis 14. Oktober 2021). Denn obwohl das Thema Security mehr als zuvor durch die Pandemie in den Fokus gerückt ist, konnte ein Treffen heuer „nur" digital stattfinden. Von Stephanie Englert

Dennoch hat sich der Veranstalter, die Messe Nürnberg ein neues Konzept für eine Alternative 2020 überlegt. Unter dem Motto „Solutions – Networking – Knowledge" wurde die it-sa 365 ins Leben gerufen. Die neue digitale Dialogplattform zum Thema IT-Sicherheit startete erfolgreich am 6. Oktober. Das ganzjährig erreichbare Portal offeriert etwa ein gut gefülltes Anbieter- und Lösungsverzeichnis sowie Informationen zur Cybersicherheit und ist sozusagen die Alternative in diesem Covid-19-Messejahr gewesen.

Dabei greift it-sa 365 bekannte Elemente der europaweit größten IT-Sicherheitsmesse it-sa auf und bleibt als Wissens-Plattform an 365 Tagen im Jahr erreichbar und ist damit Anlaufstelle für aktuelle Fachinformationen und den Austausch innerhalb der IT-Security-Branche. Ein digitales Muss sozusagen. Im Interview mit Messechef Frank Venjakob wurde noch einmal konkretisiert.

Frank Venjakob,
Director it-sa, NürnbergMesse

„Natürlich hat die Covid-19-Pandemie den Prozess der Umsetzung einer Digitalplattform beschleunigt."

IoT 4 Industry & Business: „Ein umfangreiches Anbieter- und Lösungsverzeichnis, interaktive Dialogformate und Neues aus der Welt der Cybersicherheit" – das versprach die it-sa 365. Mit welchen Erwartungen haben Sie dieses neue Konzept ins Leben gerufen?

Frank Venjakob: it-sa 365 knüpft ein Band zwischen den Messeterminen. Wir können Anbietern und Experten so ein ganzjähriges Angebot machen, sich untereinander zu vernetzen und stets auf dem Laufenden über neue Lösungen im Bereich der IT-Sicherheit zu bleiben.

IoT: Wie kann man sich das neue Format vorstellen?

Venjakob: Unter dem Motto „Solutions – Networking – Knowledge" startete it-sa 365 am 6. Oktober. Das ganzjährig erreichbare Portal mit einem umfassenden Anbieter- und Lösungsverzeichnis, interaktiven Dialogformaten und aktuellen Informationen zur Cybersicherheit greift bekannte Elemente der it-sa auf: Produktneutrale Beiträge, die it-sa insights, Vorträge zu Management und Technik sicherer IT-Infrastrukturen, die Special Keynote des ehemaligen Anonymous-Aktivisten Jake Davis, erweitert durch Workshops, machten den Live-Charakter während der Launch Days aus.
Das Programm lief bis zum 8. Oktober. Nun sind die Beiträge online. Regelmäßige Updates bringen die Teilnehmer immer wieder auf den neuesten Stand in Sachen IT-Sicherheit. An 365 Tagen im Jahr bietet it-sa 365 somit regist-

rierten Teilnehmern zusätzlich die Gelegenheit, Experten und Lösungsanbieter unkompliziert und schnell zu finden und direkt zu kontaktieren.

IoT: An wen richtet sich it-sa 365?
Venjakob: An alle Experten und Entscheider aus IT und Sicherheit, die sich dem Thema IT-Security beruflich widmen.

IoT: Wie viele andere Messeformate wurde auch die it-sa 2020 als physische Veranstaltung auf 2021 verlegt. Dennoch gibt es Bundesländer, die wieder Messen erlauben und durchführen. Wann war klar, dass dies nicht für die it-sa 2020 in Frage kommt und weshalb?
Venjakob: Wir haben Mitte Juni entschieden, dass die diesjährige Veranstaltung aussetzt. Der Entschluss war rückblickend richtig. Wichtig war uns, den Ausstellern Planungssicherheit zu geben, weil in den letzten Monaten vor einer Messe maßgebliche Vorbereitungen für die Teilnahme erfolgen müssen.

IoT: Gehen Sie davon aus, dass durch das vermehrte Telearbeiten derzeit auch die Branche der Security eine viel größere Rolle spielen wird und dies auf der it-sa 2021 zu sehen sein wird?
Venjakob: Von vielen Anbietern wird die enorm gestiegene Zahl der vom Homeoffice aus Tätigen als zusätzlicher Risikofaktor für die Unternehmens-IT der Kunden identifiziert. Das hat unsere jährliche Umfrage, die wir unter Ausstellern der it-sa Expo&Congress durchführen, gezeigt.
Die Absicherung der Unternehmens-IT über das firmeneigene Netzwerk hinaus ist also eine besondere Herausforderung, der sich alle Beteiligten stellen müssen. Nachdem der Wechsel ins Homeoffice für viele Unternehmen so gut geklappt hat, werden Mitarbeiter die damit verbundenen Vorteile auch in Zukunft noch stärker einfordern. Daher kann ich mir gut vorstellen, dass sich das an einem noch stärkeren Sicherheits-Angebot auf der Messe auch spiegeln wird.

Messe 2020 ist nicht zu vergleichen mit den Erfahrungen der Messen in den Jahren zuvor.

IoT: Wäre das Format it-sa 365 auch ohne Pandemie entstanden?
Venjakob: Wir befassen uns schon seit Längerem mit den Möglichkeiten der Digitalisierung und der Frage, wie klassisch Messeformate um digitale Komponenten ergänzt werden können. Natürlich hat die Pandemie den Prozess der Umsetzung einer Digitalplattform beschleunigt. In der aktuellen Situation sehen wir diese Herausforderung als Chance, neue Wege zu gehen und das „Home of IT-Security" auch online zu stärken.

IoT: Und mit welchen allgemeinen Erwartungen gehen Sie ins kommende Messejahr 2021?
Venjakob: Digitale Angebote bieten der Branche zusätzliche Möglichkeiten zum fachlichen Dialog. Das Bedürfnis, sich persönlich zu treffen und auszutauschen, ist in den letzten Monaten bei allen Beteiligten aber sehr gewachsen. Daher freuen wir uns jetzt schon darauf, wenn sich die IT-Security-Experten vom 12. bis 14. Oktober 2021 das nächste Mal in Nürnberg treffen! Parallel zu den Messevorbereitungen bauen wir unser digitales Angebot kundenorientiert weiter aus. Wir sind damit ein starker Partner in beiden Welten, offline und online.

www.it-sa.de

Security ist bei vielen Unternehmen weltweit nur ein Thema von vielen, es sollte jedoch mehr Aufmerksamkeit erhalten.

SECURITY?

Sergej Epp ist CSO Central Europe bei Palo Alto Networks, einem Anbieter von Cybersicherheitslösungen. Das Unternehmen beauftragte im Frühjahr 2020 Forrester Consulting mit der Durchführung der Studie „The State of Security Operations". Weltweit 315 Entscheidungsträger im Bereich des Sicherheitsbetriebs wurden befragt. Von Stephanie Englert

Mitte September war es soweit, eines von vielen Telefon-Meetings stand an, doch dieses hatte eine besondere Bedeutung und zwar insofern, als dass es Mitten in einer Neuen „Ära" mehr Relevanz hatte wie selten zuvor. Es ging um Security. Seit Mitte März 2020, der Zeit, in der plötzlich fast alle Unternehmen weltweit das Thema Telearbeit in die Tat umsetzen mussten, änderte sich auch für viele ihre Einstellung oder ihr Investitionsverhalten in Bezug auf Security. Denn ohne Sicherheit kann das Homeoffice schnell zur Gefahr für den Betrieb werden.

Die Ergebnisse der Studie „The State of Security Operations", stellte in einer Videokonferenz Sergej Epp vor und er betonte gleich eingangs, dass „mit dem wachsenden Tempo, Umfang und der Raffinesse von Cyberangriffen viele zu kämpfen haben." Er ergänzt: „Security steht bei vielen einfach nicht auf der Agenda" und sprach damit ein weit verbreitetes Phänomen an. Weiters mahnte Epp, dass „viele Mitarbeiter nicht genügend sensibilisiert werden, wenn es um die betriebsinterne Sicherheit von Anlagen oder Produktionsprozessen etc. geht." Doch warum ist das im Jahr 2020 nachwievor so?

Offene Antworten auf eindeutige Fragen. Die Umfrage zeigt, dass nur 46 Prozent mit ihrer Fähigkeit, Cybersicherheitsbedrohungen zu erkennen, zufrieden sind. Seit Beginn der Covid-19-Krise ist die Rate der Angriffe in die Höhe geschnellt. Dabei sind Cyberangreifer unerbittlich und werden raffinierter. Unternehmen sind ständigen Angriffen ausgesetzt. Ein Sicherheitsbetriebsteam erhält pro Tag im Schnitt elf Sicherheitswarnungen. Der Bericht kommt zu dem Ergebnis, dass die Mehrheit der Unternehmen nicht in der Lage ist, auf die meisten oder alle Sicherheitswarnungen, die sie an einem einzigen Tag erhalten, zu reagieren. Die Sicherheitsteams sind durch isolierte Anwendungen und manuelle Prozesse gelähmt. 28 Prozent der Alarme werden schlicht nie bearbeitet, was nicht gerade beruhigend ist.

Ein Teufelskreis. Trotz umgehender Bemühungen sind die Sicherheitsbetriebsteams nicht in der Lage, entscheidende Vorgaben wie die mittlere Untersuchungszeit, die Anzahl der bearbeiteten Vorfälle, die mittlere Reaktionszeit, die Bedrohungsbewertung und die Anzahl der Warnungen einzuhalten. Weniger als 50 Prozent der Teams geben in der Umfrage an, dass sie diese Metriken in den meisten Fällen erfüllen. Auf der Grundlage der Umfrage fand Forrester Consulting zwei Hauptgründe für diese Diskrepanz:

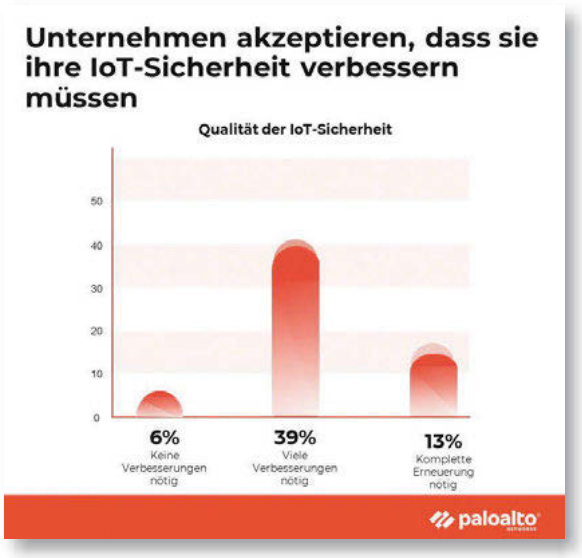
- **Lücken bei den Ressourcen:** IT-Entscheider sagen, dass es eine große Herausforderung ist, erfahrene Mitarbeiter für den Sicherheitsbetrieb und genügend Analysten zu finden und zu halten, um die Arbeitslast zu bewältigen.
- **Technologische Lücken:** SecOps-Teams verwenden im Durchschnitt über zehn verschiedene Kategorien von Sicherheitstools, darunter Firewalls, E-Mail-Sicherheit, Endpunktsicherheit, Bedrohungsanalyse, Schwachstellenmanagement und mehr. Diese Tools sind jedoch in der Regel isoliert, und die Implementierung ist oft mangelhaft.

Epp fordert daher alle auf, „proaktiver zu handeln." Einen weiteren wichtigen Unterschied sprach er an: „Viele machen einen entscheidenden Fehler. IoT-Security ist nicht das Gleiche wie IT-Security. Und hier herrscht oft Verwirrung." Solange auch hier ein Defizit herrsche, ist ein effektives Arbeiten seiner Ansicht nach schwer. Aber, und so zeigt es laut Epp auch das Studienergebnis (Grafik re.), seien immerhin 39 Prozent bereit dazu „Verbesserung vorzunehmen" – was immer das in der Praxis bedeuten kann.

Automatisierung und Sichtbarkeit. Laut den Ergebnissen nutzen zudem nur 13 Prozent der befragten Unternehmen den Wert von Automatisierung und maschinellem Lernen zur Triage, Analyse und Reaktion auf Bedrohungen. Gleichzeitig finden versierte Cyberangreifer rasch neue Wege, um dieselben Instrumente zur Skalierung des Umfangs und der Auswirkungen ihrer Operationen einzusetzen. Laut Forrester Consulting gibt es Möglichkeiten und Lösungen, die Unternehmen nutzen können, um die Kontrolle und Sichtbarkeit der gesamten Infrastruktur zu erhöhen. Beispielsweise kann eine erweiterte Erkennungs- und Reaktionslösung (Extended Detection and Response, XDR) helfen, was die Ermüdung von Analysten, die Ineffizienz von Tools und die allgemeinen Sicherheitsergebnisse betrifft:

- Verbesserung der Sichtbarkeit durch einheitliche Technologie, die Telemetrie aus verschiedenen Quellen nahtlos integriert.
- Nutzung von Sicherheitsanalysefähigkeiten wie maschinelles Lernen, um verborgene Angriffstechniken an die Oberfläche zu bringen.
- Automatisierung der Ursachenanalyse.

Ein paar Highlights. In der Studie wurde auch gefragt, welches die „auffälligsten" Geräte waren, die (versehentlich) mit dem Firmennetzwerk verbunden wurden und das Ergebnis ist interessant. Denn die größte Anzahl machten tatsächlich „medizinische Geräte" wie etwa Fitnessuhren aus (44 Prozent), dicht gefolgt von smarten Küchengeräten (43 Prozent). Ganze 27 Prozent immerhin gingen an „Connected Cars", was viele Fragen offen lässt. Doch auch „automatische Seifenspender" oder „smarte Mistkübel" bis hin zu Leuchtstoffröhren waren bei den Antworten zu finden.
Ebenfalls bemerkenswert sei auch laut Epp, dass das Studienergebnis aufzeige, dass sich Unternehmen im EMEA-Raum weitaus fitter fühlen in Bezug auf IoT-Security im Vergleich zu Unternehmen aus Nordamerika. Es heißt wörtlich: „48 percent in EMEA said they had a lot to do, or needed to overhaul strategy, compared to 52 percent of North American respondents."



Ziemlich bemerkenswert ist auch die Aussage aus deutschen Unternehmen, die besagt: „German IT decision makers are fairly confident that they have visibility of the devices connected to their network: 57 percent are completely confident; 38 percent are somewhat confident." Doch was können Verantwortliche aus diesen Ergebnissen schlussendlich für Schlüsse ziehen?
Epp meint: „Sicherere Passwörter und Aufklärung sind schon mal ein Schritt in die richtige Richtung um Mitarbeiter zu sensibilisieren und das Unternehmen fit für die digitale Zukunft werden zu lassen." Zudem brauche das Thema Security bei den Entscheidern einen höheren Stellenwert, doch dieser scheint auch durch Covid-19 und die Folgen gewachsen zu sein. Es wäre wünschenswert.

www.paloaltonetworks.com

Hier geht es zu den Studienergebnissen:

Hier geht es zur Fact Sheets Studie:

BESTENS GERÜSTET

Im März standen viele Unternehmen vor einer neuen Herausforderung. Durch den plötzlichen Anstieg von Telearbeit musste auch das Thema Security in den Mittelpunkt des Tagesgeschäftes rücken. Wer die Nase vorn hatte und was zu beachten ist – nachwievor – weiß Reinhard Mayr von Copa-Data aus Salzburg.

IoT 4 Industry & Business: Das Thema Security spielt heutzutage eine immens wichtige Rolle. Was bieten Sie als Copa-Data Kunden diesbezüglich an?
Reinhard Mayr: Als Copa-Data bieten wir vor allem unser Know-how und eine gewisse Sicherheit als verlässlicher Partner für den Kunden an; dies zeigt sich unter anderem auch in der Zertifizierung unseres Entwicklungsprozesses (Secure Development Lifecycle) nach IEC 62443-4-1 durch den TÜV Süd. Unsere Plattform zenon bietet dementsprechend auch die Möglichkeit sichere Architekturen in der OT-Welt zu bauen. Architekturen wie sie von den gängigen Standards wie NIST, ISO, IEC empfohlen werden.
Die zenon-Plattform lässt sich dabei hervorragend in bestehende Infrastrukturen integrieren und kann auch problemlos mit anderen Security-Komponenten interagieren, z.B. ein zentrales Security Logging über Syslog oder eine zentrale Benutzerverwaltung auf Basis einer Active Directory-Infrastruktur. Zusätzlich bieten wir noch einen Hardening-Guide für den Anwender und gezielte Workshops bzw. Beratung zum Thema wie man die zenon-Produktfamilie optimal betreiben kann.
Last but not least gibt es einen dedizierten Security-Newsletter.

IoT: Das klingt nach einem sehr umfangreichen Angebot, das Sie in der „Tasche" haben. Hierzu ergibt sich dann auch gleich die nächste Frage: Es heißt, dass ein erfolgreiches Cyber Security-Konzept eine „absolute Grundvoraussetzung für einen Weg in Richtung Smart Factory" sei. Wie viele Ihrer Kunden weisen bereits ein derartig sicheres Konzept auf?
Mayr: Das ist schwer in Zahlen zu fassen, aber es trifft heute vor allem die Branchen Energie und kritische Infrastruktur. Wobei die Automobilindustrie auch bereits einen immer stärkeren Fokus auf das Thema setzt; diese entwickelt auch einen eigenen Security-Standard – den Tisax.
Erste Anzeichen für eine Vertiefung des Themas sehen wir auch in der Pharmaindustrie. Also in Summe kurzfristig mehr als 80 % des aktuellen Copa-Data-Marktes. Mittelfristig wird es keine Industrie bzw. Kunden geben, die durch dieses Thema nicht betroffen sein werden.

IoT: Wo genau liegen die Schwachstellen?
Mayr: Das Hauptproblem liegt in genau drei Bereichen und zwar nachwievor bei der Awareness, denn vielen unserer Kunden sind die Risiken und Probleme nicht bewusst bzw. werden zur Seite geschoben, die sich ergeben. Zweitens – und das ist sicherlich die größere Herausforderung – ist eine klassische IT Security-Strategie nicht 1:1 auf Industrielle OT-Prozesse umzulegen.
In der Produktion steht die Verfügbarkeit der Anlagen an erster Stelle. Hier müssen Prozesse, aber auch Technologien und Strategien erst angepasst werden, damit sie den gewünschten Effekt erzielen. Hinzu kommt noch eine Know-how-Thematik, denn

es gibt ganz wenige Personen, die für beide Seiten (IT und OT) das entsprechende Fachwissen aufbringen oder die passende Sprache sprechen. Das Thema ist leider auch in der Ausbildung des künftigen Personals nicht präsent.

IoT: Seit dem 2. Quartal 2020 hat sich nun durch Covid-19 und den plötzlichen Lockdown viel verändert. Welche besonderen Bedürfnisse haben sich bei Ihren Kunden herausgestellt?

Mayr: Copa-Data hatte sicherlich den Vorteil, dass wir bereits sehr viele Dinge in Betrieb hatten, die uns in der Krise geholfen haben – sei es bei den Online-Interaktionen mit Kunden, dem Online-Ticketing-System oder auch eine im Web verfügbare Knowledge Base.
Für unsere Kunden denke ich war vor allem die Kommunikation in einer sehr frühen Phase das Wichtigste. Hierbei spreche ich etwa davon, dass wir als Unternehmen voll operativ bleiben und für unsere Kunden und Partner jederzeit zur Verfügung stehen bzw. standen.

IoT: Dennoch stieg zeitlich auch die Vulnerabilität von Unternehmen in Bezug auf Security. Es heißt: „Kritische Infrastrukturen mit weitverzweigten Kommunikationsnetzen sind ein besonders verwundbares und attraktives Ziel für Cyberattacken". Weshalb?

Mayr: Das größte Problem liegt sicherlich in den „in die Jahre gekommenen", so genannten Legacy-Protokollen bzw. -Infrastrukturen. Diese wurden alle vor 15, 20 Jahren – oder noch länger – geplant und in Betrieb genommen – mit den damals vorhandenen technischen Möglichkeiten.
OT-Security oder Datenschutz waren zu dieser Zeit einfach kein Thema. Diese Strukturen sind von daher auch extrem verwundbar, da es quasi keine integrierten Security-Maßnahmen/Technologien gibt und sie müssen „nachgerüstet" werden.
Es gibt hier bereits speziell für die Kommunikationsprotokolle sehr gute Ansätze in Bezug auf eine Absicherung über TLS (Transport Layer Security) nach dem IEC 62351-Standard.
Es fehlt aber klar noch an Lieferanten (Hard- und Software), die in der Lage sind, hier Lösungen überhaupt zu liefern. Copa-Data hat diesen Schritt bereits ge- >>

macht und kann für energierelevante Protokolle wie IEC 60870 oder DNP3 eine passende Lösung anbieten. Wobei man nicht nur die Kommunikations-Protokolle im Blick haben darf; auch die eingesetzten Hard- und Software-Komponenten sind in die Jahre gekommen. Die Industrie ist nicht unbedingt bekannt dafür gerne auf neue Versionen/Generationen zu wechseln. Es gilt Updates zu machen.

IoT: Was hat sich bei den Angriffen auf kritische Infrastrukturen geändert? Gibt es auch bei „Angreifern" Trends, die zu beobachten sind?

Mayr: Dazu gibt es sehr gute Untersuchungen auch auf EU-Ebene (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape). Zusammenfassend sind aktuell zwei Dinge zu erkennen:

1. Eine deutliche Professionalisierung der Angriffe durch kriminelle aber auch staatlich gelenkte Organisationen. Wir haben es hier nicht mehr mit den so genannten Script Kiddys zu tun.
2. Angriffe mit inkludierten Lösegeld-Forderungen nehmen deutlich zu und leider auch damit verbunden eine sehr hohe Dunkelziffer von Vorfällen, die gar nicht publik werden.

IoT: Was würden Sie Unternehmen raten, auf was sie sich künftig, auch in Bezug auf vermehrter Telearbeit, einstellen müssen, was die eigene Security im Haus bzw. bei Anlagen betrifft?

Mayr: Ich denke jedes Unternehmen sollte sich zuerst einmal bewusst darüber werden über welche Assets es verfügt, die geschützt werden müssen bzw. auch, welchen Risiken es ausgesetzt ist.

Erst danach – so denke ich – kann man abschätzen, ob das Thema Teleworking überhaupt neue Risiken birgt bzw. schützenswerte Assets betroffen sind. Wenn Teleworking zum Einsatz kommt, sollte dies vor allem ein geplanter erprobter Prozess sein. Vor allem die Abläufe und Regelungen sollten klar sein, also Dinge wie: Wer hat Anspruch? / Wo macht es Sinn? / Was

Es gilt Systeme in Anlagen und Mitarbeiter zu schützen, denn die Angriffe werden nicht weniger.

mache ich, wenn ich in einem Team einen Covid-Fall habe? / Wie kann ich sinnvoll isolieren? / Wie lange bleibt die Regelung aufrecht? / Wie wird der Zugang eingerichtet? / Wer genehmigt das Ganze? usw.

Dann erst sollten auch die technischen und inhaltlichen Dinge geklärt werden wie z.B.: Wie sichere ich den externen Zugriff ab? Oder: Erlaube ich den Einsatz privater Geräte und wie sichere ich diese ab? / Wie stelle ich sicher, dass Leute nur auf Ressourcen Zugriff haben, die sie wirklich brauchen? / Wie kann ich ein Monitoring einrichten? Und auch das Thema Datenschutz darf nicht vergessen werden. Gibt es also DSGVO-relevante Daten, die sich durch Teleworking meiner Kontrolle entziehen?

IoT: Kommen wir zur Copa-Data-Plattform zenon. Was gibt es hier derzeit Neues bzw. was ist noch geplant?

Mayr: Wir arbeiten momentan intensiv daran, die zenon-Plattform noch unabhängiger von Dritt-Komponenten zu machen also noch offener zu werden. Dazu zählen Themen wie eine plattformunabhängige Visualisierung oder auch komplette Runtime-Systeme.

Ein weiteres globales Thema ist es die zenon-Plattform so zu erweitern, dass moderne Architekturen bzw. Technologien problemlos genutzt werden können. Dazu zählt die Umsetzung von Micro Service-Architekturen oder Edge-Komponenten zum Einsatz in Kombination mit Cloud-Technologien – oder eben auch die Unterstützung moderner IT-Werkzeuge wie Docker oder Kubernetes-Technologien.

IoT: Abschließend eine allgemeine Frage: Hat Ihrer Ansicht nach durch die Corona-Pandemie bezugnehmend auf Unternehmen, sich deren Digitalisierungsstrategie beschleunigt?

