itmanagement
NOVEMBER 2019

www.it-daily.net

PROCESS MINING

Schlechte Performance war gestern

ERP SECURITY

Erhebliche Kontrollmängel

SERIE: RPA

So nicht! Oder doch?

SD-WAN

Dynamische Ansätze für's Ziel

SAP GTS AUS DER CLOUD

SICHER WELTWEIT HANDELN

Siegfried Klein, PwC

www.it-daily.net

cisco Partner
Global Gold Certified

LOGICALIS
Business and technology working as one

IT & OT wachsen zusammen.

Wir kennen den Weg.

» Connected Factory

» Industrial Cyber Security

» Data Management

www.logicalis.de

info@logicalis.de

WERBUNG VS. FREIES LESEN

Des einen Freud ist des anderen Leid. Gibt es ein Recht auf Werbefreiheit im Sinne von Werbe-Dauerberieselung? Nein, das hat just das Bundesverfassungsgericht in Karlsruhe entschieden und die Verfassungsbeschwerde der Axel Springer SE nicht zur Entscheidung angenommen. Damit ist das Verfahren gegen das Softwareunternehmen eyeo GmbH, das den weltweit genutzten Werbeblocker Adblock Plus vertreibt, vollumfänglich abgewiesen.

Bereits im April 2018 war Axel Springer mit seiner Klage durch alle Instanzen bis vor den Bundesgerichtshof gescheitert, dennoch hatte das Unternehmen anschließend Verfassungsbeschwerde gegen das Urteil eingelegt, um es aufheben zu lassen. Axel Springer versuchte zu argumentieren, dass die Anzeige von Werbung unter den Schutz der Pressefreiheit fiele. Ich finde, die Argumentation allein ist schon eine Frechheit ersten Grades.

Mit der Entscheidung des Bundesverfassungsgerichts, diese Beschwerde nicht einmal anzuhören, ist klar, dass aufgezwungene Werbeanzeigen nicht unter die Pressefreiheit fallen. Und das ist gut so. Der Rechtsstreit diesbezüglich ist damit endgültig beendet. Beifall von meiner Seite.

Die einzige Alternative, die ich hier für richtig halte wäre, Adblocker-Usern den Zugang zu gratis Informationen zu verwehren. Warum? Weil (fast) nichts auf der Welt gratis ist. Damit kann kein Unternehmen seine Rechnungen bezahlen. Oder wie der Banker sagt: There is no free lunch! Keine Werbung zuzulassen und gleichzeitig auf gratis Informationen zu bestehen ist inakzeptabel. Punktum.

In diesem Sinn, viel Spaß beim Lesen dieser Ausgabe, die nur ein „wenig" Werbung enthält und die damit alle Seiten glücklich macht!

Herzlichst Ihr

Ulrich Parthier

INHALT

IT MANAGEMENT

21

10

COVERSTORY

52

SLACK

SCHÖN ABER NICHT SICHER

Egal ob Start-up oder Konzern: Collaboration Tools wie Slack sind auch in deutschen Unternehmen überaus beliebt. Sie lassen sich besonders leicht in individuelle Workflows integrieren und sind auf verschiedenen Endgeräten nutzbar

Sie stellt allerdings eine Herausforderung für die Datensicherheit dar, die nur mit speziellen Cloud Security-Lösungen zuverlässig bewältigt werden kann.

In wenigen Jahren hat sich Slack von einer relativ unbekannten Cloud-Anwendung zu einer der beliebtesten Team Collaboration-Lösungen der Welt entwickelt. Ihr Siegeszug in den meisten Unternehmen beginnt häufig mit einem Dasein als Schatten-Anwendung, die zunächst nur von einzelnen unternehmensinternen Arbeitsgruppen genutzt wird. Von dort aus entwickelt sie sich in der Regel schnell zum beliebtesten Collaboration-Tool in der gesamten Organisation.

Mit den Produktivitätsvorteilen, die Slack bietet, gehen allerdings auch Risiken für die Datensicherheit einher. Nutzer können eine Vielzahl von sensiblen Dateien in der App miteinander teilen, von Architekturdiagrammen und proprietärem Code bis hin zu persönlichen und unternehmenssensiblen Daten, wie beispielsweise Finanzinformationen. Mit einfachen Best Practices, wie beispielsweise einer guten Passworthygiene und der Schulung von Mitarbeitern für einen sensiblen Umgang mit Daten und Zugriffsarten, lässt sich zumindest ein Mindestmaß an Sicherheit herstellen. Sämtliche Datenströme, die durch die Anwendung laufen, können allerdings kaum manuell durch das IT-Sicherheitspersonal überwacht werden. Darüber hinaus haben IT-Administratoren aufgrund der privaten Kanäle und der Direct Messaging-Funktionen von Slack oft keinen Überblick, welche Informationen untereinander ausgetauscht und gemeinsam genutzt werden.

