SOFTIES

„Die digitale Transformation und der Generationswechsel machen vor IBM-i-Anwendungen keinen Halt“, warnen die Experten der Ravensburger **PKS Software GmbH**. Das neue, kostenlose Whitepaper „Anwendungsentwicklung auf IBM i“ erweitert daher klassische Themen wie Anwendungsbetreuung und Weiterentwicklung mit gezielten strategischen Beratungen für die Antwort auf die entscheidende Frage: Wie kann der Spagat zwischen Standard und Eigenentwicklung, Flexibilität und Innovation so gelingen, dass man auch Nachwuchstalente begeistern kann?

www.pks.de

Gemeinsam mit **IBM** will **Noname Security**, kalifornischer Anbieter von API-Sicherheit, den Schutz von IBM API Connect vor Schwachstellen, Fehlkonfigurationen und Designfehlern verbessern. Mit dem neuen Produkt „Noname Advanced API Security für IBM“ lässt sich die API-Sicherheitslösung von Noname in Kombination mit den Sicherheitsfunktionen von IBM Data Power nutzen, um eine zusätzliche Schutzebene für API Connect zu schaffen. Die API-Verwaltung soll Erstellung, Verwaltung, Schutz, Verwertung und auch Monetarisierung von APIs ermöglichen.

www.nonamesecurity.com

Tool für die Profi-Datenpflege: Mit Filescope bietet **Raz-Lee** einen universeller Datenbank-Editor für IBM i, mit dem Anwender können schnell und einfach IBM-i-Datenbankdateien anzeigen, durchsuchen, bearbeiten, verknüpfen und drucken können; auch Datenkonvertierungen sind möglich.

www.razlee.de

Inklusive Drittanbieter-Apps: Ein neue Funktion in der Kace Cloud ermöglicht automatisiertes Patching in der Cloud über eine einzige Plattform, meldete deren Hersteller **Quest Software**. Die neu gestalteten Cloud-Plattform bahne neue Wege in Sachen Endpunktmanagement, als All-in-One-Lösung für mehr als 10.000 Patches und über 350 Anwendungen von Drittanbietern, darunter neben **Microsoft** auch **Adobe, Cisco, Google** Chrome und **Slack**.

www.quest.com

Schutz sensibler Daten: Ein neues Verschlüsselungsprogramm auf Feldebene für Daten in IBM-i-Anwendungen bietet das US-Softwarehaus **Precision Solutions Group (PSGi)** an. Die Software Field Level Security Manager fungiert als einfach zu bedienender Wrapper für das Db2-Feature „Row and Column Access Control“ (RCAC) zur Datenbankverschlüsselung und vereinfacht das Festlegen von Regeln für die Anzeige „geschwärzter“ Daten für Benutzer auf der Grundlage von anpassbaren Berechtigungen auf Feldebene. Diese Software nutzt zwar die RCAC-Funktionalität von IBM i, macht es aber für nicht-technische Benutzer viel einfacher, Regeln und Berechtigungen festzulegen und zu ändern.

www.precisionsg.com

Die Stuttgarter Software-Schmiede **Elo Digital Office** bringt mit der Version 23 das jüngste Long-Term-Support- bzw. LTS-Release ihrer ECM-Suite auf den Markt – mit Neuerungen in den Bereichen Technologie, digitale Zusammenarbeit sowie Anbindung vorhandener Drittsysteme wie **SAP**, **Datev** oder **Salesforce**. Kunden erhalten zudem alle Funktionserweiterungen der in den vergangenen beiden Jahren publizierten Feature-Releases, darunter ein einheitliches Metadaten-Modell sowie die Automatisierungskomponente Flows.

www.elo.com

Die Top-Drei-Sorgen der Automotive-Entwickler bei der Software-Erstellung sind funktionale Sicherheit (30 Prozent), Security (27 Prozent) sowie Qualität (26 Prozent). Das zeigt der jährlichen Report „State of Automotive Software Development“, für den das US-Softwarehaus **Perforce** rund 400 Fachkräfte der Branche befragte. Zwar bleibt Safety demnach oberste Priorität, doch nimmt die Notwendigkeit zu, die elektronischen Systeme, Kommunikationsnetze und Software in Fahrzeugen abzusichern.

www.perforce.com

Parradee Kietsirikul / iStock / Getty Images Plus

Die Vorbereitung ist das A und O

DMS-Einführung als Motor der Digitalisierung

VON HERMANN SCHÄFER

Der Motor der deutschen Wirtschaft, die mittelständischen Unternehmen, müssen bei der rasant voranschreitenden Digitalisierung mit den großen Konzernen mithalten, denn die stellt viele bewährte Strategien und Geschäftsmodelle infrage. Es gibt aber durchaus praxisbewährte Methoden für den gelungenen Einstieg des Mittelstandes in die Digitalisierung.