Mayr: Ich kann aus meiner Sicht noch keinen generellen Trend erkennen. Es gibt sehr wohl einige Unternehmen auf die das zutrifft. Vor allem, da zum Teil die Krise auch Ressourcen frei gemacht hat, die vorher im Tagesgeschäft nicht frei waren. Es hat aber bei fast allen Unternehmen dazu geführt, dass die IT-Strukturen einer Art Härtetest unterzogen wurden und Schwachstellen in Prozessen oder eben auch der IT beinhart aufgezeigt wurden. (se)

www.copadata.com

Laut dem Cybersecurity-Spezialisten Stormshield ist eine solide Strategie zur Stärkung der Cyberresilienz kritischer Organisationen eine Frage der Verantwortung.

STRATEGISCHE INFRASTRUKTUREN UND CYBERRESILIENZ

Dem österreichischen Programm zum Schutz kritischer Infrastrukturen sind laut Bundeskanzleramt Organisationen oder Einrichtungen zugeordnet, „die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren Störung oder Zerstörung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen haben würde" (Zit. APCIP 2014).

Der Großteil dieser Organisationen, von den Fertigungsanlagen über Gesundheitseinrichtungen, Museen und Einkaufszentren bis hin zu den öffentlichen Verkehrsmitteln, nutzen operative (OT-) Informationssysteme, um es uns zu ermöglichen, unseren Alltag „normal", ggf. sogar komfortabler und sicherer zu leben. Doch infolge der zunehmenden „Smartisierung" dieser Infrastrukturen und der Allgegenwart digitaler Technologien werden diese traditionell isolierten Systeme zwar effizienter und agiler, aber auch anfälliger für neue Cyberrisiken.

Als europäische Referenz für Cybersecurity im Bereich IT- und OT-Systeme, kritischer Infrastrukturen und sensibler Daten ist Stormshield der Meinung, dass die unaufhaltsame Vernetzung strategischer Organisationen und die damit verbundenen Fragen der Cybersicherheit nicht länger als rein technische Anliegen betrachtet werden dürfen. Beide sind laut Meinung des Herstellers heute Grundpfeiler der geschäftlichen Belastbarkeit dieser Infrastrukturen und deren Fähigkeit, trotz möglicher Krisensituationen lebenswichtige Dienste zu erbringen.

Es kommt auf die richtige Kombination an. Der Ansatz der Resilienz zielt darauf ab, die Auswirkungen einer Cyberattacke auf den Betrieb des Unternehmens zu minimieren und sich von deren Folgen zeitnah zu erholen. Wie bei allen Prozessen im Krisenmanagement muss die Cyberresilienz als erste unerlässliche Schutzschicht bereits gewährleistet sein, bevor es zu einem Vorfall kommt. Es gilt hierbei zu bedenken, dass es sich um kein einmaliges Verfahren handelt: Das eigene Cyberresilienz-Niveau muss regelmäßig getestet werden. Ein neues Geschäftsprojekt kann etwa das Risiko für einen Cyberangriff erhöhen, und wenn diese Gefahr nicht rechtzeitig erkannt wird, ist die gesamte Strategie wirkungslos.

Die Cybersicherheit spielt hier eine wesentliche Rolle. Laut Stormshield müsste dabei die Absicherung von Daten, Maschinen und Infrastrukturen strategischer Organisationen auf das Prinzip der umfassenden Verteidigung setzen, die trotz des empfehlenswerten Einsatzes verschiedener vertrauenswürdiger Technologien, von Anfang bis Ende konsistent sein sollte und keine Arbeitsbereiche und -werkzeuge vernachlässigen dürfte. Die Auswahl der richtigen Technologien, die teilweise Überlagerung der Sicherheitsmaßnahmen zur Gewährleistung einer zweiten Verteidigungslinie, die Implementierung einer punktgenauen Segmentierung der Netze und adäquater Sicherheitspolicies genießen dabei laut dem Hersteller Vorrang.

Die menschliche Komponente ist ebenfalls entscheidend. Man darf sich nicht nur darauf verlassen, dass die automatisierten Prozesse und technischen Security-by-Design-Maßnahmen greifen. Für die Erlangung der Cyberresilienz bedarf es ebenfalls fachkundiger Teams und der weitreichenden Sensibilisierung der Mitarbeiter für das Thema Cybersicherheit und digitale Hygiene. Und schließlich sollte dasselbe auch innerhalb der gesamten Versorgungskette der strategischen Organisationen verlangt werden, denn eine Kette ist nur so stark wie ihr schwächstes Glied.

www.stormshield.com/de

Der Autor:

Uwe Gries

... ist Country Manager DACH bei Stormshield.

ANGRIFF AUS DEM NETZ

Moderne Wirtschaftsspionage kommt zunehmend aus dem Netz. Wer sich nicht um eine Security-Strategie kümmert, kann seine Produkte rasch als billigen Nachbau am Markt wiederfinden. Wie man sich davor schützen kann, erklärt Torsten Wiedemeyer, Regional Director Central & Eastern Europe bei Adaptiva. Von Barbara Sawka

IoT 4 Industry & Business: Wie sieht denn Ihr persönliches Bild eines Hackers aus?
Torsten Wiedemeyer: Das ist auf jeden Fall nicht der Typ in der Kapuze. Für mich stellt sich eher die Frage, welche Motivation der Hacker hat. Sind das irgendwelche Jungs, die schauen wollen, was sie können? Die sollte man zu einer Security-Firma schicken, weil die wissen, was sie tun. Diese ganzen Ransomware-Geschichten sind mühsam und wenn man sich gar nicht schützt, dann können sie auch sehr ärgerlich sein. Aber sie haben keinen signifikanten Effekt auf ein Unternehmen. Absolut gefährlich sind jene Organisationen, die an der Intellectual Property eines Unternehmens interessiert sind. Das führt zum Schaden von Unternehmen oder auch ganzen Wirtschaftszweigen. Ich habe mit deutschen Unternehmern gesprochen, die bis zu einem Hackerangriff geglaubt haben, dass sie nicht so wichtig und damit nicht gefährdet sind. Sie waren es aber offensichtlich doch. Es ist unangenehm, wenn in einem anderen Land exakte Kopien seiner Produkte auftauchen, die nur durch die Verfügbarkeit der Konstruktionszeichnungen möglich waren.

IoT: Reichen solche Schauergeschichten, um die Unternehmen dazu zubringen in ihre Sicherheit zu investieren?
Wiedemeyer: Die Keule ist auf jeden Fall gut. Aber was ich sehe ist, dass es einen zunehmenden Austausch zwischen Unternehmen über diese Thematik gibt. Und das hilft natürlich weit mehr, als wenn ein IT-Dienstleister erzählt, wie grausam die Zukunft sein könnte.

IoT: Kann man sich gegen diese Angriffe überhaupt wehren?
Wiedemeyer: Wenn man es dramatisch formulieren würde, dann könnte man sagen: Das ist tatsächlich ein Cyberkrieg um Wissen. Man kann sich zwar nicht hundertprozentig schützen, aber man kann sehr gute Verteidigungslinien aufbauen. Und dann ist die Wahrscheinlichkeit, dass diese Attacken erfolgreich sind, niedriger.

IoT: Was sind denn die häufigsten Schwachstellen, mit denen Sie bei den Unternehmen konfrontiert sind?
Wiedemeyer: Das sind ganz klar User-Endgeräte. Das sind auch die Themenbereiche, die wir bei Adaptiva bearbeiten. Bei

Im Cyberkrieg um Wissen gibt es zwar keinen hundertprozentigen Schutz, aber sehr gute Verteidigungslinien.

Windows-Geräten ist der Multiplikator immens. Hier muss man zuerst durch entsprechende Policies und mit den richtigen Tools ansetzen. Vor einiger Zeit gab es einen Hacker-Kongress in den USA. Die Aufgabe war, industrielle Steuerungssysteme zu hacken. Und es sind alle gehackt worden. In traditionellen Produktionsbereichen, in denen die Produktionsnetze meistens noch abgeschottet sind, gibt es weniger Probleme. Aber wenn ich in die Hoch-Automatisierung gehe und über Digitalisierung spreche, zum Beispiel als Konstruktionsunternehmen, in dem die Produktionsanweisungen direkt an die Maschine des Herstellers geschickt werden, dann ist man plötzlich im Internet und offen. Und dann könnte es theoretisch leicht sein, dass irgendwer eine Produktionslinie lahmlegt. Einfach weil er es kann. Und wenn ich sehe, dass die Software-Seite der Industrie 4.0 anfällig ist, dann bereitet mir das Sorgen.

IoT: Aber gerade diese Internet-Anbindung in der Produktion ist ja das, was Industrie 4.0 benötigt.

Wiedemeyer: Ich habe mit relativ vielen Unternehmen in diesem Bereich gesprochen. Es gibt natürlich einen Enthusiasmus in Richtung Industrie 4.0, weil sie einfach unglaubliche Möglichkeiten bietet. Aber, wenn es dann tatsächlich in Richtung Implementierung geht, dann kommen die Themen Risikobewertung und Security auf. Und wir sehen, dass es heute noch keine wirklich zufriedenstellenden Lösungen gibt. Das führt dazu, dass Industrie 4.0 trotzdem noch als Insellösung oder abgeschottet funktioniert. Das ist sicherlich ein Zielkonflikt, den es aufzulösen gilt.

IoT: Wie sieht das Schwachstellenmanagement von Adaptiva aus?

Wiedemeyer: Unser Fokus liegt auf Automatisierung. Normalerweise setzt sich bei Attacken auf Windows-Systeme, speziell in großen Organisationen, eine eigene Maschinerie in Gang. Der Chief Security Officer wird gerufen und man überlegt, was man tun sollte. Dann kommt man drauf, dass man einen neuen Patch braucht, der erst vom Hersteller zur Verfügung gestellt werden muss. Und es muss getestet werden. Währenddessen ist man ungeschützt. Wir haben uns Statistiken angesehen, die besagen, dass im Schnitt von der Bekanntgabe einer Vulnerability bis zur Verfügbarkeit eines Patches sieben Tage vergehen. Bis zum Patchen vergehen dann 37 Tage. Das ist extrem lange. Und es gibt ja nicht nur eine Vulnerability pro Jahr, sondern es gibt sie ständig. Das heißt, man ist im Grunde immer offen und man kämpft gegen die Zeit. Hier haben wir angesetzt. Wir verteilen die Patches nicht durch Client-Server-Modelle, sondern peer-to-peer. Das heißt, wir nutzen im Wesentlichen die Logik der bösen Jungs. Wir haben auf allen Windows-Maschinen einen kleinen Agenten, der screent entweder automatisch oder angestoßen durch den Administrator den Status der Maschine, sucht nach Schwachstellen, die noch nicht gepatcht sind und meldet sie zurück. Bei der automatisierten Version holt sich unser System den Patch und verteilt ihn viral im Netzwerk. Wir müssen natürlich auch warten, bis die Patches von den Herstellern verfügbar sind. Wir können nicht für Adobe oder Microsoft Patches schreiben. Wenn die Patches bzw. die Software verfügbar sind und sich die Größe der Software in einem vernünftigen Maß bewegt, dann können wir tatsächlich innerhalb von Stunden agieren.

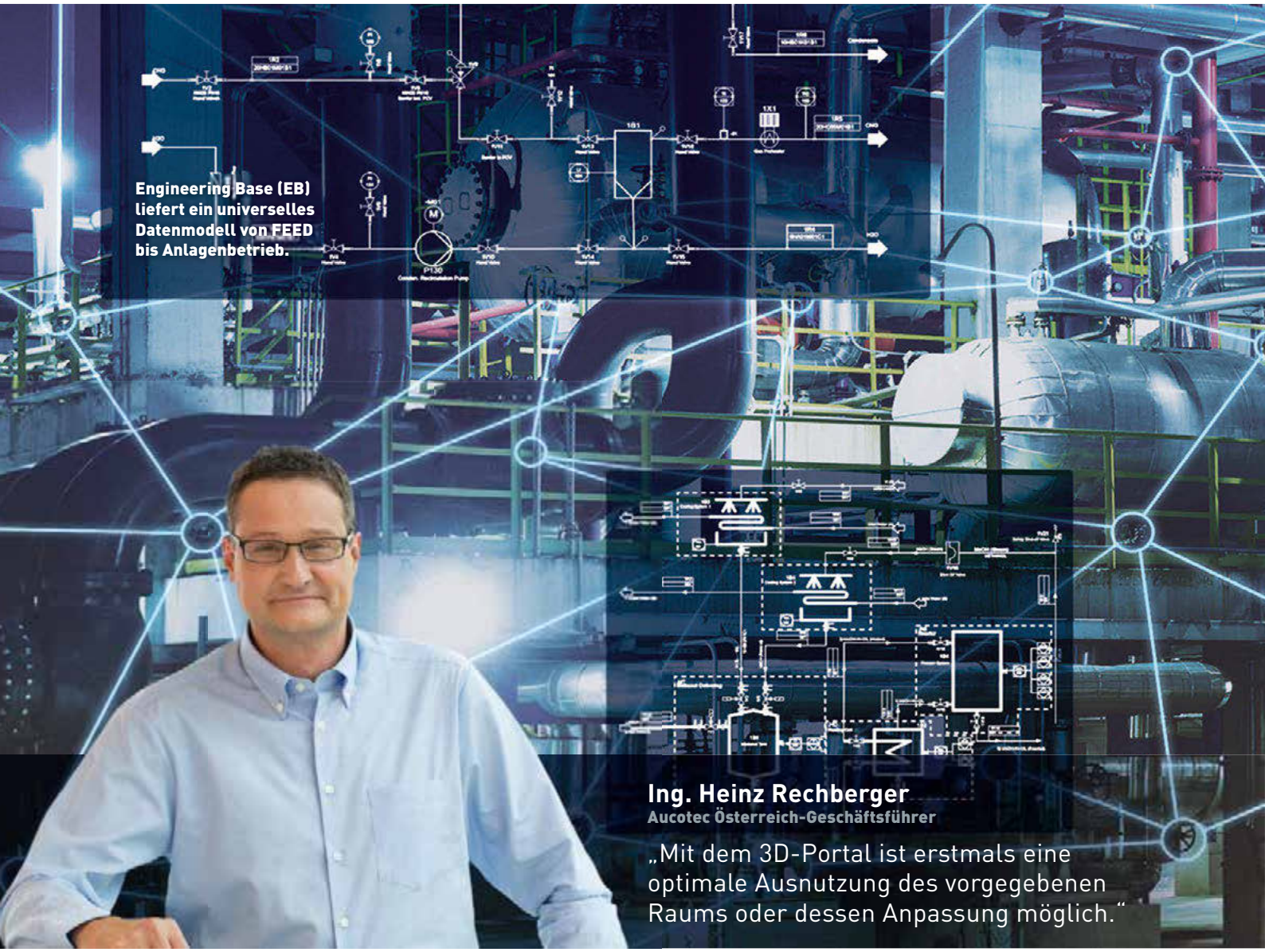
IoT: Auf was müssen Unternehmer achten, um für die Zukunft gerüstet zu sein?

Wiedemeyer: Erstens braucht es das Bewusstsein, dass ungeschützt zu agieren ein substanzielles Risiko für den Fortbestand des eigenen Unternehmens sein kann. Zweitens muss man Zeit, Geld und intellektuelle Kapazitäten in eine Security-Strategie investieren und in Richtung Automatisierung gehen, um die Schlagzahl zu erhöhen. Und drittens sollte man, insbesondere als produzierendes Unternehmen, auf dem Weg zu Industrie 4.0 den Security-Aspekt sehr gut beleuchten.

www.adaptiva.com

Torsten Wiedemeyer
Regional Director Central & Eastern Europe bei Adaptiva

„Absolut gefährlich sind jene Organisationen, die an der Intellectual Property eines Unternehmens interessiert sind."



BIG DATA ERFOLGREICH MANAGEN

Brownfield-Digitalisierung, Stillstandzeiten, Wartungs- und Umbau-Effizienz, Know-how-Sicherung: Die Herausforderungen an das Maschinen- und Anlagen-Engineering sind vielfältig und enorm. Das verlangt smarte Daten – und zwar schnell. Aber wie schafft man durchgängige, verlässliche Datenkonsistenz und -verfügbarkeit?

Bilder: © AUCOTEC

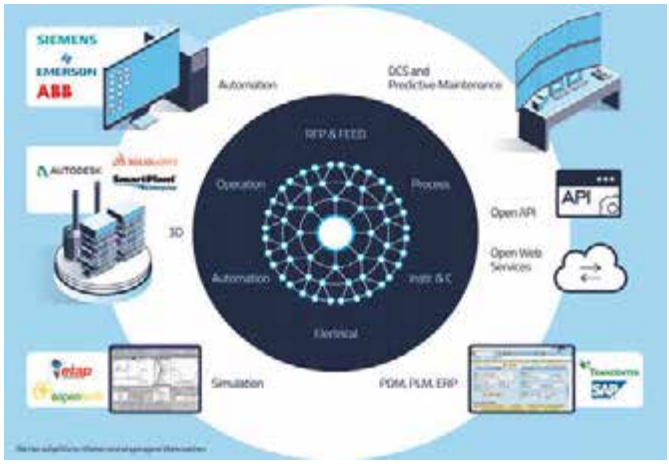
Das deutsche Software-Haus Aucotec AG hat die kooperative Plattform Engineering Base entwickelt, deren universelles Datenmodell als zentrales Element sämtliche Kerndisziplinen des Maschinen- und Anlagen-Engineerings vereint, den vollständigen digitalen Projektzwilling abbildet und konsistentes, simultanes Arbeiten auch global ermöglicht.

In allen Branchen – vom Planer bis zum Betreiber – wird Tag für Tag mit oft mehr als 100.000 Messstellen, zigtausenden dazugehörigen Folgedokumenten sowie entsprechenden Mengen an Geräten, Kabeln, Adern, Drähten oder Klemmen jongliert. Die meisten Objekte tauchen naturgemäß in mehreren Gewerken auf, doch teilweise nutzt jede Disziplin ihr eigenes System zur Datenentwicklung und -verwaltung. Das kostet nicht nur Zeit für Datenübergaben und Schnittstellenpflege. Es erschwert auch Änderungen und eine konsistente Gesamt-Dokumentation, die als Voraussetzung für die Betriebsgenehmigung einen belastbaren Nachweis des aktuellen As-built-Stands jeder Anlage liefern muss.

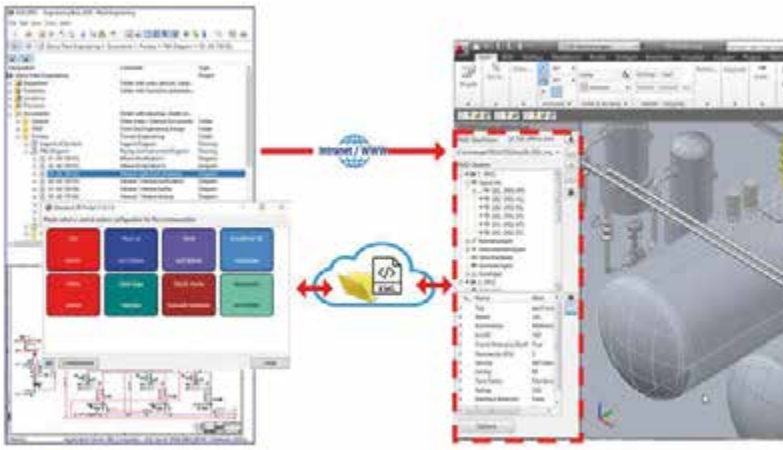
Wie viel ist Zeit wert? Stillstandzeiten werden oft länger als ein Jahr im Voraus geplant. Jeder Stillstand kann je nach Anlage pro Tag bis zu einer Million Euro Gewinnausfall verursachen. Schnellste Datenverfügbarkeit und gleichzeitig absolute Verlässlichkeit sind hier entscheidend, zum Umbau wie auch für die anschließende As-built-Dokumentation, um die Anlage wieder hochfahren zu dürfen. Hinzu kommt seit einigen Jahren eine steigende Fluktuation bei Betreibern von Brownfield-Anlagen. Billionen an Hardware-Werten haben in den letzten Jahren in Europa die Besitzer gewechselt – doch wo bleibt das Know-how zum Betrieb der Anlagen? Aus großen Standorten einzelner Industrieriesen werden Parks mit diversen Anlagen- oder Teilanlagen-Besitzern, die Nischen bedienen.

Als Beispiel sei die Grundstoffindustrie, die sich auf Asien und die USA fokussiert hat, genannt. Oft liefert hier ein zentraler Anlagenbetreiber die Infrastruktur. Die ersten denken bereits darüber nach, auch die Engineering-Software und Datenverwaltung als Service anzubieten, um sich bei Eigentumsübergängen optimal als Konstante präsentieren zu können. >>

Gut gelöst: EB bildet den gesamten Engineering-Lebenszyklus im Maschinen- und Anlagenbau ab.



Das universelle Modell in EB ist die Basis für alle Kerndisziplinen des Anlagen-Engineerings und die Kommunikation mit ergänzenden Systemen.



Aucotecs neues 3D-Portal vereinfacht die Verbindung von 2D- zu 3D-Engineering mit einem neuen Standard und beschleunigt den Austausch per Webservice.

Mit Pdf zum digitalen Zwilling? In den meisten Fällen erhält der neue Anlagenbetreiber bislang die Dokumentationen nur als „tote" Pdf oder gar Papierpläne. Diese Formate werden jedoch den intelligenten Logiken einer komplexen Anlage nicht gerecht. Daten sollten sich ihres Kontextes „bewusst", also „smart" sein. Selbst ohne Eigentümerwechsel wollen daher immer mehr Betreiber die Altdaten ihrer oft über Jahrzehnte existierenden Anlagen in ein System überführen, das in der Lage ist, den digitalen Anlagenzwilling durchgängig darzustellen – mit all seinen Vernetzungen, Logiken und leittechnikrelevanten Informationen.
Ein großer Anlagenbetreiber bezifferte einmal den Datenwert allein seines Kölner Standorts auf fünf Millionen Euro. Ein guter Grund, ihn zur optimalen Wertschöpfung zu modernisieren. Auch die Automatisierungs-Konfiguration spielt eine wichtige Rolle bei der Effizienz von Anlagenplanung und -betrieb. Das konsistente Zusammenspiel von Engineering- und Leitsystem-Software ist unter anderem eine der Voraussetzungen für effiziente Predictive Maintenance.

Verlässliche Daten. Wichtigste Konsequenz aus all diesen Herausforderungen ist: Verlässliche, smarte Daten sind alles. Dazu ist ein Engineeringsystem auf höchster Digitalisierungsstufe erforderlich, dass sie auf schnellstem Weg bereitstellt. Außerdem muss das System zudem Änderungen konsistent, unmittelbar und sicher in einen neuen As-built-Stand überführen – bei alltäglichen Wartungsaufgaben ebenso wie bei großen Umbauten.
Darüber hinaus muss es Anlagen-Know-how sichern, die Automatisierung nahtlos ins Engineering einbinden, Inbetriebnahmen effizient unterstützen und Webservices für Maintenance- und Managementaufgaben, aber auch für sicheres Engineering in der Cloud bieten. Aus all diesen Gründen bauen viele Betreiber von industriellen und infrastrukturellen Anlagen sowie Maschinenbauer auf die kooperative Plattform Engineering Base (EB) von Aucotec.

Digitalisierung ermöglichen. Der deutsche System-Entwickler hat mit dieser durchgängigen Lösung einen Nerv getroffen; besonders bei komplexen Anforderungen und höchsten Ansprüchen an Digitalisierung sind ihre Fähigkeiten gefragt. EB vereinheitlicht die System-Landschaft in den Unternehmen und eliminiert Fehlerquellen, da die Plattform sämtliche Kerndisziplinen der Anlagenplanung in sich vereint und durchgängig unterstützt. Von der ersten Anlagenidee über automatisierte Simulationsdaten-Integration, Prozess- und Detail-Engineering bis zu Leitsystemkonfiguration deckt EB alle Aufgaben ab. Das schafft wertvollen Zeitgewinn.
Grund für diese Fähigkeiten ist das universelle Datenmodell in EB. Jedes Objekt liegt nur einmal zentral in diesem Modell, das den kompletten digitalen Zwilling einer Anlage abbildet; bidirektionale Anbindungen an ergänzende Disziplinen wie 3D und ERP lassen sich ebenfalls integrieren. Das bedeutet, dass eine Entwicklung oder Änderung an nur einer Stelle im Plan sofort in sämtlichen Repräsentanzen des geänderten Objekts sichtbar ist: in Grafiken, Listen und Explorer. Im Zentrum stehen die Daten, nicht die Dokumente. Das sorgt auch für konsistente Cloudlösungen und Webapplikationen, die mobile Zugriffe und eine globale Zusammenarbeit ohne Grenzen erlauben. Als erste und einzige Plattform ohne Synchronisierungs- und Schnittstellenaufwand für alle Engineering-Kerndisziplinen ist sie ein wichtiger Digitalisierungs-Enabler der Big Data-getriebenen Prozesse.

www.aucotec.at

Interview

SO GEHT **BEEINDRUCKEND**

Aucotec Österreich-Geschäftsführer **Ing. Heinz Rechberger** spricht in einem Interview über das neue 3D-Portal in Engineering Base (EB) und welche auf der Hand liegenden Vorteile es bietet.

