COMPUTERWOCHE

Ausgabe 2022 – 16-17 25. April 2022 Nur im Abonnement erhältlich

VOICE OF DIGITAL

Frisiert IBM seine Cloud-Umsätze?

Mainframe-Einnahmen wurden als Cloud-Business verbucht, behaupten Investoren.

Seite 6

Mercedes baut Softwarefabrik

200 Millionen Euro steckt der Autobauer in seinen Electric Software Hub.

Seite 18

Der Chef als Beziehungsmanager

Was Führen auf Distanz für Führungskräfte bedeutet.

Seite 40

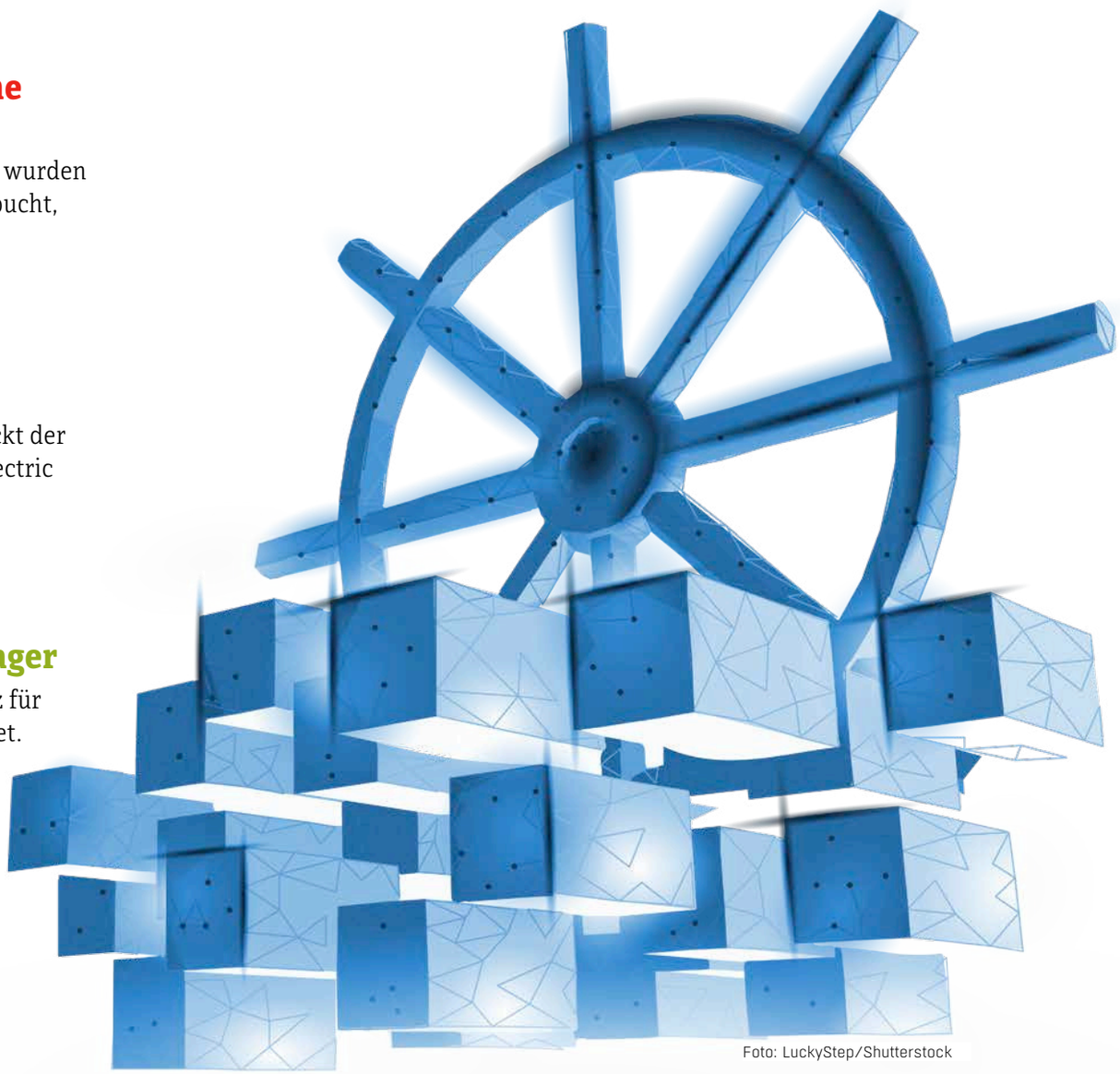

Foto: LuckyStep/Shutterstock

Open Source – ein Sicherheitsrisiko?

Neben lizenzrechtlichen Tücken müssen Anwender verstärkt auch auf Schwachstellen in ihrer Software Supply Chain achten.