Für bereits etablierte Mittelständler ändern sich aktuell die Regeln des Wettbewerbs grundlegend und sehr schnell. Sie müssen agiler, schneller und innovativer werden, um Schritt zu halten. Dass digitale Technologien dabei entscheidend sind, hat auch die Mehrheit der Unternehmen in Deutschland erkannt. Laut einer Studie des Branchenverbandes Bitkom bestätigen 52 Prozent der Befragten, dass Unternehmen, die frühzeitig in die Digitalisierung investiert haben, heute von einem Wettbewerbsvorteil profitieren.

Allerdings zeigt die Studie auch, dass vielen Unternehmen die digitale Transformation schwerfällt. So räumen 34 Prozent ein, Probleme bei der Bewältigung der Digitalisierung zu haben. Dabei ist der Einstieg mit einem Dokumentenmanagement-System (DMS) mittlerweile sehr gut zu meistern. Es kommt lediglich auf die richtige Strategie, Vorbereitung und die schrittweise Einführung an.

Hand in Hand mit dem Software-Partner

Mittelständische Unternehmen scheuen die Einführung eines neuen Systems häufig aufgrund der verbundenen Kosten und der erforderlichen IT-Ressourcen. An dieser Stelle kommen Digitalisierungspartner ins Spiel, die das Unternehmen entsprechend der Bedürfnisse beraten und während des gesamten Bereitstellungsprozesses unterstützen.

Die Auswahl des richtigen Partners ist dabei mittlerweile nicht mehr allein von der Funktionalität und dem Angebot seiner Lösungen abhängig. Kunden erwarten ein hohes Maß an Support – sowohl während der Planungs- und Implementierungsphase als auch danach. Sie schätzen die Sicherheit, den persönlichen Austausch und das Know-how, das ihnen der Digitalisierungspartner bietet. Auf diese Weise wird die Implementierungszeit massiv verkürzt und Herausforderungen lassen sich einfacher bewältigen.

Die Voraussetzungen schaffen

Grundvoraussetzung für eine erfolgreiche Digitalisierung ist, die Führungsriege des Unternehmens von dem Vorhaben zu überzeugen. Die Projektbeteiligten sollten motiviert sein, die Digitalisierungsagenda voranzutreiben. Die wichtigsten Endbenutzer sind ebenfalls von Beginn an in den Prozess miteinzubeziehen, da sie meist mehr in die täglich anfallenden Aufgaben involviert sind.

Im nächsten Schritt gilt es, vor dem Einsatz einer neuen Software alle Prozesse zu analysieren sowie die wichtigsten Meilensteine, Engpässe und Frustfaktoren vorab herauszufiltern. Fragen wie

- Was löst den Prozess aus – ein Telefonat, eine E-Mail, ein Papierformular oder Meeting vor Ort?
- Wie werden Daten erfasst und wo werden sie gespeichert?
- Wer ist alles an dem Projekt beteilig?

helfen dabei, Prozesse genau zu verstehen.


Unser Autor **Hermann Schäfer** ist Vice President Partner Sales EMEA bei Docuware, Germering.

Entwicklung einer individuell abgestimmten Lösung

Sobald sich das Team einen guten Überblick über die Geschäftsprozesse verschafft hat, unterstützt der Digitalisierungspartner dabei, eine geeignete Software auszuwählen. In der Konzeptionsphase wird festgelegt, welche Software-Komponenten und Funktionen notwendig sind und ob eine Cloud- oder On-Premises-Lösung implementiert werden soll. Die Entscheidung ist dabei von der IT-Infrastruktur des Unternehmens, den möglichen Kosten für die Aufrüstung der Hardware sowie vom Umfang und Know-how des IT-Teams abhängig.

Es ist empfehlenswert, mit einer Abteilung oder einem bestimmten Prozess zu starten. Hier eignen sich Bereiche mit einer hohen Dokumentenanzahl, wie beispielsweise die Buchhaltungs- oder Personalabteilung.