IoT 4 Industry & Business: Bisher war der Datenaustausch zwischen 2D- und 3D-Systemen nahezu unmöglich. Aucotec hat nun das 3D-Portal entwickelt. Was verbirgt sich dahinter?

Ing. Heinz Rechberger: Mit dem neuen 3D-Portal standardisiert Aucotec die Verknüpfung von 2D- und 3D-Engineering im Maschinen- und Anlagenbau. Damit ist es möglich einen 24/7-Datenaustausch mit allen gängigen 3D-Systemen sicherzustellen.

IoT: Und welche Vorteile bringt das dem Nutzer?

Rechberger: Mit dem 3D-Portal ist erstmals eine optimale Ausnutzung des vorgegebenen Raums oder dessen Anpassung möglich. Ob in großen Hallen oder im Schaltschrank: Der konkrete, physische Weg von Rohrleitungen, Kabeltrassen oder einzelnen Drähten muss für die Fertigung exakt berechnet und zuverlässig dokumentiert werden. Die dazugehörigen Anschlüsse finden sich dagegen in der 2D-Planung von EB.
Um nun eine konsistente Durchgängigkeit zu schaffen, muss eine sichere Verbindung zu den 3D-Systemen hergestellt werden, um den Datenaustausch zu vereinfachen und zu beschleunigen.

IoT: Welchen Ansatz hat Aucotec dafür gewählt?

Rechberger: Wir haben dazu zwei neue Wege gewählt. Zum einen wurde für EB eine eigene, standardisierte Kopplung entwickelt, die die 3D-Integration vereinfacht. Dieses neue „Tor" zu den 3D-Daten erlaubt über eine abgestimmte XML-Datei den Export von 2D-Informationen zum 3D-System und den Import relevanter 3D-Daten zu EB.
Es ist flexibel anpassbar und daher für alle gängigen Tools offen. Da jedes 3D-System andere Informationen braucht, sind verschiedene Vorlagen definierbar. Die grundsätzliche XML-Struktur bleibt dabei immer gleich."

IoT: Wie hoch ist dazu denn der Installationsaufwand?

Rechberger: Sehr gering. Auf 3D-Seite ist nur ein Plug-in nötig, das XML lesen kann. Die neutrale XML-Basis erfordert deutlich weniger Installationsaufwand und das Plug-in ist leichter zu pflegen als herkömmliche Schnittstellen. 2D- und 3D müssen sich nur auf dieselbe XML-Struktur einigen, damit das Lesen und Schreiben der Informationen funktioniert und für beide Disziplinen verständlich ist.

IoT: Würde sich dazu auch eine webbasierte Lösung anbieten?

Rechberger: Das ist unsere zweite Neuerung: der Webservice für den Datenaustausch. Im Normalfall muss ein Engineeringsystem gestartet sein, damit man auf seine Daten zugreifen kann. Das 3D-Portal gehört zu den ersten Microservices in EB, das heißt, dass es übers Web clientunabhängig funktioniert. Der spezielle 3D-Service ist wie eine extra Schicht in EBs-Architektur, über die man Daten jederzeit – natürlich mit den passenden Rechten – holen kann. Das ist für global verteilt arbeitende Disziplinen ebenso interessant wie für interne Netzwerke. Wartezeiten auf den Fachmann/die Fachfrau „am anderen Ende" sind passé. So öffnet das 3D-Portal nicht nur Tür und Tor für das gegenseitige „Verstehen" von zweiter und dritter Engineering-Dimension, sondern auch für mehr Flexibilität und Effizienz in der Anlagenplanung."

„VERTRAUEN IST GUT – KONTROLLE UND NACHWEIS SIND BESSER“

Viele Unternehmen, vor allem im Mittelstand, wissen nicht, auf welchem Software-Schatz sie sitzen. Dabei kommen sie durch Veräußerung ihrer Microsoft- Standardprogramme zu Geld, das sie etwa in strategisch sinnvolle IT-Neuanschaffungen stecken können. Gerade in wirtschaftlich angespannten Zeiten wie aktuell unter Covid-19 zahlt sich auf diese Weise freigewordenes Kapital aus.

Jan Minartz
Risk Advisor
Deloitte

Hirsa Navid
Director Sales Austria/Switzerland
Relicense AG

Jan Minartz, Risk Advisor Deloitte und Hirsa Navid, Director Sales Austria/Switzerland der Relicense AG skizzieren im Folgenden warum und wie Unternehmen ungenutzte Software-Assets rechtmäßig wieder zu Kapital machen.

IoT 4 Industry & Business: In Unternehmen finden sich aufgrund des Wechsels in die Cloud viele On-Premise-Lizenzen, die nicht mehr genutzt werden. Warum machen Unternehmen diese nicht einfach zu Geld?

Jan Minartz: Als Berater für Software-Asset-Management mit einem Fokus auf Microsoft kommen wir mit vielen Unternehmen in Kontakt und erleben selbst, auf welch enormem Schatz Unternehmen im Bereich Lizenzen sitzen. Durch den Gang in die Cloud liegen On-Premise-Lizenzen brach, die man nun zu Geld machen könnte. Die Herausforderung für Unternehmen ist jedoch, einen verlässlichen Partner für den Lizenzverkauf zu finden. Schließlich müssen beide Seiten sicher sein, dass ein transparenter und rechtssicher Prozess abläuft.

IoT: Das bedeutet konkret?

Minartz: Blickt man auf die großen Konzerne mit einem gut funktionierenden Lizenzmanagement, so haben diese den Lizenzverkauf bereits als Teil ihrer strategischen Beschaffungsorganisation etabliert. Vor allem diejenigen mit einem hohen Fokus auf die Marge ihrer Produkte nutzen Lizenzverkäufe strategisch. Dem Mittelstand fehlt hierbei vor allem die Erfahrung und auch die Sicherheit, den Verkaufsprozess erfolgreich anzugehen, obwohl sich gerade dort ein hohes Angebot an On-Premise-Lizenzen befindet.

Hirsa Navid: Ein weiterer Aspekt ist die fehlende Fachkompetenz. Sie ist in der Regel nur bei Unternehmen mit großer Rechts- und Einkaufsabteilung vorhanden. Lizenzverträge sind nicht leicht zu lesen, daher werden die darin aufgelisteten Bedingungen der Softwarehersteller oftmals nicht richtig interpretiert. Letztendlich führt es dazu, dass kleine und mittelständische Unternehmen meinen, sie dürften ihre Lizenzen gar nicht veräußern.

IoT: Warum sollten sich Unternehmen überhaupt mit dem Verkauf von gebrauchten Lizenzen beschäftigen?

Minartz: Software-Assets sind genauso liquide Mittel wie Maschinen und Hardware und sie sollten deshalb auch so ökonomisch wie möglich genutzt werden. Das bedeutet, Software abzustoßen, sobald sie nicht mehr benötigt wird.

Navid: Klar ist, jeder Geschäftsführer, der betriebswirtschaftlich sein Unternehmen führt, muss ökonomisch handeln. Im Bereich Hardware kauft niemand automatisch das teuerste und neueste Modell, wenn es keinen Mehrwert bietet. Dementsprechend sollte man sich auch von Software trennen, die aufgrund der Cloud-Strategie nicht mehr genutzt wird. Ein Rollback ist jederzeit möglich. Das Kapital, das durch die Veräußerung frei wird, kann reinvestiert werden.

IoT: Gibt es für Unternehmen beim Verkauf von Lizenzen Spezielles zu beachten?

Minartz: Unternehmen sollten wissen, dass es in Europa rechtens ist, seine Software zu verkaufen. Aber der Weiterverkauf muss ordnungsgemäß dokumentiert sein. Die Transfer- >>

kette vom Kauf mit dem entsprechenden Lizenz- aber auch Wartungsvertrag, mit den Nutzungsrechten der Softwareversionen, die im Umlauf sind, muss für den nächsten Käufer lückenlos nachvollziehbar sein. Nur so kann der neue Endkunde sicher sein, dass das Unternehmen das Nutzungsrecht auf ein bestimmtes Stück Software hat und dieses nun auch wieder veräußern kann.

Navid: Diese lückenlose Dokumentation ist sozusagen die Rückversicherung der Unternehmen, dass die Software rechtlich einwandfrei veräußert werden kann und letztendlich auch unsere Garantie als Wiederverkäufer.

IoT: Wie verschaffen sich Unternehmen nun aber einen Überblick über alle Lizenzen, die sie besitzen? Um in einem zweiten Schritt zu wissen, welche sie veräußern könnten?

Minartz: Hier beginnt vor allem bei mittelständischen Unternehmen die Schwierigkeit. Sie benötigen ein gutes Software-Asset-Management und dafür eine entsprechende Lösung. Nur dadurch wissen sie, welche Software aktuell im Umlauf ist, welche wirklich noch benötigt wird und welche aufgrund der aktuellen Unternehmensstrategie nicht mehr aktiv genutzt wird. Diese gilt es entsprechend herauszufiltern und zu dokumentieren. Wichtig ist zudem der Hinweis, um welche Art von Lizenzen (EA, MPSA, Open, Select) es sich handelt. Unternehmen müssen dazu alle Nachweise zu ihrer Eigentümerschaft, in welchem Land die Lizenzen gekauft wurden und ab wann sie verfügbar sind auflisten. Diese Liste zeigt ihnen, welche Produkte, Versionen und Stückzahlen sich zweifelsfrei rechtssicher übertragen lassen.

Navid: Diese Auflistung ist ohne entsprechendes Lizenzmanagement-Wissen kaum zu bewerkstelligen. Wir bieten den Unternehmen an, dass unsere Lizenzexperten sich genau die Lizenzverträge, aber auch Bilanzen in den Unternehmen anschauen. Sollten sie keine Bilanzen haben, unterstützen wir bei der Erstellung. Das ist ein entscheidendes Merkmal unseres Geschäftsmodells.

Bei der finalen Analyse kommt letztendlich auch unser Partner Deloitte ins Spiel, mit diesem Fachexperten an unserer Seite sichern wir uns auch selbst ab. Deloitte prüft für uns final die Rechtekette der Lizenzen, die zur Veräußerung stehen.

IoT: Wenn Unternehmen den Lizenzverkauf nicht ohne Partner angehen sollten, wie können Unternehmen letztendlich sicherstellen, dass sie mit einem vertrauenswürdigen Partner wie Relicense bei der Veräußerung von Softwarelizenzen zusammenarbeiten? Was zeichnet diesen aus?

Minartz: Wichtig ist, dass der An- und Verkaufspartner eine hohe Expertise im Bereich Lizenzmanagement und Wissen hat in Verwaltung und Betrieb von Software-Asset-Management- und Software-Lizenzlösungen, um die komplexe Welt der Microsoft-Lizenzmetriken richtig zu interpretieren. Ist er außerdem lange am Markt, besitzt eine ordentliche Gesellschaftsstruktur und das Kapital, Transaktionen im hohen Maße durchzuführen, ist das Unternehmen, das verkaufen möchte, mit dem Partner auf der sicheren Seite.

Navid: Natürlich ist eine Partnerschaft wie wir sie mit Deloitte haben, ein zusätzliches Qualitätsmerkmal. Alleiniges Ziel von

Deloitte ist und bleibt es, die ordnungsgemäße Abwicklung der Lizenztransfers zu überwachen.

IoT: Relicense arbeitet seit gut zwei Jahren mit Deloitte als einem unabhängigen Compliance-Partner zusammen. Wie kam es dazu?

Minartz: Bei unseren Audits und Wirtschaftsprüfungen in Unternehmen sehen wir immer wieder, dass Kunden ordnungsgemäß Gebrauchtsoftware nutzen möchten. Als Relicense auf uns zukam, um als deren unabhängiger Lizenzauditor im An- und Verkaufsbereich tätig zu werden, schloss sich der Kreis zu den an Gebrauchtsoftware interessierten Unternehmen.

Navid: Die Zusammenarbeit mit Deloitte ist ein wichtiges Qualitätsmerkmal unserer Arbeit und Firmenpolitik. Wir wollten die Lieferkette von Lizenzen von einem unabhängigen Dritten bewerten lassen, um unsere An- und Verkaufsprozesse transparenter zu gestalten. Die Auditerfahrung von Deloitte war einer der Gründe, das Unternehmen als Partner zu gewinnen. Die Beratungskompetenz sowie die Expertise, komplexe Vertragskonstrukte globaler Unternehmen zu interpretieren, sind weitere Gründe.

IoT: Wie und wann kommt Deloitte beim Ankauf von Lizenzen ins Spiel?

INFO

Der Weiterverkauf von Lizenzen ist in der EU klar geregelt und die Rechtskonformität durch EuGH und BGH bestätigt. Unternehmen können also ihre Softwarelizenzen unter folgenden Bedingungen wieder veräußern:

- Es muss sich um sogenannte getrennt verkehrsfähige Produkte wie MS Office 2016 Professional, CoreCAL 2019 User oder MS Vison 2016 Professional handeln.
- Die vom Hersteller vergebene Nutzungslizenz muss zeitlich unbeschränkt sein.
- Die Software muss rechtmäßig verbreitet worden sein.
- Die Software muss vom Weitergebenden bei sich selbst unbrauchbar gemacht werden.

Und die Unternehmen folgendes dokumentieren können:

- Offenlegung der detaillierten Lizenzkette des Ersterwerbers und intermediärer Eigentümer. Dadurch wird das entsprechende Nutzungsrecht im Abgleich mit den Produkt-Releases des Software-Herstellers abgeleitet.
- Offenlegung der relevanten Produktnutzungsrechte (abhängig von der Software-Asset-Laufzeit)
- Eigentums-/Löschungserklärung des Ersterwerbers und intermediärer Eigentümer
- Kauf-/Vertragsnachweise zum Abgleich der Transaktionsdaten

Navid: Wendet sich ein Unternehmen an uns, das seine Softwarelizenzen veräußern möchte, muss die Ankaufkette lückenlos nachvollziehbar sein. Eingebunden wird Deloitte grundsätzlich bei größeren Ankäufen bei mittelständischen Unternehmen und Konzernen, welche zu 90 Prozent die Lieferanten der letzten zwei Jahre spiegeln. Wir müssen wissen, ob es sich um eine ordnungsgemäß gekaufte Lizenz handelt, ob sie regelkonform genutzt wurde. Deloitte fungiert dabei als unsere unabhängige Kontroll- und Prüfinstanz, die wir einschalten, um letztendlich die Sicherheit zu haben, die Lizenzen ankaufen zu können.
Minartz: Basis jedes Lizenzgeschäfts ist das Urheberrecht. Es muss geklärt sein. Wir prüfen also, welche Ware der Kunde historisch gekauft hat – dabei darf es sich nur um Lizenzen aus dem europäischen Wirtschaftsraum handeln. Wir gleichen diese mit den aktuellen Produktrechten, Namen und Metriken ab und stellen fest, ob Lizenzketten inklusive Wartungsverlängerungen entsprechend vorhanden und gepflegt sind.

IoT: Wie läuft letztendlich ein optimaler Veräußerungsprozess ab?
Navid: Sobald ein Unternehmen uns seine Lizenzübersicht über die von ihm gekaufte Microsoft-Software mitteilt, prüft Deloitte diese Daten, um zu bestätigen, dass es tatsächlich das Nutzungsrecht auf ein bestimmtes Stück Software hat und dass die Kette seit dem ersten Kauf der Lizenz ununterbrochen ist. Deloitte prüft dabei, wann und wo die erste Lizenz tatsächlich gekauft bzw. in Umlauf gebracht wurde, und ob das Unternehmen hierfür ggf. die Software Assurance erneuern ließ. Daraus leitet sich im Detail das Nutzungsrecht ab.

IoT: Haben Sie ein Beispiel?
Navid: Angenommen, das Unternehmen glaubt, dass es das Recht auf Office 2019 hat, aber der Lizenzverlauf zeigt, dass es nur das Recht auf Office 2013 hat, weil die beiden letzten Software Assurance-Vereinbarungen mit Microsoft nie verlängert wurden oder die Software Assurance länger als einen Monat unterbrochen wurde. Weitergehende Nachweise konnten auch nicht beigestellt werden bzw. das Delta beheben.

IoT: Es gibt also keine Gründe, als Unternehmen nicht tätig zu werden und nicht mehr gebrauchte On-Premise-Lizenzen wieder zu Kapital zu machen?
Navid: Nein, gar keine. Läuft der Verkauf rechtskonform ab und kann das Unternehmen seine Lizenzhistorie lückenlos gemeinsam mit uns und Deloitte dokumentieren, steht einer erfolgreichen Veräußerung nichts im Wege. (bs)

www.relicense.com
www.deloitte.com

Auf der u-Control WEB ist die Real Time Engineering-Software mit integrierter Webvisualisierung sowie Applikationen wie Node-RED, OPC UA und der Fernwartungszugriff u-Link bereits am WEB-Server vorinstalliert.

„JEDES UNTERNEHMEN BESCHÄFTIGT SICH MIT DEM **EIGENEN OPTIMIERUNGSPOTENZIAL**“

Gerade jetzt ist eine Investition in die Digitalisierung und IoT-Fähigkeit mehr als jemals zuvor angebracht. Weshalb, besprach Wolfgang Weidinger, Geschäftsführer Weidmüller Österreich, mit IoT4 Industry&Business ausführlich in einem persönlichen – Abstands-konformen – Gespräch. Von Stephanie Englert

IoT4 Industry & Business: Die SPS ist für heuer „gelaufen“. Sie reiht sich ein in eine Vielzahl von Messen, die aufgrund der Corona-Pandemie nicht stattfinden bzw. digital, in einem Ersatzformat. Waren Sie überrascht?
Wolfgang Weidinger: Nein, nicht wirklich. Und wahrscheinlich ist die Absage dieser Messe auch, wie bei vielen anderen, eher von den Herstellern aus initiiert worden. Aufgrund Corona werden Reisetätigkeiten von vielen Unternehmen minimiert. Daher würden auch mit hoher Wahrscheinlichkeit etliche Besucher ausbleiben. Primär geht es allen Unternehmen um den Schutz der eigenen Mitarbeiter und um das Eindämmen der Corona-Pandemie.

IoT: Wann werden Messen, wie wir sie kennen, Ihrer Ansicht nach wieder stattfinden?
Weidinger: Das ist derzeit eine nicht zu beantwortende Frage. Dennoch gehe ich persönlich davon aus, dass frühestens Ende Q2 2021 wieder Messen stattfinden werden. Jeder Einzelne kann diesbezüglich momentan nur Prognosen abgeben, da geht es uns allen gleich.

IoT: Gilt diese Einschätzung auch für die Smart 2021 in Linz?
Weidinger: Sicherlich gilt dies auch ein Stück weit für die Smart in Linz. Wir als Weidmüller Österreich haben die Veranstaltung in unseren Planungen berücksichtigt; alles andere wird sich dann zeitnah zeigen, wie weit man mit der Entwicklung von Impfstoffen ist, wie weit entsprechende Sicherheitsvorkehrungen ausreichend sind und ob diese entsprechend eine Lösung sein werden bzw. inwiefern man Messen wieder durchführen kann.

IoT: Dennoch müssen auch Sie als Unternehmen planen und möchten Ihren Kunden Innovationen vorstellen. Was bleibt als Alternative?
Weidinger: Grundsätzlich gehe ich davon aus, dass es auch künftig Präsenzmessen geben wird. Dennoch müssen alle Hersteller ins digitale Umfeld gehen und hier Alternativen anbieten – etwa Online-Messen oder Webinare.
Aber es gibt auch Veranstaltungen, die kann man nicht als Webinar umsetzen, da fehlen Menschen vor Ort, die in den Trainingsprozess mit eingreifen. Aber auch hier kann man in

kleinerem Rahmen mit entsprechenden Sicherheitsvorkehrungen und Hygienekonzepten gut arbeiten.

IoT: Unabhängig von allen negativen Auswirkungen wird das vermehrte Telearbeiten nun auch als Push-Effekt für die Digitalisierung der Unternehmen herangezogen. Man geht davon aus, dass die Pandemie hier einen Entwicklungsschub bei vielen auslöst. Sehen Sie als Anbieter von entsprechenden Lösungen bereits eine Entwicklung in diese Richtung und eine erhöhte Nachfrage?

Weidinger: Wir als Weidmüller spüren diesen Effekt sehr stark und können bestätigen, dass die Nachfrage größer geworden ist. Jedes Unternehmen beschäftigt sich derzeit mit dem eigenen Optimierungspotenzial und Themen wie IoT und Digitalisierung. Die Frage: „Wo kann ich dieses für mich nutzen innerhalb der eigenen Produktion bzw. Maschinen?" – ist präsenter denn je und ein ziemlich „heißes" Thema.

IoT: Unbedingt „neu" ist es jedoch nicht.

Weidinger: Es gibt zahlreiche Firmen, die sich schon früher hiermit beschäftigt haben. Aber die breite Masse hat durchaus jetzt einen Denkanstoß erhalten und setzt sich nunmehr stärker mit den Themen wie Prozessoptimierung, Kosteneinsparungen, Effizienz auseinander. >>

Wolfgang Weidinger
Geschäftsführer Weidmüller Österreich

„Diesen Sprung in die Digitalisierung der Unternehmen hätten wir ohne die Corona-Pandemie ehrlicherweise so nie geschafft."

Die Lösungen von Weidmüller sind sowohl für Brown- als auch Greenfields geeignet.

Beim Thema IoT ist es eben auch der Fall, dass die Anlagen und Prozesse im Unternehmen zunächst IoT-fähig gemacht werden müssen, bevor man tiefer in das Thema einsteigt. Und hier gibt es eine breite Masse, die jetzt konkret beginnt das Thema IoT und Digitalisierung umsetzen zu wollen. Andere sind da schon etwas weiter.

IoT: Das bedeutet?
Weidinger: Als Unternehmen müssen Sie erst einmal schauen, welche Daten vorhanden sind, welche erfasst werden sollen und wie ich diese erfasse. Weiters stellen sich die Fragen: Wo fasse ich diese Daten zusammen bzw. wie verarbeite ich diese? Wie gebe ich diese weiter und schlussendlich welche Geschäftsmodelle kann ich daraus entwickeln? Diese Antworten müssen schon gegeben sein.

IoT: Und wie wissen Unternehmen, ob der Schritt in die Digitalisierung und IoT für sie der richtige ist?
Weidinger: Weidmüller hat eine Industrial Analytics-Abteilung. Hier geht es um das Projektgeschäft. D.h., wir schauen uns mit dem Kunden eine Anlage an und kreieren anschließend ein Proof-of-Concept. Und in Folge dessen wird dann auch die Frage beantwortet, ob sich für den Kunden ein Business Case ergibt und sich eine Investition in Richtung „IoT" lohnt und Potenzial vorhanden ist.

IoT: Gilt diese digitale Weiterentwicklung auch für Weidmüller selber?
Weidinger: Auf jeden Fall. Auch wir haben unser Know-how aufgrund interner Projekte und Prozessoptimierungen entwickelt. Die Corona-Pandemie und die Umstände, die sie mitbringt, hat unsere Arbeitsweise verändert. Alleine durch die vermehrte Telearbeit, die wir wahrscheinlich so in der Form nicht so rasant schnell umgesetzt hätten, sind wir ein gutes Stück weitergekommen. Wir sind nun sehr gut aufgestellt und können den neuen Herausforderungen im Arbeitsalltag bestens begegnen – auch für unsere Kunden.

IoT: Was bietet Weidmüller Kunden konkret für den Bereich Digitalisierung und IoT an?
Weidinger: Wie haben beispielsweise beim Thema Fernwartung oder webbasierte Steuerungen sehr gute Lösungen im Angebot. Hier handelt es sich um eine lizenzfreie Lösung, bei der die Softwareumgebung auf der Steuerung selbst vorhanden ist.

IoT: Welche Vorteile bietet sie?
Weidinger: Der einfache Weg ins webbasierte Engineering ist die u-control-Lösung von Weidmüller, denn sie ist zukunftssicher, autark und modular; sozusagen eine Steuerung für kleine und mittlere Automatisierungsaufgaben. Sie reduziert den anlagenweiten Datenverkehr, ist unempfindlich gegenüber Störungen im Netzwerk, erleichtert die Fehlersuche und lässt sich sehr gut mit manuellen Prozessen kombinieren. Der Kern dieser webbasierten Steuerung ist es, die IoT-Themen abzudecken, sprich: Daten sammeln und vorverarbeiten, aufbereiten und diese in einer Cloud oder auf dem eigenen Server bereit zu stellen. Den Schnittstellen sind durch die offene webbasierende Kommunikation keine Grenzen gesetzt.

