Information und Bildungsarbeit von und für die SAP®-Commun

CYBER DEFENSE FÜR SAP

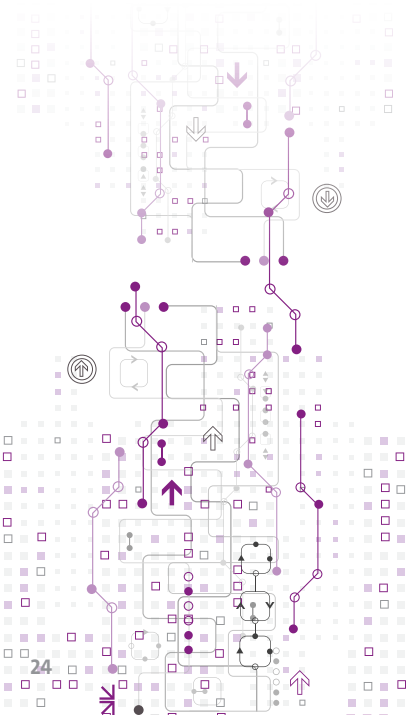
(V. l.) Piyush Pandey, Bodo Kahl und Ralf Kempf von der Pathlock-Gruppe kennen die Angriffs- und Risikoparameter, vor denen sich SAP-Bestandskunden schützen müssen. Es gilt, das gesamte Spektrum von destruktiven Cyberangriffen, Spionage und Einflussnahme zu beherrschen. Wie? Siehe Coverstory. Ab Seite 24

Das Beste aus beiden Welten Seite 18

Kernkompetenz Finance Seite 30

Cyber Defense für SAP und mehr

Die Themen Sicherheit, Zugriff und Abwehr gewinnen in einer heterogenen, mobilen und agilen IT-Landschaft immer mehr an Bedeutung. Lange Zeit stand die Herausforderung Cyber Security im Vordergrund. Das Thema muss jedoch breiter und universeller verstanden werden.



Vor knapp einem Jahr entstand Pathlock als einzigartiger Zusammenschluss international führender Anbieter für Access Governance und Application Security mit dem Ziel, gemeinsam das Verständnis und den Umfang ganzheitlicher Sicherheit auf ein neues Niveau zu heben. Heute ist Pathlock bereits der weltweit führende Security-&-GRC-Spezialist für SAP und hybride IT-Systeme. Mit 500 Mitarbeitern weltweit berät er mehr als 1200 Kunden für den Schutz geschäftskritischer Applikationen, Daten und Prozesse. So unterstützt er Unternehmen mit SAP ERP, S/4 Hana, Cloud oder Multi-Vendor-Systemen bei der Erkennung von Anomalien, Hackerangriffen, Manipulationen oder Datendiebstahl.

Erfahrung und Know-how

Beim Thema Cyber Defense geht es um Sensibilisierung, Erfahrung, Schulung, IT-Werkzeug sowie um viel Know-how. Sind frühere ERP-Generationen sozusagen noch mit Virenscannern aufgewachsen, geht es bei Cyber Defense in den komplexen heutigen Architekturen auch nicht allein um Hacker, sondern um viele, sehr unterschiedliche Angriffsparameter von innen und außen. Bodo Kahl, CEO von Pathlock Deutschland, erklärt im E3-Gespräch die Zielsetzung des Mergers: „Wir haben uns zusammengetan, um die erste umfassende automatisierte Compliance- und Risikomanagementlösung der Branche zu entwickeln. Unsere Technik führt konzertierte Finanz- und Datenschutzkontrollen durch und schützt gleichzeitig alle wichtigen Geschäftsanwendungen vor Bedrohungen der Cybersicherheit. Durch die Kombination jeweils einzigartiger Fähigkeiten können wir unseren Kunden eine Lösung anbieten, die mehr Anwendungen und mehr Arten von Risiken abdeckt als jedes andere Unternehmen zuvor.“ Dieser Cyber-Defense-Ansatz ist in einer atomisierten und agilen IT-Welt von entscheidender Bedeutung, denn der SAP-Bestandskunde hat es mit sehr vielen Bedrohungsszenarien gleichzeitig zu tun. Der Chief-Technology-Officer (CTO) von Pathlock Deutschland, Ralf Kempf, erklärt dazu: „Wir fokussieren uns auf eine breite Lösung, die mehr kann als der klassische Ansatz, der auf dem Markt üblich ist. Es gab bislang Lösungen, die entweder auf den Bereich User und Access Management oder auf den Bereich Cyber Security fokussierten, aber keine, die den Bereich ERP-Security im Allgemeinen umfasst. Also, wir reden hier über eine einheitliche Lösung, die alle namhaften ERP-Anbieter wie SAP, Microsoft und Orac-