Aufklärung ist der Schlüssel

Steht die Konzeption der Lösung, sollten alle Kolleginnen und Kollegen darüber informiert werden. Wichtig ist hierbei, zu berücksichtigen, dass es womöglich Mitarbeitende geben wird, die zunächst zögern und sich nicht von vertrauten, papiergebundenen Prozessen verabschieden möchten. Eine transparente und schlüssige Kommunikation – beispielsweise per Video – klärt die Belegschaft auf, erläutert die Vorteile der neuen Lösung und gibt einen ersten Überblick. Eine ausführliche Einführungsschulung und weitere Fortbildungen sind ebenfalls essenziell, damit die Software effizient angewendet und alle Vorteile voll ausgeschöpft werden können.

Sobald der Einstieg in die Digitalisierung mit einem DMS gelungen ist, können weitere Prozesse digitalisiert werden. Mithilfe von „Integration Platform as a Service“ bzw. iPaaS-Plattformen lassen sich auch im Nachhinein sämtliche Programme ganz unkompliziert mit dem DMS verbinden, um so für ganzheitlich digitale Workflows im Unternehmen zu sorgen. ◘


Getty Images / iStock / GettyImages Plus

Die neue Qradar Security Suite

SIEM-Plattform modernisiert und um Automatisierung und KI erweitert

Die SIEM-Software Qradar wurde am 24. April von IBM zu einer umfassenden Security-Suite erweitert, um Bedrohungen schneller zu erkennen und die Reaktion darauf zu beschleunigen. Laut Hersteller beschleunigen neue KI- und Automatisierungsfunktionen beispielsweise die Triage der Alerts durchschnittlich um 55 Prozent.

Qradar liefert heute Technologien zur Erkennung, Untersuchung und Reaktion auf Sicherheitsbedrohungen. Basis ist das auch mit IBM i nutzbare „Sicherheitsinformations- und Ereignis-Management“ (SIEM), das 2011 durch die Übernahme der Q1 Labs zu IBM kam.

Mehr als „nur“ SIEM

Das aktuelle Upgrade zur Security-Suite geht über das eigentliche SIEM weit hinaus und zielt darauf ab, Unternehmen zusätzlich auch bei der „Extended Detection & Response“ (EDR/XDR) sowie der „Security Orchestration Automation and Response“ (SOAR) zu unterstützen. Außerdem gibt es mehr als 900 vorgefertigte Integrationen, die für Interoperabilität mit Tool-Sets anderer Anbieter sorgen sollen.

Die neuen SOAR-Funktionen stammen aus der Übernahme von Resilient im Jahr 2016, EDR-Funktionen aus dem Erwerb von Reaqta im Jahr 2021. KI soll die Verwaltung und Priorisierung von Bedrohungswarnungen unterstützen. Die neue Suite automatisiert zudem Untersuchung von Bedrohungen, wobei sie auch Analysten mit Details zum Risiko und empfohlenen Maßnahmen zur Abhilfe versorgen wird. Ebenfalls neu ist ein neues Cloud-natives Produkt für Log-Management und Sicherheitsbeobachtung namens „Log Insights“.

Individuelle SaaS-Angebote

Der ab sofort über individuelle SaaS-Angebote verfügbare Service ist laut Hersteller speziell für die Anforderungen der „Hybrid Cloud“ entwickelt worden und biete eine einheitliche, modernisierte Benutzeroberfläche über alle Produkte hinweg. So können Security-Analysten schneller, effizienter und präziser mit ihren Tool-Sets arbeiten. Geplant ist außerdem, Qradar SIEM bis Ende des zweiten Quartals 2023 auch als Service auf AWS zur Verfügung zu stellen.

Gesa Müller

Das neue **Security Dashboard 2.0** der Plattform Werth Auditor für SAP-Systeme

Angriffserkennung für SAP-Systeme

Manipulationssicheres Security-Dashboard

Werth IT, ein auf SAP-Security spezialisierter Software-Hersteller aus Kamen, erweitert seine Software Werth Auditor um ein neues, manipulationssicheres System zur Angriffserkennung und Sicherheitsbewertung von SAP-Landschaften.

Das Security Dashboard 2.0, das die vom Werth Auditor erkannten Sicherheitsrisiken visualisiert und bei der Bewertung der zugehörenden Sicherheitsprozesse hilft, bereitet alle Sicherheitsinformationen in Echtzeit auf und stellt sich übersichtlich dar.