IT-Teams haben also keinen Überblick, welche Daten über die App geteilt werden und ebenso wenig, wo diese sich befinden und ob sie eventuell in falsche Hände geraten sind. Für Unternehmen bedeutet dies, Sicherheitsmaßnahmen jenseits des Netzwerkperimeters ergreifen zu müssen, um sowohl die Nutzung von als auch die Daten in Slack zu sichern. Dies gilt insbesondere für Unternehmen, die Slack regelmäßig oder als primäre Business Collaboration Software einsetzen. Sie benötigen quasi zusätzlich eine Sicherheitslösung, die eine umfassende Transparenz und granulare Kontrollmöglichkeiten bietet.

Zusatztools notwendig

Cloud Access Security Broker (CASB) setzen auf Datenebene an und bieten damit unmittelbare Kontrollfunktionen für die sichere Nutzung von Cloudanwendungen. Mit ihnen lässt sich regeln, wie und wann Benutzer auf Cloudanwendungen wie Slack zugreifen können und wie Daten darin ausgetauscht werden. Unternehmen können damit fortlaufend nachvollziehen, wer welche Art von Daten teilt und wo diese herkommen. Um zu verhindern, dass sensible Daten in die falschen Hände geraten, können Unternehmen innerhalb eines CASBs Richtlinien einrichten, die diese Daten beispielsweise bei Bedarf automatisch in Slack-Nachrichten und Dateien ausblenden.

Darüber hinaus bieten CASBs eine Vielzahl weiterer Funktionen, die für die Sicherung der Nutzung von Slack und den Schutz von Unternehmensdaten unerlässlich sind: Multi-Faktor-Authentifizierung (MFA) verifiziert die Benutzeridentität zusätzlich zum Passwort mit weiteren Merkmalen, Data Loss Prevention (DLP) erwei-

tert die Zugriffsebenen für Benutzer auf der Grundlage ihrer Bedürfnisse und Privilegien, und Advanced Threat Protection (ATP) verhindert, dass sich Malware über die Cloud verbreitet.

Durch die API-Integration mit Slack und die Proxy-Funktion kann ein CASB automatisch alle Benutzeraktivitäten und Datenströme in der gesamten Unternehmensanwendung über alle Teams und Kanäle hinweg scannen. IT-Sicherheitsteams haben die Möglichkeit, in Echtzeit Richtlinien anzuwenden, mit denen sich Daten auch bei Benutzeraktivitäten innerhalb privater Kanäle und Direktnachrichten sichern lassen. Sensible Daten sowie der Austausch derselben werden automatisch identifiziert und das Sicherheitsrisiko somit deutlich reduziert.

Die meisten CASBs operieren außerdem agentenlos, das bedeutet, es ist keine Installation von Software-Agenten auf den Mobilgeräten der Mitarbeiter nötig. Selbst wenn Mitarbeiter von Privatgeräten auf Slack zugreifen, sind die Daten gesichert und im Fall eines Geräteverlusts auch das Löschen der Unternehmensdaten aus der Ferne möglich.

