Verbesserung der SOC-Reife

Adaptive Sicherheit

Unternehmen stehen unter ständiger Bedrohung durch Cyberattacken: Jede Organisation wird früher oder später mit einem Angriff konfrontiert. Ein Security Operations Center (SOC) hilft dabei, für den Ernstfall vorbereitet zu sein: Experten identifizieren die ersten Anzeichen eines Angriffs und untersuchen sie, um angemessene Gegenmaßnahmen einzuleiten – so die Theorie. In der Praxis haben allerdings selbst 48 Prozent der großen und gut finanzierten Unternehmen noch kein SOC eingerichtet, wie eine Studie von EY [1] zeigt.

Vor allem der Fachkräftemangel stellt die Unternehmen vor große Herausforderungen: Laut der aktuellen „SANS Security Operations Center Survey 2018" des SANS Institutes [2] fehlt in 62 Prozent der Sicherheitsabteilungen das geeignete Personal, um das SOC angemessen auszustatten. Im Ernstfall muss das SOC-Team schnell reagieren können, um die Folgen eines Sicherheitsvorfalls abzumildern, aber aufgrund fehlender Mitarbeiter und mangelhafter technischer Ausstattung ist es oft nicht voll einsatzfähig. Weitere Probleme wie fehlende Prozessautomation (bei 53 Prozent) und Intransparenz der Netzwerkumgebungen (bei 41 Prozent) verschärfen laut der Umfrage die Situation.

SOC-Reife verbessern

Wie können SOCs also ihre Reife in Hinblick auf ihre Fähigkeit zur Erkennung und Entschärfung von Vorfällen verbessern? Die Studie des SANS Institutes belegt, dass eine SIEM-Lösung (Security-Information- und Event-Management) die Arbeit erleichtert, indem sie manuelle Prozesse automatisiert.

Das Potenzial dafür ist nach wie vor groß: Bei einem Sicherheitsvorfall basieren noch immer 43 Prozent der Arbeit auf weitestgehend manuellen Prozessen wie der Auswertung von Logfiles, um die Hintergründe und den Kontext des Ereignisses zu verstehen.

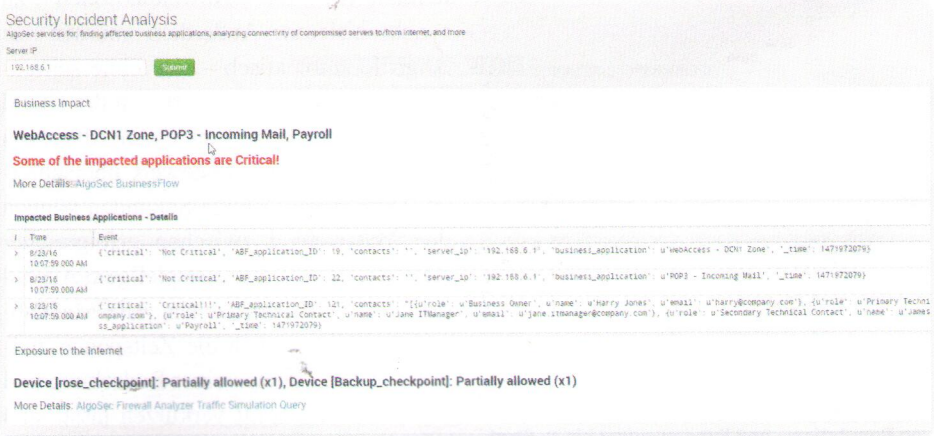
Gartner empfiehlt ein adaptives Sicherheitskonzept mit dem Betrieb von „Plattformen zum Schutz kontextbezogener Netzwerk-, Endpunkt- und Anwendungssicherheit". Diese Plattformen ermöglichen es im SOC, genau zu verstehen, welche Geschäftsprozesse ein Angriff betreffen könnte. So lassen sich passende Reaktionen anhand der Schwere des Angriffs und der betroffenen Geschäftsprozesse ermitteln, priorisieren und zukünftige Security-Maßnahmen planen.

