SAP Enterprise Threat Detection (ETD)

Wie eine gute Versicherung

Das Thema Security ist so alt wie die Geschichte der IT. Mittlerweile werden die Attacken und Angriffe immer ausgefeilter und durchdachter – unabhängig davon, ob Stadtverwaltungen, Krankenhäuser, Automobilzulieferer oder Lottogesellschaften die Opfer sind. Auf Seiten der Security-Lösungsanbieter sind ebenfalls viele Expert:innen mit Leidenschaft und Know-how bei der Sache, um Systeme und Anwender:innen zu schützen. Eine davon ist Jessica Rod, SAP Security Consultant bei der OEDIV Oetker Daten- und Informationsverarbeitung KG.

Sarah Meixner, blaupause-Redaktion

Lassen wir die Frage nach dem „Wie?" hinter uns, die nach dem „Wann?" ebenfalls. Fakt ist, jeden Tag werden Hunderte, wenn nicht gar Tausende Unternehmen von Cyber-Kriminellen angegriffen – mal mehr, mal weniger erfolgreich. Um dem Problem auf der technologischen Seite Herr zu werden, existieren die unterschiedlichsten Lösungen. Und kein „Funfact", sondern eher ein „Sadfact": Genau diese Lösungen setzen die wenigsten Unternehmen tatsächlich ein. Sei es aus Ressourcen- oder Zeitmangel, oder weil man sich für unverletzbar hält: Tür und Tor sind oft weit geöffnet für Cyber-Kriminelle.

Aktuelle Situation begünstigt Attacken

Vor allem der überall herrschende Fachkräftemangel lässt die Herzen der Cyber-Gangster :innen höherschlagen. Warum das so ist, erklärt Jessica Rod, Security-Expertin bei OEDIV: „SAP-Expert:innen sind Mangelware, solche mit Security-Hintergrund sowieso. Den Hacker:innen ist das natürlich herzlich egal, ob ein Unternehmen gerade kein Personal oder kein Geld für den Cyber-Schutz hat. Wer seine Systeme und Anwendungen schützen will und vor allem auch regulatorische Anforderungen wie die EU-Sicherheitsrichtlinie EU NIS2 (siehe Glossar Seite 54) umsetzen muss, sollte sich noch heute mit Lösungen wie z. B. SAP Enterprise Threat Detection (ETD; siehe Glossar Seite 54) beschäftigen."

OEDIV – Oetker Daten- und Informationsverarbeitung KG

Vom **Hosting** über **Managed Services** bis hin zur **IT-Beratung**: Der zertifizierte SAP- sowie Google-Cloud- und Microsoft-Partner übernimmt mit über **400 Mitarbeitenden** an acht Standorten die technische Expertise in diesen IT-Themen.

oediv.de

Vorbereitung ist alles

Kommt es zu einer Attacke, entstehen unter Umständen immense Schäden und zusätzliche Kosten für Unternehmen. „Das will niemand erleben, und dennoch: Wenn ich bei Vorträgen oder Events frage, ob Unternehmen hierfür aufgestellt sind, gehen einige Hände hoch. Frage ich konkreter nach, sind am Ende

Nutzen von SAP ETD

- Detektions-Werkzeug, um verbundene Unternehmenssysteme und Applikationen zu überwachen
- Direkte Integration im SAP-Umfeld mit minimalem Aufwand
- Schafft Transparenz in Bezug auf verdächtiges (Benutzer:innen-) Verhalten und Anomalien
- Erkennt Sicherheitsverstöße in Echtzeit, gibt sofort Meldung an das SOC weiter
- Nutzt hocheffiziente und automatisierte Prozesse auf Basis der HANA-Technologie
- Mögliche Beweisführung auf Basis der Log-Daten in ETD
- Automatisierte Use-Case-Erweiterung durch SAP-Alerts und Input des Bundesamts für Sicherheit in der Informationstechnik (BSI)
- User:innen im ETD werden immer pseudonymisiert

vielleicht noch zehn Hände oben. Das sind dann die Unternehmen, die wirklich gut vorbereitet sind", berichtet Jessica Rod.

