Ausgabe November 2018

its-people Magazin

itspeople

© Sitthiphong/istock

Schwerpunktthema

Informationssicherheit

we make the difference

Sehr geehrte Leserin, sehr geehrter Leser,

Herzlich Willkommen zu unserer 2. Ausgabe des its-people Magazins! Wir haben uns sehr über das positive Feedback zu Inhalten und Layout gefreut. Für uns ein großer Ansporn, Sie weiterhin qualifiziert mit aktuellen Themen rund um die IT quartalsweise zu informieren.

Schwerpunkt unserer heutigen Ausgabe ist die Informationssicherheit. Wie einfach war doch früher die Welt: Man erstellte ein Produkt oder einen Service und prüfte dann, welche Aspekte unter IT-Security Gesichtspunkten zu berücksichtigen waren. In einer immer komplexeren und vernetzteren Welt reicht dies heute allerdings nicht mehr aus. „Security by Design" heißt hier das Schlagwort. Bereits in der Konzeptionsphase müssen heute Anforderungen an die Informationssicherheit beachtet werden, um gegen Sicherheitsrisiken gewappnet zu sein. Diesen Aspekt greift Dirk Größer in seinem Artikel auf „Wann hatten Sie Ihre letzte Datenpanne?". Proaktives Sicherheitsmanagement, um Risiken frühzeitig zu erkennen.

Im folgenden Artikel „Security Awareness" wird aufgezeigt, dass wir möglicherweise zu einem großen Sicherheitsrisiko für die IT-Systeme werden können, ohne dass wir es bewusst wahrnehmen. In Zeiten von Phishing, dem Identitätsdiebstahl, wird es immer schwerer, Echtes von Unechtem zu unterscheiden.

Aber der Supergau für unsere digitale Welt wäre ein Leben ohne Strom! Nach wenigen Stunden keine WhatsApp Nachrichten mehr, das iPhone nicht mehr zu benutzen – unvorstellbar! Was passiert eigentlich alles, oder besser gesagt was funktioniert eigentlich nicht mehr, wenn wir ohne Strom sind. Nicht nur Marc Elsberg schreibt zu diesem Thema, sondern auch unser Gastautor Tobias Greilich. Lesen Sie in dieser Ausgabe den ersten Teil des Artikels „Blackout – die Achillesferse der Digitalisierung" und freuen Sie sich auf eine spannende Fortsetzung im nächsten its-people Magazin.

So, nun erstmal Luft holen und gegebenenfalls einen Cappuccino trinken. Dabei erklären wir Ihnen, wie Sie mit Oracle APEX Social Sign-In Funktionen einrichten und wie Sie mit SAP S/4HANA Ihre SAP Infrastruktur in die Zukunft bringen.

Und wer hätte gedacht, dass der Chaos Computer Club schon siebenunddreißig Jahre alt ist? Lassen Sie sich entführen in die Welt der „Komputerfrieks". Uwe Blenz, Seniorberater bei its-people und langjähriger Teilnehmer der CCC-Kongresse, schreibt über die Gründung, die ersten Hacks und aktuelle Veranstaltungen des Clubs. Damals war das Hacken noch die Kür für begeisterte Computerfans. Heute ist es ein gigantisches Spiel um Macht, Geld, Manipulation und Kontrolle.

Abschließend weisen wir Sie noch darauf hin, dass Sie die Chance haben, uns live zu erleben. Unsere Portfolio Manager Sabine Heimsath und Robert Marz sind auf der DOAG in Nürnberg als Speaker und Moderatoren vertreten. Die zweite Chance ergibt sich dann bei den Frankfurter IT-Tagen im Kap Europa. Hier werden wir als Gold Partner mit einem Messestand vor Ort sein und zugleich auch einen Workshop zum Oracle SQL Developer durchführen.

Bleibt uns zum Schluss nur noch zu sagen: Gönnen Sie sich eine gute Tasse Kaffee, nehmen Sie sich ein bisschen Zeit und stöbern Sie in der neuen Ausgabe des its-people Magazins.

Viel Spaß beim Lesen!
Ihr Frank Sommerer

Latte Macchiato

Wann hatten Sie Ihre letzte Datenpanne? 4
Security Awareness – brauchen wir das? 6
Blackout – die Achillesferse der Digitalisierung 8

Cappuccino

Neue Social-Sign-In Funktionen für Oracle APEX einrichten 11
SAP S/4HANA – Die Zukunft erwartet uns!? 15

Espresso

Vom „Komputerfriektreffen" zu einem der größten Kongresse Europas 17
Hätten Sie's gewusst? 18
Vorstellung interner Partner 18
Treten Sie ein in Ihre neue Zukunft 19

Café

NightRun 2018 21
DOAG 2018 21
UKOUG 2018 22
IT-Tage 2018 23

IMPRESSUM: Herausgeber: enterpriser GmbH; Redaktion: Frank Sommerer, Birgit Kraemer, Isabell Kraemer; Grafik/Design/Layout: Sarah Graf Kommunikationsdesign; Photos: Fotolia, Adobe Stock, iStock, Pixabay, Shutterstock, Matthias Klepp;

© enterpriser GmbH 11/2018; Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium als Ganzes oder in Teilen bedarf der schriftlichen Zustimmung. Die Informationen und Angaben wurden nach bestem Wissen und Gewissen recherchiert. Die Nutzung dieser Informationen und Angaben geschieht allein auf eigene Verantwortung. Eine Haftung für die Richtigkeit der Informationen und Angaben, insbesondere für die Anwendbarkeit im Einzelfall, wird nicht übernommen. Meinungen stellen die Ansichten der jeweiligen Autoren dar und geben nicht notwendigerweise die Ansicht der Herausgeber wieder.

© istock

its-people GmbH
Wir bringen Ihre Projekte auf die richtige Spur!

IT-Beratungen gibt es viele auf dem Markt. **its-people** ist aber eine deutliche Spur anders!

its-people basiert auf einem innovativen Konzept: ein Unternehmensverbund, der selbständige IT-Berater als Teilhaber einer Gesellschaft durch vielfältige Management- und Vertriebsleistungen unterstützt. Die IT-Berater sind also einerseits selbständig mit ihrem unternehmerischen Handeln und genießen gleichzeitig die Einbindung in einen starken Unternehmensverbund. So entsteht ein umfassender Kompetenzpool mit außergewöhnlichen Synergien!

its-people setzt seit der Unternehmensgründung 2003 alles daran, seine Kunden zu begeistern und gemeinsam eine optimale Lösung für deren Anforderungen zu finden!

Unser Portfolio

- IT-Security
- Datenbanken und Cloud
- Analytics und Data Warehouse
- Anwendungsentwicklung
- Customer Data Integration
- Projekt-Management Services

its-people

- IT-Consulting
- Hochqualifizierte, selbständige IT-Experten
- Mehr als 15 Jahre Erfolg am Markt
- Gemeinsam stark!

Unsere Stärken

- IT- und Fachkompetenz
- Kundenfokussiert
- Qualitätsorientiert
- Umsetzungsstark
- Partnerschaftlich
- Der Mensch im Mittelpunkt

Wann hatten Sie Ihre letzte Datenpanne?

Kann man Informationssicherheit proaktiv betreiben? Ja, man kann! Ein gutes Schwachstellenmanagement erkennt Risiken, bevor sie eintreten (z.B. die Ransomware WannaCry oder Petya). Dieser Beitrag stellt dar, wie sich Schwachstellenmanagement in ein Managementsystem für Informationssicherheit (Information Security Management System) integriert.

In der heutigen Zeit ist das unternehmerische Handeln einer wesentlich größeren Dynamik unterworfen als in der Vergangenheit. Die Rahmenbedingungen und Märkte stellen immer wieder neue Anforderungen in immer kürzeren Zeitperioden. Zudem sind eine Vielzahl unterschiedlicher, digitalisierter Informationen zu einem integralen Bestandteil von Geschäftsprozessen geworden, Stichwort „Industrie 4.0“. Die daraus resultierende wachsende Komplexität und eine immer aggressiver werdende Bedrohungslage erschweren es zunehmend, diese Informationen und Werte nachhaltig und angemessen zu schützen. Wir können das an den immer häufiger in den Medien publizierten Datenpannen ablesen.

Eine Reaktion der Politik ist die Konkretisierung der gesetzlichen und regulatorischen Anforderungen an Informationssicherheit und Datenschutz für Wirtschaft und Behörden. Als Beispiel seien hier die KRITIS VO, die Europäische Datenschutzgrundverordnung (EU-DSGVO) und die MaRisk genannt. Die Essenz der genannten Gesetze, Verordnungen und Regelungen ist, ganz allgemein gesagt, die Forderung, ein dauerhaftes und wirksames Informationssicherheitsmanagement nach dem Stand der Technik zu betreiben, welches dann in der Ausgestaltung häufig als **Managementsystem für Informationssicherheit (ISMS)** bezeichnet wird.

Ich möchte einen häufig unterschätzten Aspekt aus dem Bereich des ISMS vorstellen, nämlich den Umgang mit vermuteten Sicherheitsvorfällen. Vermutet deshalb, weil man zu Beginn einer Meldung oder eines Alarms häufig noch nicht belastbar einschätzen kann, ob es sich überhaupt um einen tatsächlichen Sicherheitsvorfall handelt.

Es sind im Vorfeld eine Kette von kausalen Schritten und Aktivitäten notwendig, um fachlich und prozessual überhaupt eine effiziente Sicherheits-

vorfallbehandlung durchführen zu können. Dabei sind die schnelle Erkennung und die angemessene Reaktion der Schlüssel, um die möglichen Auswirkungen des Vorfalls auf seine unmittelbare Umgebung zu begrenzen. Ein Angriffsversuch ist zunächst noch keine gravierende Sicherheitspanne. Wenn Sie aber Bedrohungen nicht zeitnah erkennen, priorisieren und wirksam neutralisieren können, entsteht daraus möglicherweise sehr schnell erheblicher Schaden für Ihre Organisation. Wie beispielsweise Imageschäden, verlorene Kundendaten oder Unterbrechungen durch die Nichtverfügbarkeit von Ressourcen.

Angriffsversuche sind leider häufig erfolgreich, da sich in vielen IT-Infrastrukturen von Betreibern unbemerkt Schwachstellen befinden, welche dann von Angreifern (mit den bekannten Folgen) ausgenutzt werden können. Und zu allem Übel werden solche Angriffe oft viel zu spät bemerkt.

Genau hier ist ein sinnvoll eingesetztes IT-Schwachstellen-Management (Vulnerability Management) eine wirkungsvolle Lösung. Damit sind Sie in der Lage, die Schwachstellen zu identifizieren und deren Behebung zu priorisieren, bevor Angreifer diese ausnutzen können. Außerdem qualifiziert es Sie, eine Neubewertung bezüglich der Verwundbarkeit Ihrer IT-Infrastruktur durchzuführen.