V. l. Ralf Kempf, Piyush Pandey und Bodo Kahl von der Pathlock-Gruppe kennen die Angriffs- und Risikoparameter, vor denen sich SAP-Bestandskunden schützen müssen. Es gilt, das gesamte Spektrum von destruktiven Cyberangriffen, Spionage und Einflussnahme zu beherrschen.

le am Markt abdeckt und ebenso Tools wie Salesforce."

Der Zusammenschluss zu Pathlock ergibt ein Leistungsspektrum, das viel tiefer und breiter ist als bekannte Einzellösungen. Es vereinigt sowohl die Möglichkeiten für den Bereich User Identity und Access Management auf der einen Seite als auch im Bereich Cyber Security, Vulnerability Management, Threat Detection und Data Protection auf der anderen. Zu Pathlock gehören neben Sast Solutions die früheren Appsian, Security Weaver, CSI Tools, Xpandion und QSoftware. Gemeinsam verfügt die Gruppe über 15 Standorte in den USA, Europa, Israel und Indien.

In der Praxis hat Pathlock Deutschland eine hohe Affinität zu SAP. ECC- und S/4-Architekturen sind komplex und dezentral. Unmittelbare Mehrwerte erbrachte daher die Zusammenarbeit mit den auf SAP spezialisierten CSI Tools aus Belgien und Security Weaver aus den USA. „Sie bedeutet ein sinnvoll erweitertes SAP-Portfolio – zusätzlich zum Quick Win, dass bei Bedarf sofort ein breites Lösungsangebot für alle ERP-Anwendungen bereitsteht", betont CTO Ralf Kempf im Gespräch mit E3-Chefredakteur Färbinger. „Es ist der große Vorteil dieses Mergers, dass sich nicht allein die Reichweite vervielfacht, sondern ebenso unsere Expertise. Entsprechend teilen wir unsere Cyber-Security-Lösungen für SAP und unsere Partner weltweit und können diese sofort in ihr Portfolio integrieren."

Berechtigungswesen

Ein wesentlicher Security-Parameter ist das Berechtigungswesen für die SAP-Anwender. „Viele unserer Großkunden haben Produkte wie Ariba, die SAP selbst zugekauft, aber nie so richtig in das Portfolio integriert hat. Sie erschwerten es bislang sehr, die Berechtigungen von Mitarbeitenden über alle Applikationen zu tracken und die Accounts zu managen, etwa wenn ein Mitarbeiter austritt", beschreibt Ralf Kempf einen Anwendungsfall aus seiner beruflichen Praxis.

Personalveränderungen waren stets eine große Herausforderung für das Berechtigungswesen: Verlässt eine Person das Unternehmen, sollten auch alle Accounts, alle Geräte gesperrt, alle Berechtigungen weltweit in allen Systemen entzogen werden. „Die Zugriffe in all diesen Subsystemen transparent verwalten, reviewen und so weiter – das konnten wir bislang nur für SAP. Jetzt bieten wir einen systemübergreifenden Überblick über Identitäten und Accounts", beschreibt Ralf Kempf einen der Vorteile des Mergers.

Die SAP-Community hat die Bedeutung und Nachhaltigkeit von Cyber Defense seit geraumer Zeit realisiert. Diese Sensibilisierung belegt auch der Investitionsreport 2023 der Deutschsprachigen SAP-Anwendergruppe (DSAG e. V.). Bei der Investitionsplanung der DSAG-Mitglieder liegt die Cyber Security bei 88 Prozent mit hoher und mittlerer Relevanz klar auf Platz eins. Dies kommt für den DSAG-Vorstandsvorsitzenden Jens Hungershausen nicht unerwartet: „Einem Hackerangriff vorzu-

Mit einer Security-Awareness-Kampagne unterstützt die DSAG ihre Mitglieder, ein Bewusstsein für das Thema und den Umgang mit den Bedrohungen für SAP-Systeme zu erlangen.