In der Theorie klingt Incident Response einfach. Die Erkennung eines Vorfalls erfolgt mithilfe eines SIEM-Systems, das eine Geschäftslogik und -analytik nutzt, um die zahlreichen Logfiles, die das Arsenal der Sicherheits-Tools liefert, nach Auffälligkeiten zu durchsuchen. Diese Untersuchungen verhindern Fehlalarme und kennzeichnen Ereignisse, die einer genaueren Betrachtung durch die Sicherheitsanalysten im SOC bedürfen. Diese Ereignisse werden dann gemeldet, ihre Auswirkungen analysiert, und der Angriff lässt sich stoppen oder zumindest eindämmen.

Mehrwert korrekter Informationen

In der Praxis sind Incident-Response-Prozesse bei vielen Unternehmen jedoch deutlich komplexer und langsamer. Ist ein Angriff per SIEM-Lösung identifiziert, müssen Sicherheitsspezialisten unter hohem Aufwand das Ereignis analysieren. Im ersten Schritt gilt es herauszufinden, welche Systeme zu isolieren sind, um eine Ausbreitung des Angriffs zu verhindern. Daraus folgen schnell Produktionseinbußen, Datenlecks und die Ausfälle von Websites und Applikationen. Der so entstandene Schaden reicht von einem Reputationsverlust bis hin zu Umsatzeinbußen sowie empfindlichen Strafen wegen verlorener Daten und des nicht mehr gewährleisteten Datenschutzes.

Der Schaden lässt sich eindämmen, wenn die Security-Spezialisten den Angriff direkt mit den betroffenen Geschäftsprozessen in Verbindung bringen, das Resultat abschätzen und möglicherweise einen Ersatz bereitstellen können. Kontextbezogene Daten beantworten dem Incident-Response-Team die wichtigsten Fragen:



Eine geschäftsbezogene SIEM-Lösung bietet Angaben dazu, ob die von einem Angriff betroffenen Systeme kritisch sind. Bild: AlgoSec

Welche Geschäftsanwendungen beruhen auf Systemen, die von dem Angriff betroffen sind? Wie geschäftskritisch sind solche Anwendungen und wer ist für sie verantwortlich? Verarbeiten die betroffenen Anwendungen sensible Daten und können Angreifer diese Daten entwenden?

Die Antworten auf diese Fragen bestimmen die Dringlichkeit der Reaktion und den Grad der erforderlichen Maßnahmen. In vielen Fällen lassen sich damit unnötig weitreichende Eingriffe und Störungen der Infrastruktur eines Unternehmens vermeiden. Dazu ist allerdings notwendig, dass die eingesetzte SIEM-Lösung ein Tool umfasst, das solche geschäftsrelevanten Kontextinformationen in den Prozess einbringen und Sicherheitsvorfälle direkt mit den bedrohten Elementen verknüpfen kann. Dann können die Security-Spezialisten die Risiken eines Angriffs für die Organisation gegen die betrieblichen Risiken der potenziellen Stillstandsdauer abwägen.

Richtlinien-Management

Die Kontextinformationen lassen sich zudem für ein intelligentes Richtlinien-Management heranziehen, um die Sicherheit von Cloud-, lokalen und Hybridumgebungen zu verbessern. Normalerweise ist es mit erheblichem Aufwand verbunden, die Sicherheitsrichtlinien in einem Unternehmen zu ändern: Meist betreffen Modifizierungen dieser Richtlinien viele Geräte und Abteilungen eines Unternehmens, die mitunter eigene Anforderungen stellen und mit unterschiedlichen Terminologien arbeiten. Änderungen, die dieser Vielfalt nicht gerecht werden und die involvierten Unterschiede nicht berücksichtigen, führen oft zu Compliance-Problemen, Anwendungsausfällen, einem verlangsamten Betrieb und in der Folge zu Umsatzeinbußen.