Mit IT-Schwachstellen-Management können Sie Ihre IT-Umgebung in ihrer ganzen Breite und Tiefe „wahrnehmen“ und gewinnen die Möglichkeit, Sicherheitsvorfälle wirkungsvoll und schnell zu entschärfen, bevor größere Schäden daraus entstehen können. So senken Sie erheblich das Risiko, dass eine schwere Datenpanne oder ein gravierender Cyber-Vorfall Ihrem Unternehmen teuer zu stehen kommt.

Zum Schluss noch ein Punkt, der mir in der Praxis sehr oft begegnet: Kunden sagen mir häufig, dass sie durch ihr bestehendes Patch-Management „alles im Griff haben“ und sie somit kein Schwachstellen-Management benötigen. Aber leider ist das eine absolut verfehlte Annahme: Patch-Management ist nicht Schwachstellenmanagement! Beide Prozesse liegen nahe beieinander, dürfen aber nicht miteinander verwechselt werden.

Das Schwachstellenmanagement ist ein proaktiver Prozess, welcher im zeitlichen Ablauf dem Patch-Management vorgelagert ist, um Schwachstellen zu erkennen. Gute Schwachstellen-Scanner erkennen nicht nur Schwachstellen, für welche ein Patch besteht, sondern identifizieren auch Schwachstellen zeitnah nach deren Bekanntwerden — auch wenn es noch keinen Patch dafür gibt.

Beim Patch-Management wird überprüft, inwiefern Patches für Betriebssysteme und die installierten Applikationen zur Verfügung stehen. Vom Bekanntwerden einer Schwachstelle bis zur Verfügbarkeit eines Patches kann es oft Monate dauern. Während dieser Zeit zeigt das Patch-Management keinen Handlungsbedarf an, obwohl ein Sicherheitsrisiko besteht.

Patch-Management ersetzt also nicht Schwachstellenmanagement und umgekehrt. Beide wirken wechselseitig ergänzend und steigern in geeigneter Kombination die Informationssicherheit Ihrer Organisation erheblich!

DIRK GRÖSSER
Senior Professional
its-people GmbH
dirk.groesser@its-people.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **info@its-people.de**

© jjumathaidesigners/shutterstock

Security Awareness – brauchen wir das?

© SFIO CRACHO/fotolia

Spätestens seit Einführung der neuen DSGVO ist wirklich in jedem Unternehmen das Thema Data-Security und Security im Allgemeinen in aller Munde. Doch leider unterschätzen auch heute noch viele Unternehmen die Wichtigkeit und Dringlichkeit von Informationssicherheit im Arbeitsalltag. Insbesondere der Faktor Mensch wird oft nicht entsprechend berücksichtigt. Im Folgenden werde ich das Thema Security Awareness vorstellen und beleuchten, welche Schritte aus meiner Sicht notwendig sind, wenn Sie Ihr Unternehmen und Ihre Daten sicherer machen wollen.

Die Galapagos Inseln wurden 1535 von Bruder Tomas de Berlanga entdeckt. Sie haben ihren Namen der Ähnlichkeit zwischen den Panzern der Riesenschildkröten und einem spanischen Sattel zu verdanken, dem zu dieser Zeit sogenannten „Galapago". Bis 1535 kannten die Inseln keine Räuber und die Pflanzenfresser lebten ein recht friedliches Leben. 1680 kamen dann die ersten Piraten und Freibeuter auf die Inseln. Englische Piraten bemerkten, dass die Inseln zwischen ihren Überfallen entlang der südamerikanischen Häfen ein ideales Versteck darstellten. Die Tiere waren bis dahin keine Feinde gewohnt. Die Freibeuter und Piraten bedienten sich also unbehelligt am großen Tisch und deckten sich mit Frischwasser, Früchten und dem Fleisch der Schildkröten ein. Da die großen Schildkröten lange ohne Wasser und Nahrung auskamen, waren sie ideal für die langen Schifffahrten. Auch andere Tiere fielen dem Menschen zum Opfer, da sie nicht vorgewarnt waren und sie sich nie auf Feinde einstellen mussten.

Bei **Security Awareness** verhält es sich ähnlich. Lange Zeit war es zum Beispiel so, dass ein Computervirus einen Computer befallen hat. Dieser wurde dann einfach neu aufgesetzt und die Daten, die auf Disketten gespeichert waren, wurden weiter verwendet. Die Vernetzung und Digitalisierung hat in den letzten Jahren aber rasant an Geschwindigkeit zugelegt. Es ist nun nicht mehr nur ein Rechner betroffen, sondern ein Schadprogramm kann innerhalb kürzester Zeit ein ganzes Unternehmen mit seinen kompletten Geschäftsprozessen zum Stillstand zwingen.

Viele der Betroffenen sind einfach nicht auf diese Bedrohung vorbereitet und stehen der Gefahr relativ schutzlos gegenüber!

Was ist nun beim Thema Informationssicherheit wichtig:

- ein Invest in sichere Technik?
- ein Invest in die Infrastruktur?
- ein Invest in den Umgang der Mitarbeiter mit Sicherheitsrisiken?

Lohnt es sich mehr, in sichere Technik zu investieren und über Policies und Richtlinien zu regulieren, an die sich die Mitarbeiter dann stoisch zu halten haben? Oder lohnt es sich vielleicht doch, auf die Mitarbeiter zu setzen und sie für die Gefahren der digitalen Welt zu sensibilisieren und zu schulen?

Zumeist sind interne **Security Awareness** Schulungen zeitlich auf ein paar Stunden begrenzt und verblassen in den darauffolgenden Wochen ganz schnell im „daily business". **Awareness** wurde nur kurzfristig geschaffen. Es gibt scheinbar keinen langfristigen Effekt. Oder zumindest kann dieser nicht effektiv gemessen werden. Doch wie ist es besser zu machen?

Das Thema **Security Awareness** wird auch unter Experten sehr kontrovers diskutiert. Beispielsweise **Bruce Schneier** hält es für reine Zeit- und Geldverschwendung. Er vertritt die Meinung, die Mittel lieber in sichere Schnittstellen und Entwicklungen zu investieren, was an sich ein guter Ansatz ist. Die Digitalisierung ist aber immer schneller und weiter voranschreitend. Viele Geschäftsmodelle, Prozesse und Dinge, die wir täglich erledigen, zentrieren sich immer weiter im digitalen Raum. Und nicht alle Eventualitäten lassen sich technisch oder durch Software abfangen.

WAS IST NUN SECURITY AWARENESS?

Security Awareness beinhaltet verschiedene Maßnahmen, um die Mitarbeiter für die Themen der Informationssicherheit zu sensibilisieren und sie darauf zu schulen, mit den täglichen Gefahren in der sich immer weiter vernetzenden Welt umzugehen.

Dabei werden die Mitarbeiter auf verschiedene Bedrohungen im Bereich der Computersicherheit und im Datenschutz geschult. Es wird ihnen das notwendige Wissen vermittelt, welches im optimalen Falle mit den Unternehmensrichtlinien, -prozessen, aber auch auf den Teilnehmerkreis abgestimmt ist.

So sollten die Mitarbeiter in einem Unternehmen wissen, wie sie sich bei einem Sicherheitsvorfall richtig zu verhalten haben:

- Welche Personen sind zu informieren?
- Welche Prozesse müssen gestartet werden?
- Wie ist das allgemeine Vorgehen überhaupt?

Etliche Regeln sind hinsichtlich der Produktivität zunächst einmal hinderlich. Damit stellt sich dann für viele Mitarbeiter die Frage nach der Sinnhaftigkeit einer solchen Maßnahme.

- Warum soll denn alle 8 Wochen das Passwort des Unternehmens-Accounts geändert werden?
- Warum soll man nicht den auf dem Parkplatz gefunden USB-Stick für die Firmenpräsentation verwenden?
- Und warum sollten Passwörter nicht auf Post-its am Bildschirm, sondern in einem verschlüsselten Passwortmanager abgelegt werden?

Der unbestrittene Komfort erschwert das Durchhalten eines erstellten Security Regelwerks. Vor allem dann, wenn ein offensichtlicher Grund fehlt, auf diesen ersatzlos gestrichenen Komfort und die angenehmen Funktionalitäten, die man vielleicht auch aus dem privaten Alltag kennt, zu verzichten. Wichtig ist dabei auch die **Nachvollziehbarkeit.** Viele Regeln, die aus der **Securitybrille** heraus betrachtet vollkommen sinnvoll sind, bleiben oft ohne weitere Erklärungen im Raum stehen, ohne den Hintergrund dafür zu beleuchten. Dies sollte vermieden werden. Hier schafft Transparenz mehr Sicherheit.

Ein weiterer, wichtiger Aspekt beim Training ist es im Fokus zu behalten, wer die angesprochenen Teilnehmer sind. Ein Vertriebler hat sicherlich einen anderen Schwerpunkt als ein Mitarbeiter aus der Finanzbuchhaltung und dieser wiederum eine vollkommen andere Sichtweise als bspw. ein Entwickler. Ist ein Unternehmen im Aufbau, kommen immer wieder neue Mitarbeiter an Bord oder das Unternehmen arbeitet viel mit externen Mitarbeitern zusammen. Dann macht es sogar absoluten Sinn, diesen **Awareness Prozess** in das On-Boarding zu integrieren.

Für ein hohes Maß an Informationssicherheit muss das Thema außerdem Teil der Unternehmensphilosophie sein. Durch die Verschärfung der DSGVO im Mai 2018 wurden die Unternehmen nun zumindest im Datenschutzbereich dazu verpflichtet, ihre Mitarbeiter im Rahmen einer technischen und organisatorischen Maßnahme weiterzubilden und zu schulen. Die Schulungen können als Präsenzveranstaltungen oder aber vollkommen digital, in Form eines Online-Trainings, stattfinden.

Ein wichtiger Schritt in die richtige Richtung!

Auch wenn viele Themen im Bereich der **Security Awareness** zunächst technisch getrieben sind, gilt es nicht nur den technischen Sicherheitsaspekt zu bedienen, sondern eben auch die „Awareness", also das Bewusstsein und das Verstehen zu schärfen. Das Wissen, welches sich die Mitarbeiter angeeignet haben, wirkt sich somit nicht nur auf deren Handeln im Unternehmen aus, sondern auch auf den Umgang mit den erlernten Skills im privaten Bereich. Weitergedacht ist dies auch ein Vorteil für die Unternehmen. Vor allem in Zeiten von **„Bring Your Own Device" Programmen,** die ein Unternehmen attraktiv machen und gleichzeitig Kosten senken sollen, ist Sicherheit kein zu unterschätzendes Risiko.

