ANWENDERBERICHT

Rapid7 InsightVM und InsightIDR ermöglichen 60% Zeitersparnis und erleichtern die Compliance bei Energie Südbayern

BRANCHE:
Energieversorger

GRÖSSE:
350 Angestellte

PRODUKTE:
InsightVM*, InsightIDR

DIE HERAUSFORDERUNGEN

- Die Compliance mit deutschem IT-Sicherheitsgesetz musste gewahrt bleiben.
- Eine technische Lösung war gefordert, die anomale Aktivitäten in der IT-Infrastruktur durch Intelligenz erkennen konnte, nicht nur über Regeln.

DIE LÖSUNG

- Da ESB nachweisen konnte, dass die Technologie zum Zweck der Sicherheit eingesetzt wird, stimmte der Betriebsrat zu.
- Rapid7 InsightVM und InsightIDR bieten vereinfachte Verwaltung und zentrale Berichte mit einem einzigen Agent.

Der Energiesektor in Deutschland ist ein interessantes Ziel für Hacker. Cyber-Kriminelle, Hacker und staatlich finanzierte Akteure haben heute die Motive und die Fähigkeiten, erfolgreich anzugreifen, um sensible betriebliche und Kundendaten zu stehlen, Unternehmen zu erpressen oder zentrale Kontrollsysteme zu stören oder sogar zu zerstören.

Dies sind nur einige der Bedrohungen, die Benjamin Nawrath den Schlaf rauben. Benjamin Nawrath ist Information Security Officer beim Energieversorger Energie Südbayern (ESB), der Erdgas und Elektrizität für 120.000 Haushalte in Süddeutschland bereit stellt. Als größter regionaler Anbieter beschäftigt ESB ungefähr 350 Angestellte, wobei neben Benjamin Nawrath weitere 14 Mitarbeiter in der IT arbeiten.

Compliance als Last

Eine der größten Herausforderungen für Benjamin Nawrath ist die Einhaltung des deutschen IT-Sicherheitsgesetzes (ITSG), das im Jahr 2015 beschlossen wurde und ab Juli 2017 zur Anwendung kommt. Das Gesetz verlangt von allen Betreibern kritischer Infrastrukturen ein fortschrittliches Cybersecurity-Programm, das die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Infrastruktur gewährleisten muss. Es verlangt außerdem, dass Organisationen ihre Compliance regelmäßig zertifizieren lassen. Ein Verstoß kann mit einer Buße von mehreren hunderttausend Euro belegt werden.

In einer großen und komplexen Umgebung (einschließlich 2.000 IP-Adressen), die überwacht werden muss, begrenzten personellen Ressourcen in der IT-Abteilung, einer wachsenden Compliance-Last und hoch motivierten Hackern als Gegnern benötigte Benjamin Nawrath robuste technologische Lösungen, um diesen Herausforderungen erfolgreich zu begegnen.

*Unser preisgekröntes Produkt „Nexpose“ wurde zu InsightVM weiterentwickelt. Es nutzt die Leistung der Insight-Plattform von Rapid7, unserer Cloud-basierten Lösung für Sicherheit und Datenanalyse.

Erfahren Sie mehr unter www.rapid7.com/insightvm

Grünes Licht

Die IT von ESB nutzte bereits Nexpose*, die branchenführende Schwachstellen-Management-Lösung von Rapid7. Dementsprechend lag es nahe, das Portfolio mit Rapid7 zu ergänzen. Um den Bedarf nach einer Lösung für Incident Detection and Response zu decken, wurde schnell und unkompliziert ein Proof of Concept (PoC) mit Rapid7 InsightIDR aufgesetzt, um die Qualitäten der Lösung im realen Einsatz zu bestätigen.

„Ich benötigte eine Lösung, die Intelligenz mitbrachte – nicht nur eine technische Lösung für Regeln. Ich kaufe die Intelligenz, nicht die Regeln. Das war der große Erfolgsfaktor für Rapid7 für uns bei dieser Evaluierung," sagt Benjamin Nawrath. „Splunk und andere ähnliche Lösungen sammeln nur die Logs und ich muss diese selbst auswerten. Aber ich möchte wissen, wenn etwas Seltsames oder Ungewöhnliches passiert - und genau das ist, was mir InsightIDR mitteilt. Es war die beste Lösung, die mir die benötigte Intelligenz zu einem vernünftigen Preis bereitstellt."

ESB machen mit der Kombination von InsightVM (der Weiterentwicklung von Rapid7 Nexpose) und InsightIDR – beide gestützt auf die Rapid7 Insight-Plattform – den nächsten Schritt, um branchenführendes Schwachstellen-Management und Incident Detection and Response bereit zu stellen. Benjamin Nawrath stellt fest, dass beide Lösungen sich einfach einrichten und warten ließen und dass sie vereinfachte Verwaltung und zentrale Berichte mit einem einzigen Agent ermöglichen. ESB war einer der Vorreiter bei der Einführung Cloud-basierter Dienste, dementsprechend gab es bei der Bereitstellung keine Engpässe. Und durch den Fokus auf Sicherheit erhielt die Überwachung der IP-Adressen auch vom deutschen Betriebsrat grünes Licht.

