Cloudbasierte Security und externe Dienstleister

Security Operations Center waren das Thema der mbuf Arbeitsgruppe IT-Security-Management am 6. Juli. Insgesamt 25 Teilnehmer diskutierten in der Nähe von Würzburg, was beim Aufbau und beim Betrieb eines solchen Centers zu beachten ist, und wie sich der Wechsel eines Security-Dienstleisters gestalten kann.

Ein Security Operations Center bietet Dienstleistungen für die IT-Sicherheit an. Spezialisten überwachen die IT-Systeme eines Unternehmens 24 Stunden am Tag und 365 Tage im Jahr. „Service-Mitarbeiter stellen im Schichtdienst sicher, dass niemand die IT-Systeme hackt, manipuliert, dort Daten abzieht und dem Unternehmen schadet“, berichtet Arbeitsgruppenleiter Norbert Breidohr. „Diese Dienstleistung erbringt entweder die hauseigene IT-Abteilung oder ein externer Dienstleister.“

Inhouse-Betrieb oder Security-Dienstleister

Die Diskussionen drehten sich darum, wie Unternehmen ein solches Zentrum intern oder mit einem Dienstleister aufsetzen, welche Technologie dabei zum Einsatz kommt und woher die Überwachungsplattformen ihre Daten sammeln. Vorgestellt wurden auch Dienstleister, die einen Security-Service auf Basis der Technologie von Microsoft oder eines anderen Anbieters leisten.

Vier Vorträge bildeten die Basis für den Austausch: Microsoft hat die hauseigene Cloud-Lösung Sentinel vorgestellt, während der Security-Dienstleister Ontinue beschrieben hat, wie er auf Basis dieser Technologie Dienstleistungen für Unternehmen anbietet. Ein Teilnehmer hat erläutert, wie sein Unternehmen ein Security Operations Center eingeführt hat, ein weiterer Anwendervortrag ging der Frage nach, wie der Wechsel eines Security-Dienstleisters abläuft.

Neueinsteiger diskutieren mit alten Hasen

Der Kreis der Teilnehmer war bunt gemischt, wie der zweite Arbeitsgruppenleiter Jonathan Haist berichtet: „Eines unserer Mitglieder betreibt bereits seit 2019 einen Managed Security Service, während andere so etwas gerade einführen und wieder andere noch im Auswahlprozess sind. Entstanden sind fruchtbare Diskussionen und ein reger Erfahrungsaustausch.“ Auch Breidohr lobt die Breite der Dialoge: „Zur Sprache kam sowohl die Technologie von Microsoft als auch die Lösungen anderer Sicherheitsanbieter.“

Im ersten Vortrag hat Microsoft die hauseigene Technologie Sentinel vorgestellt. Es handelt sich dabei um eine Cloud-Lösung für Security Information and Event Management (SIEM) sowie Sicherheitsorchestrierung, Automatisierung und Reaktion (SOAR). Die Lösung bietet sowohl Sicherheitsanalysen als auch Threat Intelligence. Laut Microsoft betrachtet Sentinel das gesamte Unternehmen sozusagen aus der Vogelperspektive und ermöglicht es mit einer Vielzahl von Warnungen und Lösungsansätzen, auch komplexe Angriffe in den Griff zu bekommen.

Sentinel ergänzt den Microsoft Defender

„Sentinel sammelt die Daten von Security-Lösungen wie etwa Microsoft Defender an zentraler Stelle“, berichtet Breidohr. „Dort werden sie mit Künstlicher Intelligenz ausgewertet,

und der Kunde erhält Warnungen über verdächtiges Verhalten und über Manipulationsversuche. „Dank der integrierten Orchestrierung und Automatisierung können Unternehmen bei Bedarf schnell und gezielt Gegenmaßnahmen ergreifen."

Die Analysen von Sentinel umfassen sowohl Inhouse-Applikationen als auch Cloud-Systeme. „Auch Komponenten von Drittherstellern wie beispielsweise eine Firewall können Daten an Sentinel liefern", berichtet Haist. „So erkennt die verhaltensbasierte Erkennung auf Basis Künstlicher Intelligenz zielsicher Schwachstellen und Angriffe."

Thirdparty-Integration kostet Extragebühren

Da Sentinel mit anderen Microsoft-Produkten zusammenarbeitet, hat dieser Hersteller zumindest auf den ersten Blick die Nase vorn, wenn es um die Lizenzierung geht: „Sentinel ist in einigen Lizenzpaketen enthalten, aber längst nicht in allen", warnt Breidohr. „Um sicher zu gehen, sollten Unternehmen prüfen, ob ihre Verträge diese Leistung abdecken, oder ob sie dafür nachrüsten müssen."

Zu beachten sind bei der Lizenzierung der Speicherbedarf und das Log-Volumen, wie Haist erläutert: „Je nach Vertrag wird lediglich ein gewisses Speichervolumen samt Log-Dateien kostenlos ausgewertet. Binden Unternehmen zusätzliche Dienste wie etwa die Firewall eines Drittherstellers ein, müssen sie dafür extra zahlen."

Der zweite Vortrag kam vom Security-Dienstleister Ontinue, ein Tochterunternehmen des Cybersecurity- und Netzwerkspezialisten Open Systems. Ontinue bietet Dienstleistungen auf Basis der Sicherheitstechnologie von Microsoft. Das Unternehmen verknüpft nach eigener Aussage Künstliche Intelligenz und Expertenwissen, um IT-Umgebungen kontinuierlich zu bewerten und zu schützen. Die Informationen für eine derartige Analyse erhält Ontinue über einen externen Zugriff auf das im Unternehmen eingesetzte Sentinel-System.

Zwei Teilnehmervorträge informieren über den Praxisbetrieb

Zwei Teilnehmervorträge gaben Einblick in den Praxisbetrieb eines Security Operations Centers: der erste Vortrag hat aufgezeigt, wie ein Unternehmen ein derartiges Zentrum eingerichtet hat. Der zweite Teilnehmervortrag beschrieb, wie der Wechsel eines Security-Dienstleisters ablaufen kann, und welche Hürden dabei zu beachten sind.

Lobende Worte findet Arbeitsgruppenleiter Haist über den Gastgeber des Treffens: „Wir waren eingeladen in die Zuchtstation des Saatgutherstellers KWS SAAT SE & Co. KGaA in der Nähe von Würzburg. Eine wunderschöne Lokation."

Das nächste Treffen der mbuf Arbeitsgruppe IT-Security-Management findet am 15. und 16. November in Mannheim statt. Die Themen dafür werden Ende Juli festgelegt. Mitglieder der Arbeitsgruppe sind eingeladen, Vorschläge zu machen. *Jürgen Frisch*