IoT: Das bedeutet, der Anwender ist nicht ortsgebunden und kann flexibel arbeiten?
Weidinger: Das ist richtig aber nicht nur das. Er ist auch Hersteller-ungebunden, was die Automatisierung betrifft. Die Webanbindung der Steuerung ermöglicht es von jedem Standort, mit jedem Endgerät, unabhängig vom Betriebssystem und Hersteller auf Maschinen zuzugreifen. Diese Unabhängigkeit wird durch die Verlagerung der Software vom PC auf die Steuerung sowie durch die Nutzung offener Webtechnologien erreicht. Mit HTML5, CSS3 und JavaScript lässt sich jede Anlage unabhängig von Betriebssystemen überwachen und programmieren.
Auf der u-Control WEB ist die Real Time Engineering-Software mit integrierter Webvisualisierung sowie Applikationen wie Node-RED, OPC UA und unser Fernwartungszugriff „u-Link" bereits am WEB-Server vorinstalliert. Durch die auf der Hardware – also der Steuerung – integrierte Software wird keine zusätzliche Software am Rechner benötigt, lediglich ein Display mit Webbrowser.
Das dürfte auch jenen Programmierern das Leben erleichtern, die mit den Kompatibilitäten der verschiedenen Engineering-Tools zu kämpfen haben. Gleichzeitig benötigt der Anwender keine zusätzlichen Lizenzen oder Wartungsverträge. Das spart dauerhaft Kosten und bietet immense Vorteile.

IoT: Wie sehen Sie sich als Anbieter dieser Lösung im Vergleich zu den Marktbegleitern? Lösungen gibt es für IoT-Ansätze ja genügend.
Weidinger: Sicherlich gibt es einige große Hersteller am Markt, die die Implementierung von IoT-Lösungen auch längst vorantreiben, dies sind aber meist Konzepte, die auf eine Einbindung in die eigene Steuerungswelt abzielen. Im Vergleich zu anderen Nicht-Weidmüller-Lösungen ist es so, dass wir in dieser Form der Flexibilität und Offenheit die einzige webbasierte, industrietaugliche Steuerung am Markt anbieten und somit einen besonderen Stellenwert einnehmen. Wir haben diese Lösung auch in den Weidmüller-Workshops kürzlich thematisiert, natürlich alles unter Einhaltung der bereits erwähnten, geltenden Hygiene-Richtlinien. Aber diese kleinen, aber feinen Events haben eindeutig gezeigt, dass ein großes Interesse und auch der

Bedarf, sich bei diesem Thema auszutauschen, vorhanden ist. Unsere Webcontroller-Node-RED-Workshops sind lokal aufgeteilt und werden in den einzelnen Bundesländern angeboten.

IoT: Und was kann Node-RED?
Weidinger: Node-RED hat sich in der Vergangenheit als beliebte Entwicklungsplattform für IoT-Anwendungen etabliert und sich den Weg in Industrieanwendungen gebahnt. Wir als Weidmüller setzen bei der Anbindung an das IIoT auf diese bekannte Technologie. Es ist das Tool der Wahl, um Daten aus der Steuerung in das IoT zu transportieren und Anwendungen im IoT-Bereich mit einem Baukastensystem umzusetzen. Die Programmierung erfolgt über einzelne Funktionsbausteine (Nodes). Diese werden einfach durch das Ziehen von Verbindungen kontaktiert.
Eine Vielzahl an mitgelieferten und frei verfügbaren Nodes deckt die meisten gängigen Dienste und Technologien ab. Dabei bietet vor allem die Offenheit und die Möglichkeit den Bibliotheksumfang selbst zu erweitern, dem Anwender die gewünschte Flexibilität seine Daten zu verarbeiten und an die gewünschte Stelle zu kommunizieren.
Beispielhaft kann man hier OPC UA, MQTT oder auch E-Mail-Kommunikation nennen. Auch direkte Schnittstellen zu Steuerungen, Diensten oder Applikationen anderer Hersteller, seien es nun Messanger-Apps, Webseiteninhalte oder SPS-Protokolle, sind kein Hindernis. Durch die Möglichkeit der Implementierung von JavaScript ist auch eine gewisse Unabhängigkeit von vorgefertigten Lösungen möglich, was wiederum die Vielseitigkeit unserer Lösung erhöht.

IoT: Nun stellt sich auch immer die Frage: Kann ich eine IoT-Lösung auch in bestehende Anlagen integrieren?
Weidinger: Unsere Lösungen sind sowohl für Brown- als auch Greenfields geeignet. Ob über die beiden getrennten Fast Ethernet-Schnittstellen, modular erweiterbare, digitale oder analoge Eingänge, serielle Schnittstellen oder dezentrale IP67

Der einfache Weg ins webbasierte Engineering ist die u-control-Lösung von Weidmüller, denn sie ist zukunftssicher, autark und modular.

IO-Module. Sie können also sehr wohl nachrüsten und aber nicht in bestehende Steuerungen eingreifen, wenn das nicht erwünscht ist.

IoT: Wenn sich ein Unternehmen nun dazu entscheidet, aus seinen Daten künftig neue Geschäftsmodelle zu kreieren und mittels IoT einen Schritt in die Zukunft zu gehen, braucht man auch Datenanalysten bzw. grundsätzlich geeignetes Fachpersonal. Wie sehen Sie hier die Lage am Markt?
Weidinger: Datenanalytiker oder auch Mathematiker sind nach wie vor wenig vorhanden und selbige mit Domänenwissen noch spärlicher gesät. Die Experten-Nachfrage ist groß, das Angebot wächst nur langsam.
Wir als Weidmüller haben hier ein Automated Machine Learning-Tool entwickelt, dass einem Domain-Experten oder eben Automatisierungstechniker dabei hilft, auch ohne abgeschlossenem Mathematikstudium mit tiefgreifendem Heuristik- und Statistik-Know-how ein entsprechendes mathematisches Modell zu erstellen. Die Erfahrung hat aber gezeigt, dass auch Analysten selbst auf dieses Tool als Benchmark oder Anhaltspunkt zugreifen um Modelle zu vergleichen. Somit möchten wir dem Spezialisten-Mangel etwas entgegenwirken und auch kleinen und mittleren Unternehmen die Chance geben, für die Zukunft gerüstet sein.

www.weidmueller.at

Wolfgang Weidinger
Geschäftsführer Weidmüller Österreich
„Nicht jedes Thema kann als Digitalformat umgesetzt werden. Oft benötigt man Techniker vor Ort."

WER HAT ANGST VORM HACKER?

„Hacken“ ist im Trend. Wer etwas auf sich hält, gibt sein Wissen insofern preis, als dass er die „Gehackten“ im Anschluss des Feldversuches darauf hinweist, wo ihre Schwachstellen sind. Diesen Prozess würde man dann als White-Hat-Hack bezeichnen. Doch was genau verstehen wir unter diesem Begriff? Von Stephanie Englert

Die zunehmende Digitalisierung hat zur Folge, dass sich neueste Technologien in Unternehmen verbreiten und vielerorts auch aus der Ferne gearbeitet werden kann. Das macht auch Sinn. Was jedoch nicht unbedingt parallel stattfindet, ist die Entwicklung für ein Bewusstsein dafür, dass man als Unternehmen und einzelner Mitarbeiter bzw. dass auch die Gesamtanlage eines Betriebes zur Zielscheibe werden. Weshalb? Weil auch das Thema Hacking immer ausgeklügelter wird. Doch es gibt auch hier zwei Welten, die guten Hacker und die bösen Hacker. Die SEC Consult Group ist als einer der führenden Berater im Bereich Cyber- und Applikationssicherheit weltweit bekannt und in den vergangenen Monaten mehr als gefragt gewesen. Covid-19 verstärkte die Vulnerabilität vieler. Zu den Kunden von SEC Consult zählen führende Unternehmen, Behörden und Organisationen aus verschiedensten Sektoren der Privatwirtschaft sowie der kritischen Infrastruktur. Der Spezialist für IT-Security ist an mehreren Standorten ISO 27001 CREST-zertifiziert. Als Sicherheitsberater schützt das Unternehmen wertvolle Informationen seiner Kunden durch Engagement, Fachwissen und Innovationskraft, meint Ulrich Fleck, CRO des Unternehmens mit Sitz unter anderem im 19. Bezirk in Wien.

IoT 4 Industry & Business: Herr Fleck, was versteht man unter dem Begriff „White-Hat-Hacker“ und wie sehr sehen Sie den Begriff „ethisches Hacking“ hiermit gut in Verbindung gebracht?
Ulrich Fleck: Beides bedingt einander, denn ein White-Hat-Hacker betreibt ethisches Hacking. Entsprechend der den Wildwestfilmen entnommenen Symbolik, in der der schwarze Hut die Bösen kennzeichnet und die Guten immer einen weißen Hut tragen, setzen White-Hat-Hacker ihre Fähigkeiten ein, um Unternehmen oder Organisationen vor Schaden zu bewahren.
Zwar greifen sie wie ihre kriminellen Pendants, die „Black Hats“, ebenfalls Systeme an – allerdings im Gegensatz zu diesen nur mit Erlaubnis des Kunden und um allfällige Schwachstellen in dessen Netzwerken sowie in Soft- und Hardware zu finden.

IoT: Das bedeutet, ...

Fleck: ... dass die Experten unserer ethischen Hackerteams weltweit – an unserem Hauptsitz in Wien und allen Niederlassungen in Europa, den USA und Asien – sich nicht nur mit dem Eindringen in Systeme begnügen und der Beurteilung der Sicherheitslage, sondern sie nehmen die Netzwerke quasi auseinander und versuchen sie auch zu verstehen.
In unserem Vulnerability Lab widmen wir uns der Analyse aktueller Bedrohungen und entwickeln entsprechende Vorgehen und Analysewerkzeuge, so können wir uns immer wieder einen internationalen Know-how-Vorsprung im Bereich der Netzwerk- und Applikationssicherheit gegenüber den Angreifern verschaffen.

IoT: Was ist das Ziel von dieses Ethical Hacking?

Fleck: Kurz gesagt: mögliche Einfallstore ins jeweilige System zu entdecken und ein Assessment der vorhandenen Schwachstellen durchzuführen. Die Informationen dazu werden sowohl an den Auftraggeber weitergegeben als auch an die Hersteller möglicherweise betroffener Hard- oder auch Software.
Wenn diese anhand der Hinweise unserer Mitarbeiter Patches – Korrektur-Updates zum „Beheben" bekannt gewordener Fehler und Sicherheitslücken – schneller entwickeln können, ist nicht nur dem jeweiligen Kunden gedient, sondern in weiterer Folge auch dem Hersteller betroffener Hard- oder Software und dessen andere Kunden. All dies erfolgt natürlich unter Ausschluss der Öffentlichkeit, um Cyberkriminellen nicht den roten Teppich auszulegen.

IoT: Mit welchen Herausforderungen im Zuge der Covid-19-Pandemie haben Ihrer Erfahrung nach die CIOs, die IT-Verantwortlichen von Unternehmen, Behörden oder anderen Organisationen besonders zu kämpfen?

Fleck: Eine der größten und immer noch aktuellen Herausforderungen ergibt sich daraus, dass viele Unternehmen die Umstellung auf Homeoffice in kürzester Zeit umgesetzt haben, um ihre Geschäftstätigkeit nicht zu gefährden. Geschäftskritische Informationen und essenzielles Wissen mussten sehr schnell über neue und andere Systeme verbreitet werden, was Cyberkriminellen eine besondere Angriffsfläche bietet.
Auch wenn Homeoffice-Lösungen mittlerweile vielfach etabliert sind und operativ und administrativ problemlos laufen, sollte nicht vergessen werden, dass die zu Beginn der Umstellung akuten Gefahren für die IT-Sicherheit aktuell genauso akut sind wie vor einem halben Jahr.
Vor allem mit Blick auf Herbst und Winter ist abzusehen, dass sich – je nach Bedrohungslage und Corona-Präventionsmaßnahmen – Phasen der Präsenz am Arbeitsplatz mit Zeiten im Homeoffice abwechseln werden. Hier sollten sich auch bisher von Angriffen verschont gebliebene Unternehmen und Behörden nicht in Sicherheit wiegen, sondern sich weiterhin um größtmögliche IT-Security, sowohl vor Ort als auch remote an den Heimarbeitsplätzen, bemühen. Hinzu kommt, dass, sei es in Unternehmen wie auch in Privathaushalten, immer mehr IoT-Geräte in Gebrauch sind, die gefährliche Einfallstore für >>

Treffen kann es alle: Plötzlich haben Hacker zugeschlagen und fordern Lösegeld.

das gesamte Netzwerk darstellen. Egal ob Netzwerkkameras oder Router, jedes Gerät ist ein potenzieller Angriffspunkt, den es abzusichern gilt. Spezielle Analyse-Plattformen wie etwa der IoT-Inspector ermöglichen die aktive Suche nach Sicherheitslücken in der Firmware dieser Geräte, Schutzmaßnahmen, wie z.B. Firewall-Konfigurationen, können dann rechtzeitig daran angepasst werden.
SEC Consult bietet eine Reihe von Tests an, die eine kritische Überprüfung der IT-Infrastruktur ermöglichen: Wir unterziehen Anwendungen einer Bewährungsprobe, identifizieren Schwachstellen und zeigen Lösungen zur Beseitigung von Sicherheitslücken auf.

IoT: Worauf müssen sich Unternehmen künftig besonders einstellen?
Fleck: Im Zuge der Corona-Krise kam es zu einem sprunghaften Anstieg potenziell gefährlicher E-Mails. Eine wesentliche Ursache dafür ist der „Faktor Mensch", denn in Zeiten großer Unsicherheit sind Kontaktaufnahmen, die Schutz vor einer Gefahr versprechen, besonders effektiv.
So waren etwa auch mit Malware bestückte Landkarten im Umlauf, die vermeintlich die Verbreitung des Corona-Virus visualisierten, und E-Mails mit betrügerischer Absicht rund um Corona-Wundermittel oder angeblich besonders viel Schutz bietende Masken machten die Runde. Gleichzeitig fällt das Schwarmwissen per „Flurfunk" im Homeoffice weg, wenn einander die Kollegen nicht mehr beim zufälligen Treffen auf dem Gang oder in der Kaffeeküche vor seltsamen Mails warnen können. Umso wichtiger wird es in Zukunft sein, die Awareness für die IT-Sicherheit zu erhöhen.

IoT: Das bedeutet wiederum, ...
Fleck: ... dass bereits bestehende Maßnahmen intensiviert und Heimarbeitsrichtlinien ausgearbeitet werden sollten bzw. aktualisiert gehören. Allen Mitarbeitern muss bewusst sein, dass das Unternehmensnetzwerk durch diese Situation exponiert und damit verwundbarer als sonst ist. Die Kollegen aus der IT alleine können das Problem nicht lösen, wenn ihre Bemühungen – wenn auch unabsichtlich – von den anderen torpediert werden. IT-Security ist nicht nur Sache des IT-Verantwortlichen, sie muss ganzheitlich betrachtet werden – die Angriffe betreffen ja auch alle.

IoT: Meinen Sie, dass durch die Pandemie „endlich" das Thema IT-Security in Unternehmen einen höheren Stellenwert erreicht hat und ernst genommen wird?
Fleck: Ich denke schon, dass vielen im Verlauf der Umstellungsphase zum Teleworking bewusst geworden ist, welchen Stellenwert eine funktionierende und sichere IT-Infrastruktur für den Bestand ihres Unternehmens hat. Dieses Netzwerk ist angreifbar und verletzlich und etwa ein Systemausfall oder auch Erpressung können die Existenz des Unternehmens gefährden und zum Verlust von Arbeitsplätzen führen. Wichtig wird sein, dieses Bewusstsein nach dem hoffentlich nicht allzu weit entfernten Ende der Covid-19-Krise aufrechtzuerhalten, Cyberkriminelle werden auch weiterhin nach Wegen suchen, massiven Schaden anzurichten.

https://sec-consult.com/unternehmen

Bilder: ©SEC Consult

Ulrich Fleck,
Geschäftsführer von SEC Consult Österreich

„IT-Security ist nicht nur Sache des IT-Verantwortlichen, sie muss ganzheitlich betrachtet werden."

KURZ ERLÄUTERT

Couchbase ist zum einen eine dokumentenorientierte nicht-relationale Datenbank (NoSQL-Datenbank), die Informationen in Form von JSON-Dokumenten speichert. Zum anderen handelt es sich um das Unternehmen Couchbase, Inc., das die Software weiterentwickelt und kommerzielle Produkte sowie Services rund um die Lösung anbietet. Couchbase-Datenbanken eignen sich für interaktive Anwendungen.

„NoSQL BÜGELT DIE SCHWÄCHEN RELATIONALER DATENBANKEN AUS“

In einem Kurzinterview mit Steffen Schneider, dem Senior Solutions Engineer Central Europe bei Couchbase, wird eines deutlich: ein großer Vorteil bei der Einführung einer NoSQL-Datenbank mit verteilter Architektur besteht darin, dass sie schneller, einfacher und kostengünstiger skalieren kann als eine relationale Datenbank. Von Stephanie Englert

IoT 4 Industry & Business: Ganz generell Herr Schneider: Was sind NoSQL-Datenbanken und seit wann gibt es sie?
Steffen Schneider: Der Begriff NoSQL, damals noch im Sinne von „no SQL“, wurde erstmals 1998 für eine einfache Open-Source-Datenbank verwendet, die keine SQL-Zugriffsmöglichkeit bereitstellte. Heute verbirgt sich hinter der Abkürzung NoSQL der englische Begriff „Not only SQL“. Gemeint sind Datenbanksysteme, die die Schwächen relationaler Datenbank-Management-Systeme (RDBMS) wie die mangelnde Tabellenflexibilität ausbügeln. Sie sind besonders gut darin, hohe Datenvolumina aus semi- und unstrukturierten Daten mit vielen Schreib- und Lese-Operationen zu bearbeiten.

IoT: Und welche Vorteile ergeben sich daraus?
Schneider: Einer der Hauptvorteile bei der Einführung einer NoSQL-Datenbank mit verteilter Architektur besteht darin, dass sie bei wachsendem Zugriffsvolumen deutlich schneller, einfacher und kostengünstiger skalieren als eine relationale Datenbank.

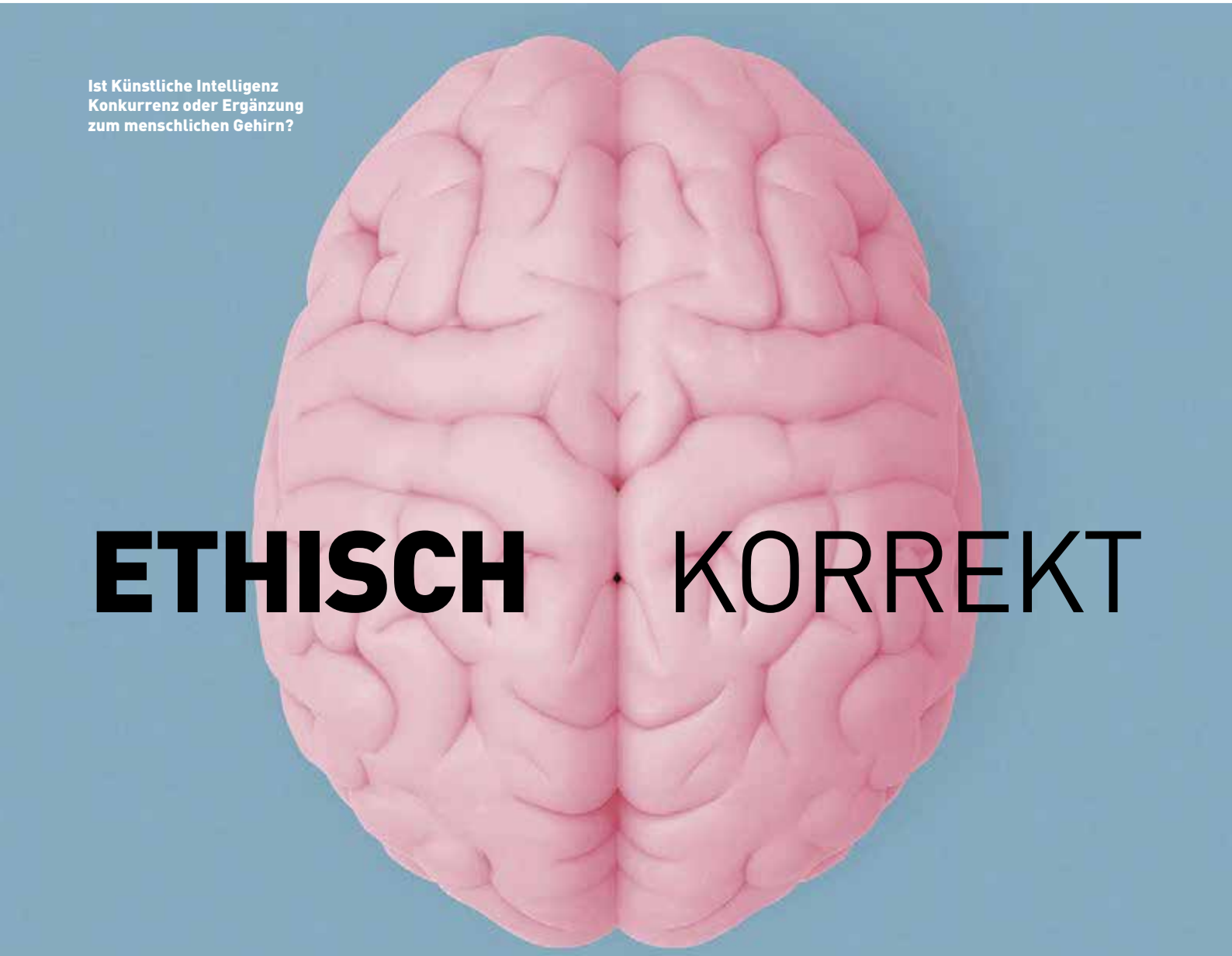
Steffen Schneider,
Senior Solutions Engineer Central Europe bei Couchbase

„Big Data braucht eine NoSQL-Datenbank.“

IoT: Mit IoT einher gehen auch große Mengen an Datenbanken. Was können NoSQL-Datenbanken hier im Besonderen leisten?
Schneider: Das Internet der Dinge – oder eben IoT – stellt hohe Anforderungen an die Datenbank, angefangen von dem Erfassen von Daten in Echtzeit über die Verarbeitung von Streaming-Events bis hin zur Sicherung größerer Mengen von IoT-Geräten und -Daten. Relationale Datenbanken sind damit mehr oder weniger überfordert. Sie werden zum Bottleneck, denn eine passende Datenbank sollte Caching und Key-Value-Store unterstützen. Eine NoSQL-Datenbank bringt auch die für IoT zwingend notwendigen Aspekte wie etwa Flexibilität; das heißt, es können problemlos unterschiedliche Datentypen und Strukturen verwendet werden, lineare Skalierbarkeit sowie die notwendige hohe Verfügbarkeit für Schreibvorgänge werden geboten.

IoT: Für welche Unternehmen bzw. Branchen kommen diese Datenbanken in Frage?
Schneider: Die Entscheidung für oder gegen eine NoSQL-Datenbank hängt weniger von der Branche ab, sondern vielmehr von der jeweiligen Anwendung. Geht es um Applikationen am Front-end wie E-Commerce mit vielen Interaktionen, einem entsprechend hohen Datenvolumen und der Notwendigkeit kurzer Reaktionszeiten, sind NoSQL-Datenbanken die erste Wahl. Auch bei unstrukturierten Daten beziehungsweise dem wilden Daten-Mix von heute haben sie ihren großen Auftritt. Sehr einfach formuliert, kann man sagen: Big Data braucht eine NoSQL-Datenbank. Entsprechend setzen Unternehmen aus dem Gesundheitswesen, der Finanzbranche, dem Online-Handel oder der Automobil- und Maschinenbauindustrie diese Datenbanken ein.

www.couchbase.com



Ist Künstliche Intelligenz Konkurrenz oder Ergänzung zum menschlichen Gehirn?

ETHISCH KORREKT

Bosch hat Anfang des Jahres einen KI-Kodex als Leitlinie für seine intelligenten Produkte ausgegeben. Christoph Peylo, Leiter des Bosch Center of Artificial Intelligence, erklärt im Gespräch, was vertrauenswürdige KI (Künstliche Intelligenz) bedeutet und dass seiner Meinung nach der Mensch Teil von Entscheidungsprozessen bleiben muss.

IoT 4 Industry & Business: Bei Künstlicher Intelligenz denkt man als Laie oft an Cyborgs, die ganz intelligente Sachen machen. Was bedeutet KI in Wirklichkeit?

Christoph Peylo: Ja, da hat die Filmindustrie gute Arbeit geleistet (lacht). Mit der Wirklichkeit hat das wenig zu tun. Bei Bosch verstehen wir unter Künstlicher Intelligenz etwas ganz anderes. Wir wollen vielmehr Künstliche Intelligenz auf die dingliche Welt anwenden, also physische Produkte oder Maschinen mit intelligenten Algorithmen kombinieren, damit sie intelligente Entscheidungen treffen können.

