proofpoint

KUNDENBERICHT

Energieunternehmen verbessert Cyberabwehr mit Proofpoint

Die Herausforderung

- Besserer Überblick über Sicherheitsbedrohungen bei geschäftskritischen Infrastrukturen und Assets
- Schnellere Erkennung von Bedrohungen und bessere Reaktion auf Zwischenfälle
- Verbesserte Erfassung von Forensikdaten

Die Lösung

Proofpoint Identity Threat Defense

- Proofpoint Shadow

Die Ergebnisse

- Nur True-Positive-Warnmeldungen über Angriffsaktivitäten
- Echtzeiteinblicke in Angreiferaktivitäten
- Um zwei Drittel kürzere Untersuchungszeit
- Sofortige Bereitstellung detaillierter Forensikdaten, die Maßnahmen mit unwiderlegbaren Beweisen unterstützen
- Aufbau einer echten Partnerschaft mit Proofpoint im Laufe des Bereitstellungszyklus

Das Unternehmen

Das Unternehmen versorgt Millionen Verbraucher und Partner auf der ganzen Welt mit Energie und zugehörigen Dienstleistungen. Zudem ist der internationale Konzern in der Suche und Gewinnung von Energieträgern tätig. Energie ist für unseren Alltag und die nationale Sicherheit von entscheidender Bedeutung. Das Unternehmen setzt daher auf technologische Innovation und entwickelt modernste Produkte, Anwendungen und Dienstleistungen. Da die Sicherheit stets an erster Stelle steht, beauftragte das Unternehmen Proofpoint mit der Entwicklung maßgeschneiderter Funktionen zur Erkennung schädlicher Aktivitäten und Bereitstellung sofortiger Forensikdaten.

Die Herausforderung

Eine große Herausforderung bei der Sicherheit eines Energieunternehmens ist die Absicherung der komplexen Angriffsfläche. Das Unternehmen arbeitet mit lokaler und Cloud-basierter Infrastruktur sowie mit einem geschäftskritischen SCADA-Netzwerk (Supervisory Control and Data Acquisition) und zugehörigen Geräten. Aufgrund der großen Anzahl externer Partner muss das Netzwerk über zahlreiche Ein- und Ausgänge verfügen. Zudem ist es durch den Fokus auf DevOps nötig, die Endpunktabsicherung auf eine größere Zahl von Entwicklern auszurichten sowie den Anwendungscode und die Testsysteme abzusichern. Um als Energieanbieter Branchenvorschriften, die Datenschutz-Grundverordnung (DSGVO) und andere Sicherheitsanforderungen einhalten zu können, sind ein genauer Überblick über die Sicherheitsinfrastruktur und die Erfassung von Telemetriedaten im Falle einer erkannten Bedrohung nötig.

Das Unternehmen verfolgte bereits einen mehrschichtigen Schutzansatz und arbeitete kontinuierlich an der Implementierung und Verbesserung empfohlener Vorgehensweisen. Bevor Proofpoint einbezogen wurde, hatten Insider in mehreren Fällen Alarm im Sicherheitssystem des Unternehmens ausgelöst. Wenn in einem solchen Fall im Sicherheitskontrollzentrum (SOC) eine Warnmeldung eintraf, mussten sich die Mitarbeiter den Laptop des Anwenders beschaffen und ihn manuell untersuchen. Das bedeutete, die Systemregistrierungen zu durchsuchen und in mühevoller Kleinarbeit genügend Forensikdaten zusammenzutragen, um ein Bild des Geschehenen zu rekonstruieren. Selbst wenn das Sicherheitsteam den Laptop zügig beschaffen konnte, dauerte die Untersuchung meist Stunden. Um die Reaktionszeit zu verkürzen, startete das Unternehmen eine Sicherheitsinitiative, bei der es vor allem darum ging, die Sicherheit von Laptops und Workstations zu erhöhen.

Die Lösung

Bei der Suche nach einer Lösung schaute sich das Unternehmen zunächst herkömmliche Honeypot-Technologien an und erfuhr im Zuge dessen von Proofpoint Identity Threat Defense, der endpunktbasierten Täuschungstechnologie. Schließlich fiel die Wahl auf Proofpoint Shadow.

„Erst dachte ich, dass Proofpoint Shadow nur ein Honeypot ist“, so der Information Security Manager. „Schnell wurde allerdings klar, dass der Proofpoint-Ansatz wesentlich komplexer ist.“

Die agentenlosen Täuschungen von Proofpoint Shadow, die auf Bedrohungsdaten basieren und auf jedem Endpunkt verteilt sind, imitieren reale Informationen, Anmeldedaten und Verbindungen. Wenn nun ein krimineller Akteur oder Insider mit legitimem Netzwerkzugriff seinen Weg durch das System finden will, steht er vor einer Vielzahl an gefälschter Ressourcen, die täuschend echt aussehen. Sich sicher und unbemerkt zu bewegen, wird nahezu unmöglich, da bereits ein einziger Fehltritt genügt, um das SOC auf seine Anwesenheit aufmerksam zu machen. Wenn eine Falle zuschnappt, fängt das System an, umfangreiche Forensikdaten von den Systemen zu erfassen, in denen der Angreifer operiert. Die detaillierten Echtzeitdaten werden genutzt, um schnelle und individuelle Reaktionsmaßnahmen zu ergreifen.

