Online Version

Cloud Integration	Industrie 4.0 Internet of Things	Big Data Analytics	CxO Innovation Service

CxO Innovation Platform:
IT-Innovationen für den Unternehmenserfolg entdecken!

PAC CxO Innovation Monthly

- Oktober 2016 -

Liebe Leserin, lieber Leser,

heute möchte ich mit einem Appell beginnen:
Lassen Sie uns nach den richtigen Lösungen suchen und nicht die Zukunftstrends verteufeln!

Digitalisierung ist ein Trend, der vielleicht als (wenig konkreter) Begriff kritisiert werden kann, ABER der Einfluss auf unser zukünftiges berufliches und privates Leben ist kaum abzustreiten. Trotzdem wird dies immer wieder in der Öffentlichkeit zelebriert (siehe die Talkrunde von Anne Will zu „digitalen Arbeitswelten).

Sicher birgt die Digitalisierung für viele Gesellschaftsschichten Risiken, aber eben auch Chancen. So wird, aufgrund der Alterspyramide in Deutschland, eine Verlängerung der Lebensarbeitszeit (bzw. des Renteneintrittsalters) für viele Berufe nur möglich sein, wenn körperlich schwere Tätigkeiten „digitalisiert“ werden und somit der Mensch entlastet wird. Dazu gehören dann auch neue Möglichkeiten in präventivem Gesundheitswesen und Life Science. Wir sind gerade dabei, einige dieser Beispiele für unser Innovation Register zu analysieren und aufzubereiten.

Das Thema Security wird oft als „Show Stopper“ missbraucht. In der heutigen Ausgabe setzen wir daher wieder einen Schwerpunkt zu diesem Thema, u.a. mit dem Artikel: „Digitalisierung in SAP-Umgebungen: Sensible Daten schützen, auch gegen sorglose Mitarbeiter“. Hier geht es um Bewusstsein und Lösungen, nicht um negative Publicity. Auch weitere Security-Aspekte – im Zusammenhang mit Industrie 4.0 und IoT – greifen wir in dieser Ausgabe auf.

Mit freundlichen Grüßen

Andreas Zilch
Susanne Grebe

Thema des Monats

Digitalisierung in SAP-Umgebungen:

Sensible Daten schützen, auch gegen sorglose Mitarbeiter

Die IT-Sicherheit spielt in deutschen Unternehmen eine zentrale Rolle. Die Bereitschaft zu Investitionen ist vorhanden, und anders als in früheren Jahren wird die IT-Sicherheit nicht ausschließlich als lästige Pflichtaufgabe wahrgenommen, sondern als bedeutsamer Schutz von kritischen und wichtigen Unternehmenswerten. Aufgrund der medialen Berichterstattung rücken vielerorts Maßnahmen zur Abwehr externer Angreifer ins Zentrum des Interesses, obwohl vor allem den CIOs und den Sicherheitsverantwortlichen durchaus bewusst ist, dass die größte Gefahr für die Datensicherheit von den eigenen Mitarbeitern oder Partnern mit Zugang zu sensiblen Unternehmensdaten ausgeht.

Abbildung 4: *Viele Unternehmen erachten Mitarbeiter als Sicherheitsrisiko. Das ist kein Misstrauensvotum. Oft bereitet der unachtsame Umgang mit Daten Sorge.*

Dabei müssen Verfehlungen beim Datenschutz und bei der IT-Security durch eigene Mitarbeiter oder durch Partnerfirmen gar nicht immer vorsätzlich geschehen. Eine Personalakte hat den Schutz der gesicherten IT-Umgebung eines Unternehmens verlassen, sobald sie der wohlmeinende Kollege auf seinen USB-Stick geladen hat, um sie nach Feierabend zu Hause noch zu bearbeiten. Derartige Unachtsamkeiten im Umgang mit unternehmens-kritischen Daten wie etwa Materialstücklisten oder Konstruktionszeichnungen können wirtschaftliche Schäden anrichten, wenn die Daten über Umwege etwa in die Hände von Konkurrenten gelangen.

Doch auch der Gesetzgeber versteht in Sachen Datenschutzverletzung keinen Spaß. Unternehmen wie auch den Verantwortlichen drohen rechtliche Konsequenzen, wenn mit dem Datenschutz und der Gefahrenabwehr fahrlässig umgegangen wird. Da in der Mehrzahl der großen deutschen Unternehmen Lösungen von SAP als zentrale Business-Applikationen im Einsatz sind, konzentriert sich dieses Whitepaper auf IT-Sicherheit und Datenschutz sowie GRC-Aspekte (Governance, Risk, Compliance) in SAP-Umgebungen.