Schnellere Reaktion auf Störfälle

InsightIDR spart der IT von ESB Zeit und hilft ihr, viel schneller auf Vorfälle zu reagieren. Mit der Vereinigung von SIEM, User Behavior Analytics (UBA) und Endpoint Detection and Response (EDR) liegt der Schwerpunkt des völlig neu entworfenen InsightIDR auf der frühestmöglichen Erkennung von Angriffen, so dass die Bösewichte keine Zeit haben, sich zu verstecken.

„Ehrlich gesagt gab es überhaupt keinen Incident Response-Prozess, bevor wir InsightIDR einführten. Ich bekam einfach eine E-Mail von einem Anwender, der mir sagte, etwas sei ‚anders als sonst'. Dann musste ich mich von Hand einarbeiten und Protokolle durchsuchen, was eine Menge Zeit kostete," sagt Benjamin Nawrath. „InsightIDR hat mir dabei geholfen, schneller auf Vorfälle zu reagieren. Es ist sehr einfach zu nutzen und die Agents bieten einen großartigen Einblick."

Benjamin Nawrath nutzt die Funktionen des Live-Dashboard, um fehlgeschlagene Anmeldeversuche von speziellen Usern zu überwachen. „Einer der vielen Vorteile ist, dass ich InsightIDR nicht vorgeben muss, was ein Dienstkonto ist – es erkennt das einfach." ergänzt er.

Das einfach zu verwaltende Portal erlaubt ihm, ungewöhnlich hohe Werte im Blick zu behalten, wenn sich Mitarbeiter aus anderen Ländern remote anmelden oder andere Metriken auf Compliance-Verstöße hindeuten. Warnungen per E-Mail runden das Bild ab und werden zudem an andere Mitglieder des IT-Teams geschickt, so dass auch diese reagieren können, wenn böswillige Handlungen entdeckt werden.

Risikosenkung mit InsightVM

Zur Überwachung einer komplexen IT-Umgebung, einschließlich sensibler industrieller Steuerungssysteme, benötigte Nawrath außerdem Schwachstellen-Management auf höchstem Niveau mit einer engen Integration in InsightIDR. InsightVM von Rapid7 sammelt, überwacht und analysiert automatisch jegliche Schwachstellen im Unternehmensnetzwerk,

„InsightIDR hat mir dabei geholfen, schneller auf Zwischenfälle zu reagieren. Es ist sehr einfach zu nutzen und die Agents bieten einen großartigen Einblick."

bietet fortschrittliche Analysen und Berichte, damit Nutzer Risiken priorisieren und abstellen können.

Bei ESB wird Erfolg durch Risikoreduzierung definiert - eine Aufgabe, bei der sich InsightVM als hervorragend erwiesen hat.

„Ich prüfe regelmäßig und bekomme schon mit Benutzerrechten so viel Informationen, wie ich benötige. Wir haben fast keine Fehlalarme, was großartig ist," sagt Benjamin Nawrath. „InsightVM hilft uns zudem bei der Identifikation alter Systeme, die erneuert, aktualisiert oder sogar abgeschaltet werden müssen. Wir erhalten einen großartigen Einblick in die Risikoevaluierung. Es ist schön zu sehen, wie das Risiko sinkt, wenn wir Gegenmaßnahmen ergreifen."

Die Agents sparten zudem Zeit bei regulären Scans. Der Vorteil der engen Integration mit InsightIDR erlaubt einen großen Effizienzgewinn durch hoch akkurate Korrelationen zwischen Sicherheitsereignissen und Schwachstellen.

Ausblick

Unter dem Strich spart die geballte Leistung von InsightIDR und InsightVM Benjamin Nawrath 60% seiner Zeit. Das wiederum erlaubt ihm mehr Zeit für die Verifizierung der Schwachstellen selbst und die Vorbereitung einer bevorstehenden OSCP-Prüfung. Darüber hinaus konnte er mit den von Rapid7 erzeugten Daten seine Position in der Organisation festigen.

„Das Top-Management hat wenig mit dem Thema IT-Sicherheit zu tun, aber dank beider Rapid7-Produkte bin ich in der Lage, sie von der tatsächlichen Risikosituation zu überzeugen. Ich erhalte dafür mehr Respekt für meine Arbeit," sagt er. „Und da die Lösungen nicht so teuer waren, war es kein Problem, das notwendige Budget zu bekommen."

Für die Zukunft plant Benjamin Nawrath die Implementierung des Remediation Workflow von InsightVM. Damit kann er Aufgaben an seine Kollegen delegieren. Hauptsächlich aber, so ist er sich sicher, wird die Kombination aus InsightIDR und InsightVM den notwendigen Schutz bieten, der für die Auflagen des IT-Sicherheitsgesetzes notwendig ist – und ESB damit in den kommenden Jahren sicher und compliant halten.