Die zentralisierte Visualisierung sämtlicher Sicherheitsinformationen aller miteinander kommunizierenden Systeme der kompletten SAP-Landschaft in nur einem Dashboard ist laut Geschäftsführer Thomas Werth „eine echte Innovation und ein Alleinstellungsmerkmal“. Zudem können Security-Fachkräfte aus dem Haupt-Dashboard heraus die für ihren Verantwortungsbereich relevanten detaillierteren Einzel-Dashboards ansteuern und tiefgreifende Informationen zu einzelnen Bereichen abrufen, denn das Dashboard zeigt in Echtzeit und en Détail, wie sicher die SAP-Landschaft aufgestellt ist, welche Rubriken zu verbessern sind und wo unmittelbares Handeln erforderlich ist.

Der Werth Auditor bietet SAP-Kunden mit über 2.000 Prüfungen und einem kontinuierlichen Monitoring eine umfassende Angriffserkennung: Er enttarnt Angriffe, deckt Sicherheitsrisiken auf und visualisiert die zugehörigen Sicherheitsinformationen – in allen miteinander kommunizierenden Systemen der IT-Landschaft. Jederzeit und in Echtzeit analysiert die Security-Lösung die Sicherheitskonfiguration, weist auf fehlende SAP-Security-Notes und Patches hin und überprüft den gesamten Abap-Quellcode – und zwar nicht nur den für Kunden zugängigen Bereich, der lediglich einen kleinen Teil das Abap-Codes ausmacht. Ferner werden das Betriebssystem, die Datenbank, alle Schnittstellen sowie die Berechtigungen geprüft. Zusätzlich lässt sich anhand der Entwicklung des Security-Reifegerades sowie an der Lebensdauer von Schwachstellen die Wirksamkeit der internen Security-Prozesse ablesen und analysieren.

Während herkömmliche Prüfsysteme die erhobenen Daten häufig in Tabellen darstellen, verwendet Werth IT die Technologie „Security Information and Event Management“ (SIEM), mit deren Hilfe alle gesammelten Sicherheitsdaten vollständig über Schlagworte und beliebige Zeiträume filterbar sind und ganzheitliche, tiefgreifende Sicherheitsanalysen aller Systeme ermöglichen. Dies bedeutet zugleich maximale Effizienz für Threat Detection, Vulnerability Management und Patch Management.

Für die Sicherheits-Teams und die Verantwortlichen stehen mehrere vollständig anpassbare Dashboards zur Verfügung. Ebenfalls wichtig: Die Software arbeitet mit „Zero Footprint“, benötigt als weder Software-Installation noch Agenten auf dem lokalen System, und funktioniert ohne permanente Internet-Verbindung. Deshalb sind alle Sicherheitsdaten manipulationssicher, denn Angreifer der überwachten SAP-Systeme können weder auf die Prüflogik noch auf das Dashboard oder dessen Daten zugreifen.

Elke von Harsdorf

Höchste Priorität für Cyber-Security

Interview mit Thomas Werth, Geschäftsführer der Werth IT GmbH

Herr Werth, was kann ein Unternehmen tun, um Cyber-Risiken und Bedrohungen schneller und besser zu erkennen bzw. zu beseitigen?
Thomas Werth: Wir empfehlen den Einsatz eines manipulationssicheren Security-Systems, das mögliche Angriffe und Risiken erkennt und zudem die Sicherheit der gesamten SAP-Landschaft bewertet. Eine automatisierte Sicherheitslösung entlastet die Mitarbeiterinnen und Mitarbeiter bei der Steuerung der internen Sicherheitsprozesse und hilft, die Sicherheit im Unternehmen zu erhöhen. Ein weiteres wichtiges Kriterium für den größtmöglichen Schutz des SAP-Systems ist die Darstellung der Security-Analysen in Echtzeit.

Welche Rolle spielt ein Dashboard in diesem Zusammenhang?
Werth: Mit der Anzahl der zu schützenden Systeme steigt die Komplexität der sicherheitsrelevanten Informationen. Ein Security-Dashboard bündelt diese Daten effizient und erlaubt somit einen schnellen Überblick zum Sicherheitsstatus sowie dem Reifegrad von Sicherheitsprozessen und Compliance. Mit diesen Informationen lassen sich dann die Prozesse im Unternehmen kontrollieren und steuern, um eine effektive Sicherheit zu erreichen und mögliche Angriffe schnell zu erkennen.