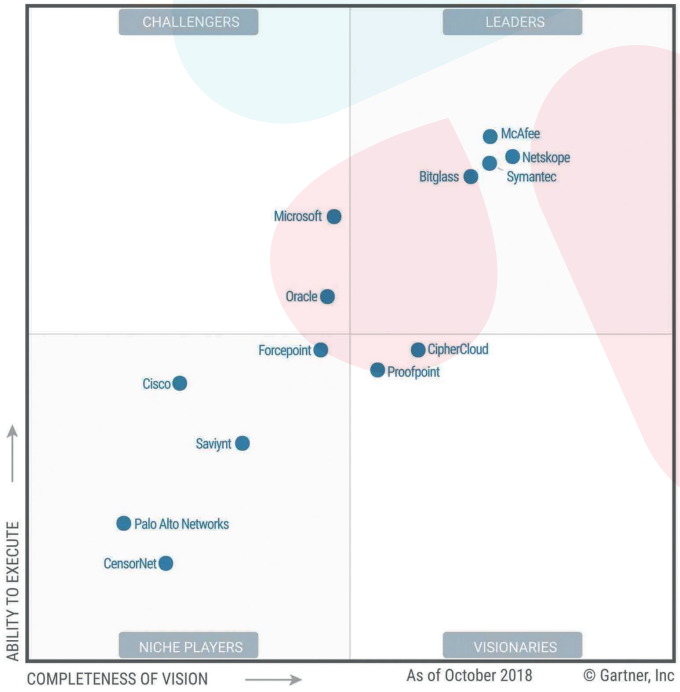
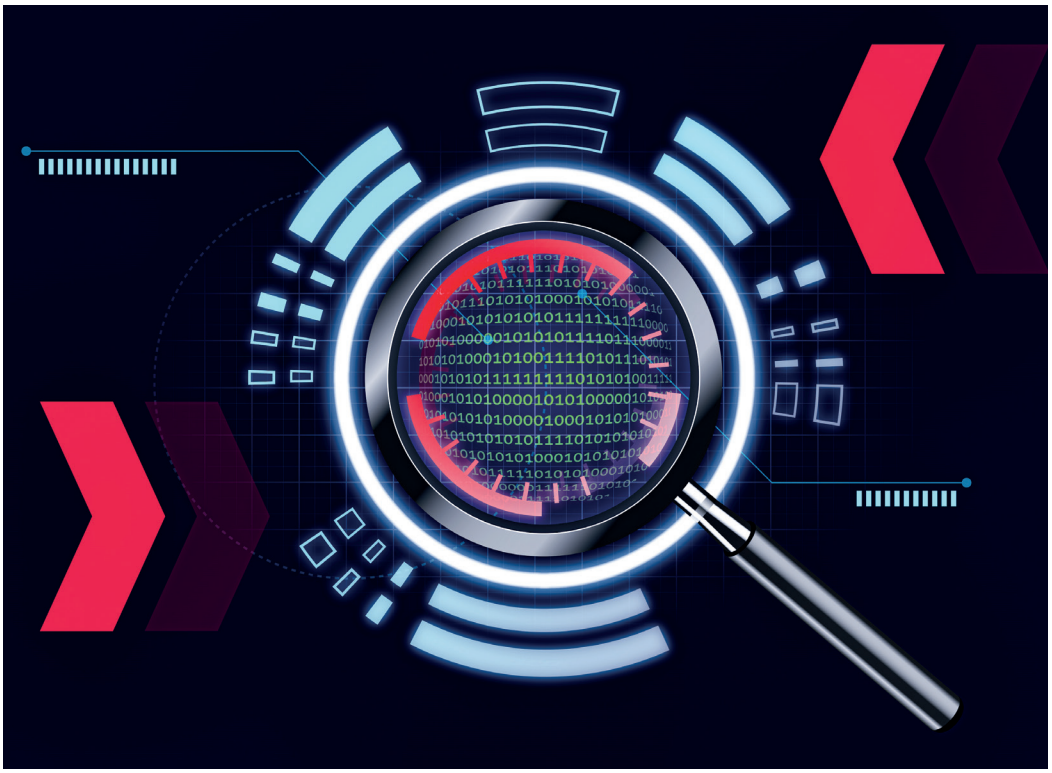


Bild:
Magic Quadrant for Cloud Access Security Brokers

Datenzentrierte IT-Sicherheit

Der Wechsel zu Cloudanwendungen wie Slack markiert für Unternehmen auch einen Wandel in ihrer IT-Security-Strategie. Daten sind in der digitalen Unternehmenswelt die wichtigste Ressource und verlangen ebenso sorgfältigen Schutz wie die Netzwerkinfrastruktur. Der Einsatz von CASBs kann dazu beitragen, den Wandel hin zu einer datenzentrierten Sicherheitsstrategie zu vollziehen.

www.bitglass.com



Quelle: Fraunhofer SIT

NEUER CODESCANNER

FINDET SOFTWARE-SCHWACHSTELLEN OHNE QUELLCODE

Fehler und Sicherheitslücken in Software verursachen Schäden in Milliardenhöhe, können den Ruf eines Unternehmens ruinieren und gefährden im schlimmsten Fall die Sicherheit von Menschen.