Seite 24

Mehr Transparenz für mehr Sicherheit

Mit der wachsenden Komplexität und wechselseitigen Abhängigkeiten werden IT-Systeme immer anfälliger. Hacker haben das längst bemerkt und attackieren die Software Supply Chain.

Martin Bayer,
Deputy Editorial Director

Nicht erst der seit Wochen tobende Cyberkrieg führt uns vor Augen, wie verletzlich unsere Infrastrukturen sind. Dabei steht viel auf dem Spiel. Krankenhäuser können nicht arbeiten, weil ihre IT-Systeme verschlüsselt wurden, und Energieversorger gehen in die Knie. Gerade jetzt greifen russische Cyberbanden den US-amerikanischen Energiesektor an. Fachkräfte befürchten, dass die Hacker bereits tief in die Steuerungsanlagen eingedrungen sind und es Jahre dauern könnte, sie daraus zu vertreiben.

Hier geht es längst nicht mehr nur um das oft beschworene Hase-Igel-Spiel zwischen Angreifern und Verteidigern. All diese Schreckensszenarien offenbaren ein viel tiefer sitzendes Problem. Unsere IT-Systeme sind über die Jahre immer komplexer geworden. Das Geflecht aus verschiedensten Anwendungen und Diensten im eigenen Data Center und aus der Cloud sorgt für kaum noch zu kalkulierende Abhängigkeiten zwischen den einzelnen Komponenten. Jede Veränderung, jede neue API, jedes neue Tool sorgt für zusätzliche Sollbruchstellen. Dazu wächst der Druck auf die Entwickler, immer schneller Software an den Start zu bringen. Das funktioniert nur mit Hilfe vorgefertigter Code-Module und -Bibliotheken. Gerade im Open-Source-Universum finden sich viele zehntausende davon.

Die Frage, wie sicher das Ganze ist, fällt dabei oft unter den Tisch. Schließlich kostet es viel Zeit und Ressourcen, die Software Supply Chain auf Sicherheitslücken hin abzuklopfen. Doch noch viel teurer kann es werden, nicht darauf zu achten. Hacker haben diese Schwachstelle längst entdeckt. Mehr denn je brauchen Unternehmen heute ein sauberes und transparentes IT-Architekturmanagement, auch wenn es dadurch an der einen oder anderen Stelle etwas langsamer geht.

Herzlich,
Ihr

Martin Bayer

IT-Spezialist zum Cyberwar:
Warum Systeme nicht per Software veränderbar sein dürfen, erklärt Joachim Popp, vom Anwenderverband VOICE auf CSO online:
www.csoonline.com/de/3673867

Praxis

Job & Karriere

Foto: Irina Anosova/Shutterstock

IBM soll Cloud-Erlöse künstlich aufgepumpt haben

Angeblich hat das IBM-Management Mainframe-Einnahmen als Umsätze für Zukunftsthemen wie die Cloud verbucht, um höhere Boni einzustreichen. Investoren haben deshalb in den USA Klage gegen IBM eingereicht.

Von Martin Bayer, Deputy Editorial Director

Konkret soll IBM Einnahmen aus dem lukrativen, aber wenig zukunftsträchtigen Mainframe-Geschäft (siehe auch Seite 20) in strategische, für die Entwicklung des Unternehmens wichtigere Geschäftsfelder umgeleitet haben. Die Klage wurde am 5. April vor einem Gerichtshof im südlichen Bezirk von New York eingereicht. Beschuldigt werden neben IBM als Firma auch die langjährige IBM-CEO Virginia Rometty und der ehemalige Finanzchef Martin Schroeter, der heute als Chef des IBM-Spin-off Kyndryl fungiert, sowie die amtierenden Geschäftsführer Arvind Krishna (CEO) und James Kavanaugh (CFO).

IBM „hat in unzulässiger Weise und unter Verstoß gegen die allgemein anerkannten Rechnungslegungs-Grundsätze (Generally Accepted Accounting Principles – GAAP) einen betrügerischen Plan verfolgt, um Einnahmen in Milliardenhöhe von seinem Mainframe-Geschäftsbereich in die Bereiche Strategic Imperatives und CAMSS zu verlagern“, heißt es in der Anklageschrift. CAMSS steht für Cloud, Analytics, Mobile, Social und Security. IBM hatte diesen Zukunftsmarkt bereits 2014 in der Ära Rometty definiert und angesteuert. 2015 wurde die neue Ausrichtung mit dem Begriff Strategic Imperative (SI) umschrieben. Rometty hatte IBM als Nachfolgerin von Samuel Palmisano von Anfang 2012 bis Ende 2020 geführt.

Hat IBM die Finanzmärkte in die Irre geführt?

Die Investoren fordern im Rahmen der Wertpapier-Sammelklage Schadensersatz. Wie viel, ist noch nicht bekannt. Mit den Bilanzmanipulationen hätten die IBM-Verantwortlichen dem Markt Erfolge in wichtigen CAMSS-Zukunftsmärkten vorgegaukelt und selbst höhere Boni

Verdi fordert Aufklärung: Hat SAP seine Mitarbeiter ausspioniert?