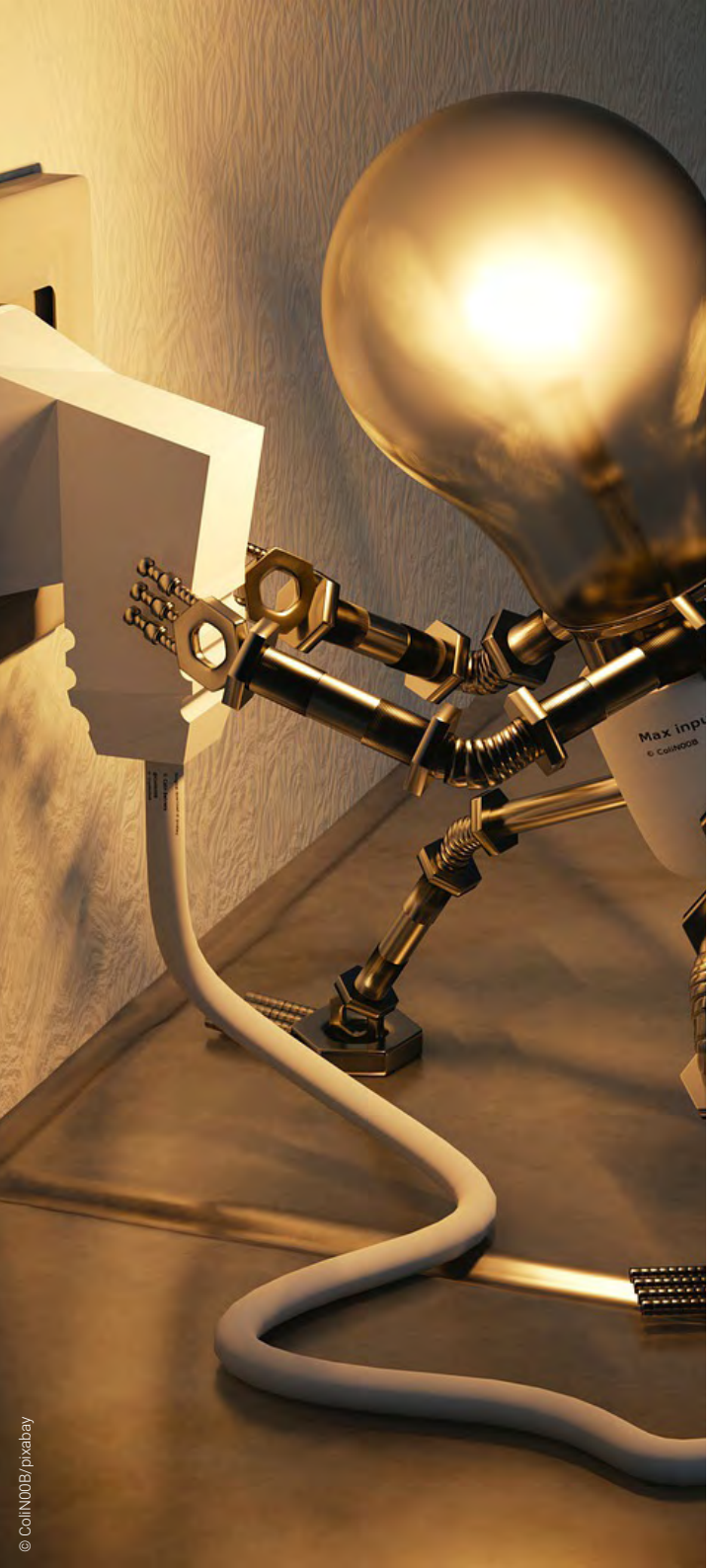
Es gibt immer mehr Software auf dem Markt, die Geschäftsanwendungen in einer Sandbox zum Laufen bringen, damit die Daten das Unternehmen nicht verlassen und die Compliance eingehalten wird. Aber fatal wird es dann doch, wenn sich ein Schädling über einen USB-Stick oder ein unzureichend gesichertes mobiles Gerät im Netzwerk verbreitet und das Tagesgeschäft zum Erliegen bringt.

Ziel der **Security Awareness** bleibt es, den Mitarbeitern das nötige Wissen zu vermitteln, bei einem potenziellen Sicherheitsvorfall das Richtige zu tun. Dabei hilft nur das Wissen über die möglichen Gefahren und die Transparenz der Prozesse. Ist im Unternehmen vielleicht sogar ein Sicherheitskonzept vorhanden, lässt sich dieses aber auch nur effektiv durchsetzen, wenn die Mitarbeiter des Unternehmens es kennen und leben.

Wir sollten also nicht den Kopf einziehen und hoffen, dass der Sturm an uns vorüberzieht… Nein, sondern ein absolut lohnendes Investment in die Informationssicherheit eines Unternehmens führt letztendlich zum Vertrauen beim Kunden und damit zu einem erfolgreichen Unternehmen.

SVEN BRÖMER
Senior Professional
its-people GmbH
sven.broemer@its-people.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **info@its-people.de**



© ColiN00B/pixabay

Blackout – die Achillesferse der Digitalisierung

Teil 1: Über Risiken und Wahrscheinlichkeiten

Alles, was man heute mit Innovation verbindet, hat mit Digitalisierung zu tun: die zukunftsträchtigsten Entwicklungen, die erfolgversprechendsten Geschäftschancen, die größten Wachstumstreiber.

Regelrecht banal, ja geradezu von gestern, wirkt dagegen die Binsenweisheit, dass alles Digitale nichts ist ohne Strom. Energieversorgung erinnert an Wasserleitungen und Klärwerke, an gewöhnliche, wenn nicht gar überholte Technik, jedenfalls an nichts Modernes. Apple ist cooler als RWE. Strom wird einfach vorausgesetzt.

Doch das ist ein Trugschluss!

RISIKEN

Um Ihre Aufmerksamkeit für dieses wichtige Thema zu gewinnen, möchte ich mit einem Schlagwort starten, das Ihnen sicherlich vertraut ist: **Cybercrime.** Dass die Risiken des Cyberspace eine Gefahr für die Stromversorgung und damit auch für das digitale Business darstellen, hat sich angesichts der Vielzahl der Vorfälle inzwischen herumgesprochen.

Bekannt geworden sind beispielsweise Angriffe auf Systeme zur Überwachung und Steuerung iranischer Kernkraftwerke, auf die Steuerungssoftware vor allem spanischer Gaskraftwerke, Ölleitungen und Windturbinen, auf die IT-Netzwerke ukrainischer Stromversorger oder auf das Sicherheitssystem eines Kraftwerkes in Saudi-Arabien. Aus deutscher Sicht ist das vor allem deshalb bedeutsam, weil hierzulande die gleichen Triconex-Sicherheitssysteme, SCADA-Systeme und sonstigen Steuerungssoftwares im Einsatz sind und auch deutsche Infrastrukturen infiziert waren, ohne allerdings geschädigt zu werden.

Längst haben Innenpolitiker, Behörden und Sicherheitsanbieter ganz konkret auf die Möglichkeiten von Hackern hingewiesen, durch Schadsoftware Kraftwerke anzugreifen sowie gezielt einzelnen Straßenzügen oder ganzen Landstrichen den Strom abzuschalten. Auch überregional.

Bemerkenswert ist, dass wir trotzdem beispielsweise die **Einführung des smarten Stromnetzes** mit Smart Grids und Smart Metern vorantreiben. Nicht nur der Schriftsteller Marc Elsberg hatte mit seinem viel beachteten Roman „Blackout" auf die Sabotagefähigkeit intelligenter Stromzähler hingewiesen, die wie jedes vernetzte Informations- und Kommunikationssystem prinzipiell aus der Ferne sabotierbar sind.

Auch den Behörden ist die Problematik bewusst. Experten haben längst Schwachstellen gefunden, aber aufgrund der hohen Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), mangelt es bislang an bestimmten Gerätezulassungen. Gleichwohl überwiegt das politische Ziel.

Das gilt auch für die Frage der **Versorgungssicherheit** infolge von **Atomkraft- und Braunkohleausstieg.** Mir geht es nicht um die politische Bewertung der Energiewende an sich, sondern um die ganz nüchterne Betrachtung des Themas unter dem Aspekt der Versorgungssicherheit. Denn dass die Anzahl der energieerzeugenden Anlagen in Deutschland binnen zehn Jahren von rund 1000 auf über 1,7 Millionen angestiegen ist, erhöht nicht nur die Komplexität, sondern hat auch **enorme**

Erzeugungsschwankungen im Bereich **erneuerbarer Energien** zur Folge – je nachdem, ob und wie stark beispielsweise die Sonne scheint oder der Wind weht.

Um Sie nicht mit den physikalischen Grundlagen der Energieerzeugung zu langweilen, lassen Sie uns bitte gemeinsam voraussetzen, dass im Netz immer genauso viel Strom erzeugt werden muss, wie verbraucht wird, um die physikalisch erforderliche Frequenz von 50 Hertz zu halten. Fossile Energieträger haben sozusagen einen Speicher in der Primärenergie. Das heißt, es kann beispielsweise jederzeit mehr oder weniger Kohle, Gas oder Öl verbrannt werden, um Strom zu erzeugen. Die Verfügbarkeit der wichtigsten erneuerbaren Energieträger Wind und Sonne ändert sich hingegen wetterabhängig.

Genau dann, wenn die bevorzugten regenerativen Erzeuger – etwa während Dunkelflauten – nicht zur Verfügung stehen, werden zusätzlich vorgehaltene konventionelle Kapazitäten gebraucht. Umgekehrt muss bei Überproduktion Strom aus dem Netz genommen werden, etwa durch das Hochfahren zusätzlicher Verbraucher.

Um es kurz zu machen: Das Ausmaß, das solche Eingriffe inzwischen angenommen haben, hat sich in den letzten Jahren vervielfacht und birgt in zunehmendem Maße das Risiko, dass sie auch einmal nicht mehr ausreichen, um **Netzsicherheit** und **Netzstabilität** aufrecht zu erhalten.

Dem soll vor allem mit dem Bau neuer Leitungen zwischen Energieerzeugern und -verbrauchern begegnet werden. Damit überschüssiger Strom aus der einen Region in eine andere, wo er in diesem Moment gebraucht wird, transportiert werden kann, soll das Netz ausgebaut werden. Konkret geht es um mehrere sogenannte **Stromautobahnen** aus dem Norden Deutschlands, wo die großen Windparks und Sonnenfarmen stehen. Der Strom soll in die Ballungsräume und Industriezentren im Süden mit ihrem immensen Energiebedarf gebracht werden.

Nach mehreren Verzögerungen werden die Stromtrassen nach aktueller Planung im Jahr 2025 fertiggestellt, was an sich nicht besonders problematisch wäre – wenn die Politik nicht gleichzeitig daran festhalten würde, dass die letzten deutschen Kernkraftwerke bis Ende 2022 vom Netz gehen und – wenn nicht gleichzeitig ein **vorzeitiger Braunkohleausstieg** vorangetrieben werden würde. Für einen mehrjährigen Übergangszeitraum wird also mindestens die Kernenergie bereits wegfallen, während die Netze noch nicht fertiggestellt sein werden, durch die der Ersatz transportiert werden soll. Das bedeutet eine Periode nochmals **gesteigerter Gefährdung.**

Noch gar nicht berücksichtigt ist dabei der steigende Strombedarf, zu dessen wesentlichen Treibern die Digitalisierung zählt. Auch weiterhin werden mechanische durch elektrische oder elektronische Lösungen ersetzt und Mechanik wird digital steuerbar gemacht – etwa durch die Konzepte des Smart Homes im privaten Bereich oder der Industrie 4.0 in der Wirtschaft. So verbraucht ein iPhone pro Tag im Durchschnitt mehr Strom als ein Kühlschrank – nicht direkt, aber durch die Prozesse, die es woanders auslöst, etwa in Rechenzentren.