Jens Hungershausen, Vorstandsvorsitzender, DSAG e. V.

beugen ist zwar unmöglich. Doch es gibt eine Reihe von Maßnahmen, mit welchen sich Unternehmen und Anwender vorbereiten können." Und hier zeigt sich die Innovationskraft und Effizienz der neuen Pathlock-Gruppe.

Dashboards

Security-Dashboards stehen als zentrales Element zur Kontrolle und Abwehr sicherheitsrelevanter Vorfälle bereits seit Jahren auf der Forderungsliste der DSAG. Gemeinsam mit SAP arbeitete die DSAG an einer entsprechenden Lösung zur Gesamtübersicht für alle Security-Aspekte, die automatisiert anzeigt, welche sicherheitsrelevanten Einstellungen vorgenommen werden müssen und wo Sicherheitslücken in der jeweiligen SAP-Landschaft des Unternehmens vorhanden sind. Nun kann Pathlock, ebenfalls Teilnehmer des DSAG-Arbeitskreises, den Erfolg vermelden: Die Entwicklung der Pathlock-Dashboards ist erfolgreich abgeschlossen und umfasst deutlich mehr als reine SAP-Landschaften. „Denn", so erklärt Piyush Pandey, Pathlock-CEO, im E3-Exklusivgespräch, „die Zeit statischer singulärer ERPs war gestern.

SAP-Lösungen sind nach wie vor wichtigster Bestandteil der Line-of-Business-Infrastruktur vieler Unternehmen, aber die Lösungen anderer Anbieter, insbesondere von Oracle, gewinnen zunehmend an Bedeutung. Beispielsweise verwalten viele unserer SAP-Kundenunternehmen eine oder mehrere Oracle-ERP-Instanzen als Ergebnis von Fusionen und Übernahmen. Die Verwaltung von Zugriffsberechtigungen, einschließlich Rollen, aber auch SoD-Regeln (Segregation of Duties) und andere Aspekte rund um Identität, Zugriff und Sicherheit sind für den Schutz dieser geschäftskritischen Anwendungen unerlässlich."

Hinzu kommt: Viele geschäftskritische Systeme folgen dem Trend, sich in die Cloud zu verlagern, etwa mit Lösungen von SAP wie SuccessFactors oder Ariba. Damit erweitert sich der Anwendungsbereich für zentralisierte Zugriffskontrollen über die traditionellen Abap-Systeme und sogar über SAP hinaus. Die Anforderungen an die Lösungen steigen, entweder durch die Unterstützung einer breiteren Palette von Systemen oder durch die Bereitstellung von geeigneten Integrationspunkten mit anderen Lösungen. Für die erfolgreiche Umsetzung angemessener Kontrollen ist es von entscheidender Bedeutung, dass alle Systeme durch eine wirksame Lösung für das Risikomanagement abgedeckt sind, und zwar für die Verwaltung der Zugriffskontrolle und der SoD-Kontrollen sowie für die Umsetzung einer angemessenen Access Governance.

Dies spiegelt sich auch in der Ankündigung für den diesjährigen Leadership Compass des führenden Technologie-Analysten Kuppinger-Cole wider, in dem eine umfassende Unterstützung sowohl für SAP-Umgebungen als auch für die Geschäftsanwendungen anderer Anbieter im Mittelpunkt steht: „Die Anforderungen der Kunden an Zugangskontrolllösungen für ihre Geschäftsanwendungen ändern sich rapide. Viele Unternehmen benötigen Lösungen, die eine Reihe ERPs verschiedener Anbieter abdecken und in unterschiedlichen Modellen betrieben werden."