Die Dienstleistungsgewerkschaft Verdi hat ein internes Datenleck bei SAP öffentlich gemacht. Sensible Informationen aus der Belegschaft sollen allgemein zugänglich gewesen sein.

In der Arbeitnehmervertretung von SAP verschieben sich die Machtverhältnisse. Überraschend hat die IG Metall kürzlich die Betriebsratswahlen bei SAP gewonnen. Die Liste „Pro Mitbestimmung" schickt neun Vertreter in den nächsten 45-köpfigen Betriebsrat des deutschen Softwarekonzerns. Damit hat erstmals eine Gewerkschaftsliste die meisten Stimmen erhalten. Gemeinsam mit der Verdi-Liste „Upgrade", die die Zahl ihrer Sitze von vier auf sechs erhöhen konnte, stellen die beiden DGB-Gewerkschaften mit zusammen 15 Sitzen ein Drittel des künftigen SAP-Betriebsrats.

Foto: SAP SE

Mit dem Sieg bei den SAP-Betriebsratswahlen im Rücken, gehen die Gewerkschaften auf Konfrontationskurs mit dem Softwarekonzern. Die Verdi-Betriebsgruppe hat eigenen Angaben zufolge ein Datenleck in den betriebsinternen Systemen bei SAP entdeckt und fordert nun lückenlose Aufklärung.

Betroffen ist den Angaben zufolge der intern entwickelte und nur der SAP-Belegschaft zugängliche Onlinedienst „SAP Interactive Broadcast", der für Mitarbeiter- und Betriebsversammlungen des Betriebsrats genutzt wird. Neben Audio- und Videoinformationen biete der Dienst auch die Möglichkeit, Fragen zu stellen und darüber abzustimmen. Diese Funktionen sollten standardmäßig anonym erfolgen.

Gläserne Beschäftigte – Verstoß gegen demokratische Grundsätze

Laut der Verdi-Gruppe „Upgrade" im SAP-Betriebsrat waren in der Vergangenheit jedoch alle Fragen sowie das Abstimmungsverhalten dazu eindeutig einzelnen Personen zuzuordnen. Diese Informationen seien zudem automatisch auf alle an den Versammlungen teilnehmenden Rechnern aufgespielt worden und damit faktisch der gesamten Belegschaft zugänglich gewesen. „Die Rückverfolgbarkeit war trivial herzustellen. Der geübte Programmierer konnte den Ansatz auf den ersten Blick sehen", stellt Verdi-Betriebsratsmitglied Andreas Hahn fest.

Der Konzern habe die Rückverfolgbarkeit nach der sofortigen internen Meldung der Verdi-Betriebsgruppe an die interne Cyber-Security zwar zeitnah gestoppt und den Vorfall jüngst auch intern an die Belegschaft kommuniziert, berichten Gewerkschaftsvertreter. Jedoch blieben viele Fragen nach wie vor offen. „Der Arbeitgeber muss den Datenleck-Vorfall lückenlos aufklären", fordert Christine Muhr, SAP-Unternehmensbetreuerin von Verdi. „Personenbezogener Datenschutz muss mit der höchsten Priorität abgesichert sein, ebenso das verbriefte Recht auf freie Meinungsäußerung in Unternehmen. Wo das nicht gewährleistet ist, werden Beschäftigte zu gläsernen Beschäftigten. Das wäre ein Verstoß gegen demokratische Grundsätze."

Gewerkschafter Hahn fordert von SAP „volle Transparenz gegenüber der Belegschaft und den Mitbestimmungsgremien darüber, wie lange diese Rückverfolgbarkeit bereits möglich war und welche internen Veranstaltungen davon betroffen waren." Zudem müssten alle möglicherweise noch existierenden Daten nachvollziehbar gelöscht und die technischen Details über die Funktionsweise des Dienstes mit den Mitbestimmungsgremien geteilt werden.

SAP nennt Datenschutz sehr hohes Gut

SAP räumt ein, dass es ein Problem mit dem Datenschutz gegeben habe. „In diesem Fall konnte durch die Aufmerksamkeit eines Kollegen eine theoretisch mögliche Umgehung unserer Sicherheitsmaßnahmen aufgedeckt und sogleich behoben werden", heißt es in einer Stellungnahme des Softwarekonzerns. „Datenschutz ist für SAP ein sehr hohes Gut und wir respektieren die Privatsphäre jedes Einzelnen." Interne Tools würden regelmäßig geprüft und auf dem aktuellen Stand gehalten. Dabei beschäftigten sich die Kolleginnen und Kollegen auch mit den jeweiligen technischen Sicherheitsanforderungen. *(ba)*