Weil ich Ihnen damit nichts Neues erzählen werde, will ich die Beispiele des Minings von Kryptowährungen oder der **zunehmenden Elektromobilität** mit Blick auf den damit verbundenen Energiebedarf nur kurz anreißen. Dabei wiederholt sich bei der Elektromobilität das grundsätzliche Problem der Energiewende: Weil sich E-Autos trotz staatlicher Kaufprämien noch nicht im gewünschten Maße durchgesetzt haben, erwägt die Europäische Union eine **Elektroquote** für Neuwagen. Das politische Ziel ist gesetzt. Für 2030 ist eine Quote von 15 Prozent im Gespräch. Doch dass auch der Strom, der für das saubere Autofahren benötigt wird, erst irgendwo herkommen und irgendwie produziert werden muss, scheint dabei vergessen zu werden. Jedenfalls ist das deutsche Stromnetz für diese Menge an Elektromobilen nicht ausgelegt, zumal die Kapazitäten das gleichzeitige Laden vieler Elektrofahrzeuge erlauben müssen. Vernünftigerweise sollte dem Ausbau der Elektromobilität ein Ausbau des Stromnetzes vorausgehen…

Nun könnte ich noch auf Risiken wie menschliches oder technisches Versagen, Bauarbeiten oder Aging Infrastructures, physische terroristische Anschläge auf die Infrastruktur der Stromversorgung, die strukturelle Versorgungssicherheit oder den Ausfall der Primärenergie eingehen. Ich könnte Ihnen die Gefahren durch Naturereignisse, Extremwetter oder Klimawandel darstellen. Und wenn Sie hart im Nehmen wären, könnte ich auch noch auf einen längst überfälligen „Koronalen Massenauswurf“ der Sonne (KMA), einen „Elektromagnetischen Puls“ (EMP) oder eine offenbar bereits eingeleitete „Polumkehr“ eingehen, die übrigens nicht dem esoterischen Spektrum zuzuordnen sind, sondern weltweit seriöse Wissenschaftler und Behörden beschäftigen.

Aber ich denke, dass bereits deutlich geworden ist, dass es verschiedene Risiken gibt, die eine **ernsthafte Gefahr für die Energieversorgung** darstellen – und das in weiter zunehmendem Maße!

WAHRSCHEINLICHKEITEN

Falls Sie sich schon mit der Frage der Energieversorgung beschäftigt haben, werden Sie vermutlich den im Übertragungsnetzbetrieb geltenden Grundsatz des (n-1)-Kriteriums einwenden, der ursprünglich für Systeme mit lokaler Netzabdeckung und geringen Transportentfernungen gedacht war. Das **(n-1)-Kriterium** bedeutet nichts weiter, als dass Störungen oder Ausfälle einzelner elektrischer Betriebsmittel – ob Leitung, Transformator, Generator oder ganzes Kraftwerk – im Notfall über andere Betriebsmittel ausgeglichen werden, ohne dass es zu Ausfällen in der Versorgung kommt. Es müssen also mindestens zwei Ereignisse zusammenkommen, also zwei Betriebsmittel ausfallen, damit es zu einem Stromausfall kommt. Oder die Systeme müssen nicht korrekt betrieben worden sein.

Erschütternd ist, wie oft es trotzdem vorkommt. Und damit meine ich nicht nur die großen Vorfälle.

Allein in den zurückliegenden 15 Jahren

- hatten in Deutschland eine Viertelmillion Menschen fast eine Woche lang keinen Strom
- ging von Deutschland ein Stromausfall aus, der auch die Niederlande, Belgien, Frankreich, Spanien, Italien und Österreich erfasste
- traf ein Stromausfall in Italien die sagenhafte Zahl von 57 Millionen Menschen

Diese Aufzählung ließe sich beinahe beliebig fortsetzen. Auch in Westeuropa oder im Bereich der G7-Länder, die sich als bedeutendste Industrienationen der westlichen Welt verstehen.

Noch viel häufiger treten kleinere Vorfälle auf, also lokale oder regionale **Stromausfälle** von überschaubarer Dauer. Was schätzen Sie, wie oft der Strom in Deutschland ausfällt? Laut offizieller Statistik der Bundesnetzagentur gibt es pro Jahr 172.600 Ausfälle, das sind 472 pro Tag! Das ist viel, oder?

Aber es ist noch nicht die ganze Wahrheit, denn zahlreiche Stromausfälle werden gar nicht erfasst. Rechnet man etwa die nicht berücksichtigten

- Versorgungsunterbrechungen mit einer Dauer von bis zu drei Minuten
- nicht ungeplanten, also geplanten Versorgungsunterbrechungen
- ungeplanten Versorgungsunterbrechungen, die auf andere Ursachen als „Atmosphärische Einwirkungen", „Einwirkungen Dritter", „Zuständigkeit des Netzbetreibers" und „Rückwirkungsstörungen" zurückzuführen sind, und
- Versorgungsunterbrechungen aufgrund von höherer Gewalt wie Orkane, Hochwasser, Schnee- und Eislasten

hinzu, würden die tatsächlichen **Versorgungsstörungen** Berechnungen zufolge wohl beim Zehnfachen der offiziellen Zahlen liegen, nämlich bei 4700 Stromausfällen pro Tag!

Und Ihnen brauche ich ja auch nicht zu erklären, dass im IT-Bereich selbst Ausfallzeiten im Sekundenbereich Dominoeffekte sowie erhebliche Schäden auslösen können.

Ein Beispiel eines solchen Ausfalls, der eigentlich gar nicht hätte passieren dürfen, war ein Stromausfall in Frankfurt am Main Mitte April 2018, der auch den **Internetknoten DE-CIX** betraf und zu einer Einschränkung des Internets führte. Denn DE-CIX ist nicht nur einer der weltweit wichtigsten Umschlagplätze für den Datenverkehr im Internet, sondern er hat mit mehr als sechs Terabit pro Sekunde den höchsten Datendurchsatz der Welt. Was war passiert?

Die Systeme dieses Internetknotens sind zwar über 21 verschiedene Rechenzentren in der ganzen Stadt verteilt, aber der Stromausfall in einem dieser Rechenzentren genügte. Und das, weil neben der Stromversorgung über das Netz, auch die Notstromversorgung durch Dieselgeneratoren nicht mehr funktionierte und die mehrfach redundante Infrastruktur schlichtweg versagte!

AUSBLICK

In diesem 1. Teil meines Beitrags bin ich auf einige Risiken für die Versorgungssicherheit eingegangen und habe einen Überblick über die kleineren und größeren Stromausfälle gegeben, die heute bereits stattfinden oder stattgefunden haben.

Im 2. Teil meines Beitrags, der in der nächsten Ausgabe des its-people Magazin erscheinen wird, werde ich die Auswirkungen beschreiben. Hier etwa die wechselseitigen Abhängigkeiten von Stromnetz

© xijian/istock

und Internet, die Folgen eines Stromausfalls für Hardware, Internet und Telekommunikation sowie die Bedeutung für Ihr Geschäft und das Ihrer Kunden.

Zudem werde ich auf bestehende Vorsorgemöglichkeiten eingehen, auf die Notwendigkeit individueller, maßgeschneiderter Lösungen und auf wichtige Aspekte, die in jedem Konzept eine Rolle spielen.

TOBIAS GREILICH
hat ein wirtschaftswissenschaftliches Studium absolviert und ist Master of Business Marketing (MBM). Er war unter anderem in Unternehmen der Elektrotechnik sowie des IT-Consultings als Bereichsleiter tätig. Außerdem arbeitet er als freier Journalist und Fachbuchautor und ist beratend tätig. Sein aktuelles Buch befasst sich mit dem Blackout-Schutz **(Titel: Bedrohung Blackout – Wahrscheinlichkeit, Risiken, Vorsorge)**
Tobias.Greilich@gmx.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **info@its-people.de**

Neue Social-Sign-In Funktionen für Oracle APEX einrichten

In vielen Webanwendungen bekommen Benutzer häufig die Möglichkeit, anstatt einen neuen User-Account anzulegen, ihren bestehenden Facebook oder Google Account zu verwenden. Insbesondere für Anwender, die häufig verschiedene Internetdienste verwenden, ist diese Authentifizierungsmethode sehr hilfreich. Die Anwender müssen sich nämlich nur noch einen Account für die unterschiedlichen Plattformen merken. Viele Anwender sind sowieso automatisch mit dem Start des Rechners per Facebook oder Google angemeldet und es ist daher nicht nötig, erneut das Kennwort einzugeben. Die Anmeldung über Facebook oder Google erhöht daher die Akzeptanz eines Benutzers, einen Internetdienst zu verwenden.

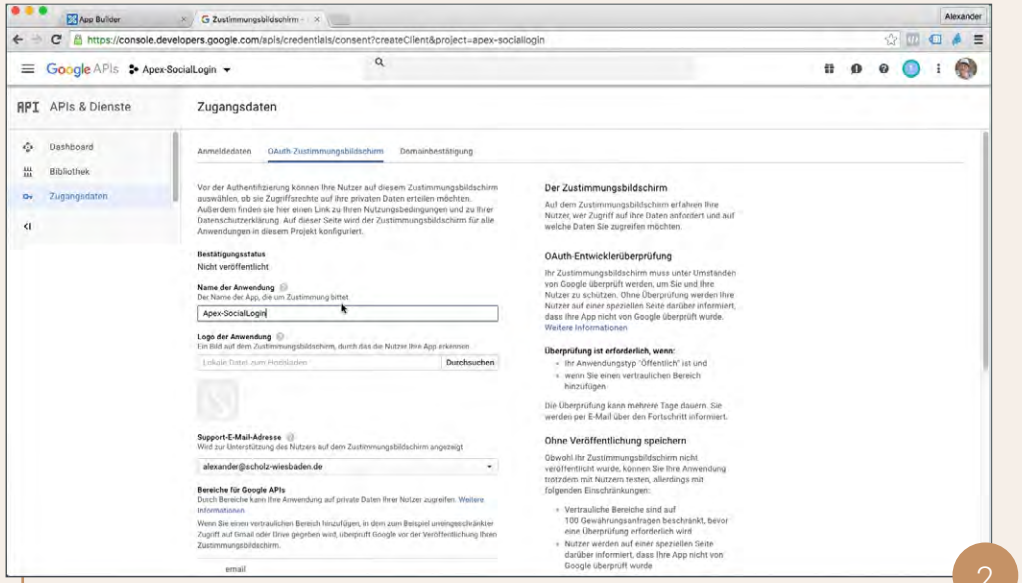
Mit der Oracle APEX Version 18.1 steht diese Authentifizierungsmethode auch in APEX-Anwendungen zur Verfügung. Diese neue Funktionalität wird als Authentifizierungsschema vom Typ **Social-Sign-In** implementiert. Hiermit ist es möglich, die Benutzerauthentifizierung von APEX über Google, Facebook oder einen beliebigen anderen Anbieter, der den **OAuth2-Standard** unterstützt, durchzuführen. Das **Social-Sign-In** ist für solche APEX-Anwendungen sinnvoll, die im Internet zur Verfügung stehen sollen und von einer unbestimmten Anzahl von Anwendern benutzt werden können. Damit wird Oracle APEX als Plattform zur Erstellung von Webanwendungen auf Basis einer Oracle-Datenbank auch für den B2C-Markt immer interessanter.