Gibt es besondere Aspekte zu beachten, wenn Software der SAP als ERP-System genutzt wird?
Werth: Die SAP-Plattform ist hochkomplex und benötigt spezielle Lösungen, die in der Lage sind „in“ die SAP-Layer zu schauen. Herkömmliche Sicherheits-Scanner können oft nicht die Besonderheiten innerhalb dieser Applikation prüfen – und somit wäre eine zusätzliche manuelle Kontrolle erforderlich. Nur spezielle Sicherheitslösungen für SAP-Systeme ermöglichen ein Security-Monitoring. Diese sollten manipulationssicher Bedrohungen erkennen und die Sicherheit der Systeme kontinuierlich überwachen.

Warum ist Manipulationssicherheit in diesem Bereich wichtig – und wie lässt sich diese erreichen?
Werth: Sieht man sich die etablierten Standards der Cybersicherheit in der IT-Welt genauer an, wird schnell das Prinzip der Segmentierung deutlich: Ein Intrusion-Detection-System, SIEM / Logserver oder auch die zentrale Steuerung der Antivirus-Software wird immer dediziert und besonders geschützt betrieben. Der Grund ist klar: Die Security-Prozesse müssen unerreichbar für Angreifer sein und dürfen sich nicht deaktivieren lassen. Für das SAP-System bedeutet dies, dass auch hier die Sicherheitslösungen „außerhalb“ zu betreiben sind, damit ein Angreifer diese nicht manipulieren oder deaktivieren kann. Andernfalls ist ein Szenario wie bei Stuxnet denkbar, der einfach alle Kontrollen auf „grün“ manipuliert hat.

Mit welchen ersten Maßnahmen kann ein Unternehmen mit SAP-basierter ERP-Infrastruktur sowohl seine Sicherheit als auch die Compliance entscheidend verbessern?
Werth: Cyber-Security muss im Unternehmen eine hohe, wenn nicht die höchste Priorität haben und die Rückendeckung der Geschäftsführung sowie des Managements besitzen. Entsprechend der Relevanz sind personelle und finanzielle Ressourcen erforderlich. Mit Hilfe leistungsstarker, automatisierter Tools lassen sich dann schnell kritische Verwundbarkeiten in den SAP-Systemen identifizieren. Auch deren Ausnutzung sowie bedrohliche Aktivitäten können in Echtzeit erkannt und gestoppt werden. Die geschaffene Transparenz der Systemsicherheit dient im Anschluss als Reiseführer auf dem Weg zur besseren Sicherheit und Compliance.

Welche Rolle können hier Künstliche Intelligenz und Maschinelles Lernen heute schon spielen – und wie bewerten Sie die weitere Entwicklung in diesem Bereich?

„Das Know-how des Menschen wird beim Einsatz von KI eventuell durch eine ‚Black-Box‘ ersetzt, deren Kontrolle nicht unproblematisch ist.“
Thomas Werth

Thomas Werth ist Geschäftsführer der Werth IT GmbH, Kamen.

Werth: Die Qualität des Resultats wird hier durch das Training der Maschinen definiert. Insbesondere im Bereich der Log-Analysen existiert bereits viel Erfahrung, und entsprechend kann dies auch schon zur Erkennung von Anomalien genutzt werden. Die Entwicklung der KI ist rasant, doch es ist fraglich, ob die aktuell vorherrschenden Modelle geeignet sind, um die Bewertung der Systemsicherheit fehlerfrei zu leisten. Zudem könnte der Mensch das derzeitig vorhandene Know-how verlieren. Dieses wird beim Einsatz von KI eventuell durch eine „Black-Box“ ersetzt, deren Kontrolle nicht unproblematisch ist.

Herr Werth, vielen Dank für das Interview!

Geheimwaffe gegen Cyberkriminelle

Security Bridge, Hersteller der gleichnamigen Software-Plattform für die Sicherheit von SAP-Anwendungen mit Sitz in Ingolstadt, positioniert sich gemeinsam mit Beratern als „Geheimwaffe“ für eine sichere Zukunft in der Ära der Cyberkriminalität.

CEO Christoph Nagy nennt „Managed Security Services“ durch externe Anbieter angesichts immer ausgefeilterer Cyberangriffe „ein probates Mittel für Unternehmen, ihre IT-Sicherheit zu schützen“. Allerdings seien damit speziell im Bereich der SAP-Security „besondere Herausforderungen“ verbunden – insbesondere wenn es um die Erfüllung von Compliance-Anforderungen geht. Oftmals fehlten interne Ressourcen, um komplexe SAP-Systeme zu überwachen und effektive Sicherheitsmaßnahmen umzusetzen, so dass die Sicherheitsplattform mit der Expertise eines Beratungsunternehmens zu „Managed SAP Security Services“ veredelt werden sollte.

‘www.securitybridge.com