PAC möchte mit diesem Report für die Gefahren durch den unkontrollierten Datenabfluss sensibilisieren und auf Wege für einen sorgsamen Umgang mit unternehmenskritischen Daten hinweisen. Vor allem erscheint es uns wichtig, dass Unternehmen ihre herkömmlichen Wege der Gefahrenabwehr und des Datenschutzes kritisch durchleuchten und neue Lösungen in Betracht ziehen, die dem Schutz der Datenquelle eine größere Beachtung schenken.

Fünf Handlungsfelder für mehr Sicherheit in zentralen ERP-Installationen:

- Informieren Sie Ihre Mitarbeiter über datenschutzrelevante Aspekte im Umgang mit kritischen Daten. Dabei sollten keine gesetzlichen und juristischen Argumente im Vordergrund stehen, sondern reale Szenarien aus dem jeweiligen Arbeitsumfeld.
- Analysieren Sie Ihre vorhandene Security-Installation und ERP-Umgebung auf Schwachpunkte hinsichtlich der Möglichkeit, kritische Daten und Dokumente zu downloaden und lokal zu speichern.
- Machen Sie Bestandsaufnahme der digitalen Inhalte. Welche Art von Dokumenten, aber auch welche strukturierten Daten werden besonders häufig bearbeitet und heruntergeladen? Wie geschäftsrelevant und sensibel sind die Inhalte?
- Installieren Sie besondere Schutzmechanismen für besonders kritische Daten. Achten Sie darauf, dass die anwenderfreundliche Nutzung erhalten bleibt. Datenschutz und Security dürfen die Abläufe nicht komplizierter machen, sonst werden Schutzmechanismen von Mitarbeitern unterlaufen.
- Sorgen Sie für Transparenz bei der Bearbeitung und Speicherung kritischer Daten und Dokumente. Veränderungen sollten auch aus Compliance-Gründen dokumentiert werden.

Lesen Sie weiter und erfahren Sie, warum es wichtig ist, dem Schutz auf inhaltlicher Ebene mehr Beachtung zu schenken, indem etwa Dokumente und Daten je nach ihrer unternehmenskritischen Bedeutung klassifiziert und geschützt werden:

Link zum Whitepaper

Vendor-Profil des Monats:

Download: Sopra Steria

NEW – CUSTOMER BENEFITS

(Innovation Register – ausgewählte Best Practices)

Die in diesem Use Case vorgestellte Spedition unterhält seit vielen Jahren Geschäftsbeziehungen zu bedeutenden Anbietern der Systemgastronomie. Das Unternehmen positioniert sich als Full-Service-Provider für sämtliche Waren rund um den Betrieb von Restaurantketten. Es versorgt die Restaurants sowohl mit frischen und tiefgefrorenen Lebensmitteln als auch mit Verbrauchsgütern aus dem Non-Food-Bereich. Die Spedition ist weltweit tätig, mit Schwerpunkt auf Deutschland und Europa, unterhält eine Vielzahl von Distributionsstützpunkten und gewährleistet damit den Kunden schnelle Lieferung bei geringer Lagerhaltung. Aufgrund der jahrelangen Geschäftsbeziehungen kennt die Spedition die Bedarfe der Kunden sehr genau. Die Lieferungen und jeweiligen Mengen werden seit Jahren genau dokumentiert. Die somit angesammelte große Datenbasis birgt demnach einen enormen Wissensschatz.
Aus der Kombination von Big Data, Analytics und Smart Logistics wurde eine innovative Geschäftsidee entwickelt. Kern der neuen Kundenservices bilden Tracking & Tracing-Lösungen zur optimalen Steuerung der Fahrzeugflotte sowie Business-Intelligence-Anwendungen zur Bedarfsanalyse der Kunden und jeweiligen Restaurants.
Die grundlegende Idee ist, dass die gesamte Supply Chain an den künftigen Bedarfen am Point of Sale ausgerichtet wird. In die Prognose fließen sowohl Analysen historischer Daten als auch externe Paramater wie Trends, Jahreszeiten, Feiertage, Events und besondere Werbeaktionen ein. Sämtliche Einflussfaktoren werden mit Hilfe analytischer und statistischer Methoden ausgewertet und zu einer genauen Bedarfsprognose verdichtet, die die erwarteten Verkäufe pro Tag, Verkaufsstelle und Einheit enthält.

„Einzelhändler sind gut beraten, die herkömmliche Bedarfsplanung, die sich vor allem am Point of Sale orientiert, durch Predictive-Analytics-Technologie zu ersetzen. Predictive Analytics ist eine anspruchsvolle Technologie, die Informationen aus verschiedenen Quellen zusammenführt; hierzu zählen externe Quellen wie soziale Medien, Wetter, aktuelle Ereignisse, Bevölkerungsmuster und sogar Verkehrsmeldungen. Sie können den Einzelhändlern dabei helfen, Nachbestellungspunkte sowie Bestandssortimente zu planen."