Normalerweise sind dynamische Änderungen von Sicherheitsrichtlinien ein kritisches Thema für die IT-Security, ihre Vernachlässigung birgt ein großes Sicherheitsrisiko. Gibt ein Unternehmen die Verwaltung dieser Richtlinien in die Hände einer intelligenten Management-Lösung, kann man diese Hindernisse umgehen. Mithilfe der Geschäftsinformationen lassen sich die Prozesse, die hinter einem Richtlinienwechsel stehen, planen und anhand der Risiken sondieren. Dazu erstellt eine Richtlinien-Management-Plattform ein Mapping des Unternehmens im Kontext der Geschäftsaktivitäten und simuliert vor der Änderung bereits ihre Folgen in Hinblick auf die Auswirkungen auf das Tagesgeschäft, mögliche Risiken und die Wirtschaftlichkeit. Damit vereinfacht sie die Umsetzung neuer Strukturen und Richtlinien sowie die Incident Response.

In den meisten größeren Unternehmen ist das SOC das Nervenzentrum der Cyberabwehr, aber ihre Ausrüstung und Umsetzung befindet sich noch in einer frühen Ausbauphase. Um eine Organisation besser zu schützen, muss das SOC einen höheren Reifegrad erzielen und sich an die Geschäftsstrategien und -abläufe anpassen. Das beschleunigt die Incident Response, entlastet die Security-Teams und hilft, langfristige Verbesserungen strategisch zu planen.

Zu den wichtigsten Tools gehören intelligente SIEM-Lösungen, die auf Informationen zum Geschäftskontext aufbauen, weil sie einen Großteil der Fleißarbeit übernehmen. Dazu zählt die Priorisierung von Sicherheitsereignissen und die Verwaltung von Sicherheitsrichtlinien. Das macht sie zu einem wichtigen SOC-Bestandteil, um einen hohen Reifegrad zu erreichen und im Ernstfall wertvolle Zeit zu sparen.

Robert Blank/wg

Robert Blank ist Regional Sales Manager DACH bei AlgoSec, www.algosec.com.

Quellen

[1] EY, „Cybersecurity Regained: Preparing to Face Cyber Attacks", 2017.

[2] SANS Institute, „The Definition of SOC-cess? SANS 2018 Security Operations Center Survey", 2018.

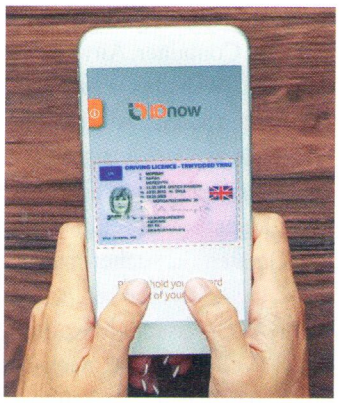
Produkt-News

IDnow mit KI-basierter Identity-as-a-Service-Plattform

Automatisierte, bild- und videogestützte Online-Identifizierung

IDnow offeriert Unternehmen für die Online-Identifizierung mit seiner Plattform eine videobasierte, automatisierte Basis für das Identity-Management mittels künstlicher Intelligenz (KI): Die Bausteine AutoIdent, VideoIdent, eSign und eID sollen helfen, Antragsprozesse kundenfreundlicher zu gestalten. AutoIdent dient der fotogestützten Online-Identifizierung per mobilem Endgerät. Damit lasse sich die Online-Identifizierung innerhalb von ein bis zwei Minuten bequem per Smartphone abwickeln. Die Software erfasst via Zugriff auf die Smartphone-Kamera den maschinell lesbaren Teil des Ausweisdokuments, zudem auch die nicht maschinenlesbaren Teile. Dann überprüft sie Sicherheitsfunktionen der Ausweise wie Hologramme. Der Prozess umfasst eine kurze „Liveness Detection" (Erkennung, ob es sich um eine lebende Person handelt) per Kamera. Damit errechne die Lösung einen Risikoindex und schließe je nach Ergebnis den Vorgang ab. Dies ist laut IDnow problemlos in die Service-App eines Unternehmens integrierbar. AutoIdent wie auch die Videolösung VideoIdent erkennen laut Hersteller Ausweisdokumente aus 193 Ländern, darunter Deutschland. wg

Info: IDnow
Web: www.idnow.io



IDnow AutoIdent ermöglicht die Identifizierung einer Person per Smartphone. Bild: IDnow