Deshalb „Vorhang auf“: das Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt VUSC – hat einen neuartigen Codescanner entwickelt. Sein Name: VUSC – die Abkürzung für Vulnerability Scanner. Er hilft Unternehmen und Entwicklern, Schwachstellen in fremdem Code innerhalb von Minuten aufzuspüren. Im Gegensatz zu herkömmlichen Analysetools benötigt VUSC nicht den Quellcode der zu untersuchenden Software. Außerdem lässt sich der Codescanner im eigenen Netzwerk betreiben, sodass sensible Informationen nicht ungewollt das Unternehmen verlassen.

Experten schätzen, dass die jährlichen Verluste durch Softwarefehler und Sicherheitslücken allein in Deutschland rund 84 Milliarden Euro betragen. Für Entwickler, Softwarehersteller und Anwender ist deshalb die Fehlerfreiheit und Sicherheit ihrer Software entscheidend. Doch wie erkennen IT-Abteilungen, ob die neu gekaufte Softwarelösung sicher und fehlerfrei ist? Wie überprüfen Hersteller eingekauften Code von externen Entwicklern auf Fehler? Und wie weiß der Entwickler, ob seine App keine Schwachstellen enthält?

Schnelle Ergebnisse und Risikoeinschätzung

Mit dem neuen Codescanner lassen sich diese Fragen innerhalb von Minuten beantworten. „Die zu untersuchende Datei wird einfach per drag and drop in den Scanner geladen“, erklärt Dr. Steven Arzt, Projektleiter VUSC und Abteilungsleiter am Fraunhofer SIT. Für den Scan-Vorgang benötigt VUSC keinen Quellcode – „das ist ein Alleinstellungsmerkmal unserer Entwicklung“, sagt Steven Arzt. VUSC findet nicht nur Fehler und Sicherheitslücken, sondern klassifiziert diese auch. So können Nutzer mit einem Blick erkennen, ob die gefundene Schwachstelle ein niedriges, mittleres oder hohes Risiko darstellt. VUSC arbeitet außerdem on premises, sodass sensible Daten jederzeit beim VUSC-Nutzer bleiben und nicht an fremde Server geschickt werden.

www.sit.fraunhofer.de/vusc

INNOVATIVE SYSTEMARCHITEKTUR

OPTIMIEREN UND AUTOMATISIEREN

IFS stellt eine neue Architektur für intelligente und autonome Enterprise-Lösungen vor. Sie soll die Basis für Service Management, Enterprise Resource Planning (ERP) und Enterprise Asset Management (EAM) als Grundlage für schnelle Innovationen, die Vorschau auf Technologien, die den nahtlosen und pragmatischen Einsatz von Schlüsseltechnologien wie KI, Machine Learning und Augmented/ Mixed Reality ermöglichen und Evergreen IT dienen: die aktuelle Version ist immer verfügbar und es ist keine Downtime bei Updates erforderlich. Die weiterentwickelte Architektur der IFS Lösungen soll ab 2020 verfügbar sein.

Die digitale Transformation sorge für schnellen Fortschritt – aber auch für Unsicherheit durch permanente Disruption, so das Unternehmen. Firmen brauchen Software-Partner, die nicht nur auf die Technologie achten, sondern vor allem auch darauf, welche Ergebnisse sie bringen. Diesen ergebnisorientierten Ansatz zeigt IFS anhand einer konkreten Vision, wie neue Technologien nahtlos in die Architektur der Kern-Anwendungen integriert und kunden- und branchenspezifisch gestaltet werden können.

Die neue Architektur wird die Basis für das gesamte Produktportfolio von IFS für Fertigungs-, Projektmanagement- und Servicelösungen sein. Sie erlaubt es Anwendern, Schlüsseltechnologien wie das Internet der Dinge (IoT), Augmented- und Mixed Reality-Anwendungen (AR/MR), Künstliche Intelligenz (KI) sowie Machine Learning (ML) pragmatisch und zielgerichtet in ihre IFS-Lösung zu integrieren. So können sie ihre Geschäftsprozesse mühelos optimieren und automatisieren sowie bessere Vorhersagen und Interaktionen im gesamten Unternehmen ermöglichen.

Die grundlegende Technologie für diese Struktur hat IFS im Zuge eines intensiven und nachhaltigen Entwicklungsprozesses realisiert. Dies beinhaltete unter anderem die deklarative, modellgetriebene Entwicklung, eine intuitive IFS Aurena-Anwenderoberfläche sowie das native API-Enablement des gesamten Funktionsspektrums. Diese Neuerungen ermöglichen eine schnellere Entwicklung von Innovationen im gesamten IFS-Ökosystem und eine schnellere Verfügbarkeit für die Kunden.