Steven Rodgers – Vice President of Business Development, HAVI Global Solutions
Source: HAVI & Magazine Storebrands

Find more information: Use Case ID: 2015-07-0077

Innovation Register

Aktuell:
300 Cases online

Entdecken Sie interessante Anschauungsbeispiele, die Ihnen als Best Practices für eigene Initiativen dienen können.

kuppingercole ANALYSTS

Cognitive Security – the next big thing in security?

There are good reasons for the move towards "Cognitive Security". The skill gap in Information Security is amongst the most compelling ones. We just don't have sufficient skilled people. If we can make computers step in here, we might close that gap. On the other hand, a lot of what we see being labeled "Cognitive Security" is still far away from really advanced, "cognitive" technologies. Marketing tends to exaggerate. On the other hand, there is a growing number of examples of advanced approaches, such as IBM Watson – focusing on filtering the unstructured information and delivering exactly what an Information Security professional needs.

Cognitive Security: The Future of Cybersecurity is Now

The proverbial 'Computing Troika' that KuppingerCole has been writing about for years does not show any signs of slowing down. The technological trio of cloud, mobile and social computing, as well as their younger cousin, the Internet of Things, has profoundly changed the way our society works. Modern enterprises were quick to adopt these technologies, which create great new business models, open up numerous communication paths to their partners and customers, and, last but not least, provide substantial cost savings. We are moving full speed ahead towards the Digital Era, and the future is full of promise. Or is it?

Webinar:
Sicherheit in den operativen Systemen der Industrie 4.0

Donnerstag, 17. November – 10.00 Uhr

Mit der Entwicklung zur Industrie 4.0 wird die Grenze zwischen klassischer IT und Operational Technology zunehmend durchlässiger. Während dies einerseits die Effizienz und die Agilität bei der Administration erhöht, führt diese IT/OT-Konvergenz zu einer rapide anwachsenden Gefährdung kritischer Systeme. Waren diese bislang physikalisch und/oder logisch isoliert und konnten durch Zugangskontrolle vermeintlich angemessen geschützt werden, sind sie heute vom Unternehmensnetzwerk oder aus dem Internet erreich- und kontrollierbar.

Dieses Webinar konzentriert sich auf Aspekte und Mitigationsstrategien für die Absicherung privilegierter Accounts in ICS/OT-Umgebungen:

- Quantifizierung der Risiken und Reduzierung der Angriffsfläche
- Absicherung und Überwachung der Zugriffe von außen
- Schutz vor Angriffen durch Malware, etwa Ransomware
- Erkennung verdächtiger Aktivitäten

zur Anmeldung

Matthias Reinwarth
Senior Analyst,
KuppingerCole

IoT in Produktion und Logistik

3 Fragen an:
Joachim Hackmann

Wie gut sind Unternehmen der Fertigungs- und Logistikbranche heute auf das Thema IoT vorbereitet?

Das Interesse an IoT in den Branchen ist sehr groß, doch die infrastrukturellen Voraussetzungen sind vielerorts noch nicht ausreichend vorhanden. Insgesamt zeigt sich beispielsweise, dass viele Unternehmen ihre Produktions- und Logistikumgebung zwar vernetzt haben, für durchgehende IoT-Funktionalität reicht die aktuelle Installation aber nicht aus. Logistiker sind heute bereits deutlich besser vernetzt als Unternehmen aus der Produktion. Das liegt unter anderem daran, dass sie schon immer mit mobilen Gütern umgehen mussten und sich sehr früh um Tracking & Tracing-Lösungen bemüht haben. Ihr besonderes Interesse, die IoT-Verfahren noch intensiver in ihre Lieferprozesse einzufügen, liegt nicht zuletzt auch an dem hohen Innovationstempo der Online-Händler, die mit neuen Lieferkonzepten die etablierten Speditionen unter Druck setzen.

Webinare

Alexei Balaganski,
Lead Analyst, KuppingerCole
Reinventing Smart Cards for the Modern Agile, Connected Enterprise

03. November 2016,
16.00 Uhr, Webinar (EN)

Martin Kuppinger, Principal Analyst, KuppingerCole
Beyond User names and Passwords: 3 Steps to Modern Authentication

10. November 2016,
16.00 Uhr, Webinar (EN)

Veranstaltungen

Micro Smart Grid
Innovative Energiesysteme in der Praxis – Fraunhofer IAO

01. November 2016,
Stuttgart

7. Aachener Informationsmanagement-Tagung vom

07. – 09. November 2016,
Aachen

Industrie 4.0 - konkret

08. November 2016,
Lippstadt

BARC Congress für Business Intelligence und Datenmanagement

08.- 09. November 2016,
Würzburg

CRM Summit

08. – 09. November 2016,
Würzburg

Was sind die wichtigsten Motivationsfaktoren für Investitionen in IoT-Projekte?