Zu Künstlicher Intelligenz gehört mittlerweile ganz viel. Man versucht das Verhalten, das man als intelligent empfindet, auf verschiedene Hardwareebenen zu implementieren. Lernen gehört natürlich dazu. Man kann ja ganz verschiedene Sachen lernen: Lernen aufgrund von Ähnlichkeiten, aufgrund von Fehlern, aufgrund von statistischen Gegebenheiten und Häufigkeitsverteilungen. Und da kann KI natürlich helfen. Aber auch Themen wie entscheidungsunterstützende Systeme, Wissensverarbeitungen, Sprachverarbeitung, Sprache verstehen sind auch Aspekte von Künstlicher Intelligenz.

IoT: Sie haben einmal in einem Beitrag geschrieben: Man muss an vertrauenswürdiger Künstlicher Intelligenz arbeiten. Was meinen Sie damit?
Peylo: Künstliche Intelligenz kann die Lebensqualität von Menschen in ganz unterschiedlichen Bereichen verbessern. Sie kann helfen, Arbeit leichter, Verkehr sicherer, Gebäude energieeffizienter zu machen. Eine Voraussetzung dafür ist, dass die Lösungen akzeptiert werden und Menschen ihnen vertrauen. Was versteht man aber unter Vertrauen? Auf die Industrie bezogen, kommt man hier dem Begriff der Produktqualität sehr nahe. Wenn Sie etwa ein Elektrowerkzeug von Bosch Power Tools kaufen, dann machen Sie das, weil Sie von der Produktqualität überzeugt sind, dass Sie sich nicht verletzen werden, dass es ein gutes Werkzeug ist. Das bedeutet Vertrauen in ein Produkt und das versuchen wir auch mit KI umzusetzen.

IoT: Der Kunde hat aber auch über Jahrzehnte gelernt, dass ein Bosch-Werkzeug verlässlich ist.
Peylo: Das stimmt. Qualität und Verantwortung sind traditionelle Stärken von Bosch. Jetzt wollen wir zeigen, dass sich daran auch und gerade mit KI nichts ändert. Unser Leitbild „Technik fürs Leben" und die menschlichen Bedürfnisse stehen weiterhin im Vordergrund. Dafür gibt unser KI-Kodex klare Leitlinien vor. Dazu gehört die Beachtung nationaler und internationaler Gesetze, aber auch die Orientierung an unseren eigenen Werten. Durch den Einsatz von Künstlicher Intelligenz ändert sich daran nichts. Das heißt, die Produkte werden nicht unberechenbarer, sondern ganz im Gegenteil: Die Produkte werden eigentlich noch besser, weil sie sich noch besser an das anpassen, was der Kunde braucht. Und unsere oberste Leitlinie „Technik fürs Leben" bleibt unangetastet. Und das – denke ich – ist für uns ein ganz wesentlicher Aspekt einer vertrauenswürdigen KI. Von unserem Firmengründer Robert Bosch stammt der im Unternehmen oft verwendete Satz, dass es der Sinn hinter der Technik ist, dem Menschen zu dienen und das Leben für den Menschen besser zu machen. Bei Bosch hat es Tradition, sich mit gesellschaftlichen Fragen zu befassen und sie in den Produkten umzusetzen. Unser Anspruch ist, Innovationen und gesellschaftliche Verantwortung zu verbinden. Das ist untrennbar.

IoT: Kennen Sie auch andere Stimmen, die sagen: Die Maschine ist viel intelligenter als der Mensch. Den brauchen wir nicht mehr?
Peylo: Ich kenne diese Stimmen, stimme ihnen jedoch nicht zu. Die Künstliche Intelligenz, die uns heute zur Verfügung steht, ist vor allem auf die Erfüllung klar definierter Aufgaben ausgerichtet. Sie ändert die Herangehensweise an Probleme nicht. Stattdessen greift sie auf Methoden zurück, die ihr für die Lösung von konkreten Problemen zur Verfügung gestellt werden. KI ist also eine Ergänzung zur menschlichen Intelligenz. Es geht uns um die Zusammenarbeit zwischen Mensch und Maschine – also um die intelligente Mannschaft. Darüber hinaus ist es für uns enorm wichtig, dass der Mensch bei allen Entscheidungsprozessen der KI die Kontrolle behält.

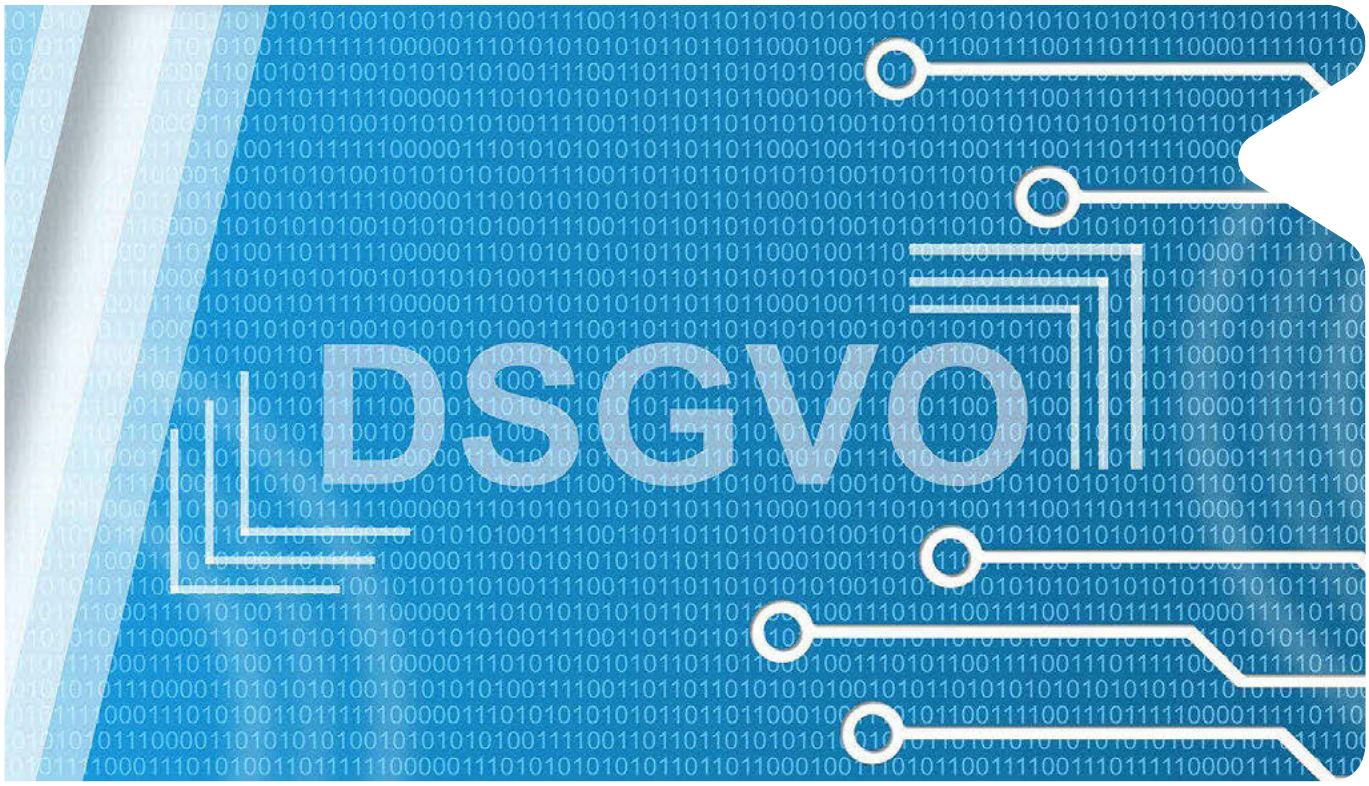
IoT: Welche Formen der Zusammenarbeit zwischen Mensch und Maschine gibt es?
Peylo: Wir unterscheiden drei Fälle. Erstens gibt es „human in command", da dient KI nur der Entscheidungsunterstützung. Ähnlich wie in Navigationssystemen, die Ihnen Routen vorschlagen, Sie aber den Weg bestimmen. Zweitens „human in the loop". Das heißt, dass der Mensch in den Entscheidungsprozess eingebunden bleibt, ähnlich wie bei einem intelligenten Parkassistenten. Sie können sich vom Auto einparken lassen, aber jederzeit eingreifen. Und drittens gibt es noch „human on the loop". Hier wird tatsächlich die Entscheidung delegiert, der Mensch kann die Entscheidung im Nachgang jedoch nachvollziehen und bei Bedarf das System anpassen; etwa wie bei Airbag- oder Notbrems-Systemen. Wir wollen, dass der Mensch immer Teil von Entscheidungsprozessen ist und bleibt.

IoT: Ein anderes Thema. Nach Corona wird uns auch weiter das Klima beschäftigen. Wie weit kann Künstliche Intelligenz beim CO_2-Sparen ihren Beitrag leisten?
Peylo: In einer gewachsenen Werksstruktur mit vielen lokalen Steuerungen und einem heterogenen Maschinenpark ist es schwierig alle Maschinen in optimalen Betriebszuständen laufen zu lassen und die Übersicht zu bewahren. Künstliche Intelligenz kann hier sehr helfen, indem man genügend Datenpunkte in der Gebäude- oder Produktionssteuerung aufnimmt und dann anhand dieser Datenpunkte optimiert. Das heißt: diese Datenaufnahmepunkte wirken wie virtuelle Sensoren. Hier kann KI unterstützen und enorme Einsparungen realisieren. (bs)

www.bosch.at

Christoph Peylo
Leiter des Bosch Center of Artificial Intelligence

„Künstliche Intelligenz kann die Lebensqualität von Menschen in ganz unterschiedlichen Bereichen verbessern."



VERTRAUEN SCHAFFEN

Search Guard ist ein Open-Source-Plug-in für den Schutz von Elasticsearch-Clustern beim Einsatz im Bereich Enterprise Search. Und Jochen Kressin ist Geschäftsführer der floragunn GmbH, dem Hersteller des Security-Plug-ins Search Guard. In puncto Daten, Datenschutz und DSGVO ist er mit zwei wachsamen Augen und Ohren unterwegs. Weshalb, erläutert er in einem Gespräch mit Stephanie Englert.

IoT 4 Industry & Business: Welches sind die größten Herausforderungen denen sich Unternehmen ob der DSGVO immer noch stellen müssen, vor allem in Bezug auf Big Data?
Jochen Kressin: Zwei Aspekte machen CIOs im Hinblick auf Big Data und DSGVO zu schaffen: exponenziell steigende Datenmengen innerhalb kurzer Zeit und die Tatsache, dass sowohl personenbezogene Daten, so genannte PII-Daten, als auch sensitive Informationen wie IP-Adressen in vielen verschiedenen Systemen und auch in Logfiles gespeichert sind.

IoT: Was sind die Folgen?
Kressin: Die Folgen daraus sind, dass Unternehmen oft gar nicht wissen, wo genau PII-Daten gespeichert sind und wer darauf Zugriff hat. Wie sollen Daten so geschützt oder Datenlecks rechtzeitig erkannt werden? Diese Vorgehensweise wird wider besseres Wissen in Kauf genommen, obwohl sie zwei zentralen Bestandteilen der Grundverordnung widerspricht. Dazu gehören, den Zugriff auf personenbezogene Daten nachverfolgen zu können und zu reglementieren und das „Recht auf Vergessenwerden", also als Kunde von einem Unternehmen die Löschung eigener Daten verlangen zu können.

Das Risiko, die Anforderungen der DSGVO nicht erfüllen zu können, ist damit sehr hoch und Verstöße dagegen leider an der Tagesordnung.

IoT: Was bedeutet das in Folge?
Kressin: Dass die vielleicht größte Herausforderung für IT-Entscheider sein wird, Management, Führungskräfte und Mitarbeiter im eigenen Unternehmen zu sensibilisieren. Es braucht die Awareness, dass der Vertrauensverlust, der bei Datendiebstahl oder zweckentfremdeter Verwendung bei den Kunden entsteht, einen höheren Schweregrad hat, als sechs- oder siebenstellige Bußgelder.

IoT: Stellt Big Data für den Datenschutz denn auch ein mögliches Datenrisiko dar?
Kressin: Es ist so: Steigende Datenmengen bedeuten immer ein steigendes Datenrisiko. Big Data ist heute aber branchenübergreifend eine wichtige Grundlage für die Planung effizienter und wirtschaftlicher Unternehmensprozesse.
Aus der Analyse von Umsatzströmen werden Personaleinsatzpläne abgeleitet, Warenlieferungen und Lagerkapazitäten

geplant und Prognosen errechnet. Nicht immer sind Big Data personenbezogenen und nicht für alle Analysen müssen sie personenbezogen sein.
Gerade in einer Pandemie, wo der physische Kontakt mit Kunden stark eingeschränkt ist, suchen Unternehmen jedoch den digitalen Kontakt zum Kunden und sammeln gezielt Informationen. Hacker wissen das. Wer seine Kundendaten nicht schützt, ist jetzt leichte Beute für Angriffe, denn mit dem Verkauf personenbezogener Daten erzielen Cyberkriminelle den größten Gewinn.

IoT: Wie kann man dem vorbeugen?
Kressin: Es kommt darauf an zu wissen, wo personenbezogene Informationen gespeichert sind. Im zweiten Schritt muss das System bestmöglich vor inneren und äußeren Angriffen geschützt werden.
Eines der meist genutzten Tools zur zentralen Speicherung und Analyse großer Datenmengen sind Elasticsearch-Datencluster. Die Verantwortung für die DSGVO-konforme Speicherung und Bearbeitung der Daten liegt jedoch bei dem Unternehmen, dass die Daten erhebt und bearbeitet.

IoT: Ist man generell sensibler in puncto Hackerangriffe geworden und inwiefern gewährleisten Lösungen wie Search Guard ein risikofreies Arbeiten?
Kressin: Die Sensibilität für die weitreichenden Folgen eines Hackerangriffs haben sich in den letzten Jahren nur bedingt verbessert. In Organisationen ab zirka 1.000 Mitarbeitern teilen viele Führungskräfte die Meinung, dass sich die IT-Sicherheitslage im eigenen Unternehmen mit Einführung der DSGVO verbessert hat, wie der Deloitte Cyber Security Report 2019 zeigt.
Trotzdem gelingt es nicht, Datenlecks zu schließen und Datendiebstahl im großen Stil zu vermeiden. Dies zeigt der Fall von Conrad Electronic. Im November 2019 wurde bekannt, dass Angreifer monatelang Zugriff auf fast 14 Millionen Kundendatensätze hatten, die in einer Elasticsearch-Datenbank gespeichert waren. Search Guard ist der einzige Anbieter, der Features zur DSGVO-konformen Bearbeitung von Daten in Elasticsearch anbietet. CIOs können damit Sicherheitsrisiken reduzieren und die Compliance ihres Unternehmens erhöhen.

IoT: Inwiefern?
Kressin: Als Security-Plug-in ist es unser Ziel Daten, die in einem Elasticsearch-Cluster gespeichert sind, vor unberechtigtem Zugriff und Diebstahl zu schützen. Mit unseren Kunden teilen wir die Auffassung des „Prinzip des geringsten Privilegs". Zugriffskontrollen sollten es autorisierten Benutzern ermöglichen, nur auf die minimal notwendigen Informationen zuzugreifen, die für die Ausführung von Arbeitsaufgaben erforderlich sind.

IoT: Wird Smart Data somit zum Thema bei Unternehmen, hervorgerufen durch die DSGVO-Bestimmungen?
Kressin: Smart Data sind „sortierte" Daten, die gesammelt, geordnet und analysiert worden sind. Dies kann die Ursache in DSGVO-Bestimmungen haben, muss aber nicht notwendigerweise so sein.

IoT: Welche technischen Herausforderungen müssen bedacht werden, um Daten DSGVO-konform bearbeiten zu können?
Kressin: Die wichtigsten Ansprüche, die Kunden gegenüber Unternehmen in Bezug auf ihre Daten haben sind, das Recht zu erfahren, wer auf ihre Daten zugegriffen hat, wann und warum, welche Daten gespeichert wurden, wie sich diese im Lauf der Zeit verändert haben und die nachweisliche Löschung der eigenen Daten.
Voraussetzung, um Informationen, die in einem Elasticsearch-Cluster oder in Logfiles gespeichert sind, gemäß der gesetzlichen Vorschriften zu verwalten und zu bearbeiten, sind folgende: eine rollenbasierte Zugriffskontrolle (RBAC) für jeden Index, eine Zugriffskontrolle auf PII-Dokumente und PII-Felder, die Verschlüsselung und Anonymisierung von Daten sowie die Verfolgung des Datenzugriffs und der Datenänderungen. Zudem die Protokollierung von Datenlöschungen, das Überwachen der Datenzugriffe auf Anomalien und eine zeitnahe Meldung dieser. Die Search Guard Compliance Edition deckt diese Anforderungen ab. Je nach zugewiesener Rolle werden Felder mit PII oder sensiblen Daten wie Klarnamen, Email-Adressen und Kreditkartendetails unberechtigten Benutzern nicht angezeigt, wenn Dokumente, die diese Informationen enthalten, aufgerufen werden.

https://search-guard.com

Hier geht es zur Langfassung:

Jochen Kressin
Geschäftsführer floragunn GmbH

„Es braucht die Awareness, dass der Vertrauensverlust bei Datendiebstahl einen höheren Schweregrad hat, als sechs- oder siebenstellige Bußgelder."

KRISE? NEIN DANKE!

Bastian Karweg hat eine Vision: Jedes Unternehmen soll in die Lage versetzt werden, systematisch externe Informationen, aktuelle Ereignisse und sich stetig verändernde Daten automatisch und in Echtzeit auszuwerten und nutzbar zu machen.

IoT 4 Industry & Business: Herr Karweg, was treibt Sie an, auch in herausfordernden Zeiten zu expandieren?
Bastian Karweg: Ich glaube, dass wir als Software-Unternehmen ein Teil der Lösung sind. Digitalisierung ist aktuell genau der Weg, wie Unternehmen trotz der Krise Geschäfte machen können.
Auch wenn Messen ausfallen oder der Außendienst nicht zum Kunden fahren kann, hat man mit Echobot dennoch die Möglichkeit, sein Business fortzuführen. Das ist auf der einen Seite für uns als Anbieter sehr positiv, auf der anderen Seite auch für unsere Kunden, weil sie mit Echobot durch diese schwierige Zeit kommen. Aus diesem Grund haben wir uns dazu entschieden, gerade jetzt unsere Investitionen zusätzlich hochzufahren. denn wir haben bemerkt, dass die Pandemie unsere Produkte begünstigt und die Nachfrage steigt. In dieser Zeit zu investieren, ist also das absolut Richtige.

IoT: Weshalb jetzt auch noch der Schritt nach UK?
Karweg: Großbritannien ist für uns das Sprungbrett für die Internationalisierung. Im nächsten Schritt wollen wir europäisch agieren. Englisch als Weltsprache ist dabei die erste logische Wahl, weil sie nicht nur den UK-Markt, sondern die internationalen Märkte stark öffnet. Und irgendwo muss man anfangen.

IoT: Aber es folgt der Brexit.
Karweg: Großbritannien ist auch gerade deswegen spannend, weil aktuell mit dem Brexit-Thema viel in Bewegung ist. Firmen aus Großbritannien müssen sich ebenso neu orientieren, wie sie künftig Geschäfte mit Europa machen. Hier wollen wir Lösungsanbieter sein und uns gleichzeitig für andere Märkte in der Zukunft rüsten. Wir erwarten diesbezüglich einen sehr starken Wachstumsschub und sehen in der Internationalität eine langfristige Perspektive und eine große Chance.

IoT: Inwiefern hat Sie die Corona-Pandemie zum Umdenken bewegen müssen?
Karweg: Homeoffice funktioniert viel besser als erwartet! Und die Leute sind sehr kreativ in der Art und Weise wie sie Homeoffice und ihre Organisation in verschiedenen Teams organisieren. Ich denke, dass Corona auch unser Recruiting in Zukunft beeinflussen wird, da es uns in die Lage versetzt, auch Leute zu rekrutieren, die primär an anderen Standorten arbeiten. Aktuell ist eine Kollegin nach Mallorca umgezogen und zwei weitere arbeiten in Kanada. Früher wäre das ein Problem gewesen. Mittlerweile ist das selbstverständlich.
Wir möchten neue Kollegen hauptsächlich zum Onboarden vor Ort holen. Das ist eine Sache, die sicherlich zum Umdenken bewegt.

IoT: Ist die Digitalisierung nun auch schneller vorangeschritten, wie prophezeit?
Karweg: Man überlegt sich schon, wie schnell die Digitalisierung durch die Krise plötzlich vorangeschritten ist. Jeder musste auf das Thema reagieren und hat es irgendwie hinbekommen. Denn: Wenn man will, dann geht es auch!

IoT: Was erwarten Sie sich 2021?
Karweg: In Bezug auf Echobot erwarten wir viel Wachstum, ein neues Büro, neue Kunden, neue Kollegen sowie ein starkes Changemanagement. Es ist einfach ein großer Unterschied, ob eine Firma aus knapp 30 oder 100 Personen besteht. Das heißt, wir werden uns da neu sortieren und organisieren müssen – darauf bin ich schon sehr gespannt!
Nach außen blickend erhoffe ich mir natürlich, dass wir irgendwann zur Normalität zurückkehren können. Ich hoffe, wir werden die Pandemie überwinden oder zumindest Wege finde, besser mit ihr zu leben. Ich wünsche mir diesbezüglich mehr Positivität und einen gestärkten Blick in die Zukunft. (se)

www.echobot.de

Bastian Karweg
Geschäftsführer Echobot

„Ich denke, dass Corona auch unser Recruiting beeinflussen wird."

4. IoT- FACHKONGRESS:

CORONA, TRACING UND DIE SACHE MIT DER PRIVATSPHÄRE ...

Um Infektionsketten nachverfolgbar zu machen, erfassen Tracing Apps persönliche Kontakte. Das Handling der erfassten Daten ist derzeit höchst unterschiedlich und heftig umstritten. Was fehlt, ist ein einheitlicher Standard. Am 4. November wird beim 4. IoT- Fachkongress Austrian Standards dazu diskutiert. Der Autor ist Herbert Hirner.

Die Andeutung einer möglicherweise verpflichtenden Nutzung von „Corona-Apps" hat die Diskussion über Bürgerrechte und Datenschutz in Österreich angefacht. Tracking und Tracing sind dabei die Schlüsselbegriffe: „Klassische" Tracking Apps dienen dazu, den Aufenthaltsort von Personen zu überwachen und aus dem Kontext Daten abzuleiten. Für die Warnung vor einem potenziellen Ansteckungsrisiko ist eine derart weitreichende Überwachung allerdings überschießend. „Um Infektionswege aufzuspüren, ist es wesentlich sinnvoller, sich auf ‚Contact Tracing' zu beschränken", erklärt Andreas Petersson. „Damit lässt sich die Begegnung von zwei Geräten mittels Bluetooth und Ultraschall sehr gut quantifizieren. Es wird dabei nur festgehalten, welche zufällig vergebenen ‚Identitäten' einander ‚gesehen' haben", erklärt der Dezentralisierungsexperte und Geschäftsführer von Capacity Blockchain Solutions.

Thema Datenerfassung. Im Gegensatz zu Tracking Apps, wo die Optimierung von Werbung im Vordergrund steht, dient die Datenerfassung bei Tracing-Anwendungen ausschließlich der Gesundheit der Nutzer. Wie man eine solche Anwendung richtig realisiert, hat Andreas Petersson im Verein Novid 20 gezeigt, wo er an der Entwicklung der gleichnamigen Open Source Tracing App beteiligt war. Anfang 2020 waren zum Thema Contact Tracing allerdings noch keine Standards vorhanden. „Wir haben deshalb die Strategie verfolgt, durch Zusammenarbeit mit der europäischen Corona-App-Initiative PEPP-PT internationale Kompatibilität herzustellen", erklärt Petersson.

Andreas Petersson ist Managing Director bei Capacity Blockchain Solutions.

Contact-Tracing-Schnittstelle als erster Schritt. Mit der im April veröffentlichten Contact Tracing-Schnittstelle von Apple und Google (GACT) lag schließlich ein Quasi-Standard vor, auf den Programmierer aufsetzen konnten. Die Schnittstelle beinhaltet Verbesserungen bei der Privatsphäre und bietet einige essenzielle Vorteile für Entwickler. Allerdings ist sie nur für den Betrieb mit einer einzigen – von Gesundheitsbehörden erstellten – App ausgelegt. Ein praxisnaher, länderübergreifender Datenaustausch zum Schutz und zur Warnung von Reisenden ist damit (derzeit) nicht möglich.