Rollenmodelle

Allerdings fehle vielen Anbietern noch die langjährige Erfahrung mit Best-Practice-Rollenmodellen, kritischen Zugriffsregelsätzen und SoD-Rollensätzen für Nicht-SAP-Lösungen, konstatierte Martin Kuppinger bereits 2022 und hebt als Ausnahmebeispiel Pathlocks tiefgreifende Unterstützung für Oracle-Systeme hervor. Er betont, durch den Pathlock-Zusammenschluss sei „ein großer Konkurrent für SAP auf dem Security-Markt entstanden". Ralf Kempf kommentiert: „Dieses Urteil nehmen wir als Kompliment und Bestätigung, aber vor allem als Ansporn, der Entwicklung immer einen Schritt voraus zu sein und mit unserer Pathlock Suite, sei es on-premises, webbasiert oder hybrid, für SAP und viele weitere ERPs und Lösungen die umfänglichste und beste Cyber Defense zu realisieren." (pmf)

pathlock.com/de

SAP Security der nächsten Generation

Dashboards für Entscheider

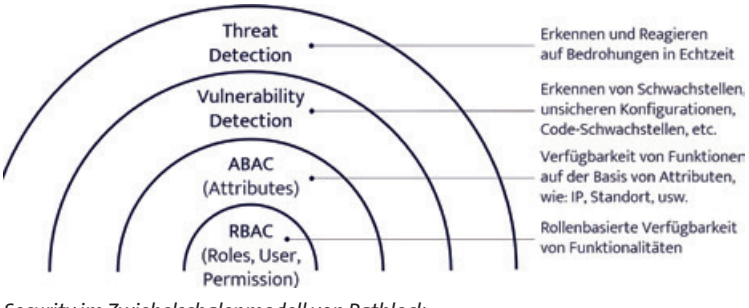
Alljährlich erneuert der DSAG-Arbeitskreis Vulnerability Management seine Forderung an SAP nach einem Security Dashboard. Angesichts der Bedrohungslage kommen die neuen Dashboards von Pathlock zur rechten Zeit.

Von Clemens Gütter und Raphael Kelbert, Pathlock Deutschland

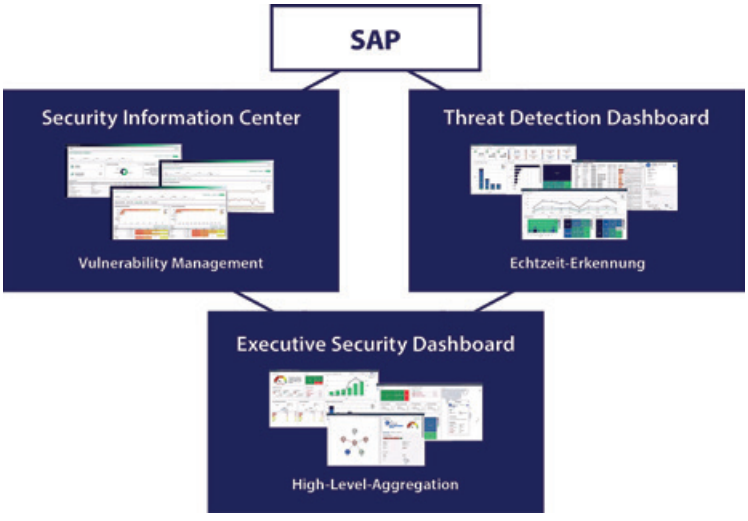
Für immer mehr Unternehmen ist der ganzheitliche Überblick über die aktuelle Risikosituation und die Informationsdarstellung eine zunehmende Herausforderung. Benötigt werden Management-Views auf die aktuelle Risikolage und deren Änderungen im zeitlichen Verlauf ebenso wie detaillierte Arbeitslisten und Hilfestellungen für anschließende Maßnahmen. Piyush Pandey, CEO von Pathlock, betont, wie entscheidend es ist, dass CISOs und IT-Abteilungen über die richtigen Informationen verfügen, die sie dem CEO oder Vorstand vorlegen: „Nur wenn die CEOs die Bedrohungslage und die finanziellen und geschäftlichen Folgen von Sicherheitsverstößen verstehen, können die Geschäftsbereiche auch das für sie erforderliche Budget erhalten."

Dies erfordert, dass im Vorfeld in Kontrollmaßnahmen investiert wird, etwa zur Erkennung von Bedrohungen in Echtzeit. „Durch proaktive Analysen sind selbst Unternehmen mit geringeren Budgets in der Lage, ihre größten Risiken zu identifizieren, sodass sie Investitionen und Maßnahmen zur Mängelbeseitigung nach Prioritäten ordnen können. Einen entscheidenden Vorteil bieten hier Executive Dashboards", erklärt er. Der Fokus liegt dabei auf der ganzheitlichen Betrachtung regelmäßiger, punktueller Parameterprüfungen in Kombination mit Threat Detection in Echtzeit.