Um **Social-Sign-In** für APEX zu nutzen, muss zunächst ein neues Google-Projekt bzw. eine neue Facebook App erstellt werden. Anschließend werden in APEX entsprechende **Web Credentials** angelegt. Danach wird ein neues **Authentication Schema** erstellt. Die einzelnen Schritte werden nachfolgend am Beispiel von Google und Facebook beschrieben. Eine ausführliche Beschreibung mit den entsprechenden Screenshots finden Sie ab sofort in unserem **its-people Blog.**

EINRICHTUNG VON SOCIAL-SIGN-IN IN ORACLE APEX FÜR GOOGLE

Für die Einrichtung des **Social-Sign-In** für Google ist folgendermaßen vorzugehen:

1. Unter **console.developers.google.com** mit dem eigenen Google Account anmelden und ein neues Projekt erstellen.



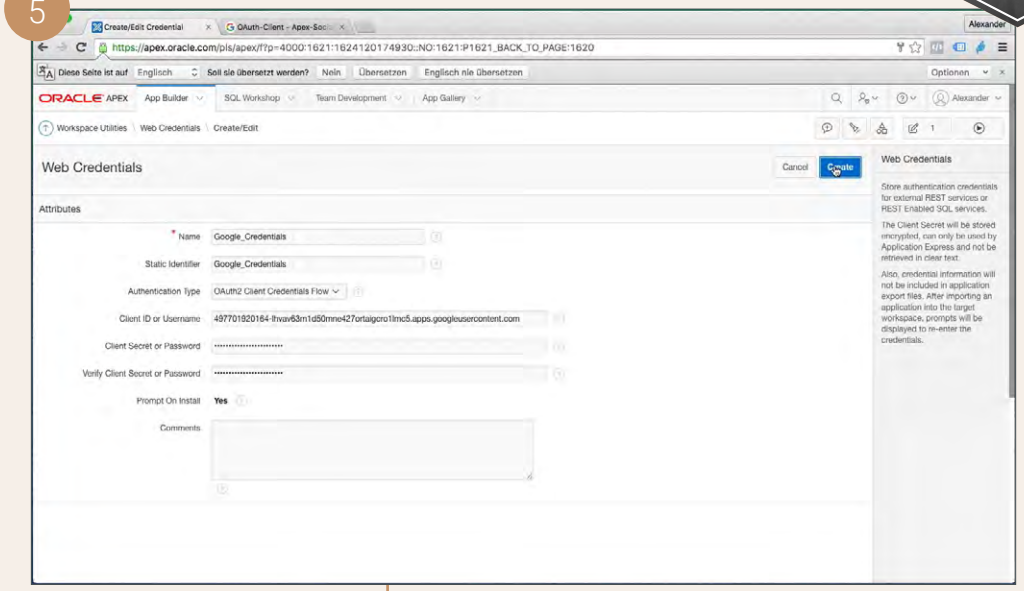
2

2. In den Zugangsdaten des neuen Projektes im Abschnitt **OAuth-Zustimmungsbildschirm** den Namen des Projektes eintragen und die richtige Domain in das Feld **Autorisierte Domain** eintragen.

3. Jetzt unter dem Reiter Anmeldedaten neue Anmeldedaten vom Typ **OAuth-Client-Id** erstellen.

4. Den Anwendungstyp auf **Webanwendung** einstellen, einen beliebigen Namen und die autorisierte **Weiterleitungs URI** eingeben.

5



5. Nach dem Erstellen der **OAuth Zugangsdaten** können in APEX die **Webcredentials** erstellt werden. Dazu wird die **Client-ID** und der **Clientschlüssel** aus den OAuth Zugangsdaten des Google Projekts benötigt.

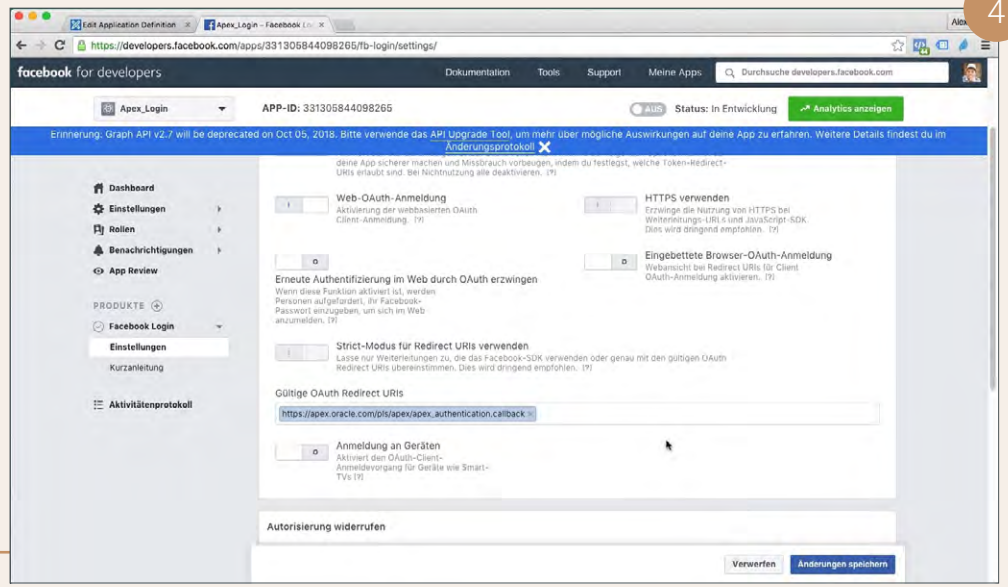
6. In den **Shared Components** der APEX-Anwendung ein neues **Authentication Scheme** vom Typ **Social Sign-In** mit dem Authentication Provider Google und den vorher definierten **Webcredentials** erstellen.

7. Als Scope **profile,email** und bei Username Attribute **email** eintragen.

8. Ab jetzt erfolgt die Anwendungsauthentifizierung über Google. Allerdings ist ein Logout nach erfolgreicher Google-Authentifizierung noch nicht möglich. Hierzu muss noch die Logout URL **http://accounts.google.com/logout** im Bereich Post-Logout URL des Authentication Scheme eingetragen werden.

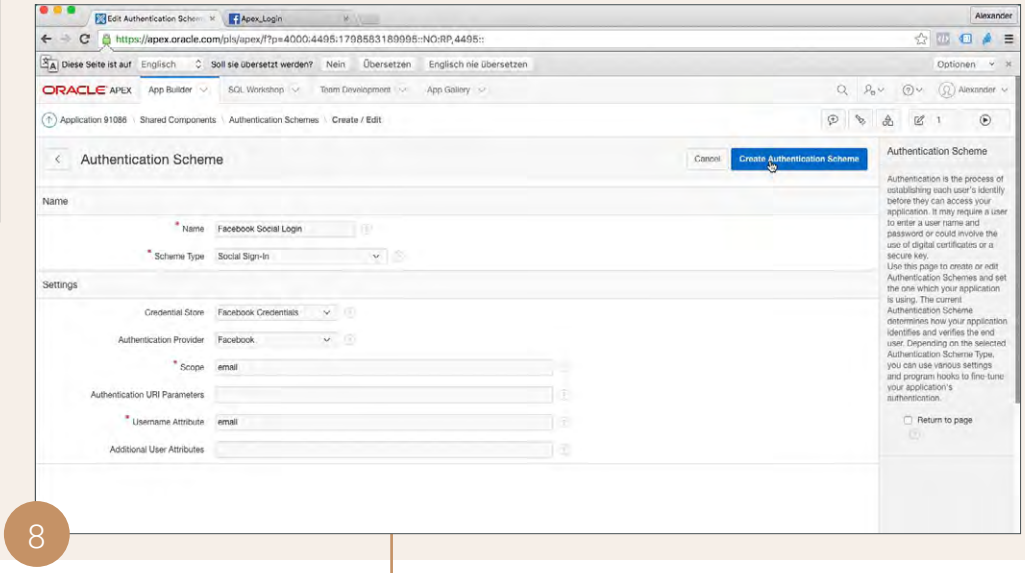
EINRICHTUNG VON SOCIAL-SIGN-IN IN ORACLE APEX FÜR FACEBOOK

Die Einrichtung von **Social-Sign-In** für Facebook erfolgt ähnlich wie die Einrichtung für Google. Allerdings ist aktuell die Einrichtung des **Social-Sign-In** für Facebook auf apex.oracle.com nicht möglich; ein Bug in Oracle 12.1 verhindert das. Es gibt zwar einige Workarounds, mit denen die Einrichtung möglich ist, diese erfordern aber entweder einen eigenen Server oder zumindest Administratorzugang zum Oracle Server. Beides ist aber für Anwendungen auf apex.oracle.com nicht möglich. Nachfolgend wird ungeachtet des Bugs das generelle Vorgehen für die Authentifizierung über Facebook beschrieben.



1. Unter **developers.facebook.com** eine neue App erstellen.
2. Als Programmtyp für die App ist Facebook Login auszuwählen. Als Plattform für die neue App ist **Web** auszuwählen.
3. Jetzt muss die URL der APEX-Anwendung eingegeben werden.
4. Unter **Facebook Login > Einstellungen** die richtige **OAuth Redirect URI** eintragen.

5. Unter **Einstellungen > Allgemeines** die App Domains, unter denen die APEX-Anwendung erreichbar ist, eintragen.
6. Analog zur Google-Authentifizierung können jetzt die **Webcredentials** für Facebook in APEX eingerichtet werden. Als Client-ID wird die Facebook App-ID eingetragen. Als **Client Secret** wird der App-Geheimcode eingetragen.
7. Als letztes muss noch ein neues **Authentication Scheme** der APEX-Anwendung hinzugefügt werden.



8. Als **Credential Store** sind die Facebook Credentials und als **Authentication Provider** ist **Facebook** auszuwählen. Bei **Scope** und **Username** Attribute ist **email** einzutragen.

