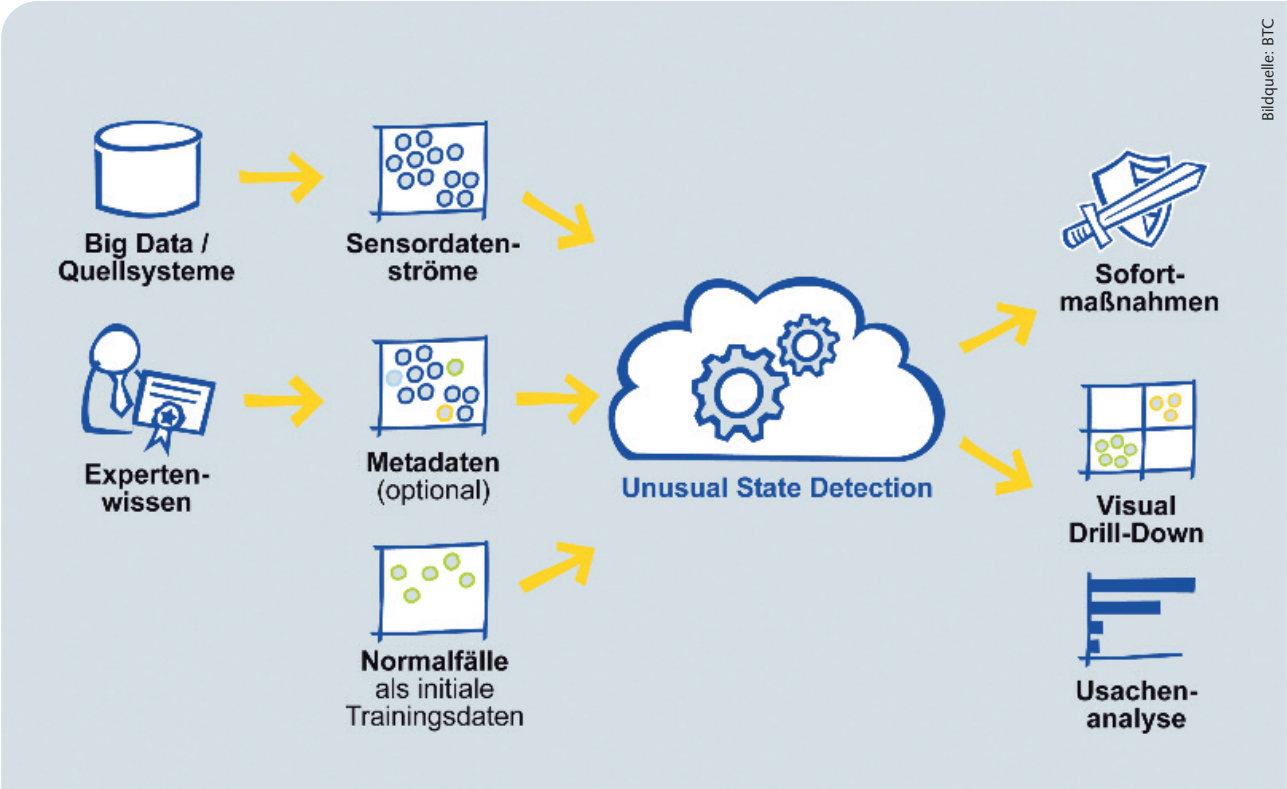
Handeln – bevor Kriminelle angreifen

Die zunehmende Vernetzung aufgrund der Digitalisierung macht IT-Infrastrukturen verwundbarer. SAP-Umgebungen bilden hier keine Ausnahme. Denn die zunehmende Komplexität durch das Zusammenspiel von immer mehr SAP-Komponenten erhöhen das Gefährdungspotenzial. Mittels geeigneter technischer und organisatorischer Maßnahmen lässt sich gegensteuern. Verfahren wie Penetrationstest, „Unusual State Detection" und SAP Enterprise Threat Detection unterstützen dabei, Sicherheitslücken und Angriffe frühzeitig zu identifizieren.



Ständige und automatisierte Beobachtung des SAP-Systems mit einem Unusual-State-Detection-System.