Einheitliche europäische Standards: fehlendes Commitment in Europa. Dass sich die GACT-Schnittstelle dennoch als Quasi-Standard etablieren konnte, liegt hauptsächlich an fehlendem Commitment in Europa. Denn um einen einheitlichen europäischen Standard erarbeiten zu können, wäre ein eindeutiges Bekenntnis der Gesundheitsbehörden dazu notwendig, erklärt Petersson. Darum werde man aber auch in Zukunft nicht herumkommen, ist er überzeugt, denn „die Privatsphäre hört auch in herausfordernden Zeiten nicht auf zu existieren". Wie Novid 20, das in Georgien unter dem Namen „Stop Covid" als Tracing App eingesetzt wird, diese Herausforderung gemeistert hat, verrät Andreas Petersson beim IoT-Fachkongress am 4. November.

IoT-Fachkongress– erstmals virtuell. Der 4. IoT-Fachkongress – „Mit Standards in die Zukunft" findet am 4. November 2020 erstmals als Online-Veranstaltung statt. Neben dem Vortrag von Andreas Petersson stehen auch Live Best Practices auf dem Programm, unter anderem zu Security by design, Artificial Intelligence, Industrie 4.0, IoT und IIoT, Predictive Maintenance, Open Innovation, Tracking und weiteren Themen.

www.austrian-standards.at

4. IoT-FACHKONGRESS

Wann?	**4. November 2020, 9 bis 14 Uhr**
Wie?	**Digital, live und interaktiv**
Anmeldung:	**www.austrian-standards.at/iot**

Mit der virtuellen Konferenz Explore. hat Sick erstmals in der Branche ein zusammenhängendes Bild zum Thema Digitalisierung geschaffen.

ERFOLGREICH DURCH DEN DIGITALISIERUNGS-DSCHUNGEL

Mit der virtuellen Konferenz Explore. kreierte Sick erstmals in der Branche ein zusammenhängendes Bild zum Thema Digitalisierung. In der Vergangenheit wurde zu diesem Thema bereits viel präsentiert, ein konkreter und ganzheitlicher Ansatz fehlte bis dato.

Der Industrie 4.0-Maturity-Index ist ein Leitfaden für eine erfolgreiche digitale Transformation und besteht aus fünf Schritten. Er verfolgt einen gesamtheitlichen Ansatz, und ermöglicht es jedem Unternehmen zu eruieren, an welchem Punkt der Digitalisierung es steht und dementsprechend Ansätze zu finden, um sich weiterzuentwickeln. Denn unabhängig davon, an welchem Punkt ein Unternehmen steht, für jedes ist die digitale Transformation realisierbar und ein wichtiger Schritt für den zukünftigen Unternehmenserfolg. Wichtig dabei ist, sich nicht auf einzelne Produkte, sondern unvoreingenommen auf ganzheitliche Lösungen zu konzentrieren.

Maturity-Index – in fünf Schritten zur Digitalisierung. Konnektivität, Sichtbarkeit, Transparenz, Prognosefähigkeit und Adaptierbarkeit – in dieser Reihenfolge geht es in Richtung Digitalisierung. Hier darf kein Schritt übersprungen werden, denn es gilt: Ohne Sensoren und Konnektivität gibt es keine Daten – ohne Daten keine Visualisierung und Transparenz – und ohne Digitalisierung keine Industrie 4.0.

Explore. – die virtuelle Konferenz. Im Rahmen der Explore., die Ende Oktober stattfand, hat Sick die Inhalte basierend auf dem Maturity-Index in zwei parallelen Tracks zielgruppenspezifisch aufbereitet: einen für Techniker und Experten und einen für Manager und Entscheider. Für alle, die nicht bei der virtuellen Konferenz dabei sein konnten, gibt es die Möglichkeit, die einzelnen Sessions nachzuhören unter https://s.sick.com/ag-en-virtual-conference-explore.

Konnektivität – der Schlüssel zu Industrie 4.0. Technikern wird dabei gezeigt, wie sie Konnektivität Realität werden lassen können, was die Grundlagen für eine erfolgreiche Integration sind und wie die Sensoren parametriert und integriert werden. Für Manager wird hervorgehoben, dass Daten Konnektivität brauchen und warum es ihre Aufgabe sein sollte, diese Grundlage für Digitalisierung zu schaffen, um die Entwicklung in ihrem Unternehmen voranzutreiben. Mit der Vorstellung von realisierten Kundenprojekten wird gezeigt, wie Dank Konnektivität die Produktivität gesteigert werden kann.
Es werden intelligente Sensoren benötigt, die, über das gewöhnliche I/O-Signal hinausgehend, bidirektional kommunizieren können. Hier kommen IO-Link und die smarten Sensoren von Sick ins Spiel. Sie erfassen reale Betriebszustände, wandeln diese in digitale Daten um und stellen sie der Prozesssteuerung zur Verfügung.

Sichtbarkeit/Visualisierung – was passiert auf meiner Maschine? Im technischen Part wird hervorgehoben, wie einfach Sensordaten visualisiert und diese Daten für eine vorausschauende Wartung herangezogen werden können. Im Management-Part tauschen sich die Teilnehmer über die Möglichkeit von Industrie 4.0 Retrofitting bei bestehenden Maschinen und Anlagen aus und welche Vorteile die Visualisierung und die Anbindung von bestehenden Maschinen an die IIoT-Welt bringt.
Hier punktet FieldEcho, ein Dashboard mit moderner, webbasierter Benutzeroberfläche, das über Browser dargestellt oder in das HMI der Maschine integriert werden kann. FiledEcho visualisiert alle konfigurierten IO-Link-Master sowie angeschlossenen IO-Link-

Sensoren bzw. -Aktuatoren und bietet einen detaillierten Einblick in die Daten – Alarmfunktionen inklusive. Beste Visualisierung bietet auch die Monitoring Box. Sie erlaubt einfaches Condition Monitoring und Datenanalyse ohne die Notwendigkeit von Programmierkenntnissen.

Transparenz – warum passiert es? In diesem Abschnitt erfahren Techniker, wie man mit Hilfe digitaler Monitoring Services eine kontinuierliche Zustandsüberwachung für Sensoren und Maschinen implementieren und dadurch Echtzeitanalysen durchführen kann. Durch die Zustandsüberwachung wird volle Transparenz im Warenfluss und damit maximale Effizienz in der Produktionslogistik ermöglicht. Managern wird das Potenzial von Big Data und Transparenz aufgezeigt und wie dadurch neue Geschäftsmöglichkeiten entstehen. Mit realisierten Use Cases zeigt Sick, wie dies bei Kunden umgesetzt wurde. Auch hier kommen wieder FieldEcho und die Monitoring-Box zum Einsatz.

Prognosefähigkeit und Adaptierbarkeit: Was wird passieren? Und wie kann autonom reagiert werden? Präsentiert wird, wie Techniker ihre erste Deep Learning-Applikation implementieren und wie sie komplexe Daten nutzen können. Im Manager-Part werden anhand realer Kundenbeispiele die Vorteile von Konnektivität, Transparenz und Datenmanagement gezeigt und wie man dadurch für das gerüstet ist, was passiert.
Anwendungsorientierte Softwarelösungen ermöglichen Vorhersagen. Etwa, das künftige Versagen einer Komponente oder die Planung eines Serviceintervalls, damit es erst gar nicht so weit kommt. Damit sorgt „Analytics“ von Sick für eine höhere Systemperformance, eine Beschleunigung von Entscheidungsprozessen und eine verbesserte Lieferanten-Compliance dank einfachem Bild- und Datenaustausch. Automatisierte Reaktionen und Maßnahmen verlangen nach entsprechend innovativen Software-Lösungen, wie zum Beispiel einer KI, die eine Maschine laufend überwacht und optimiert. Ausgesuchte Beispiele und Anwendungen gibt es bereits heute schon. So setzt Sick etwa in der Bildverarbeitung auf Deep Learning.

Unabhängig davon, an welchem Punkt ein Unternehmen steht, für jedes ist die Digitalisierung umsetzbar.

Der Sick IntegrationSpace. Kunden stehen heute vor Herausforderungen, die mit klassischer Automatisierungstechnik rund um Sensorik, Logik und Aktorik nicht mehr viel zu tun haben. Es geht vielmehr darum, den Geschäftsprozess so zu gestalten, dass er erheblich effizienter wird. Dafür sammelt der Sensor Daten die helfen, das Problem zu lösen und bringt sie auf die Datenebene. Die Plattform Sick IntegrationSpace ermöglicht den Zugriff auf die virtuelle Repräsentanz des Sensors und seiner Daten. Damit eröffnet der Lösungsanbieter eine neue Dimension in der Welt von Sensoren. In dieser Dimension werden die Daten der Sensoren in intelligente digitale Services integriert. Mit kontinuierlich weiterentwickelten digitalen Services, aufbauend auf Sick AssetHub und LiveConnect, werden die Möglichkeiten kundenindividuell nutzbar. Die gewonnene Transparenz der Sensordaten bietet die Grundlage für neue Optimierungspotenziale in den Geschäftsprozessen. Die Plattform Sick IntegrationSpace bietet dem Kunden eine einfache und selbstständige Verwaltung und Buchung der digitalen Services.

Mit dem Maturity-Index kann jedes Unternehmen eruieren, an welchem Punkt der Digitalisierung es steht.

www.sick.at

Mit einer Fernwartungslösung ist ein Servicetechniker im Wartungsfall innerhalb kurzer Zeit mit der Anlage verbunden und kann die Ursache schnellstmöglich beheben.

FERNWARTUNG STATT FLUGTICKET

Die Globalisierung schreitet mit großen Schritten voran. Dennoch hat sich in der jüngsten Vergangenheit gezeigt, dass es nicht immer problemlos möglich ist, spontan von A nach B zu fliegen. Maschinenbauer müssen trotzdem für Servicearbeiten bei Kundenmaschinen vorbereitet sein. Doch wie?

Ist eine Maschine beim Kunden fertig installiert, haben Maschinenbauer in den meisten Fällen wenig bis gar keine Verbindung mehr zu ihren ausgelieferten Maschinen. „Viele Maschinenbauer schrecken vor Fernwartungslösungen zurück, da sie als kompliziert gelten und ein vermeintliches Sicherheitsrisiko darstellen“, sagt René Blaschke, Produktmanager für IoT bei B&R. Oft werden bei der Fernwartung sensible Maschinendaten über das Internet übermittelt, was für viele der Grund ist, auf Fernwartung zu verzichten. Dabei kostet jede Minute Stillstand den Betreiber bares Geld. Diese Kosten könnten durch Fernwartung auf ein Minimum reduziert werden.

Eine gelungene Investition. Darüber hinaus wollen Maschinenbauer keine Ressourcen für die komplizierte Implementierung einer digitalen Wartungslösung investieren. Mitarbeiter sollen sich auf ihre spezifischen Aufgaben konzentrieren anstatt auf Fernwartung. „Daher haben wir eine Lösung entwickelt, die ganz einfach umzusetzen ist“, sagt Blaschke. Eine Fernwartungslösung bietet Maschinenbauern einen enormen Vorteil – im Wartungsfall ist ein Servicetechniker innerhalb kurzer Zeit mit der Anlage verbunden und kann die Ursache schnellstmöglich beheben.
Mit Secure Remote Maintenance von B&R stellen Maschinenbauer Systemdiagnosen aus der Ferne oder spielen Updates von einem zentralen Ort aus ein. „Im Wartungsfall setzt sich ein Servicetechniker einfach vor den PC und nicht in ein Flugzeug und greift digital auf die Kundenmaschine zu, anstatt ein Flugticket zu kaufen“, sagt Blaschke. „Die Fernwartung spart somit Zeit und Geld.“ Bei der Wartung per digitaler Verbindung stellt der Techniker dann fest, ob zum Beispiel ein Kabel fehlt oder eine Hardware defekt ist.
In wenigen Schritten ist die B&R-Fernwartungslösung installiert und der Servicetechniker greift einfach auf Maschinen in aller Welt zu. „Die entsprechende Hardware, der sogenannte SiteManager, muss lediglich mit der Maschinensteuerung verbunden werden und baut anschließend den Fernwartungs-Tunnel auf, indem sie sich mit der Zentrale, dem sogenannten GateManager, verbindet“, erklärt Blaschke. Wie jede B&R-Hardware kann auch der SiteManager über das Engineeringtool Software Automation Studio konfiguriert werden. >>

René Blaschke
Produktmanager für IoT bei B&R

„Durch die Verwendung moderner Protokolle, Technologien und Infrastrukturkomponenten ist unsere Lösung optimal geschützt.“

Nachgefragt

René Blaschke ist Produktmanager für IoT bei B&R und weiß um die Vorteile von Fernwartungslösungen, aber auch um deren Schwächen.

IoT 4 Industry & Business: Es heißt, dass Fernwartungslösungen immer mehr Einklang in die Arbeitsabläufe von Unternehmen erhalten auch, damit „vor Ort" nicht erst nach einer Anreise gearbeitet werden kann. Kommt man aber auch dem möglichen Mangel an geeigneten Fachkräften mit diesen Lösungen entgegen?
René Blaschke: Ja, denn besonders regionalem Fachkräftemangel kann so entgegengewirkt werden, da es nicht ausschlaggebend ist, wo ein Techniker sitzt. Fernwartung bietet die Möglichkeit, schnell und effektiv auf Vorkommnisse in aller Welt zu reagieren. Die Qualität und auch die Geschwindigkeit der Services wird dadurch verbessert.

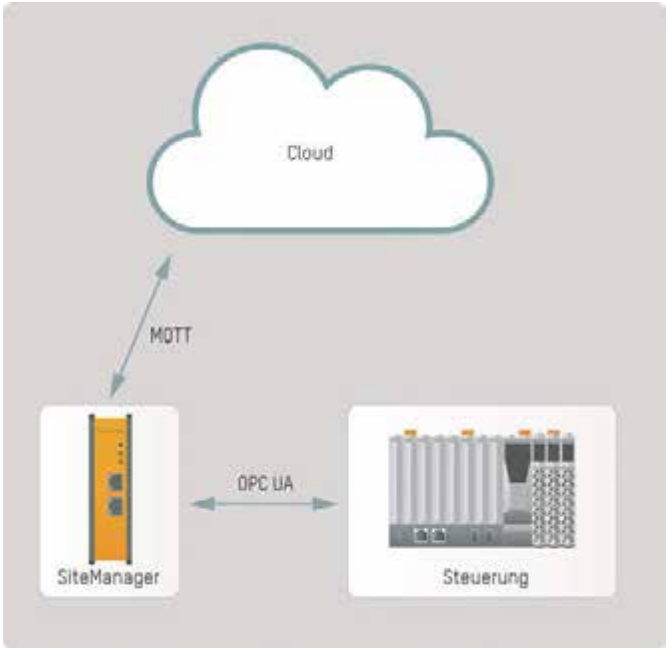
IoT: Inwiefern schützt man sich bei dieser Arbeitweise vor möglichen Hackerangriffen bzw. was bietet B&R an Lösungen an?
Blaschke: Mit einer State of the Art-Verschlüsselung und Sicherheitsmechanismen, wie sie zum Beispiel auch beim Onlinebanking verwendet werden, erreichen wir maximale Sicherheit. Der Fernwartungszugriff basiert auf einer VPN-Verbindung und der SiteManager verfügt über eine integrierte Firewall. Zudem werden die Fernwartungskomponenten laufend nach den gängigen Sicherheitsstandards auditiert.

IoT: Und wurde durch die Covid-19-Pandemie eine erhöhte Nachfrage festgestellt?
Blaschke: Der Markt hat sich durch die Coronakrise definitiv verändert. Wie von Ihnen schon richtig angenommen, hat Secure Remote Maintenance heuer eine verstärkte Nachfrage erfahren.
Ich gehe davon aus, dass diese auch nach der Pandemie noch bleiben wird, da die Anwender nun die großen Vorteile der Fernwartung kennen und merken, dass ihre Sicherheitsbedenken unbegründet sind.

Sicherheit steht an erster Stelle. Innerhalb weniger Augenblicke kann der Nutzer eine sichere Verbindung herstellen, eine Ferndiagnose durchführen, Maschinenparameter anpassen und mögliche Fehler beheben – so als wäre er direkt vor Ort. Jeder Zugriff wird genau registriert, protokolliert und ist jederzeit nachvollziehbar. Der B&R-SiteManager kann sowohl initial in einer Maschine eingebaut als auch nachträglich bei Bestandsanlagen nachgerüstet werden. In beiden Fällen ist die Lösung nahtlos in das System integriert.
Eine sichere Verbindung ist eine der wichtigsten Voraussetzungen bei der Fernwartung. Trotz voller Datentransparenz sollen die Maschinendaten sicher übermittelt werden. Die B&R-Fernwartungslösung Secure Remote Maintenance erfüllt die Anforderungen an eine sichere und zuverlässige Verbindung. „Durch den Einsatz moderner Protokolle, Technologien und Infrastrukturkomponenten ist unsere Lösung optimal geschützt", erklärt Blaschke. „Die Sicherheitsstandards bei der Fernwartung sind vergleichbar mit solchen, die zum Beispiel beim Onlinebanking eingesetzt werden." Die Verschlüsselung der Daten bei der Übertragung schützt vor Hackerangriffen.
Bei einem Zwischenfall sendet der SiteManager Alarme, Ereignisse oder Statusaktualisierungen per Textnachricht oder E-Mail an den Maschinenbetreiber. Diese Benachrichtigungen werden direkt über die Fernwartungs-Hardware vorkonfiguriert. Auf diese einfache Weise wird ein transparenter Maschinenbetrieb geschaffen und der Anwender weiß zu jeder Zeit über den Status seiner Anlagen und Maschinen Bescheid.

Eine Lösung, viele Anwendungsgebiete. Secure Remote Maintenance wird nicht nur im Wartungsfall eingesetzt. Auch eine Inbetriebnahme ist aus der Ferne möglich. Verschickt ein Maschinenbauer eine Anlage oder Maschine zu einem Kunden, muss für deren Inbetriebnahme kein Servicetechniker mehr um die halbe Welt reisen. Sobald der SiteManager an der Maschine konfiguriert ist, kann eine digitale Verbindung aufgebaut und die Inbetriebnahme durchgeführt werden.
Alle Anlagen und Maschinen eines Maschinenbauers können an einer zentralen Stelle verwaltet werden. So ist der Maschinenbauer dem Kunden näher und kann Zusatzdienste mit erheblichem Mehrwert anbieten. Neue Geschäftsmodelle sind möglich, zum Beispiel die Zustandsüberwachung von Anlagen und deren Leistungskennzahlen, um Service-Intervalle optimal abzustimmen.

Die B&R-Fernwartungs-Hardware, der sogenannte SiteManager, muss lediglich an der Maschine platziert werden und baut anschließend den Fernwartungs-Tunnel auf.



Der B&R-SiteManager ermöglicht das sichere Übertragen von Daten in die Cloud.

Sichere Datenübertragung in die Cloud. Der B&R-SiteManager ermöglicht außerdem das sichere Übertragen von Daten in die Cloud. „Dazu verbindet sich der SiteManager mit der Steuerung der Maschine über OPC UA und überträgt die Daten mit dem Nachrichtenprotokoll MQTT in die Cloud", erklärt Blaschke. Der Anwender definiert bei der Konfiguration, welche Daten übertragen werden sollen. Es ist auch möglich, unterschiedliche Daten an unterschiedliche Cloudanbieter zu übertragen. Die Konfiguration erfolgt auf einfache Weise in der Weboberfläche des SiteManagers.
Zusätzlich zum Cloud-Interface stehen diverse Aggregationsmöglichkeiten für die gesammelten Daten zur Verfügung, wie Minimal- und Maximalwertberechnung oder die Berechnung des Mittelwerts. Eine integrierte Store-and-Forward-Database sorgt im Falle von Verbindungsproblemen dafür, dass keine Informationen verloren gehen.

Kurze Reaktionszeit im Wartungsfall. Maschinen und Anlagen werden heute weltweit verkauft. Der weltweite Absatz stellt Maschinenbauer auch vor neue Herausforderungen. Wartungsarbeiten, die sich nur mithilfe des Herstellers bewerkstelligen lassen, beanspruchen viele Ressourcen. „Mit einer Fernwartungslösung ist dies Geschichte", sagt Blaschke. Maschinenbauer können sich zu jeder Zeit mit jeder Anlage und Maschine im Feld verbinden und Servicearbeiten innerhalb kurzer Zeit aus der Ferne erledigen. Das spart Zeit und Geld.

www.br-automation.com

CYBERANGRIFFE AUF UNTERNEHMENSDATEN – DATENSCHUTZSTRATEGIE UNERLÄSSLICH

Die vergangenen Monate haben IT-Sicherheitsfragen in Unternehmen wieder in den Vordergrund gerückt. Zum Beispiel hat das verstärkte Aufkommen von Homeoffice während der Pandemie Firmen und ihren Mitarbeitern neue Möglichkeiten eröffnet, es erhöhte aber auch das Gefährdungspotenzial in Sachen Cyberangriffen.

Tatsächlich ist die Entwicklung einer wirksamen Strategie gegen Cyberattacken für Unternehmen aber nicht erst seit der Zunahme von Remote Work angeraten, denn Ransomware-Attacken haben bereits vorher zugenommen, alleine das Jahr 2019 verzeichnete eine Steigerung um 41 Prozent. Die Auswirkungen von Cyberattacken können verheerend sein – der Data Protection Trends-Report 2020 von Veeam hat ermittelt, dass ein einstündiger Ausfall von normal-priority-Anwendungen in großen Unternehmungen mit rund 60.000 US-Dollar zu Buche schlägt.

Zusammenspiel von Maßnahmen hilft. Eine solide Abwehrstrategie gegen Cyberattacken besteht im Wesentlichen aus folgenden Maßnahmen: Schulung der Mitarbeiter, Implementierung sicherer Netzverbindungen bei Remote Work und einer sorgfältigen Handhabung von Endgeräten, regelmäßigen Updates der IT-Systeme, besonders der kritischen IT-Kategorien wie Betriebssystemen, Datenbanken und Applikationen – und soliden Maßnahmen bezüglich Backups, Recovery und Restore, die bereits im Vorfeld gesetzt werden müssen.

Mitarbeiter in Datensicherheit schulen. Mitarbeiter können bereits viel dazu beitragen, Cyberkriminellen den Zugriff auf Unternehmensdaten zu erschweren. So verwenden IT-Verantwortliche in ihrer täglichen Arbeit häufig Remote Desktop Protokolle (RDP). Doch auch wenn diese durch spezielle IP-Adressen, umgeleitete RDP-Ports oder komplexe Passwörter geschützt sind, können sie – wenn sie direkt mit dem Internet verbunden sind – ein Einfallstor für Schadsoftware sein. Eine weitere häufige Eintrittsmethode in Firmennetzwerke sind Phishing Mails, die von Mitarbeitern geöffnet werden. Hier gilt es, Mitarbeiter gezielt zu schulen, damit sie derartige Mails und Links zweifelsfrei erkennen können und ungeöffnet löschen.

Remote Work – „if you connect it, protect it". Wird von peripheren Geräten auf das Firmennetzwerk zugegriffen, ist eine VPN-Verbindung unerlässlich. Sie funktioniert wie ein Datentunnel und stellt sicher, dass die Daten beim Übertragungsvorgang vor Zugriffen aus dem (restlichen) Internet geschützt sind. Außerdem ist es wichtig, die im Homeoffice verwendeten Endgeräte – Laptop, Tablet oder Smart Phone – mit Sicherheitssystemen auszustatten und Daten und Applikationen von diesen Geräten am Ende ihrer Lebensdauer oder bei Übertragung an andere Personen sorgfältig zu entfernen.

Backup, Recovery and Restore. Effizienter Datenschutz ist nur dann möglich, wenn auf sorgfältige Datensicherung im Vorfeld geachtet wurde, die 3-2-1-Regel von Veeam ist dabei ein guter Leitfaden: Unternehmungen sollen zumindest drei Kopien wichtiger Daten verfügbar haben, auf zumindest zwei verschiedenen Arten von Speichermedien, wovon eines off-site aufbewahrt werden sollte. Zumindest eine Kopie in der 3-2-1-Strategie muss ultra-belastbar sein – das bedeutet physisch getrennt, offline oder unveränderlich, wie zum Beispiel Tapes, unveränderliche Backups in S3 oder S3-kompatibler Objektspeicherung oder Software-as-a-Service for Backup and Disaster Recovery.

Umfassender Datenschutz ist eine der wichtigsten Aufgaben von Unternehmen. Ressourcen, die für eine Datenschutz-Strategie aufgewendet werden, sind gut investiert, denn damit minimieren Unternehmen das Risiko von Datenverlust, finanziellen Schäden oder auch Reputationsverlust.

www.veeam.com/de

Der Autor:

Mag. (FH) Mario Zimmermann

Country Manager Austria
Veeam

„DATENSCHUTZ IST EINE ERRUNGENSCHAFT“

Das Kippen des Privacy Shields durch den europäischen Gerichtshof zeigt einmal mehr, in welcher unsicheren Rechtslage sich der internationale Datentransfer mit den USA befindet, denn dieses Land hat eine ganz eigene Vorgehensweise hinsichtlich Datenschutz, die nicht unbedingt mit den europäischen Standards im Einklang steht.