FAZIT

Mit der Einführung der Google- und Facebook-Authentifizierung entwickelt sich Oracle APEX immer weiter hin zu einer universell einsetzbaren Plattform, mit der Webanwendungen basierend auf der Oracle Datenbank im B2B- und B2C-Bereich erstellt werden können. Leider stecken diese neuen Funktionen noch etwas in den Kinderschuhen. Die Facebook-Authentifizierung ist über die Cloud-Plattform apex.oracle.com noch nicht nutzbar, und für beide Authentifizierungsfunktionen gibt es noch keine ausführlichen Anleitungen von Oracle. Zur Umsetzung gibt es derzeit nur einige Blogbeiträge wie zum Beispiel

Dimitri Gielis oder **Adrian Png**

Bis diese Funktionen ihren flächendeckenden Einzug in die APEX-Authentifizierung finden, wird es sicherlich noch einige Zeit dauern. Bis dahin bleibt festzuhalten, dass eine Authentifizierung über Google oder Facebook in APEX grundsätzlich möglich ist, aber sicher nur von experimentierfreudigen Entwicklern umgesetzt wird.

ALEXANDER SCHOLZ
Senior Professional
its-people GmbH
alexander.scholz@its-people.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **info@its-people.de**

© Bloomicon/shutterstock

SAP S/4HANA – Die Zukunft erwartet uns!?

Ein kleiner Ausblick auf die Veränderung TEIL 1

Durch die Meldung von SAP SE den Support für das SAP ECC 6.0x Ende 2025 einzustellen, wurden die mittelständischen Unternehmen sehr verunsichert. Mit diesem Artikel möchte ich Sie auf die kommenden, wesentlichen Veränderungen im Bereich Daten und Datenverwaltung hinweisen. Da ein Gesamtüberblick jedoch Bücher füllen könnte, werde ich Ihnen in dieser Ausgabe nur einen ersten Teil der wichtigsten Veränderungen erläutern. In der nächsten Ausgabe des its-people Magazins folgen dann weitere Aspekte.

DATENVERWALTUNG

Eine der größten Veränderungen ist die neue Datenverwaltung. Diese hat entsprechend auch Einfluss auf alle SAP-Funktionsbereiche. SAP verwendet die Technologieplattform **SAP HANA** mit einer In-Memory-Datenbank zur Datenverwaltung. Um eine Datenhaltung in dieser Form überhaupt möglich zu machen, waren tiefgreifende Veränderung in den Datenstrukturen und Anwendungen notwendig. So will SAP in der neuen Business-Suite **S/4HANA** dem Prinzip folgen, dass es nur noch einen Lösungsansatz geben soll (Principle of One), um eine Anforderung zu erfüllen. Beispiel hierfür ist das klassische und neue Hauptbuch (zukünftig nur noch das neue HB).

DATENHALTUNG

Auch bei der Datenhaltung wurden die redundanten Daten abgeschafft, da sie den meisten Speicherplatz verbrauchten. Hintergrund hierbei ist, dass es für die Performance-Sicherheit in SAP ECC 6.0 notwendig war, Daten teilweise schon aggregiert bereitzustellen. Beispielsweise gab es in der Bestandsführung unter SAP ECC 6.0, 24 Aggregationstabellen, 2 Stammdatentabellen und 2 Bewegungsdatentabellen (MKPF, MSEG). Diese wurden in **SAP S/4HANA** durch zwei weiterhin existierende Stammdatentabellen (MARC, MARD) und einer einzigen Bewegungsdatentabelle (MATDOC) abgelöst.

Aggregate-Tabellen	Historien-Tabellen	Stammdaten-Tabellen	Beleg-Tabellen	S4/HANA - Beleg
~~MARCH~~		MARC	~~MKPF~~	MATDOC
~~MARDH~~		MARD	~~MSEG~~	
~~MCHB~~	~~MCHBH~~	(ohne Aggregation)		
~~MKOL~~	~~MKOLH~~			
~~MSKA~~	~~MSKAH~~			
~~MSKU~~	~~MSKUH~~			
~~MSLB~~	~~MSLBH~~			
~~MSPR~~	~~MSPRH~~			
~~MSSA~~	~~MSSAH~~			
~~MSSQ~~	~~MSSQH~~			
~~MSTB~~	~~MSTBH~~			
~~MSTE~~	~~MSTEH~~			
~~MSTQ~~	~~MSTQH~~			

Diese Reduktion von Daten und Anwendungen (im SAP Sprachgebrauch Simplification) ist nur durch die neue Technologie der In-Memory-Datenbank möglich, da Abfragen und Auswertungen hier quasi in Echtzeit erzeugt werden können. Eine vollständige Liste (Simplification List) ist im SAP Help Portal verfügbar.

Die Veränderung der Datenhaltung ist notwendig geworden, um der immer größer werdenden Datenmengen (Big Data) aus der digitalen Transformation und dem Internet of Things (IoT) Herr zu werden. In der „alten" SAP-Welt waren hierfür oftmals zwei verschiedene Arten von Systemen: OLTP-Systeme (Online Transaction Processing) und OLAP-Systeme (Online Analytical Processing) nötig. Durch die In-Memory-Datenverwaltung ist jetzt theoretisch nur ein System notwendig. In diesem Zusammenhang möchte ich noch erwähnen, dass **S/4HANA** die Datenspeicherung überwiegend nicht in der zeilenorientierten (klassischen) Form durchführt, sondern eine spaltenorientierte Speicherung bevorzugt, um eine weitere Reduzierung von redundanten Daten zu erhalten. Dadurch wird eine Komprimierung mit einem Faktor von 15–20 erreicht, was ebenfalls der In-Memory-Technik zugutekommt.

Zeilenorientiert

Zeile	Name	Vorname	Straße	PLZ	Ort
1	Meier	Stephan	Turmstrasse	50667	Köln
2	Hirsch	Sabine	Chausseestrasse	10553	Berlin
3	Meier	Stefan	Opernplatz	13587	Berlin
4	Müller	Sabine	Bahnhofstrasse	50667	Köln
5	Meyer	Stephan	Turmstrasse	20359	Hamburg

Spaltenorientiert

Dictionary	Name
1	Meier
2	Hirsch
3	Müller
4	Meyer

Dictionary	Vorname
1	Stephan
2	Sabine
3	Stefan

Dictionary	Straße
1	Turmstrasse
2	Chausseestrasse
3	Opernplatz
4	Bahnhofstrasse

Dictionary	PLZ
1	50667
2	10553
3	13587
4	20359

Dictionary	Ort
1	Köln
2	Berlin
3	Hamburg

Werte	Name
1	1
2	2
3	1
4	3
5	4

Werte	Vorname
1	1
2	2
3	3
4	2
5	1

Werte	Straße
1	1
2	2
3	3
4	4
5	1

Werte	PLZ
1	1
2	2
3	3
4	1
5	4

Werte	Ort
1	1
2	2
3	2
4	1
5	3

Abfrage (Aufbau erst bei Abfrage als Liste):

Zeile	Name	Vorname	Straße	PLZ	Ort
1	1 = "Meier"	1	1	1 = "50667"	1
2	2 = "Hirsch"	2	2	2 = "10553"	2
3	1 = "Meier"	3	3	3 = "13587"	2
4	3 = "Müller"	2	2	1 = "50667"	1
5	4 = "Meyer"	1	1	4 = "20359"	3

STAMMDATENVERWALTUNG

In der Stammdatenverwaltung ist als die primäre Veränderung die Ausweitung des Geschäftspartners zu sehen. Die Stammdaten werden in **S/4HANA** zentral verwaltet. Sie sind dadurch jederzeit konsistent, aktuell und frei von Redundanzen. Sie sind außerdem in Sichten gegliedert, die Organisationseinheiten zugeordnet sind (z.B. einem Werk oder einer Organisationseinheit).

© Profit_Image/shutterstock

Dank der segmentierten Struktur von Stammsätzen können die verschiedenen Organisationsstrukturen eines Vorgangs flexibel abgebildet werden. Geschäftspartner können als Person, Gruppe oder Organisation (juristische Person oder Teil einer Unternehmung, beispielsweise Abteilung) kategorisiert werden. Des Weiteren kann der Geschäftspartner in unterschiedlichen Rollen verwaltet werden (z. B. Lieferant, Kreditor oder Kunde).

Ein weiteres Highlight in **S/4HANA** ist die 40-stellige Materialstammnummer. In SAP ECC 6.0 ist bei 18 Stellen Schluss. Diese Funktion steht aber erst nach Aktivierung zur Verfügung und lässt sich danach auch nicht einfach wieder rückgängig machen.

BEREITSTELLUNG

Wenn man über Datenverwaltung spricht, muss zwangsläufig auch die Bereitstellungsform des Systems erwähnt werden. **S/4HANA** ist in zwei unterschiedlichen Versionen verfügbar. Es gibt auf der einen Seite die klassische On-Premises-Version oder eine Cloud-Lösung, die noch weitere Möglichkeiten bietet.

Bei der Cloud-Lösung gibt es die Ausprägung als „Private Option“, als „Public Option“ oder als „SAP HANA Enterprise Cloud“. Die Unterschiede der einzelnen Cloud-Versionen beziehen sich auf die Lizenzkosten, wer die Infrastruktur bereitstellt, welcher Funktionsumfang gewünscht/gebraucht wird und welche Version von **S/4HANA** zur Verfügung gestellt wird.

Man spricht hier auch von Cloud-Services-Modellen, bei denen die Bereitstellung von IT-Infrastruktur wie z.B. Speicherplatz, Rechenleistung oder Anwendungssoftware den Unternehmen als Dienstleistungen über das Internet angeboten werden. Die Services werden nutzungsorientiert pro Arbeitsplatz und pro Monat bezahlt. Die Unternehmen zahlen also nur dafür, was sie tatsächlich nutzen und reduzieren so ihre Investitionskosten. Zu den Cloud-Lösungen gilt es noch zu erwähnen, dass die SAP noch weitere Cloud-basierende Software im Angebot hat, die einfacher miteinander verbunden werden können (z.B. ARIBA, HYBRIS).

Bei der On-Premises-Version erfolgt die Bereitstellung im kundeneigenen Netzwerk, wobei von den Kunden auch Hardware und IT-Struktur gestellt werden müssen. Zusätzlich zur Investition müssen dann die weiteren Unterhaltungs- und Wartungskosten, sowie die Lizenzkosten berücksichtigt werden.

Damit endet meine heutige Vorstellung zu **S/4HANA.** Im nächsten Magazin finden Sie dann weitere Informationen zur Benutzeroberfläche, Lagerverwaltung und noch einiges mehr.

MATTHIAS KLEPP
Senior Business Consultant ERP Logistics
bcs-people GmbH
matthias.klepp@bcs-people.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **bcspeople@its-people.de**

Vom „Komputerfriektreffen" zu einem der größten Kongresse Europas

Rund 20 Teilnehmer trafen sich am 12.9.1981 in der Berliner taz-Redaktion. Aufgerufen hatten dazu mit der „tu-wat"-Einladung Tom Twiddlebit (korrekter Name: Klaus Schleisiek), Wau Holland (korrekter Name: Herwart Holland-Moritz), Wolf Gevert, Wulf Müller und Jochen Büttner. Dies war die Geburtsstunde des „Chaos Computer Club".