Zunächst eine Verortung der Dashboards im Zwiebelschalenmodell: Ein gutes Rollenkonzept zur Bereitstellung von Funktionalitäten ist Kern eines sauberen SAP-Systems. Darauf aufbauend lässt sich als weitere Sicherheitsbarriere die Verfügbarkeit von Funktionalitäten attributbasiert aussteuern, etwa über die IP-Adresse oder die Uhrzeit des Zugriffs. Erlaubt zum Beispiel das Rollenkonzept zwar einen Zugriff des Users auf technische Zeichnungen, wird dieser bei Zugriff außerhalb der üblichen Arbeitszeit dyna-



Security im Zwiebelschalenmodell von Pathlock



SAP Security Dashboards – maßgeschneidert auf User-Bedürfnisse.

misch blockiert. Als weitere Schalen fungieren das Vulnerability Management, bei dem es um die zyklische Erkennung von Schwachstellen geht, und schließlich die Threat Detection zur Bedrohungserkennung in Echtzeit. Die Pathlock Dashboards sind in diesen äußeren Schalen angesiedelt und stellen deren Informationen zur Sicherheitsabwägung und Transparenz sinnvoll dar.

Dashboard-Strategie

Wie sieht nun eine Strategie aus, um den IT-Bereich SAP zu monitoren und dort mit Dashboards zu reagieren? Dafür gibt es auf der einen Seite das Security Information Center, um das Vulnerability Management, also die zyklische Überwachung, grafisch und visuell dar- und bereitzustellen. Dem gegenüber steht das Threat Detection Dashboard, mit dem alle Erkenntnisse aus dem Bereich Echtzeiterkennung gesammelt und visualisiert werden. Nachgelagert werden die wesentlichen Punkte beider Bereiche zusammengefasst und aggregiert auf Managementebene im Executive Dashboard bereitgestellt, um für Entscheider einen Überblick über den gesamtheitlichen Sicherheitskontext zu erhalten.

Information Center

Das Security Information Center beinhaltet unser Vulnerability Management. Grundsätzlich ist dem voranzustellen, dass für dieses eine softwaregesteuerte Unterstützung notwendig ist, weil es faktisch nicht machbar ist, alles per Hand zu überprüfen. In diesem Fall ist dies das Pathlock Risk and Compliance Management, mit dem zyklische Prüfungen laufen, sogenannte Auditprüfungen, die verschiedenste Bereiche des Schwachstellen-Managements abdecken. Und mit dem Security Information Center lässt sich auf einen Blick sehen, was diese Auswertungen ergeben haben. Zum Beispiel, ob es irgendwelche fehlenden OSS Notes, kritische Konfigurationen oder Lücken in der Überwachung einer SAP-Landschaft gibt. Ergebnisse von Auditausführungen im Zeitverlauf lassen sich als Trend darstellen, um kritische Änderungen der Sicherheitssituation unmittelbar zu identifizieren.

Prinzipiell gibt es die Möglichkeit, beliebig viele Auditpläne einzusteuern, auch für mehrere Systeme und mit frei wählbaren Zeitplänen. Überprüfungen, etwa ob alle OSS Notes up to date sind, können somit wöchentlich oder gar täglich laufen, wenn es um Systeme geht, die einen sehr hohen Sicherheitsstandard haben. Oder man richtet eine große allgemeine Prüfung über alle Systeme ein Mal im Monat ein, je nach eigenem Use Case. Und daraus können sich dann verschiedene Darstellungen ergeben, die man jeweils einzeln oder aggregiert überblicken kann.