Auf dem Digitalgipfel 2019 Ende Oktober in Dortmund eröffnete das Bundeswirtschaftsministerium das europäische Digital-Großprojekt zur Stärkung der Industrie im internationalen Wettbewerb.

„Diese Entscheidung ist auch ein Signal an die heimische Wirtschaft, sich über die eigenen firmenrelevanten Daten intensiv Gedanken zu machen. Für produzierende Unternehmen in Österreich ist die Frage der Datensicherheit und Datensouveränität überlebenswichtig geworden – in erster Linie hängt davon nämlich ihre internationale Wettbewerbsfähigkeit und letztlich euch ihre Existenz ab“, betonte vor einiger Zeit Andreas Hajek, führender Experte für IT-Infrastruktur bei dem Schaltschrank- und IT-Infrastrukturspezialisten Rittal GmbH, die Entscheidung.

„Damit sollten auch die letzten Zweifler erkannt haben, dass der strenge europäische Datenschutz eine Errungenschaft ist, die es gilt, nicht leichtfertig aufs Spiel zu setzen. Umso wichtiger ist es daher, an einer effizienten und zukunftsträchtigen europäischen Cloud- und Dateninfrastruktur zu arbeiten – die Initiativen wie Ö-Cloud in Österreich oder Gaia-X in Deutschland gehen in die richtige Richtung“, erklärt Hajek weiter.

Gemeinsam voran. Und er ergänzt: „Zum einen arbeiten wir hier intensiv mit unserer Schwesterfirma aus der Friedhelm Loh Gruppe, German Edge Cloud, zusammen, welche ein Gründungsmitglied der Gaia-X-Initiative in Deutschland ist, und zum anderen ist unsere eigene, auf Industrie 4.0-basierende, vollautomatisierte Fabrik im deutschen Haiger ein funktionierender Gaia-X-Showcase.“ Denn Datenschutz und Datensouveränität sind laut Rittal als Produktionsunternehmen und Weltmarktführer unerlässlich. Der Showcase zeigt, dass übergreifende Wertschöpfung aus einem innovations- und technologiegetriebenen Ecosystem von Zulieferern, Logistik, Integratoren bis hin zum Kunden und Sicherheit für alle Beteiligten keine sich ausschließenden Themen sind. „Rittal und die German Edge Cloud sind hier Top-Innovatoren in Europa“, führt Hajek fort.

Gaia-X klingt mystisch... …ist es aber nicht – im Gegenteil. Gaia-X ist ein sehr realistisches Projekt zum Aufbau einer leis-

ONCITE

Die Friedhelm Loh Group ist mit ihrer Tochtergesellschaft German Edge Cloud eines der Gründungsmitglieder von Gaia-X, gemeinsam mit jeweils elf deutschen und elf französischen Unternehmen, Institutionen und Vereinigungen. Dazu zählen unter anderem die Fraunhofer-Gesellschaft, Atos, Bosch, die Deutsche Telekom, SAP, BMW und Siemens. Die Gründungsmitglieder bilden ein gemeinsames Projektteam.

Die Friedhelm Loh Group war auch auf technologischer Seite bereits aktiv: Die F.L.G.-Unternehmen German Edge Cloud und Rittal haben mit dem Fraunhofer Institut und Bosch eine Lösung entwickelt und an den Markt gebracht, die als Beitrag zu Gaia-X dient: Oncite ist das erste schlüsselfertige Edge-Cloud-Rechenzentrum für echtzeitfähige und datensouveräne Industrie 4.0-Anwendungsszenarien.

tungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa, das von Vertretern der deutschen Bundesregierung, Wirtschaft und Wissenschaft getragen wird. Der Name des Projektes leitet sich den Angaben zufolge zwar von einer der ersten aus dem Chaos entstandenen griechischen Gottheiten „Gaia“ ab, die in der Mythologie als personifizierte Erde für die Gebärerin steht. Der breiten Öffentlichkeit wurde das Projekt beim Digital-Gipfel 2019 in Dortmund vorgestellt – und das aber sehr realistisch und greifbar.

Die Gaia-X-Initiative gab zudem kürzlich bekannt, dass sie ihrem Ziel der Entwicklung einer vertrauenswürdigen, souveränen digitalen Infrastruktur für Europa einen Schritt näher gekommen ist: Die 22 Gründungsmitglieder unterzeichneten offiziell die Gründungsurkunden für die Gaia-X AISBL (association internationale sans but lucratif nach belgischem Recht), einer gemeinnützigen Vereinigung, die das Projekt auf die nächste Stufe heben wird.

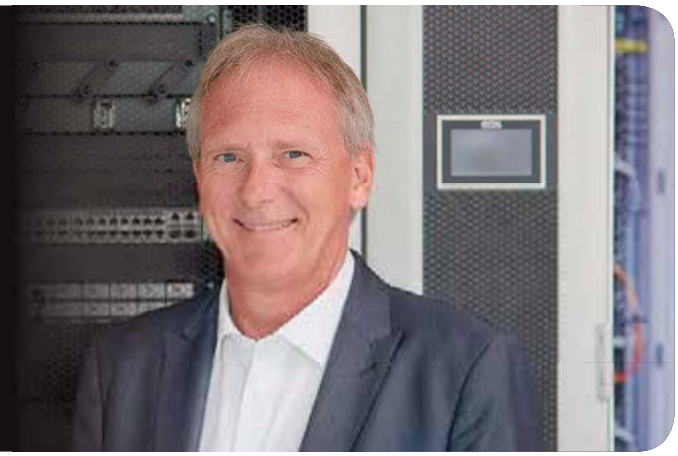
Die Vereinigung soll die Finanzierung und das Engagement der Mitglieder sicherstellen, um die Vision der Initiative für Europa zu verwirklichen. „Wir sind äußerst motiviert, den Herausforderungen der europäischen digitalen Wirtschaft zu begegnen“, sagte hierzu erklärend Servane Augier, Chief Operating Officer bei 3DS Outscale. „Mit Gaia-X bauen wir gemeinsam eine souveräne und verlässliche digitale Infrastruktur und ein Ökosystem für Innovationen in Europa auf. Auf diese Weise stärken wir die digitale Souveränität von Unternehmen, in Forschung und Bildung, von Regierungen und der Gesellschaft als Ganzes.

Die Gründungsmitglieder der Gaia-X AISBL laden nationale und multinationale, europäische und außereuropäische Unternehmen sowie Partner aus Wissenschaft und Politik ein, die europäische Standards und Werte teilen, indem zur aktiven Teilnahme und Mitgliedschaft aufgefordert wird. Die Mitglieder der Vereinigung sind der Motor für Fortschritt und Innovation. Sie arbeiten eng zusammen, um Standards sowohl aus Anbieter- als auch aus Anwenderperspektive zu definieren sowie Prototypen und Lösungen zu entwickeln.

Finale Züge. Noch ist der Gründungsprozess formell nicht ganz abgeschlossen. Die nächsten Schritte sind die Hauptgeschäftsstelle in Brüssel einzurichten und wichtige Organisationsstrukturen aufzubauen. Außerdem plant die Vereinigung einen Gaia-X-Summit für Mitte November 2020. Die Gaia-X-Gründungsmitglieder streben eine Kultur des Vertrauens, des Wissensaustauschs und der Transparenz an. Gaia-X wird mit wachsender Mitgliederzahl einen zunehmenden Einfluss auf Innovation und die Zusammenarbeit bei der Entwicklung von technischen Lösungen und Standards für Wirtschaft, Wissenschaft und Gesellschaft in ganz Europa ausüben.

Aus dem Bereich der Automobilwirtschaft hat sich die BMW Group wie folgt zu dem Projekt geäußert: „Die BMW Group sieht die Zukunft von automobiler Software in der Cloud – ob wegweisende IT-Lösungen für die Entwicklung und Produktion von Premiumfahrzeugen, neue digitale Services für unsere Kunden oder innovative Funktionen im Auto“, so Marco Görgmaier, Leiter DevOps-Plattform and Cloud Technologies der BMW Group.

www.rittal.at



Andreas Hajek
IT-Infrastrukturexperte bei Rittal Österreich

„Es ist wichtig, an einer effizienten und zukunftsträchtigen europäischen Cloud- und Dateninfrastruktur zu arbeiten, etwa Gaia-X.“

WISSENS-TRANSFER **VIA CLOUD**

Am 15. September war es soweit und die Eplan Virtual Fair startete erneut als erfolgreiches Online-Event. Insgesamt 16 Stunden lang konnten virtuell Live-Sessions besucht und Fragen an Experten gestellt werden. Eine Win-Win-Situation und heuer wahrscheinlich noch mehr als die Jahre zuvor.

Die in ePulse hinterlegten Projektdaten fungieren sowohl als Systembeschreibung für die eigene Fertigung als auch zur Kundendokumentation aller automationsrelevanten Aspekte.

Die Eplan Virtual Fair fand 2020 nicht zum ersten Mal statt. Sie erfreut sich kontinuierlich steigender Besucherzahlen und war heuer vor allem auch durch die so genannten Länder-Pavillons ein Höhepunkt der digitalen Veranstaltung. Die Besucher bekamen in zahlreichen Live-Demos einen sehr detaillierten Einblick in die Eplan-Angebote. Dabei gaben Experten Tipps für die tägliche Arbeit im Engineering und standen für Fragen parallel in Q&A-Räumen zur Verfügung.

Gabriele Geiger, Marketingleiterin bei Eplan, freute es in diesem Zusammenhang vor allem, dass Eplan beim Thema Digitalveranstaltung bereits auf ausgiebiges Expertenwissen zurückgreifen kann. „Wir haben direkt auf die Corona-Einschränkungen reagiert und sofort zahlreiche länderspezifische Formate im Stil einer virtuellen Roadshow initiiert. Für uns ist von Vorteil, dass wir unsere Konzepte über die Jahre immer weiter optimiert haben und genau wissen, worauf es unseren Besuchern ankommt“, so Geiger im Eplan-Blog. Dabei zählen vor allem die zeitliche und örtliche Unabhängigkeit der Besucher zu den ausschlaggebenden Argumenten, eine virtuelle Veranstaltung zu besuchen, aber auch Kosten sind ein wesentliches Thema.

Cloud Computing ist Zukunft. Ein Thema, das Eplan für die Gegenwart und Zukunft im Fokus hat – und das nicht nur während der Virtual Fair – ist das Arbeiten in der Cloud. Cloud-Lösungen sind schon länger ein bewährtes Tool, um auch die Standardisierung von Prozessen und Daten voranzutreiben. Denn der Vorteil der Cloud liegt für die Anwender klar auf der Hand: Man arbeitet mit gleichen Voraussetzungen bzw. dem gleichen Wissensstand und Aktualisierungen sehen alle Teilnehmer zur gleichen Zeit und haben somit die gleiche Arbeitsbasis. Die Cloud bietet demnach einen Ort, um Engineeringdaten auszutauschen – egal wo und wann. Und Cloud Computing-Angebote spielen nicht erst durch neue Arbeitsbedingungen (wie durch die Covid-19-Pandemie ausgelöst) eine immens wichtige Rolle im Arbeitsalltag. Eplan bietet mit dem offenen, cloudbasierten Engineering-System ePulse seinen Kunden eine Möglichkeit, Daten und Projekte, Disziplinen und eben auch Ingenieure in einem Netzwerk zusammen zu bringen. Der Bedarf an Lösungen wie diesen entwickelt sich seit einigen Jahren kontinuierlich. Dies wurde auch in diversen Impulsvorträgen während der Eplan Virtual Days mehrfach betont. Das Ziel von Eplan ist es mit Eplan ePulse für diverse Dateiformate und Schnittstellen zu Systemen anderer Anbieter eine offene Austauschform zu gestalten und damit hat Eplan eindeutig die Nase vorn.

Neu seit Juni. Seit Anfang Juni 2020 ist auch die neue Version des Eplan-Data-Portals am Markt, die Anwendern webbasiert Komponenten- und Gerätedaten zur Projektierung bereitstellt. Das Portal ist exklusiv in der Cloud-Umgebung von Eplan ePulse integriert. Elektro- und Fluid-Planer wählen dort benötigte Artikeldaten aus und übernehmen sie direkt in ihr Eplan-Projekt. Das reduziert den Projektierungsaufwand und sorgt für standardisierte Daten in der Dokumentation. Eine komplett neue Bedienoberfläche mit intuitiver Such- und intelligenter Vorschlagsfunktion macht die Anwendung im Portal einfacher, schneller und komfortabler. Direkten Zugang finden Anwender der aktuellen Version 2.9 der Eplan-Plattform nach Registrierung unter www.epulse.com.

www.eplan.at
https://www.eplan.blog/topic/eplan-epulse
www.epulse.com

VORTEILE LIEGEN AUF DER HAND

Ing. Martin Berger ist Eplan-Geschäftsführer in Österreich. Was ePulse Anwendern bietet, beantwortet er im Folgenden.

IoT 4 Industry & Business: Eplan setzt auf ePulse. Was können sich Anwender konkret für Vorteile erwarten?
Ing. Martin Berger: Zusammenarbeit über alle Grenzen hinweg wird immer mehr Thema. Die ortsunabhängige Zusammenarbeit in Engineering-Projekten ist heute mehr denn je gefordert. ePulse ist die optimale Ergänzung zur Eplan-Plattform und bietet Softwarelösungen in der Cloud.

IoT: Das bedeutet konkret?
Berger: Zum einen ist das das Eplan-Data-Portal. Mit diesem haben Eplan-Anwender direkten Online-Zugriff auf hochwertige Produktkataloge namhafter Komponentenhersteller. Neueste Highlights mit Vorteilen für Anwender ebenso wie Hersteller sind die verbesserte Datenqualität und -tiefe sowie ein brandneues Nutzer-Interface mit intelligenter Suchfunktion.
Weiters exklusiv auf ePulse verfügbar ist Folgendes: Mit Eplan eView setzen wir Review-Prozesse im Engineering digital um. Die kostenlose Software ermöglicht eine strukturierte Zusammenarbeit mit Kollegen, Kunden und Dienstleistern. Damit können standortunabhängig per Browser Projektdaten gesichtet und Änderungen über Redlining-Workflows kommentiert werde. Und dann gibt es noch die Möglichkeit, in der Cloud Engineering durchführen zu können. Eplan eBuild macht den entscheidenden Schritt in Richtung automatisiertes Engineering. Vorgefertigte oder auch individuell erstellbare Bibliotheken ermöglichen es Eplan-Anwendern, bei ihrer täglichen Arbeit Schaltpläne praktisch auf Knopfdruck zu erstellen.

IoT: Ihre Einschätzung bitte: Waren die Covid-19-Pandemie und schlussendlich die Folgen im beruflichen Umfeld für viele ein positiver Impuls für die ePulse-Strategie von Eplan?
Berger: Generell wäre es besser gewesen, diese Pandemie nicht zu haben. Denn es hat viel Leid und Sorgen gebracht. Aber Krisen sind immer ein Zeitpunkt, wo Unternehmer ihr Handeln überdenken sollten und müssen, um auch in Zukunft wettbewerbsfähig zu bleiben.
Generell haben sich natürlich auch unsere Kunden Gedanken über deren Arbeitsweise gemacht und sind dabei, ihre aktuelle Arbeitsweise entlang der gesamten Wertschöpfungskette zu überdenken und das Thema Digitalisierung mehr in den Vordergrund zu stellen. ePulse ist da ein Baustein dafür.
Wir haben auch die Erfahrung gemacht, dass gerade in dieser schwierigen Zeit viele neue Kunden zu Eplan gekommen sind. Ich denke hier zählt neben der zukunftsorientierten Technologie auch die Investitionssicherheit. (se)

Das klimaneutrale Areal des Euref-Campus in Berlin erfüllt schon seit 2014 die Klimaziele der Bundesregierung für 2050.

WIE DIE ZUKUNFT GELINGT

Wer in die Zukunft schauen möchte, kann das am Euref-Campus in Berlin machen. Hier ist mit Hilfe von Schneider Electric ein Reallabor der Energiewende entstanden. Barbara Sawka war vor Ort.

Dank der klimaneutralen Energieversorgung, dem intelligenten Energienetz, energieeffizienten Gebäuden und einer Testplattform für die Mobilität der Zukunft ist es auf dem Euref-Campus im Berliner Stadtteil Schöneberg rund um den alten Gasometer gelungen, die Klimaziele der deutschen Bundesregierung von 2050 schon im Jahr 2014 zu erreichen. In diesem innovativen Stadtteil hat Schneider Electric seinen Standort und kümmert sich als Euref-Projektpartner rund um die Themen Energie, Umweltschutz und Ressourcenmanagement am Campus.

Zukunftsfähiges Wirtschaften. Dass man es bei Schneider Electric ernst meint mit dem Thema Nachhaltigkeit, zeigen zwei Auszeichnungen in diesem Jahr. Das Unternehmen wurde am 15. September vom FAZ Institut für „Exzellente Nachhaltigkeit 2020“ ausgezeichnet. Stellvertretend für das Unternehmen nahm Christine Beck-Sablonski, Vice President Marketing Communication DACH, die Ehrung im Rahmen einer in diesem Jahr weitgehend digitalen Veranstaltung in Frankfurt am Main entgegen. „Wir freuen uns ganz besonders über diesen Preis, denn er bestätigt und motiviert uns in dem Bestreben, mit unseren IoT-fähigen Lösungen für Automatisierung und Energiemanagement verantwortungsbewusstes und nachhaltiges Wirtschaften für immer mehr Unternehmen zu ermöglichen“, so Beck-Sablonski.
Anfang des Jahres wurde Schneider Electric, anlässlich des Weltwirtschaftsforums in Davos, für sein ökologisches Engagement geehrt. In der Rangliste der „Global 100 Most Sustainable Corporations“ von Corporate Knights belegt das Unternehmen den ersten Platz im Peer-Group-Ranking und Rang 29 in der Gesamtwertung. Zudem wurde Schneider Electric in die „Climate Change A List“ des Carbon Disclosure Projects (CDP) aufgenommen und ist damit zum neunten Mal in Folge in den A-Listen der Non-Profit-Organisation vertreten.
Mit dem unternehmenseigenen Schneider Sustainability Impact (SSI) setzt sich das Unternehmen selbst hohe Ziele in Sachen Nachhaltigkeit. Vierteljährlich veröffentlicht, misst der SSI anhand von 21 Indikatoren die Fortschritte bei den selbstgesteckten Nachhaltigkeitsbemühungen. Für das erste Halbjahr 2020 sind beispielsweise bereits 193 der weltweit 200 Standorte abfallfrei.

The new normal. Die Corona-Krise ist auch an Schneider Electric nicht spurlos vorüber gegangen. Sowohl im Bereich Energy Management als auch in der Industrial Automation muss das Unternehmen einen Rückgang von rund zehn Prozent verzeichnen, die Software- und Service-Produkte hingehen sind relativ stabil, wie Christophe de Maistre, CEO & Zone President DACH im Rahmen einer Presseveranstaltung erklärte und dabei auf eine neue Normalität verwies. Dem schloss sich auch Jürgen Siefert Vice President Industrial Automation DACH an. Dennoch sei Schneider Electric gut durch die Krise gekommen. Die Kundenzufriedenheit konnte in den letzten Monaten um 24 Prozent gesteigert werden. Auch die letztes Jahr installierte Businessplattform „Exchange“ kann sich über Zuwächse freuen. Mittlerweile nützen 67.000 User die Community, in der sie Zugriff auf APIs, Analysen und Datensätze haben und im Austausch neue Lösungen entstehen sollen.

www.se.com

DEUTSCHE UNTERNEHMEN IM FOKUS VON HACKERN

Wie eine Umfrage des Kriminologischen Forschungsinstituts Niedersachsen Anfang des Jahres ergeben hat, sahen sich 41 Prozent der befragten deutschen Unternehmen in den letzten zwölf Monaten Cyber-Angriffen ausgesetzt. Dabei werden große Organisationen häufiger Opfer derartiger Attacken als kleine.

E-Mail bleibt das wichtigste interne und externe Kommunikationsmittel für Unternehmen und ist daher der Hauptangriffsvektor für Kriminelle. Hier wird hauptsächlich auf Phishing und Social Engineering gesetzt. Besonders beliebt ist der CEO-Fraud, bei dem sich der Angreifer als Vorgesetzter oder Geschäftsführer ausgibt, um den Empfänger der Mail zur Herausgabe von Daten oder gar Geldüberweisungen zu bringen. Da viele Firmen sowie ihre Mitarbeiter über eine Social-Media-Präsenz verfügen, ist es für Angreifer ein Leichtes, Informationen über Hierarchien, Events oder andere nützliche Interna zu erhalten, mit denen sie ihre Phishing-Nachrichten authentisch wirken lassen können.

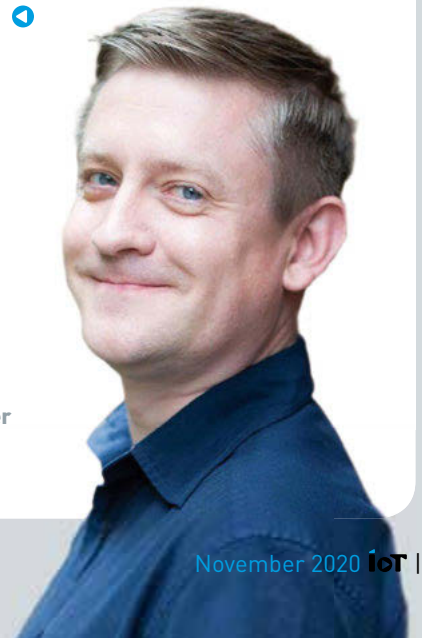
Die Erkenntnisse der Umfrage decken sich weitestgehend mit denen des Threat Intel Reports von Mimecast, der im letzten Quartal 2019 über 92 Milliarden Spam-Mails auf ihr Schadpotenzial hin untersucht hat. Besonders die Impersonation-Attacken sind hier auf dem Vormarsch, die entweder dem Einschleusen der Malware Emotet oder Ransomware dienten. In Deutschland sahen sich insbesondere Unternehmen aus dem Transport- und Speditionsgewerbe Spam-Mails ausgesetzt.

Gegen Angriffe wappnen. Carl Wearn, Head of E-Crime bei Mimecast, dazu: „Die Umfrageergebnisse des Forschungsinstituts decken sich mit unseren eigenen Forschungen. Unternehmen müssen sich gegen Angriffe per E-Mail wappnen. Wir werden mit ziemlicher Sicherheit eine Zunahme solcher und ähnlicher Aktivitäten künftig sehen. Kriminelle werden zweifellos die aktuelle Krise ausnutzen, um ihre Kampagnen voranzutreiben. Ich würde jedem, der gerade auf die Kommunikation per Mail angewiesen ist, zu besonderer Wachsamkeit raten und bei Links und Anhängen ein gesundes Misstrauen an den Tag zu legen."

Darüber hinaus sollten sich Unternehmen über Lösungen zum E-Mail-Schutz und der Cyber-Resilience stets informieren. Ersterer sorgt dafür, dass schädliche Mails erst gar nicht zugestellt werden, während Resilience für Betriebe bedeutet, selbst im Falle eines erfolgreichen Angriffs kommunikations- und damit geschäftsfähig zu bleiben. Auch Mitarbeiterschulungen zum Thema sichere Security Awareness sind essenziell, da sie die Sicherheitslücke Mensch schließen – oder zumindest beträchtlich verkleinern.

Mimecast ist ein Cybersicherheitsanbieter der dabei hilft, E-Mail-Verkehr sicherer zu machen und die Cyber-Resilience zu stärken. Die erweiterte Cloud-Suite von Mimecast befähigt Unternehmen, eine umfassende Cyber-Resilience-Strategie umzusetzen.

www.mimecast.com



Der Autor:

Carl Wearn

... ist Head of E-Crime bei Mimecast und ein erfahrener Sicherheitsexperte auf seinem Fachgebiet.

ERFOLGREICHE VÖSI-SOFTWARE DAYS 2020

Unter dem Motto „Autonomous Things, Drive & Disruption" ging der bereits vierte **Vösi Software Day** – mit Einhaltung aller coronagerechten Sicherheitsvorkehrungen und dadurch bedingten Programmänderungen – am 29. September in Wien gut über die Bühne. Digitalisierungsministerin Margarete Schramböck und NASA-Spezialist Robert Karban wurden live zugeschalten.

„Software is the key – der Schlüssel zum Erfolg für nächste Generationen, deswegen liegt auch ein Schwerpunkt in der Entwicklung digitaler Kompetenzen in der gesamten Bevölkerung", betonte Schramböck. Sie unterstrich auch den hohen Stellenwert der Software-Branche in Österreich: „Nichts geht mehr ohne Software. Die Krise hat uns gezeigt:

Je stärker digitalisiert eine Volkswirtschaft ist, desto stärker ist sie und desto höher ist auch ihre Resilienz, ihre Widerstandskraft." Darüber hinaus schaffe die ICT-Branche rund 20.000 neue Arbeitsplätze im Jahr.