*Von Christian Bruns**

Sechs Milliarden Dollar – auf diese Summe werden binnen drei Jahren laut einer von Cybersecurity Ventures jüngst veröffentlichten Studie die weltweiten Schäden durch Hackerangriffe und Internetkriminalität klettern. Ende Juli warnte das US-amerikanische Heimatministerium explizit, dass Cyberkriminelle SAPs und Oracles ERP-Software ins Visier genommen hätten. In den Untersuchungen von Digital Shadows und Onapsis, die der Warnung zugrunde liegen, wird von mehr als 9000 Sicherheitslücken berichtet. Dass in den vergangenen Jahren in einschlägigen Hackerforen im Dark Web der Austausch über ERP-spezifische Exploits und Verwundbarkeit enorm anzog, wird daher niemanden überraschen. Mit regelmäßigen Security Patches mühen sich die Anbieter gegenzusteuern. Erst im Juli veröffentlichte SAP beispielsweise elf sicherheitsrelevante Updates, wovon eines ein besonders kritisches Loch beim Business Client im Webbrowser stopfte. Das wachsende Interesse an ERP-Hacks ist eine unliebsame Begleiterscheinung der digitalen Transformation und globalen Erreichbarkeit über das Internet, da sich die prinzipielle Angriffsfläche rapide vergrößert. Suchmaschinen wie shodan.io erleichtern dabei den Hackern die Arbeit. Eine Anfrage nach SAP NetWeaver AS Java listet beispielsweise für Ende Juli Angaben zu weltweit 2486 Systemen einschließlich Versionsdaten auf. Mit dem Wissen zu bekannten Schwachstellen aufgrund der veröffentlichten Sicherheitsupdates lassen sich so problemlos Systeme identifizieren, die aufgrund eines überholten

Christian Bruns ist Management Consultant Information Security bei der BTC AG.

Release-Standes anfällig für potenzielle Angriffe sind.

Vollständiges Lagebild der Sicherheit fehlt

Bedauerlicherweise sind oftmals die offenen Flanken in der SAP-Landschaft hausgemacht, da in Unternehmen trotz steigendem Sicherheitsbewusstsein oftmals ein vollständiges Lagebild zur Sicherheit fehlt. Andererseits wächst das Leistungsvermögen der verfügbaren Schutzmechanismen, um sich gegen die steigenden Risiken zu behaupten, aber auch Compliance-Anforderungen zu erfüllen. Mit externer Unterstützung lassen sich geeignete technische und organisatorische Maßnahmen für einen passenden Schutzschirm der SAP-Systeme im Unternehmen auswählen.

Basis eines ganzheitlichen, auf die individuellen Belange eines Unternehmens abgestimmten Schutzkonzepts ist ein Sicherheitsprozess, der im Wesentlichen von den drei Handlungsfeldern Prävention (Vorsorgen), Monitoring (Erkennen von Risiken und Verletzungen) und Störungsmanagement (Abwehren, Reagieren) gebildet wird. Eingebettet ist alles in einen kontinuierlichen Verbesserungsprozess, um das Sicherheitsniveau stetig zu verbessern. Damit ein Eindruck des Sicherheitsniveaus der SAP-Systemlandschaft gewonnen werden kann, steht zu Beginn eine Prüfung sicherheitsrelevanter Aspekte auf allen Ebenen an. Wertvolle Unterstützung an dieser Stelle liefert ein Prüfwerkzeug wie der werthAUDITOR, den BTC häufig im Rahmen von Security Audits nutzt. Ohne zusätzliche Komponenten auf den zu prüfenden SAP-Systemen ausbringen zu müssen, liefert das Werkzeug vollumfassend Informationen zum Sicherheitsstand des SAP-Systems. Anschließend werden diese durch die Sicherheitsexperten bewertet und zu Lagebildern aufbereitet.

Sicherheitschecks und Penetrationstests

In den Berichten werden kritische Berechtigungen und Rechtekombinationen aufgezeigt oder die Sicherheit der SAP-Schnittstellen geprüft. Es werden Konfiguration und Systemhärtung wie Profilparameter für die Passwortrichtlinien als auch der Stand der Sicherheitsupdates getestet. Ebenso lassen sich Quellcode-Analysen automatisiert durchführen. Mit Blick auf Prüfung der DSGVO-Compliance von SAP-Systemen setzt der werthAUDITOR außerdem den entsprechenden Kontrollrahmen um, der zusammen mit dem BSI und der Allianz für Cybersicherheit entwickelt wurde. Unter anderem werden hier im Rahmen des Tests zum Minimalprinzip die tatsächlich genutzten TCODEs für den Zugriff auf ERP-Funktionen und Reports mit den tatsächlich vergebenen Berechtigungen abgeglichen. Als Ergebnis sieht der Auditor, welches Programm den Zugriff effektiv benötigt.