Laut dem Ergebnis unserer aktuellen Studie sind Effizienzdruck (77 Prozent), die Steigerung der Wettbewerbsfähigkeit (73 Prozent) sowie die Erhöhung der Agilität und Flexibilität (71 Prozent) die wichtigsten Faktoren. Nach Einschätzung der befragten Entscheider muss dazu aber der Grad der Vernetzung deutlich steigen: 82 Prozent der Befragten streben in vier Jahren eine Umgebung an, die zu mehr als der Hälfte vernetzt ist. Stand heute hat weniger als die Hälfte der Befragten eine Vernetzung, die mindestens 50 Prozent der Produktions- und Logistikumgebung abdeckt. Von einer besseren IoT-Durchdringung versprechen sich die Unternehmen vor allem eine fortwährende Optimierung der Produktion und Logistik (88 Prozent); 87 Prozent zielen auf mehr Transparenz über den aktuellen Stand von Anlagen, Maschinen und mobilen Gütern ab und 83 Prozent würden durch IoT-Projekte gern ungeplante Standzeiten vermeiden.

In welchen Bereichen wird in Zukunft verstärkt investiert?

Künftig wollen Unternehmen unter anderem in Sensorik und vor allem in sicherheitsrelevante Aspekte investieren. Denn: Je mehr Produktionsanlagen vernetzt sind, desto anfälliger sind sie für Attacken. Dass Unternehmen den digitalen Wandel nicht immer alleine schaffen können, ist ihnen offenbar bewusst: So planen 65 Prozent, bei ihren IoT-Vorhaben die Unterstützung eines externen Dienstleisters in Anspruch zu nehmen.

Link zur Studie

Joachim Hackmann
Principal Consultant –
Software & Related Services
j.hackmann@pac-online.com

Blogbeiträge & Research Notes, White Paper

Jetzt bringt Amazon die künstliche Intelligenz ins Wohnzimmer

IoT: Die Vernetzung ist erst am Anfang

Bauen 4.0: So digitalisiert Rhomberg den Bau

VW Nutzfahrzeuge startet Logistik-Cloud

Digitized Trucking: Betriebskosten von Fernverkehrs-LKW sinken durch digitale Fahr- und Assistenzsysteme um bis zu 15 %

Microsoft Cloud Deutschland: Azure IaaS-, PaaS- und IoT-Dienste aus deutschen Rechenzentren verfügbar

Big Data läuft nicht einfach so nebenher

Telekommunikations- und Automobilunternehmen gründen globale branchenübergreifende 5G Automotive Association

Wo steht Security 4.0 in Industrie 4.0?

09. November 2016,
Köln

11. ÖCI-BARC-TAGUNG

16. November 2016,
Wien

MEDICA HEALTH IT FORUM

14. – 17. November 2016,
Düsseldorf

**Workshop KuppingerCole:
Der neue Datenschutz –
Crashkurs für IT-Professionals**

07. Dezember 2016,
Frankfurt / Main

Digital Finance World 2017

01. - 03. März 2017,
Frankfurt

Business Intelligence Agenda

27. - 28. März 2017,
Zürich

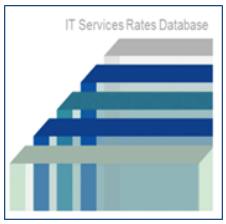
**Eic2017
European Identity & Cloud
Conference 2017**

09. - 12. Mai 2017,
München

**BARC:
BI- & Planungssysteme im
direkten Vergleich 2017**

16. - 17. Mai 2017,
Würzburg

Informationen



Wurde Ihnen diese E-Mail weitergeleitet, und Sie möchten regelmäßig von PAC Deutschland informiert werden,

können Sie sich hier für den Newsletter-Empfang registrieren.

Wenn Sie diesen Newsletter abbestellen möchten, senden Sie bitte eine kurze E-Mail mit dem Titel "unsubscribe CxO Monthly" an **s.grebe@pac-online.com**

PAC Deutschland
Holzstraße 26
80469 München
Tel: +49 (0)89 23 23 68-0
PAC Blog / LinkedIn / Twitter / E-Mail
Impressum

Bitte beachten Sie, durch aktivieren des "unsubscribe Buttons" am Ende dieser Mail werden Sie von allen PAC Verteilern entfernt.