Threat Detection

Das Threat Detection Dashboard basiert im Wesentlichen auf einer Sammlung verschiedener Datenquellen, wo Logeinträge geschrieben werden und Korrelationen innerhalb dieser Datenquellen zu erkennen und auszuwerten sind. Das Dashboard dient zunächst dazu, den Zustand der Datensammlung festzustellen: Laufen die Datenkollektoren in den Intervallen, wie sie laufen sollen, senden sie entsprechend Daten und finden sie alle Datenquellen für jedes System? So ergibt sich auf einen Blick, ob die Datenbeschaffung fehlerfrei funktioniert. Dann bietet das Dashboard verschiedene Aggregationen an, um Events zu clustern. Man kann Filter etwa auf einzelne Eventbereiche anlegen, um auf eine bestimmte Systemgruppe oder einen einzelnen Mandanten zu schauen. Verschiedene Datenquellen lassen sich in Bezug auf einzelne User dediziert ansehen, man kann Filter für Critical Access Events hinterlegen, aber auch einen Überblick über das Gesamtdatenaufkommen darstellen: Aus welchen Quellen kommen Daten, von welchen Usern werden sie erzeugt? Wie ist die Kritikalität und Verteilung bezüglich produktiver Development- und Testsysteme, aber auch entsprechend des Schweregrads? Was sind kritische Daten, wie viele kritische Events passierten auf welchen Systemen? Von dort lässt sich direkt in

Threat Detection Dashboard – alles im Blick durch hochgradig individualisierbare Ansichten.

den Eventmonitor des Dashboards abspringen, um detaillierte Loginformationen zu erhalten, korrelative Analysen vorzunehmen und Zusammenhänge zwischen einzelnen Events und Logeinträgen festzustellen. Als weitere Option steht Nutzern des Threat Detection Dashboards die Trendansicht zur Verfügung. Sie zeigt die Verteilung von Events nach Herkunft, Benutzern und anderen Kategorien über einen Zeitraum. Dabei lassen sich weitreichende Individualisierungen in der Darstellung umsetzen, mit allein acht verschiedenen Diagrammen zur Auswahl ist das Threat Detection Board hochgradig auf die User-Bedürfnisse anpassbar.

Drei Dashboards

So bedient das Security Information Center die Security-Administration im weitesten Sinne, also jeden, der sich mit Audits bzw. der Konfigurationsüberwachung befasst, aber auch zum Beispiel den CISO, der sich ansieht, wie sich Probleme im Verlauf entwickelt haben und ob Audits erfüllt sind. Beim Threat Detection Dashboard sind es eher Security-Analysten, die hier arbeiten und zum Beispiel den Eventmonitor benutzen, mitunter auch Security-Entscheider, die detailliertere Informationen benötigen oder einen bestimmten Trend verfolgen. Mit dem neuen Release von Pathlock kommt nun ein weiteres Level, das Executive Dashboard, hinzu, um die Daten aus der Threat Detection und dem Vulnerability Management zu aggregieren und auf einen Blick darzustellen.

Executive Level

Die wichtigsten Informationen finden sich sofort beim Dashboard-Einstieg: Ist eine Landschaft gefährdet? Wie problematisch ist es? Wie sieht die Systemlandschaft insgesamt aus und wurden Compliance-Kriterien eingehalten? Daneben finden sich verschiedene Trendinformationen: Wie entwickeln sich die Schwachstellen in Bezug auf die Bedrohungen und gibt es da eine Korrelation? Falls ein Aspekt tiefergehend betrachtet werden soll, sind immer auch verschiedene Follow-up-Informationen mit Detailansichten gegeben, etwa zum Patch Level – also spezifischere Informationen, die vielleicht nicht für den CEO, aber für den CIO oder den Infrastrukturmanager interessant sind. Das Executive Security Dashboard bietet zudem Visualisierungen zum Monitoring-Netzwerk: Wie sind die Verbindungen vom zentralen System zu den Managed Systems? Gibt es Verbindungen, die momentan nicht funktionstüchtig sind? Diese sind dann durch eine rote Linie gekennzeichnet, wobei das konkrete Finding nicht genau spezifiziert wird, denn ein Entscheider muss nicht bis ins kleinste Detail informiert sein. Er erhält stattdessen High-Level-Informationen: Gibt es ein Problem und wie gravierend ist es? Wer ist der Ansprechpartner für dieses System, wen muss ich kontaktieren, damit die Problemlösung in Gang gesetzt wird? Mit dem neuen Executive Security Dashboard können Verantwortliche also künftig mit geringstmöglichem Aufwand bestmöglich informierte und fundierte Entscheidungen treffen und deren Umsetzung unmittelbar in die Wege leiten.