Neben dem auf ein bestimmtes System oder eine Systemlandschaft fokussierten Sicherheitscheck stellt die Durchführung von Penetrationstest ein geeignetes Verfahren dar, um sich insbesondere in Umgebungen mit hohem Schutzbedarf ein Lagebild zur Wirksamkeit der eigenen technischen und organisatorischen Sicherheitsmaßnahmen zu verschaffen. Dazu werden das Vorgehen und die Technik krimineller Hacker nachgeahmt, um in kritischen Bereichen Sicherheitslücken aufzuspüren, bevor diese tatsächlich zu böswilligen Angriffen führen können.

Die Auswertung der Ergebnisse der in den Unternehmen durchgeführten Sicherheitschecks zeigen, dass es oft kleinere technische und organisatorische Schwächen sind, die den kriminellen Hackern die Arbeit erleichtern. Zu den häufig anzutreffenden Unzulänglichkeiten zählen beispielsweise, dass Rollen und Zuständigkeiten für Prozesse und Systeme unter Sicherheitsaspekten nicht sauber definiert sind und keine zentrale Verantwortung institutionalisiert ist. Einmal vergebene Berechtigungen und Gruppenkennungen werden bei Stellen- oder Aufgabenwechseln nicht gelöscht oder geändert. Eine Konsequenz: Auszubildende oder Trainees, die unterschiedliche Abteilungen durchlaufen, verfügen über die meisten Zugriffsrechte. Die wachsende Komplexität von SAP-Infrastrukturen führt dazu, dass gehärtete Konfigurationen oder das Einspielen von Updates nicht an jeder Stelle konsequent durchgeführt werden. Auch werden unternehmenskritische SAP-Produktionssysteme häufig mit weniger wichtigen Büro-Servern in einem gemeinsamen Netzwerkabschnitt betrieben.

24x7-Betrieb erlaubt keine Wartung

Anhand der Analyseergebnisse erfolgt eine Bewertung und Priorisierung der identifizierten Sicherheitslücken, die sich am Schutzbedarf der zu schützenden Systeme und den darauf aufbauenden Geschäftsprozessen orientieren. Im Anschluss können die kritischsten Schwachstellen systematisch und ressourcenschonend behoben werden.

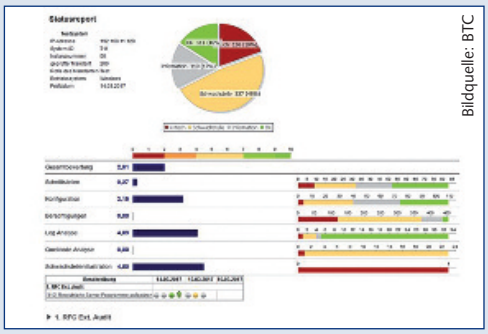
Denn mitunter sind es betriebliche oder sachliche Gegebenheiten, die dem Beseitigen einer registrierten Verwundbarkeit im Wege stehen. Der Klassiker in dieser Hinsicht ist ein 24x7-Produktivbetrieb, der kein Wartungsfenster für die unterstützenden ERP-Systeme vorsieht und mit Blick auf die kaufmännischen Nachteile einer Produktionsunterbrechung in absehbarer Zeit auch keines vorsehen wird. Vergleichbar verhält es sich, wenn im Rahmen von Customizing ein SAP-Account zum Zugriff auf weiterführende Funktionen herangezogen wird. Hierdurch wird die Sicherheitsarchitektur ausgehebelt, da damit der Weg für sicherheitskritische Aktivitäten wie Log-File-Änderungen frei ist. Dennoch wird der Einsatz toleriert, da niemand den durch die Systemanpassung generierten, hohen Prozessgewinn missen möchte und keine alternative Implementierungsoption in Sicht ist.