„Wir haben gemeinsam mit der Wirtschaftskammer auch ein eigenes Covid-19-Präventionskonzept entwickelt und am Software Day gehörigen Personalaufwand betrieben – ich denke, das hat sich gelohnt", betonte Peter Lieber, Präsident des Vösi und Eigentümer von SparxSystems Software, Lieber-Lieber Software und 4biz consulting. Lieber verkündete auch den Anschluss des Vösi an den ÖGV (Österreichischer Gewerbeverein). Peter Lieber ist seit Juni auch Präsident des ÖGV.

www.softwareday.at
www.voesi.or.at

NEU AUFGESTELLT

Fortinet, Anbieter von umfassenden, integrierten und automatisierten Cyber-Security-Lösungen, reagiert auf das starke Wachstum auf den deutschsprachigen Märkten. Durch das Anpassen interner Strukturen sowie der Beförderung des Deutschen **Christian Vogt** (Bild Mitte) zum Vice President DACH soll die Dynamik im deutschsprachigen Raum weiter vorangetrieben werden.

Für Österreich bedeutet das ebenfalls neue Agilität, da **Karl Freundsberger**, Country Manager Österreich, nun direkt an Vogt berichtet. Zuvor agierten die Märkte Deutschland und „Alps" mit Österreich und der Schweiz getrennt. „Wir surfen derzeit auf einer Erfolgswelle – und das wollen wir auch in Zukunft weiter so machen", brachte es Vogt bei einem Medienfrühstück in Wien klar zum Ausdruck.

www.fortinet.com

GEWACHSEN

Cryptas, österreichischer PKI-Spezialist, expandiert und baut seine Standorte aus. Der Lösungsanbieter in den Bereichen Public Key Infrastructure, starke Authentisierung, digitale Identität und elektronische Signatur betreibt seit 2016 ein eignes TrustCenter in Graz. Nach Expansionen nach Deutschland und in den skandinavischen Raum soll nun auch hierzulande weiter ausgebaut werden. Laut Stefan Bumerl, CEO Cryptas, profitiere man stark von der Digitalisierung.

www.cryptas.com

Stefan Bumerl, CEO Cryptas

DAMENPOWER

Julia Wagner, Digital Marketing-Managerin

Tech Data, heimischer Distributor, erweiterte heuer sein Marketing-Team in Richtung Digital und zwar mit der gebürtigen Niederösterreicherin Julia Wagner (Bild). Sie ist als Digital Marketing-Managerin in das Team von Alexander Kremer geholt worden und vor allem für die Entwicklung und den Einsatz der neuen digitalen Marketing-Tools verantwortlich. Die Absolventin der IMC FH-Krems – sowohl Unternehmensführung und E-Business Management als auch Tourism und Leisure Management – hat in der Vergangenheit vielfältige Erfahrung unter anderem bei Österreich Werbung und Humanbrand Media gesammelt. Seit Ende 2018 war sie bei Tech Data Sales & Marketing Consultant für den Bereich Modern Workplace tätig.

www.techdata.at

IIoT-KONZEPTE FÜR UNABHÄNGIGE ZUSTANDSÜBERWACHUNG

Ausfälle von Maschinen und Anlagen erzeugen für den Betreiber erhebliche Kosten. Im Maschinen- und Schaltschrankbau werden deshalb Konzepte für die Zustandsüberwachung und vorbeugende Wartung der Betriebsmittel immer wichtiger. Die **IoTmaxx GmbH** aus Hannover liefert Lösungen, die so individuell wie nötig und so einfach wie möglich sind und mit denen Hersteller die Steuerung und den Zustand der Anlagen unabhängig vom produktiven Datennetz des Kunden fernüberwachen können. Die Sicherheit der Datenkommunikation und die Unabhängigkeit des externen Zugriffs durch Maschinenhersteller oder Dienstleister von den Produktionsnetzwerken des Anlagenbetreibers sind wichtige Sicherheitskriterien für IIoT-Anwendungen. IoTmaxx setzt auf das für die Anbindung von Sensoren optimierte 4G LTE Gateway GW4101. Die reichhaltigen Schnittstellen des Gateways bieten die Möglichkeit zum direkten Anschluss marktüblicher Sensoren.

www.iotmaxx.com

IoT4 INDUSTRY & BUSINESS

IM TEAM

Mit Anfang Juli hat **Dieter Ferner** (Bild) die Position als neuer Vice President Sales und Marketing bei **NTT Ltd.** in Österreich übernommen. Damit ist das österreichische Managementteam rund um Country Managerin Nora Lawender für die Zukunft optimal aufgestellt. Ferner verfügt über 20 Jahre Erfahrung in

internationalen IT-Unternehmen, davon 15 Jahre in führenden Positionen. Zuletzt war er als Country Manager für Suse Linux in Österreich tätig. Den inhaltlichen Fokus legt Ferner auf Themen wie Managed Services, Cloud, Security und IT-Infrastructure.

https://hello.global.ntt

KOOPERATION

OVHcloud und **T-Systems** haben sich auf eine Zusammenarbeit nach den Prinzipien der europäischen Cloud-Initiative Gaia-X geeinigt. Ziel dieser Partnerschaft ist es, für den deutschen, französischen und weitere europäische Märkte ein vertrauenswürdiges Public-Cloud-Angebot für alle Branchen zu schaffen, in denen Datensouveränität und DSGVO-Konformität eine bedeutende Rolle spielen. In diesem Rahmen werden OVHcloud und T-Systems gemeinsam an der Entwicklung einer einzigartigen öffentlichen Openstack-Cloud-Plattform arbeiten.

www.telekom.com

ÜBERNOMMEN

PTC hat die ioxp GmbH, ein deutsches industrielles Startup für kognitive AR- und KI-Software, für einen nicht genannten Betrag übernommen. ioxp ist ein Spinoff des Deutschen

Forschungszentrums für KI (DFKI). ioxp ist ein Pionier auf dem Gebiet der videobasierten Augmented Reality und bietet kognitive AR- und KI-Lösungen für Wissenstransfer, Schulung und Qualitätssicherung an. Das Startup wurde mit zahlreichen Innovations- und Forschungspreisen ausgezeichnet, darunter Ausgezeichneter Ort im Land der Ideen, IKT Innovativ, Weconomy, Pioneer Geist, Innovation BW, Best Tech Startup, Idea of the Year und Captivate Silicon Valley. Darüber hinaus war ihre Technologie eines von nur vier Bundeskanzlerinnen-Exponaten, die Angela Merkel während des IT-Gipfels 2016 präsentiert wurden.

www.ptc.com

NEUE HOLOLENS 2 ERHÄLTLICH

Microsoft hat im Rahmen der Microsoft Ignite, der jährlichen Entwicklerkonferenz, angekündigt, dass die Auslieferung von Microsoft HoloLens 2 in Österreich beginnt. Interessierte Kunden können den holographischen Computer ab sofort im Microsoft Store bestellen. Und: Die nächste Generation des ersten kabellosen Computers auf Basis der Microsoft Mixed Reality-Plattform wurde erstmals auf dem MWC Barcelona präsentiert. Im Vergleich zum Vorgänger bietet Microsoft HoloLens 2 ein mehr als doppelt so großes Sichtfeld, deutlich verbesserten Tragekomfort durch einen optimierten Schwerpunkt und erlaubt eine intuitivere Interaktion mit Hologrammen.

Microsoft HoloLens 2 gilt als Vorzeigegerät im Bereich Intelligent Edge – hiermit sind AI-fähige Technologien gemeint, die Daten auch ohne eine zuverlässige Internetverbindung sammeln sowie verarbeiten können – und die einige oder alle diese Daten mit der intelligenten Cloud teilen können, wenn sie verbunden sind. So ermöglicht das Gerät auf Basis künstlicher Intelligenz und Cloud-Computing eine instinktive Zusammenarbeit und einen Wissensaustausch über Hologramme, unabhängig von Raum und Zeit.

www.microsoft.at

DURCHDACHT

ABB stellt den neuen RobotStudio AR-Viewer vor, eine Visualisierung auf dem Smartphone oder Tablet zeigt einfach

und schnell auf, wie sich Roboter in bestehende Prozesse und Anlagen integrieren lassen. Die neue Lösung ist ab sofort Bestandteil der leistungsstarken PC-basierten Offline-Programmiersoftware RobotStudio von ABB. Mit dem AR-Viewer lässt sich jedes in RobotStudio erstellte Modell für den gewünschten Einsatz testen. Nutzer erhalten anschaulich einen Eindruck von der Größe und dem Maßstab eines Roboters oder einer Roboterzelle und erkennen schnell, ob und wie sie in eine vorhandene Produktionsanlage passen.

www.abb.at

NEUE VERSION

ownCloud, Spezialist für Digital Collaboration, hat die neue Version seiner Enterprise-File-Sync- und -Share-Lösung veröffentlicht. ownCloud Server 10.5 bringt unter anderem eine vereinfachte Bereitstellung und File Locking mit. Mit der Veröffentlichung der Serverversion 10.5 konsolidiert ownCloud sein Angebot in zwei Paketen: Das minimalistische Paket enthält den Server und erforderliche Komponenten, das Komplettpaket beinhaltet alle unterstützten Erweiterungen. Das bedeutet, dass die Verfügbarkeit der Enterprise-Funktionen nur von einem Lizenzschlüssel abhängt und keine Registrierung für den ownCloud-Marktplatz mehr nötig ist. So können alle ownCloud installieren und die Enterprise-Funktionen 30 Tage testen. Eines der neuen Features der Version 10.5 ist File Locking. Damit ist es ab sofort möglich, Dateien in der Web-App zu sperren, sodass sie während der Bearbeitung nicht von anderen gespeichert werden können.

www.owncloud.com

GAIA-X UNTERSTÜTZT VON BECKHOFF

Gerd Hoppe, Corporate Management, Beckhoff Automation

Mit der von der internationalen Non-Profit-Organisation Gaia-X Foundation, Brüssel, vorangetriebenen Data-Space-Initiative soll eine sichere, vertrauenswürdige Dateninfrastruktur und damit auch die digitale Souveränität von Europa erreicht werden. Im Rahmen der Initiative Gaia-X haben bisher bereits mehr als 170 Teilnehmer und über 150 Organisationen aus Frankreich und Deutschland, aber auch aus Finnland, Italien, den Niederlanden, Schweden, der Schweiz und Spanien in zwei umfassenden Themen-Workstreams zusammengearbeitet. Vertreten sind dabei die User-Domänen Energie, Gesundheitswesen, Industrie 4.0/KMU, Mobilität, öffentliche Infrastruktur und Verwaltung sowie Smart Living, Finanzwirtschaft und Landwirtschaft.
Nun haben 22 Unternehmen und Organisationen aus Frankreich und Deutschland – darunter auch die **Beckhoff Automation GmbH & Co. KG**, Verl – mit der Gründung der Gaia-X Foundation einen weiteren großen Schritt hin zu einer europäischen digitalen Infrastruktur getan. Deren Aufbau soll sich mit Adressierung, Datenverfügbarkeit, Interoperabilität, Portabilität, Transparenz und fairer Beteiligung befassen. Die große Bedeutung der Kundenorientierung bestätigt Gerd Hoppe: „In zahlreichen Gesprächen mit Kunden und Organisationen wurde und wird der Bedarf an einem gemeinsam nutzbaren, europäischen Daten-Ökosystem zunehmend deutlich. Entscheidend ist dabei, dass dieses sich von allen Infrastrukturanbietern und -nutzern in einer Anwendungsdomäne und über Domänengrenzen hinweg nutzen lässt. Außerdem sind für eine möglichst schnelle Akzeptanz im Markt individuelle und domänenspezifische Standards zu übernehmen."

www.beckhoff.at

FINDET HYBRID STATT

Auf der **Hypermotion**, der multimodalen Innovationsplattform, wagen hochkarätige Speaker vom 10. bis 12. November 2020 einen Blick in die Zukunft und beleuchten die neuesten Mobilitäts- und Logistikkonzepte. Networking der Messe- und Konferenzteilnehmer steht im Vordergrund. Im Hypermotion-Lab, das als zentrale Bühne für Newcomer, Experten und Weiterdenker dient, werden disruptive Konzepte direkt an der Schnittstelle für Mobilität und Logistik diskutiert. Hier dreht sich alles um revolutionäre Ideen, Projekte und innovative Technologien, die unsere bisherige Art des Fortbewegens und Transports von Grund auf verändern können.

Weltraum in IoT. IoT dringt in den Weltraum vor. Wie kann IoT genutzt werden, um eine reibungslose Datenkommunikation und Konnektivität aller technischen Geräte zu gewährleisten? In einer Podiumsdiskussion sprechen Experten über den Einsatz von Satellitensystemen und Zukunftstechnologien im erdnahen Orbit.

3D-Druck in der Stadtlogistik. Könnte der Traum vom eigenen gedruckten Auto bald wahr werden? Durch additive Technologien ist es schon heute möglich ein Produkt in unterschiedlichen Ausfertigungen anzubieten und in kürzester Zeit Sonderanfertigungen herzustellen. Mit On-Demand-Modellen sparen Unternehmen eine Menge Lagerkosten ein und die benötigten Güter können individuell nach Bedarf produziert werden. Über die Chancen und Herausforderungen wird mit Experten diskutiert.

Drohnentechnologien. Wie kann der Luftraum derzeit und in Zukunft für neue

Mobilitäts- und Logistikkonzepte genutzt werden? Ob als Lieferdrohne, Flugtaxi oder praktisches Werkzeug zur Datenerfassung – Drohnen werden zunehmend im industriellen Bereich und Transportwesen genutzt. Sie sind vielseitig einsetzbar und bieten gerade für den Warentransport eine emissionslose Alternative zu anderen Fluggeräten. Das Thema Drohnen-Boom wird ebenfalls von Experten näher beleuchtet.

https://hypermotion-frankfurt.messefrankfurt.com

IIoT-LÖSUNGEN FÜR INTELLIGENTE VERBINDUNGSLÖSUNGEN

Autos, Kühlschränke, Industriemaschinen: Dinge werden immer smarter und tauschen über das Internet oder untereinander vernetzt Informationen aus. Die Industrie hat das Potenzial für sich erkannt – kombiniert mit dem Industrie 4.0-Ansatz entstehen Lösungen zum Industrial Internet of Things (IIoT).

Das IIoT hilft, Produktionsprozesse zu optimieren und vor allem Ausfälle von Komponenten zu erkennen, bevor sie ganze Fabriken lahmlegen. Auch Lapp hat bereits Lösungen für das Industrielle Internet der Dinge im Angebot und baut dieses weiter aus. Nun zeigt der Marktführer für integrierte Kabel- und Verbindungssysteme drei vielversprechende Neuentwicklungen und Konzepte.

Predictive Maintenance Box: Ausfallprognose für Ethernet-Leitungen. Das erste Konzept hat Lapp bereits vor einigen Monaten vorgestellt, jetzt ist es als seriennaher Prototyp einsetzbar: die Predictive Maintenance Box, kurz PMBx, ist jetzt klein, kompakt, robust und flexibel auch in bestehende Systeme integrierbar. Sie meldet rechtzeitig, wann eine Ethernet-Leitung ausfallen wird. Damit vermeidet die Box überraschende und dadurch teure Anlagenausfälle und hilft bei der Planung von Wartungsarbeiten. Was die Lösung von Lapp von allen anderen Konzepten unterscheidet: die Box wird einfach in Serie an die Datenleitung gesteckt, spezielle Sensorelemente in der Leitung oder gar ein zweites Gerät am Leitungsende sind unnötig. Somit ist die Eignung auch als Retrofit für ältere Anlagen gegeben. Anwender können die Box per WiFi über das IoT-Protokoll MQTT an ein Gateway oder eine Cloud anbinden. Aber auch das leitungsgebundene Abgreifen des Signals über einen digitalen Ausgang oder IO-Link sind möglich. Die Box berechnet kontinuierlich den Lapp Predictive Indicator und schlägt Alarm, wenn die Übertragungseigenschaften einer Leitung nachlassen und ein Ausfall droht.

Smarter Service Loop mit eingebauter Sensorik. Für Sonderleitungen bietet es sich an, dass eine Überwachungssensorik direkt in das Kabel verbaut wird. Das ist zum Beispiel der Fall bei sogenannten Service Loops, wie sie oft auf Offshore-Bohrinseln zum Einsatz kommen. Diese Hybridleitungen versorgen die Anwendung neben Energie und Daten in der Regel auch mit Druckluft und hydraulischer Energie. Ihre Alterung vorherzusagen war bisher schwierig, vor allem aufgrund der unterschiedlichen Einsatzbedingungen und Aufbauten. Deshalb werden sie sicherheitshalber nach einem festgelegten Zeitintervall ausgetauscht. Mit dem Smarten Service Loop von Lapp ist das nicht mehr nötig. Es enthält eine Referenzleitung, Sensoren zur Überwachung der Umgebungsbedingungen sowie einen Mikrocontroller mit WiFi-Verbindung, der in der Verankerung des Kabels integriert ist oder im Schaltschrank untergebracht wird.

IoTKey: Fernüberwachung mit Plug and Play. Große Industrieanlagen etwa in der Öl- oder Chemieindustrie werden zunehmend mit Sensoren ausgerüstet, die Temperatur, Druck und andere Größen messen, um drohende Ausfälle zu erkennen oder die Produktqualität zu optimieren. Doch wie kommen die Daten über weite Distanzen in die Steuerzentrale? Mit dem neuen drahtlosen Mess- und Fernüberwachungssystem IoTKey offeriert Lapp eine praktische Plug and Play-Lösung für die drahtlose Ferndiagnose. Das System sammelt die Messwerte von bis zu drei Sensoren und überträgt sie zuverlässig und störungsfrei in anspruchsvollen industriellen Umgebungen. Die Übertragungsdistanzen können über Hunderte von Metern innerhalb von Gebäuden oder im Freien mit dem LoRaWAN-Protokoll (Long Range Wide Area Network) betragen. Der batteriebetriebene IoTKey-Transmitter kann je nach Bedarf in Anlagenteilen eingebaut werden; eine auf Energieeinsparung optimierte Elektronik garantiert einen störungsfreien Betrieb über Jahre hinweg. Die Inbetriebnahme dauert nur wenige Minuten.

www.lappaustria.at

VERANSTALTUNGSKALENDER

OKTOBER 2020

it-sa 365
seit 6.10.2020 | online

Digital Transformation World Series
7.10.-12.11.2020 | virtuell

NOVEMBER

ICS Industrial Control Cyber Security Europe
3.-4.11.2020 | virtuell

Confare #IDEE2020
4.11.2020 | Wien

IoT-Fachkongress - Austrian Standards
4.11.2020 | virtuell

IT-Security Expertinnen NOW - VÖSI
4.11.2020 | Wien

IoT Forum - Succus
5.11.2020 | Wien

electronica virtual
9.-12.11.2020 | virtuell

AfricaTech Festival
9.-13.11.2020 | virtuell

Hypermotion
10.-12.11.2020 | Frankfurt/Main, hybrid

Cloud Strategies
11.11.2020 | virtuell

Digital Austria – AI konkret
12.11.2020 | Wien

VWE – Virtual Workplace Evolution
16.-17.11.2020 | Berlin

Rethink! IT Security
16.-17.11.2020 | Berlin

The Women in Technology World Series
16.-20.11.2020 | virtuell

Connected Germany
17.-18.11.2020 | virtuell

Smart City Live
17.-18.11.2020 | virtuell

Swiss IT Conference
18.11.2020 | Zürich

Digital X
19.-20.11.2020 | Köln

A1 IoT Show
23.11.2020 | virtuell

Cyber Crime Forum Wien
23.11.2020 | Wien

JVM-Con
23.-25.11.2020 | Köln

IoT Tech Expo Europe virtual
24.-25.11.2020 | virtuell

Big Data Conference Europe Online
24.-26.11.2020 | virtuell

SPS Connect
24.-26.11.2020 | virtuell

DEZEMBER

Ertl-Yang CIO Enterprise Summit
1.12.2020 | München

Web Summit
2.-4.12.2020 | virtuell

Smart Inside IT Security
9.12.2020 |virtuell

Paris Blockchain Week Summit
9.-10.12.2020 | Paris, hybrid

FEBRUAR 2021

Smart Inside IT Security
23.2.2021 |virtuell

DACH StrategyForum Internet of Things
23.2.2021 | virtuell

secIT by Heise
24.-25.2.2021 | Hannover

MÄRZ

embedded world
2.-4.3.2021 | virtuell

DHK Technologieforum
4.3.2021 | Wien

Internet World Expo
9.-10.3.2021 | München

IoT Tech Expo Global
17.-18.3.2021 | London

CloudFest
20.-25.3.2021 | Europa-Park/Rust

APRIL

WeAreDevelopers World Congress
15.-16.4.2021 | Berlin

MAI

Tech Jobs Fair Vienna
6.5.2021 | Wien

IoT Solutions World Congress
11.-13.5.2021 | Barcelona

StrategieTage Big Data
18.-19.5.2021 | Köln

Digital Transformation Expo Manchester
19.-20.5.2021 | Manchester

.NET Day Switzerland
20.5.2021 | Zürich

More-IP
26.-27.5.2021 | Amsterdam

JUNI

Datacloud Global Congress
1.-3.6.2021 | Monaco

VORSCHAU

IoT4 NR. 1 | Erscheinungstermin: **8. März 2021**

AFRICA TECH FESTIVAL

Wer davon ausgeht, dass Künstliche Intelligenz, Blockchain, Big Data oder IoT keine Themen in den Ländern Afrikas sind, hat vieles nicht mitbekommen. Diese Technologien sind auch dort, allen voran in den SSA- (Sub Sahara Africa) Ländern, in verschiedener Ausprägung zu finden – und sie wachsen. Auf dem im November stattfindenden Africa Tech Festival ist IoT4 Industry&Business anwesend und berichtet in der kommenden Ausgabe im 1. Quartal 2021 über die Highlights.

IT TRENDS 2021?

Nach einem auch für die Security-Branche aufwirbelnden Jahr 2020 wird es 2021 vermutlich nicht besser werden. Hacking ist nachwievor Thema, fragile technische Infrastrukturen ebenfalls. Somit spielen im Bereich Security Entwicklungen und Trends eine immens wichtige Rolle, die wir auch in der kommenden Ausgabe wieder detailliert beleuchten.

Impressum

Medieninhaber und Verleger:
Technik & Medien Verlags Ges.m.b.H.
Traviatagasse 21-29/8/2, 1230 Wien
Tel.: +43/(0)1/ 876 83 79-0
Fax: +43/(0)1/ 876 83 79-15

Chefredaktion:
Stephanie Englert
+43/(0)676/848 205 11
s.englert@technik-medien.at

Freie Mitarbeiterin:
Mag. Barbara Sawka

Anzeigenverkauf:
Thomas Lunacek, DW 13
+43/(0)676/848 205 13
t.lunacek@technik-medien.at

Mag. (FH) Gudrun Lunacek
+43/(0)676/848 205 12
g.lunacek@technik-medien.at

Administration, Redaktionsassistenz, Abo-Service:
Gilda Csokor, DW 14
+43/(0)676/848 205 14
g.csokor@technik-medien.at

Anzeigenverkauf Schweiz:
Arack-Media
Tel.: +41 62 87 19 162
info@arack.ch

Art Direction:
Tom Sebesta

Druck:
Ferdinand Berger & Söhne GmbH
Wiener Straße 80, 3580 Horn

Der Verlag nimmt Manuskripte zur kostenlosen Veröffentlichung an. Honorare ausschließlich nach Vereinbarung. Für unverlangt eingesandte Manuskripte wird keine Verantwortung übernommen. Nachdruck oder Kopien von Beiträgen bzw. Teilen davon nur mit Genehmigung. Der Verlag behält sich vor, Beiträge auch in anderen verlagseigenen Zeitschriften zu publizieren bzw. für Sonderdrucke zu verwenden. Das Copyright der Bilder liegt, wenn nicht anders angegeben, bei den jeweiligen Firmen bzw. beim Verlag.

4. Jahrgang

Auflage: 13.000 Exemplare

IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

Zum kostenlosen Abo

HABEN SIE NOCH FRAGEN?

Stephanie Englert, Chefredaktion
s.englert@technik-medien.at

Gudrun Lunacek, Vertrieb und Marketing
g.lunacek@technik-medien.at

T&M TECHNIK & MEDIEN VERLAGSGMBH

www.iot4industry.info

Make your life easier.

Nutzen Sie die Softwareplattform zenon zur Automatisierung Ihrer Smart Factory:

- *Berichte unmittelbar erstellen und analysieren*
- *Ergonomisch visualisieren und steuern*
- *Daten umfangreich erfassen und verwalten*
- *Applikationen schnell projektieren und warten*

www.copadata.com/zenon

zenon
by COPA-DATA