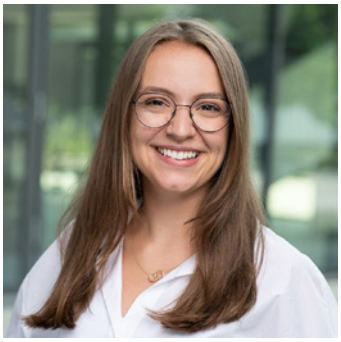
Mögliche Gründe für die Versäumnisse sieht sie zum einen darin, dass in der Presse selten ausführlich über Vorkommnisse wie interne Bedrohungsszenarien („Insider-Threats") berichtet wird. Zum anderen wollen sich nur wenige Unternehmen eingestehen, dass ein großer „Feind" auch von innen kommen kann: der oder die eigene Mitarbeitende. „Hier setzen wir bei OEDIV an. Wir nehmen den Kunden mit unserem ETD-Service genau diese Überwachungsarbeit ab. Und wir rufen nachts wirklich nur an, wenn tatsächlich eine Entscheidung getroffen werden muss, was bisher wirklich nur einige wenige Male pro Kunde passiert ist", sagt die Security-Spezialistin. Sie ergänzt: „Wir sind wie eine gute Versicherung: Solange man nichts von uns hört, sind alle glücklich. Es gibt vieles, was wir als Provider direkt erledigen können: User:innen sperren, Sessions blocken, Transparenz erzeugen, um auffälliges Verhalten von der ersten Sekunde an identifizieren und im Blick behalten zu können."

Alarmanlage mit Auswirkungen

Während man von den einen – hier den OEDIV-Security-Spezialist:innen – nichts hört, sieht man die anderen meist gar nicht: „Angreifer:innen sind oftmals schon um die 300 Tage unerkannt im System unterwegs, bevor der richtig große Angriff stattfindet[1]. Sie laden Informationen herunter, verschaffen sich höhere Berechtigungen, manipulieren Daten", erklärt Jessica Rod und empfiehlt: „Es lohnt sich immer, rechtzeitig in den Schutz der Systeme mit funktionierenden ‚Alarmanlagen' zu investieren. Mit SAP ETD können mit auf Kundenbedarfe individuell zugeschnittene Use-Cases angeboten werden, wie z. B. kritische Reports, Tabellen und User des Kunden, und treten nicht erst auf den Plan, wenn die Monitore schwarz werden."

ETD in der Praxis

Entscheidet sich ein Unternehmen für den Einsatz von ETD, startet das Projekt mit einem Security-Workshop, der die Ist-Situation beleuchtet. Nach dem Customizing beginnt der Betrieb – meist mit einer sogenannten Hypercare-Phase. Monitoring, Analyse und Gegenmaßnahmen liegen dann in den Händen der verantwortlichen Expert:innen. „In der Hypercare-Phase hatten wir auch schon Fälle, wo über das Wochenende bis zu 400 Meldungen eingegangen sind", berichtet Jessica Rod. „Hier ist dann Fingerspitzengefühl gefragt, und die Meldungen müssen individuell betrachtet werden, denn SAP gibt nur Empfehlungen. Wenn wir aber noch einmal genauer hingucken, entdecken wir oft →



„Wir sind wie eine gute Versicherung: Solange man nichts von uns hört, sind alle glücklich."

Jessica Rod, SAP Security Consultant bei der OEDIV Oetker Daten- und Informationsverarbeitung KG

Arbeitskreis Security & Vulnerability Management

- Identity- und Access-Management (On-Premises und Cloud)
- Berechtigungen und Berechtigungskonzepte
- Basissicherheit und Systemparametrisierung
- Security-Vulnerability-Management
- Sicherheit im NetWeaver/JAVA-Umfeld
- SAP Security Notes
- Durchführung von Sicherheitsprüfungen
- Informations-Sicherheits-Management-Systeme im SAP-Umfeld
- Sichere Prozesse in SAP-Umgebungen
- Security-Surveys

dsagnet.de/gremium/security-vulnerability-management

[1] *Vortrag SAP: SAP Enterprise Threat Detection cloud edition – The cloud-based managed cyber security service*

Mit SAP ETD erkennen, analysieren und neutralisieren Anwender:innen Angriffe in ihren SAP-Systemen, bevor es zu schwerwiegenden und kostenintensiven Schäden kommt.