In diesen Fällen müssen Unternehmen eine Risikoabwägung vornehmen und gleichzeitig korrespondierende Sicherheitsmaßnahmen einleiten, um das Gefährdungspotenzial möglichst gering zu halten. Eine Maßnahme könnte lauten, Administrationsrechte nur noch mit temporärer Gültigkeit von wenigen Stunden zu vergeben. Eine andere adressiert die Einführung weiterer Werkzeuge, die das Geschehen in SAP-Umgebungen nach verdächtigen Aktivitäten oder anderen Auffälligkeiten analysieren. SAP Enterprise Threat Detection dient beispielsweise der annähernden Echtzeitanalyse und -auswertung von Protokollinformationen angeschlossener SAP- sowie Non-SAP-Systeme. Die Daten werden zentral gesammelt und aufbereitet, um im Anschluss auf Basis einer HANA-Datenbank regelbasiert mit bekannten Angriffsmustern abgeglichen zu werden. Ein Pluspunkt gegenüber gängigen Security-Information- und Event-Management-Produkten ist, dass SAP Enterprise Threat Detection das interne Geschehen in den Systemen analysiert und die Auswirkungen versteht.

Automatisierte Analyse der Datenströme

Potenzielle Einsatzfelder liegen im Identitätsmanagement, wenn es beispielsweise den Hinweis auf einen Identitätsdiebstahl gibt, sobald sich ein Nutzer von verschiedenen Orten anmeldet. Ungewöhnlich häufige und umfangreiche Übertragungen durch Nutzer deuten auf

Es gibt keine 100 Prozent Sicherheit



Bildquelle: BTC

Einen 100-prozentigen Schutz gegen Cyberattacken kann und wird es in der IT nie geben. Mithilfe der Implementierung geeigneter technischer und – in der Regel noch entscheidender – organisatorischer Maßnahmen lässt sich das Risiko jedoch deutlich eingrenzen. Die Voraussetzung hierzu ist der Aufbau eines ganzheitlichen Sicherheitskonzepts, das auf die individuellen Gegebenheiten eines Unternehmens abgestimmt ist. Werkzeuge und Verfahren erlauben, den zugehörigen Prozess systematisch und ressourcenschonend umzusetzen. Und zwar von der Analyse des aktuellen Sicherheitsstatus über eine am Wertbeitrag orientierte Behebung von Sicherheitslücken bis hin zu einem lernfähigen Frühwarnsystem. Damit Unternehmen für Attacken gewappnet sind helfen höhere Transparenz und lückenlose Dokumentation.

eine unberechtigte Kopie sensibler Unternehmensdaten hin. Auch zur Reduzierung des Risikos von fehlenden Security-Patches lässt sich das Werkzeug heranziehen, da beim Zugriff auf als unsicher eingestufte Funktionen jedes Mal ein Alarm erfolgen kann.

Regelbasierte Verfahren wie SAP Enterprise Threat Detection basieren auf bekannten Bedrohungen und Angriffsarten, um Datenströme auf stattfindende Angriffe hin zu untersuchen. Entwicklungen wie die BTC Unusual State Detection gehen noch einen Schritt weiter. Sie sind in der Lage, mithilfe von Machine Learning selbst unbekannte Attacken in den Daten zu erkennen. Auf Basis aufgezeichneter Datenströme wird der Normalzustand der zu überwachenden Prozesse und Systeme gelernt.

Das Verfahren ermöglicht dann die automatisierte Analyse aller im regulären Betrieb anfallenden Datenpunkte in Echtzeit. Bei Abweichungen vom gelernten Normalverhalten erfolgt eine Alarmierung und es wird eine visuelle Darstellung des Datenstroms erzeugt, in der die Anomalie intuitiv untersucht werden kann.

Im Zusammenspiel mit dem Nutzer lernt die Unusual State Detection dabei mit, verbessert sich auf diese Weise selbst kontinuierlich und kann sich auf neue Situationen einstellen. Als Einsatzgebiet für ein solches System bietet sich die Erkennung von Angriffen auf komplexe und verteilte IT-Landschaften an. Es lassen sich damit Netzwerkverkehr, Log-Daten, Nutzeraktionen und Systemverhalten in Echtzeit analysieren und bei Auffälligkeiten sofort geeignete Gegenmaßnahmen – oder ergänzende Untersuchungen mithilfe der genannten SAP-bezogenen Sicherheitswerkzeuge – vornehmen. *(cr)* @