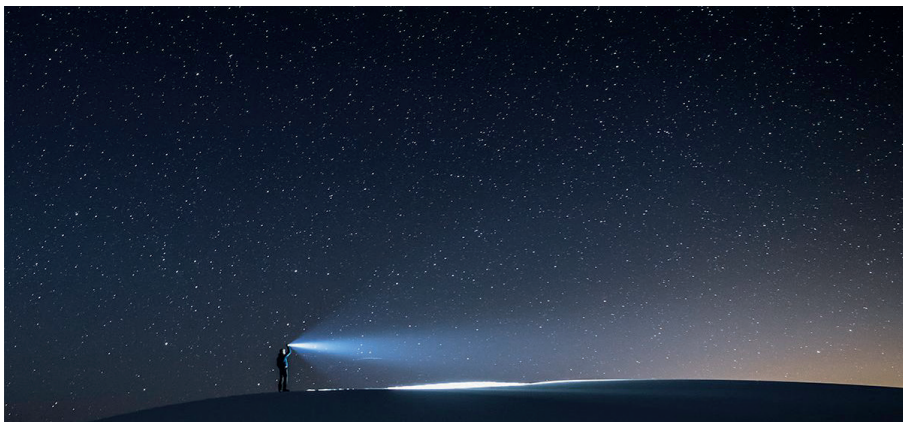
Die Architektur kann sowohl in der Cloud als auch On-Premise genutzt werden. Container-Technologie sowie Kubernetes erlauben einen Hyper-Scale-Betrieb in der Cloud ebenso wie maximale Portabilität zwischen Cloud- und On-Premise-Installationen. Zudem ermöglicht die Architektur ein dezidiertes Datenmanagement und versetzt Nutzer in die Lage, innovative Technologien via „Plug-and-Play" einzusetzen. Dazu gehören unter anderem KI, ML sowie Robotic Process Automation (RPA).

Im Rahmen der IFS World Conference, die kürzlich in Boston stattfand, stellt IFS die neuen Technologien in der Praxis vor: unter anderem einen Digitalen Zwilling und Asset Monitoring, Predictive Maintenance-Planung in Echtzeit, sowie AR/MR-getriebene Remote Assistance für zahllose Service- und Wartungsszenarien.

Dabei verfolgt IFS den so genannten „Evergreen-IT"-Ansatz: Anwender haben damit stets die aktuellste Version zur Verfügung – ohne Downtime während Upgrades. Zudem profitieren sie von besserer Planbarkeit, mehr Kontrollmöglichkeiten, sowie mehr Flexibilität bei der Planung ihrer eigenen Geschäftsentwicklung und dem Einsatz neuer Funktionen von IFS.

„Die Vision, die mein Team und ich heute präsentiert haben, ist unterfüttert von einem konkreten Angebot einer offenen, skalierbaren Architektur mit spezifischen Eigenschaften, die unsere Kunden in den verschiedenen Branchen dringend benötigen", erklärt Christian Pedersen, Chief Product Officer bei IFS. „Für IFS ging es in der Hauptsache immer um die Entwicklung einer Core-Lösung für unsere Anwendungen, der prinzipiell offen und mit maximalen Funktionsmöglichkeiten ausgestattet ist. Damit soll gezeigt werden, dass Wahlmöglichkeiten in den Lösungen gewissermaßen bereits eingebaut sind."

ifs.com/de/loesungen/



SAP GTS AUS DER CLOUD

SICHER UND KOSTENGÜNSTIG WELTWEIT HANDELN

Wenn sich in Großbritannien Regierung und Opposition über den Brexit streiten und der US-Präsident Donald Trump einen Handelsstreit nach dem anderen anzettelt, wirkt sich das auf die zoll- und außenhandelsrechtlichen Vorschriften aus. Damit Unternehmen den globalen Handel regelkonform und digital abwickeln können, bietet SAP die Software Global Trade Services (GTS) an. Warum sich gerade jetzt SAP GTS aus der Cloud lohnt und die Unternehmen den Wechsel auf SAP S/4HANA nicht abwarten müssen, erklärt Siegfried Klein, PwC, im Gespräch mit Ulrich Parthier, Herausgeber it management.