Was sich Unternehmen heute fragen sollten:

- Welche konkreten Forderungen stellen neue Vorgaben wie bspw. NIS2 seitens der Gesetzgebung?
- Ab wann gelten sie für wen?
- Ist meine Industrie, meine Branche betroffen? Und falls ja, welche Segmente?
- Wie lassen sich systematisch die nötigen Voraussetzungen und Methoden implementieren – auch hinsichtlich Compliance?
- Wie und wann den Betriebsrat miteinbeziehen, da in einem Security-Information-and-Event-Management (SIEM)-System User:innen-Daten analysiert werden?

Prozesse, die beim Kunden ganz normal sind, wie z. B. die Aktivitäten eines/r User:in über zwei Clients. In diesem konkreten Fall erfolgte die eine Aktivität über den WebDispatcher, die andere wie gewohnt über den lokalen Client. Hat man das erst einmal erkannt und entsprechend eingestellt – Stichwort Ausnahmeliste –, sind die Meldungen im niedrigen zweitstelligen Bereich angesiedelt und werden zeitnah bearbeitet."

Glossar

EU-Sicherheitsrichtlinie NIS2-Direktive (EU 2022/2555)

Die neue Direktive „Network and Information Security 2" der Europäischen Union (EU) schafft Sicherheitsanforderungen für produzierende Unternehmen. Bei Nichteinhaltung drohen Strafen von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Umsatzes. Erstmals ist neben der kritischen Infrastruktur auch die Industrie im Fokus neuer Vorgaben für Cyber-Sicherheit-Sektoren wie Chemie, Ernährung und Industrie sowie Maschinenbau, Transport, Auto und Elektrik sind direkt von der Direktive betroffen, die weiter als ihre Vorgänger NIS und KRITIS geht. Bis Oktober 2024 muss die EU-Richtlinie in nationales Recht umgesetzt sein.

SAP Enterprise Threat Detection (ETD)

ETD soll Unternehmen dabei unterstützen, Cyber-Angriffe auf die interne Infrastruktur zu verhindern. Das Monitoring-Werkzeug überwacht dafür Unternehmenssysteme und -anwendungen in Echtzeit und basiert im Gegensatz zu SAP Enterprise Resource Planning Central Component (ERP ECC) auf der neuen HANA-Datenbank, was wiederum die Echtzeitverarbeitung von Daten aus allen angeschlossenen SAP-Systemen ermöglicht. ETD soll die Betriebssicherheit erhöhen, indem bekannte Angriffsmuster erkannt und sofort an vordefinierte Stellen weitergeleitet werden. Auch Logs und Protokolle können datenschutzkonform abgespeichert und ausgewertet werden. ETD wird oft im Zusammenhang mit SIEM-Produkten (Security-Information-and-Event-Management) genutzt, die viele Unternehmen für die Angriffserkennung auf ihren IT-Systemen einsetzen.

Ein Center voller Profis

Ein Vorteil des von Jessica Rod mitentwickelten ETD-Offering ist das zugrunde liegende Security Operation Center (SOC). „Dessen Vorzüge sind schnell erklärt: Die Büchse der Pandora zu öffnen, bringt wenig, wenn sich niemand um die Meldungen kümmert", erklärt sie. Über 20 Mitarbeitende sorgen in Bielefeld dafür, dass der 24/7-Support zuverlässig ausgeführt wird. Im Notfall wird natürlich zuerst der Customer-first-Contact informiert, der vertraglich festgelegte Kundenkontakt, der vorrangig über das aktuelle Geschehen in Kenntnis gesetzt werden soll. Über 100 Use-Cases existieren bereits in einer On-Premises-Version, und deren Anzahl wächst stetig weiter. „Sei es, wenn sich ein:e User:in von zwei unterschiedlichen Terminal-Clients anmeldet oder das Passwort vom Standard-User verändert wird: Wir haben solche Aktionen ganz genau im Blick und reagieren unverzüglich mit Gegenmaßnahmen", sagt Jessica Rod.

Live ist der ETD-Service bei OEDIV seit März 2023, die Entwicklung nahm etwa ein Jahr in Anspruch. Dass die Reise weitergeht, dessen ist sich Jessica Rod sicher. Auch ihr Team wächst stetig und im Zuge des allgegenwärtigen Hypes um Künstliche Intelligenz (KI) und deren mannigfache Einsatzmöglichkeiten kommen regelmäßig weitere Service-Ideen zum bestehenden Offering dazu. ■