„Proofpoint hat die Untersuchungszeit um zwei Drittel verkürzt. Über das grafische Dashboard sehen wir, wo sich der Angreifer im Verhältnis zu unseren wichtigsten Assets befindet. Wir können schnell bestimmte Details aufrufen, und die Lösung gibt uns automatisch eine Zeitleiste dazu, was auf dem Endpunkt passiert ist. Das ist einfach unbezahlbar.“

Information Security Manager, Energieunternehmen

Mithilfe seines MSPs sowie der Proofpoint Professional Services stellte das Energieunternehmen Proofpoint Identity Threat Defense in der gesamten Unternehmensumgebung bereit. Die Lösung identifizierte umgehend kritische Pfade zu den wichtigsten Assets und mehrere Konfigurationsfehler auf älteren Systemen, die Schwachstellen darstellten.

„Proofpoint Identity Threat Defense ist außerordentlich nützlich“, erklärt der Information Security Manager. „Die Lösung erfasst Daten von den Endpunkten und schlägt dann die am besten geeigneten Täuschungen vor. Das spart Zeit und bietet uns deutlich besseren Schutz. Beeindruckt sind wir auch von den Proofpoint-Mitarbeitern. Sie kümmern sich geduldig um unsere Anliegen, helfen uns bei der Abstimmung der Abwehrmaßnahmen auf unsere Umgebung und reagieren sehr schnell."

Die Ergebnisse

Nach der Bereitstellung erkannte die Proofpoint-Lösung sofort, wenn ein unbekannter Angreifer versuchte, sich durch die Systeme zu bewegen und dabei in eine Täuschung tappte. Das Sicherheitsteam sieht nun Angreiferaktivitäten in Echtzeit und kann diese überwachen. Gleichzeitig stellt die Echtzeit-Forensik den Experten Angriffsdaten zur Verfügung, aus denen sie schnell konkrete Informationen gewinnen können, ohne dass der Angreifer erfährt, dass seine Aktivitäten gerade untersucht werden. Da das Incident-Response-Team nun weiß, welche Tools der Angreifer verwendet, kann es schnell den Untersuchungsschwerpunkt festlegen. Parallel dazu sendet Proofpoint Warnmeldungen an das ServiceNow-System des Unternehmens, was die Zuordnung von Analysten, die Priorisierung von Reaktionsmaßnahmen und das Ticket-Management vereinfacht.

„In der Vergangenheit hätten wir von diesen Aktivitäten gar nichts mitbekommen“, betont der Information Security Manager. „Erst nach Warnmeldungen mehrerer Sicherheitslösungen und mit viel Zeit hätten wir feststellen können, dass es sich um einen echten Angriff handelt. Anschließend hätten wir den Laptop isolieren und einziehen müssen, um ihn untersuchen und Beweise sammeln zu können.“

Ein enormer Fortschritt

„Die Telemetriedaten sind wirklich ein großer Fortschritt“, meint er weiter. „Proofpoint Identity Threat Defense hat die Untersuchungszeit um zwei Drittel verkürzt. Über das grafische Dashboard sehen wir, wo sich der Angreifer im Verhältnis zu unseren wichtigsten Assets befindet. Wir können schnell bestimmte Details aufrufen, und die Lösung gibt uns automatisch eine Zeitleiste dazu, was auf dem Endpunkt passiert ist. Das ist einfach unbezahlbar.“

Zudem liefert die Lösung unwiderlegbare Beweise. Wenn es sich bei einem Angreifer um einen Insider handelt, kann das Unternehmen zweifelsfrei belegen, was passiert ist, und entsprechende Schritte ergreifen. Bei den häufiger auftretenden externen Angriffen verfügt die Firma nun über detaillierte Daten zu den Zielen und Techniken der Angreifer und kann maßgeschneiderte Abwehrmaßnahmen einleiten.

Das Fundament für die Zukunft

Das Energieunternehmen plant, seinen mehrschichtigen Schutzansatz mithilfe von Proofpoint Identity Threat Defense auf weit abgelegene Kraftwerke, die SCADA-Umgebung und IoT-Geräte zu erweitern.

„Proofpoint Identity Threat Defense ist für uns ein unverzichtbares Tool“, erklärt der Information Security Manager. „Es hat sich als äußerst effektiv erwiesen. Wenn wir unsere Sicherheitstools aus irgendeinem Grund reduzieren müssten, wäre es das letzte, auf das wir verzichten würden.

MEHR ERFAHREN

Weitere Informationen finden Sie unter **proofpoint.com.de**.