Zu einem eingetragenen Verein wurde der **CCC** dann im April 1986. Dieser „intergalaktischen Hackervereinigung" gehören nach eigenen Angaben mittlerweile ca. 9.000 Mitglieder an. Dazu kommen dann noch in vielen Städten **Erfa**hrungsaustausch-Kreise und Chaos-Treffs. **Erfa**-Kreise sind in der Regel lokale Vereine mit Clubräumen, Chaos-Treffs sind lockere Zusammenkünfte von Interessierten ohne eine Mitgliedschaft.

Mit kriminellen Attacken auf Computersysteme, an die bei Hackern oft zuerst gedacht wird, haben die Mitglieder des **CCC** aber natürlich nichts zu tun. Vielmehr geht es um den im bildlichen Sinne kreativen Umgang mit der Technologie und das Aufzeigen von Schwachstellen der digitalen Gesellschaft.

GSM-Hack (1997), **T-Com-Hack** (2004), **Nedap-Hack** (2006) und **PC-Wahl-Hack** (2017) sind einige der „Hacks" in der Geschichte des Clubs. Legendär wurde der **CCC** allerdings schon mit dem **BTX-Hack** 1984 (BTX = interaktives Bildschirmtextsystem der Deutschen Bundespost). Hier konnte der **CCC** erstmals aufzeigen, dass das BTX-System bei weitem nicht so sicher war, wie es die Bundespost glaubte. Ein Datenüberlauf brachte das System dazu, eigentlich geheime Speicherinhalte, dem Benutzer anzuzeigen. So unter anderem im Klartext den Benutzernamen samt Passwort.

Kurz danach fand 1984 die erste offizielle größere Veranstaltung, der **Chaos Communication Congress,** im Eidelstedter Bürgerhaus in Hamburg unter dem Titel „CCC'84 nach Orion'64" statt.

Während die Teilnehmerzahlen stetig stiegen, wechselte der nun jährlich stattfindende Kongress mehrfach zwischen Hamburg und Berlin. 2012 bis 2016 war das Congress Center Hamburg Gastgeber. Allein hier stieg die Besucherzahl von 6.500 auf rund 13.000 Besucher. Seit dem letzten Jahr ist die Leipziger Messe der neue Veranstaltungsort des Kongresses. Im Jahr 2017 beliefen sich die Besucherzahlen dann auf rund 15.000 Teilnehmer. Das Motto des **34C3** war in Anlehnung an die Anfänge des Clubs **„tuwat".**

Auch dieses Jahr geht es zum 35. Kongress vom 27. bis zum 30. Dezember 2018 nach Leipzig. Das Motto lautet **„35C3: Refreshing Memories".** Neben dem Zusammenkommen der „Häcker", dem Vorstellen von Projekten, Community-Assemblies, Entwickler- und Projektgruppentreffen, Installationen, Lightning Talks, verschiedenen Workshops und speziellen Angeboten für Kinder und Jugendliche, gibt es wie auf einem Kongress üblich, auch viele Vorträge und Talks.

Diese sind dieses Jahr in 6 Tracks aufgeteilt:

- Art & Culture
- Ethics, Society & Politics
- Hardware & Making
- Security
- Science
- Resilience

Es verspricht wieder spannend zu werden!

Der Fahrplan der Veranstaltung wird kurz vor dem Start veröffentlicht. Unter **Media** stehen im Anschluss die meisten Vorträge zum Download bereit. Dort gibt es auch eine sehr große Auswahl an veröffentlichten Beiträgen aus den Vorjahren. Im Dezember wird es wieder einen Blog-Eintrag auf unserem **its-people-Blog** zu den Talks geben und Anfang des Jahres dann auch eine Rückschau.

UWE BLENZ
Senior Professional
its-people GmbH
uwe.blenz@its-people.de

Das hört sich interessant an? Sie möchten gerne mehr erfahren? Schreiben Sie uns unter **info@its-people.de**

© Sergey Nivens/shutterstock

Hätten Sie's gewusst?

30%

... dass rund 30% der Unternehmen in Deutschland keinerlei IT-Sicherheitsschulungen mit ihren Mitarbeitern durchführen?

Laut einer repräsentativen Umfrage durch das Bundeministerium des Inneren, für Bau und Heimat, halten 30% der deutschen Unternehmen IT-Sicherheitsschulungen ihrer Mitarbeiter für unnötig. In der anonymen Befragung wurden 2017 knapp 1000 Unternehmen bezüglich Informationssicherheitssystemen, IT-Angriffen und Maßnahmen zur Prävention von Cyber-Angriffen befragt.

28. Januar

... dass es einen offiziellen Europäischen Datenschutztag gibt?!

Seit 2007 gilt der 28. Januar offiziell als Europäischer Datenschutztag. Ins Leben gerufen durch den Europarat, soll der Tag an zunehmende Datenschutzbedürfnisse und Persönlichkeitsrechte erinnern. Die Wahl des 28.01. ist übrigens keine zufällige, sondern geht auf die Unterzeichnung der Europakonvention 108 zum Datenschutz im Jahr 1981 zurück.

Interner Partner

Dirk Größer
IT-Experte für Informationssicherheit und Datenschutz

Wir freuen uns, Ihnen Dirk Größer als neues Mitglied der its-people GmbH vorzustellen. Er nahm seine Tätigkeit im März dieses Jahres auf.

Dirk Größer beschäftigt sich seit mehr als 25 Jahren als ausgewiesener Experte europaweit mit Informationssicherheit und Datenschutz. Er verfügt über einen umfangreichen Erfahrungsschatz in allen wesentlichen Bereichen der Informationssicherheit, des Datenschutzes, der IT-Forensik und im Projektmanagement.

Seine fachlichen Schwerpunkte sind neben der Einführung und Optimierung von Informationssicherheitsmanagement- und Datenschutzmanagement-Prozessen (ISMS und DSMS), die Arbeit als Informationssicherheitsbeauftragter und externer Datenschutzbeauftragter sowie die produkt- und herstellerunabhängige Sicherheits-Konzeption und Risikobetrachtung von IT-Architekturen und Cloud-Lösungen.

Dirk Größer ist Certified Information Systems Security Professional (CISSP), VdS anerkannter Berater für Cyber-Security, zertifizierter Datenschutz-Beauftragter und Auditor sowie zertifizierter EDV-Sachverständiger (DESAG).

Wir freuen uns auf eine weiterhin erfolgreiche Zusammenarbeit mit Dirk Größer!

Gerne erhalten Sie weiterführende Information über diesen erfahrenen Professional unter **info@its-people.de**

Treten Sie ein in Ihre neue Zukunft

und lassen Sie uns darüber reden...

Sie denken schon lange darüber nach, endlich den Weg in die Selbständigkeit zu gehen? Der Zeitpunkt ist günstig! Nicht nur die deutsche Wirtschaft zeigt sich stabil, auch die Nachfrage nach IT-Experten ist ungebrochen!

Realisieren Sie diesen großen Schritt mit der Unterstützung eines starken Unternehmensverbundes! Wir stehen Ihnen mit Rat und Tat zur Seite!

»Ein alter Weg kann keine neuen Türen öffnen«

– André Loibl

UNSERE KARRIERE-VIDEOS:

its-people – Ihr Weg in die Selbstständigkeit

its-people – IT-Professionals gewähren Einblick

Sie sind bereits als selbstständiger IT-Professional unterwegs?

Eine echte Partnerschaft mit einem starken Unternehmen wäre aber noch besser?

Dann lassen Sie uns auch darüber reden!

Mehr erfahren Sie unter **www.its-people.de**

© peterschreiber.media/fotolia

its-people ist ein erfolgreicher Zusammenschluss von erfahrenen, selbständigen IT-Beratern.

Wir sind äußerst erfolgreich am Markt unterwegs und betreuen unsere Kunden rund um die Themen IT-Security, Datenbanken, Anwendungsentwicklung, Big Data, Data Warehousing, Datenintegration und ERP-Logistikberatung.

Zu unseren Kunden gehören Großkonzerne und Unternehmen des oberen Mittelstandes in den unterschiedlichsten Branchen.

Verbinden Sie die Freiheit der Selbständigkeit mit der Sicherheit unserer Community. Erleben Sie Synergien, Partnerschaft und Erfolg!

Wir freuen uns auf Ihre Bewerbung mit kurzem Anschreiben, Lebenslauf und ausführlichem Qualifikationsprofil.

Zeigen Sie uns, was Sie können!

Das erwartet Sie:
- Partnerschaft auf Augenhöhe
- Professioneller Zugang zum Markt
- Betreuung aus einer Hand
- Entlastung von nicht-fachlichen Aufgaben
- Gestaltungsfreiräume und Teamgeist
- Persönliche Weiterbildung und -entwicklung

AKTUELL GESUCHT

DATA WAREHOUSE ARCHITEKT M/W (MICROSOFT SQL-SERVER)

Ihr Aufgabenbereich:
- Beratung der Kunden zu DWH-Architektur
- Umsetzungsplanung
- Informationsbedarfsanalyse der fachlichen Anforderungen
- Konzeption und Design der DWH-Lösung (Datenmodellierung, ETL-Prozesse)

Unsere Themenschwerpunkte/ Unser Technologieumfeld:
- Microsoft SQL-Server
- Microsoft (SQL) Azure
- ETL: Microsoft SSIS oder vergleichbares Werkzeug

Das sollten Sie mitbringen:
- Exzellentes fachliches und technologisches Data Warehouse Know-how
- Langjährige Projekterfahrung im BI/DWH-Umfeld mit Microsoft Produkten
- Analytisches Denkvermögen und eine starke methodische Ausprägung
- Konzeptionelle Stärke und hohe Lösungsorientierung

SECURITY CONSULTANT M/W

Ihr Aufgabenbereich:
- Technologische und organisatorische Beratung in allen Bereichen der IT-Security
- Unterstützung bei Konzeption, Aufbau und Implementierung von Security-Prozessen
- Durchführung von Risikoanalysen und Audits

Unsere Themenschwerpunkte/ Unser Technologieumfeld:
- Informationssicherheit im Umfeld IT-Systeme, Datenbanken und Anwendungsentwicklung
- IT-Schwachstellenanalyse, Disaster Recovery
- Identity Management/Identity Rights Management
- Cloud Security

Das sollten Sie mitbringen:
- Mindestens 2 Jahre Berufserfahrung im Bereich IT-Security
- Knowhow über den Product-Life-Cycle in der Softwareentwicklung unter Security Aspekten
- Fachwissen von IT-Architekturen und IT-Infrastrukturen
- Kenntnisse der einschlägigen Security Standards sowie ISMS
- Ausgeprägte Weitsicht im Hinblick auf die Bearbeitung komplexer Themenfelder
- Ausgeprägte Kommunikationsfähigkeiten

NightRun 2018 – its-people Team bereits zum 6. Mal in Folge dabei!