Ulrich Parthier: *Herr Klein, warum ist eine Software, die zoll- und außenhandelsrechtliche Prozesse digital abbildet, so wichtig und worin unterscheidet sich die Einführung von SAP GTS von der Implementierung anderer Geschäftssoftware?*

Siegfried Klein: Was SAP GTS so besonders macht, sind die zoll- und außenhandelsrechtlichen Prozesse, die die Software abbildet. Hier besteht sehr viel inhaltlicher Beratungsbedarf, da sich die Vorschriften und Gesetze quasi täglich ändern. Es gibt also ständig rechtliche Updates, die in das System einfließen müssen.

Ulrich Parthier: *Was unterscheidet PwC als Implementierer von SAP GTS?*

Siegfried Klein: Dass wir zoll- und außenhandelsrechtliche Kompetenz haben und Beratungsleistung erbringen dürfen. Allerdings übernehmen dies nicht unsere IT-Experten, sondern unsere Spezialisten aus dem Bereich „Tax and Legal". Sie beraten Unternehmen in außenhandelsrechtlichen Fragen unabhängig von der Software.

Ulrich Parthier: *Warum sind diese rechtlichen Kompetenzen so wichtig?*

Siegfried Klein: Weil für die Unternehmen das Risiko groß ist, dass sie ungewollt gegen Zoll- und Außenhandelsrecht verstoßen. Nehmen Sie zum Beispiel die Sanktionslisten. Seit 2009 gibt es Listen mit Terrorverdächtigen oder Unterstützern von Terrororganisationen. Da diese Listen ständig aktualisiert werden, ist es schnell passiert, dass man ungewollt in eine solche Falle tappt. Selbst das Erstellen eines Angebots ist nicht erlaubt. Wer dieses Risiko vermeiden will, kommt an einer digitalen Lösung wie SAP GTS nicht vorbei.

Ulrich Parthier: *Werden solche Listen denn nicht vom GTS-Implementierer automatisch zur Verfügung gestellt?*

Siegried Klein: Das muss in der Regel das Unternehmen selbst übernehmen. Die zoll- und außenhandelsrechtlichen Inhalte werden von verschiedensten Stellen veröffentlicht. Damit sind sie aber noch lange nicht geeignet für das IT-System. Deswegen stellen sogenannte Datenprovider die Daten aufbereitet zur Verfügung, die dann möglichst schnell in das System eingepflegt werden müssen. Dieses ganze Listenhandling übernehmen wir für unsere Kunden.

Ulrich Parthier: *Welche Systeme nutzen die Unternehmen denn heute?*

Siegfried Klein: Dort wird häufig noch händisch gearbeitet. Die Listen und Gesetze liegen in gedruckter Form vor und man hangelt sich dann für die einzelnen Bestellungen und Lieferungen auf Papier durch. Diejenigen Unternehmen, die Software einsetzen, nutzen häufig eine Vielzahl verschiedener Systeme, die unterschiedliche Prozesse abdecken. Ein System für die Sanktionslisten, ein anderes für die Zollkommunikation, ein weiteres für das Import- und Exportmanagement. Mit Effizienz hat das wenig zu tun.

Ulrich Parthier: *Spricht daher nicht viel für eine SaaS-Version von SAP GTS aus der Cloud?*

Siegfried Klein: Dafür sprechen mehrere Argumente. Erstens muss dieses System wie nur wenige up to date gehalten werden. Ein Cloud-Anbieter macht diese Updates quasi einmal für alle Kunden. Die Kosten werden also auf die Mandanten aufgeteilt. Zweitens ist für viele Unternehmen die Nutzungsfrequenz der Software unregelmäßig. Die Kosten für die Lizenz fallen aber unabhängig von der tatsächlichen Nutzung an. Auch hier spricht alles für die Cloud, denn dann lassen sich Kosten nutzungsbasiert abrechnen. Was in vielen Fällen deutlich günstiger ist als eine On-Premises-Version.

Ulrich Parthier: *PwC unterscheidet explizit zwischen SaaS und On-Demand. Worin liegt der Unterschied?*

Siegfried Klein: In der On-Demand-Variante fallen neben der monatlichen Grundgebühr für den Betrieb im Rechenzentrum nutzungsbasierte Kosten an, zum Beispiel pro Exportanmeldung. Kurz gesagt: Je mehr Transaktionen, desto günstiger die Einzelaktion. Die Lizenzkosten für SAP GTS sind inkludiert. Die Gesamtzahl pro Monat ist allerdings gedeckelt.

In der SaaS-Variante gibt es keine Obergrenzen und auch nur einen monatlichen Fixbetrag. Das bietet sich für größere Mittelständler an. Und den Unterneh-