In der letzten Ausgabe des its-people Magazins haben wir unsere Teilnahme am Frankfurter NightRun mit den folgenden Worten angekündigt: „Wir hoffen auf gutes Wetter und einen tollen Abend bei dieser großen Laufveranstaltung". Am Nachmittag der Veranstaltung lautete die Wettervorhersage dann allerdings: 90% Gewitter-Wahrscheinlichkeit. Bis zum Startschuss blieb unklar, ob das Pre-Event des Frankfurter Ironmans überhaupt durchzuführen ist. Doch wir hatten Glück! Das Wetter spielte mit und der Lauf konnte stattfinden.
Nachdem die Wetterproblematik aufgehoben war, ergaben sich erneute Schwierigkeiten für die its-peopler. Jeder, der schon einmal mit dem Auto in die Frankfurter City gefahren ist, weiß, dass die Straßen häufig überfüllt, es Baustellen ohne Ende gibt und Parkplätze eher Mangelware sind. Der Lauf war kurz davor zu starten, aber noch nicht alle Teammitglieder der zwei Staffeln vor Ort, sondern stattdessen auf der Suche nach einem heiß begehrten Parkplatz.
Aber – auch hier hatten wir Glück und die sechs Staffelläufer kamen gerade noch rechtzeitig an und konnten starten. Auf der 3 x 5 km Strecke wurden dann sogar persönliche Bestzeiten erlaufen!
Zum Abschluss der Veranstaltung ging es, zusammen mit den begeisterten its-people Fans in einen nahegelegenen Biergarten, wo sich mit leckeren Speisen und Getränken gestärkt wurde. Gemäß dem Anlass waren die Hauptthemen natürlich Sport und Fitness, insbesondere Schwimmen, Laufen und Radfahren.
Sport und Spaß und auch noch etwas für einen guten Zweck tun, das war mal wieder ein voller Erfolg! Herzlichen Glückwunsch an alle its-people-Starter für diese erneute erfolgreiche Teilnahme am Nightrun 2018! Ihr seid wahre Ironmänner!

Wir freuen uns schon jetzt auf die Veranstaltung im nächsten Jahr!

Info: Der Ironman NightRun findet im Vorfeld des Frankfurter IRONMAN Laufs statt. Er ist ein Staffellauf und richtet sich an alle Freizeit- und Hobbysportler. Eine Staffel besteht aus drei Teammitgliedern. Jedes Teammitglied hat eine Strecke von 5 km zurückzulegen. Die Strecke führt in einem Rundkurs vor der Kulisse der Frankfurter Skyline am Main entlang und überquert den Fluss zweimal. Start, Staffelwechsel und Ziel finden am Mainkai/Eiserner Steg statt. Die Startgeldeinnahmen des IRONMAN NightRuns kommen der Stiftung Sporthilfe Hessen zu Gute.

Quelle Logo: http://eu.ironman.com/de-de/triathlon/events/emea/ironman/frankfurt/side-events/nightrun-by-helaba.aspx#axzz5K6KbwMNk

Quelle Banner: https://2018.doag.org/de/media

Vom 20. bis 23. November 2018 erwartet Sie in Nürnberg zur DOAG Konferenz und Ausstellung (Deutsche Oracle Anwender Gruppe) ein dreitägiges Vortragsprogramm mit internationalen Top-Rednern. Wir sind, wie in den vergangenen Jahren auch, mit unseren its-people Speakern bei diesem Event mit spannenden Fachvorträgen vertreten.

Unsere Portfolio Manager Sabine Heimsath und Robert Marz werden am Dienstag und Mittwoch in den Streams Datenbanken-Entwicklung und DevOps auf der Bühne stehen. Sabine Heimsath wird außerdem am Mittwoch, 17.00 Uhr, das Treffen der PL/SQL-Community co-moderieren und Robert Marz stellt sich am Donnerstag um 14.00 Uhr im Security-Panel zusammen mit weiteren anerkannten Security-Fachleuten den Fragen der Besucher.

Hier die Vorträge im Einzelnen:

Robert Marz, Dienstag 12 Uhr
Oracle Cloud Infrastructure – Netzwerk-Einrichtung für DBAs
Dieser Vortrag bringt Licht ins Dunkel und verknüpft die allgemeinen Konzepte mit den konkrekten Konfigurationsmöglichkeiten in der Oracle Cloud.

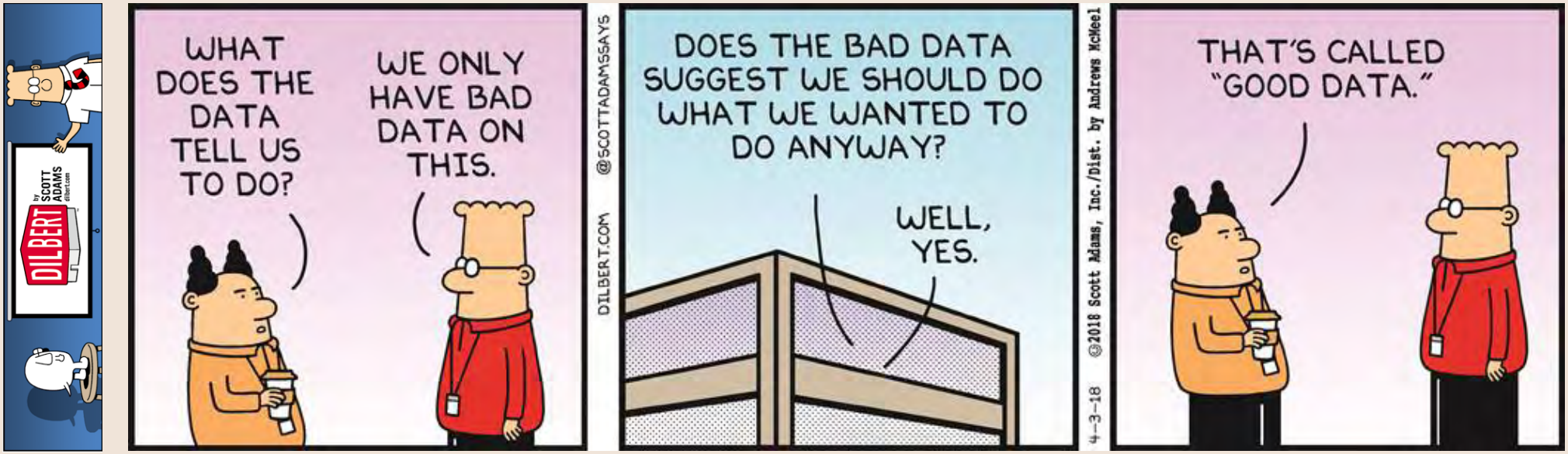
Sabine Heimsath, Dienstag, 13 Uhr
SQL Developer: Performance Tuning VOR dem Computer
Dies ist eine kondensierte Session mit den besten und wichtigsten Helferlein, die Ihnen die Arbeit mit dem SQL Developer schneller von der Hand gehen lassen.

Sabine Heimsath, Mittwoch 9 Uhr
Aus der Praxis: Die Reise von Flyway zu Liquibase
Dieser Vortrag enthält u.a. Pros und Cons des Einsatzes von Flyway-Liquibase und praktische Erfahrungen.

Die UKOUG Conference and Exhibition 2018 steht im Dezember vor der Tür!

Wir dürfen stolz ankündigen, dass **Sabine Heimsath** erneut auch auf dem internationalen Parkett mit einem Vortrag vertreten ist. Drei Tage lang (3.–5.12.2018) wird bei der **U**nited **K**ingdom **O**racle **U**ser **G**roup Technology Conference & Exhibition in Liverpool über spannende und aktuelle Themen wie Big Data, APEX oder Platform & DevOps in vielen Sessions gesprochen und diskutiert. Sabine Heimsath wird am Vortag der Veranstaltung einen Vortrag zum Thema **„The Practical Use of PL/Scope“** im Themenbereich Development halten und Einblicke in Anwendungen und Nutzung geben.

Quelle Banner: http://tech18.ukoug.org



© Scott Adams, Inc./Distr. Andrews McMeel/Distr. Bulls.

IT-Tage 2018: Die große IT-Konferenz zu Innovationen und Trends in der Softwareentwicklung

Wir freuen uns sehr, dieses Jahr mit its-people erstmalig als **Aussteller und Gold-Partner** bei den IT-Tagen 2018 im Kap Europa dabei zu sein. Die Fachmesse in zentraler Lage und unmittelbarer Nähe zum Frankfurter Messegelände verspricht an vier Tagen in 7 parallelen Tracks ein äußerst spannendes Programm mit 160 Sessions, Labs und Workshops von über 140 ausgewiesenen Expertinnen und Experten ihres Fachs.

Das Programm umfasst sowohl aktuelle Themen wie Agile Softwareentwicklung, DevOps, Continuous Delivery, Cloud-Computing, Big Data, Machine Learning, das Internet der Dinge und Microservices als auch Java, WebApps und natürlich die gesamte Palette unterschiedlichster Datenbanktechnologien wie Oracle, MS SQL Server, Postgres und MariaDB/MySQL.

Die IT-Tage 2018 wenden sich mit ihrem breiten Themenspektrum an technische Experten wie **Entwickler, Tester und Data Scientists als auch an IT-Führungskräfte.** Eine großartige Möglichkeit zum Wissensaustausch und eine perfekte Gelegenheit, sich über aktuelle IT-Trends mit ausgewiesenen Fachexperten zu informieren und zu diskutieren!

PRECON/WORKSHOPS
MONTAG, 10. DEZEMBER 2018, 9–16 UHR

Im Rahmen des Vorprogramms sind wir mit unseren beiden its-people Portfolio Managern **Sabine Heimsath und Robert Marz** außerdem Gastgeber eines ganztägigen Intensiv-Workshops zum Thema **Oracle SQL Developer.** Hier können die Teilnehmerinnen und Teilnehmer ihr Wissen in einem **praxisnahen Workshop** vertiefen. Die Schulung vermittelt einen Überblick über Konzepte und Möglichkeiten des Oracle SQL Developers, beleuchtet dabei auch einige weniger bekannten Features und versetzt die Teilnehmer in die Lage, den SQL Developer effizienter in die täglichen Arbeitsabläufe zu integrieren. Und nicht zuletzt zeigen Ihnen unsere beiden Fachexperten noch ein paar **nützliche Plugins.** Seien Sie gespannt!

Die IT-Tage 2018 sind eine ausgezeichnete Möglichkeit, sich über die aktuellen Entwicklungen und Technologien auf dem Laufenden zu halten.

Jetzt anmelden >>

Wir sehen uns auf den IT-Tagen 2018 am its-people Messestand!

its-people
we make the difference

itspeople

Als IT-Consulting-Unternehmen bündeln wir die Fachkompetenz vieler IT-Experten unter einem Dach. So können wir unseren Kunden hochqualifizierte Spezialisten des jeweiligen Fachgebietes anbieten.

Die besten IT-Professionals:
Flexibel im Einsatz, kompetent in den Projekten!

Kunden begeistern ist unser Antrieb!

IT-SECURITY

DATENBANKEN & CLOUD

ANALYTICS & DATA WAREHOUSE

ANWENDUNGS-ENTWICKLUNG

CUSTOMER DATA INTEGRATION

PROJEKT-MANAGEMENT SERVICES

Das hört sich interessant an? Sie möchten gerne mehr erfahren?
Besuchen Sie uns auf **www.its-people.de**

© from2015/istock