Forcepoint

Kundenbericht

BAYERNOIL erfüllt mit Forcepoint NGFW die strengen deutschen Vorschriften für kritische Infrastrukturen

Die in Bayern ansässige Ölraffinerie setzt die Forcepoint Next Generation Firewall des Partners Software Symbiose ein, um eine bessere Transparenz zu erreichen, das Netzwerksicherheitsmanagement zu verbessern, Cloud-Anwendungen zu unterstützen und vor allem die gesetzlichen Anforderungen zu erfüllen.

Bayern mag für Bier, Bratwürste und das Oktoberfest bekannt sein, aber BAYERNOIL ist auch ein bedeutender regionaler Produzent von etwas, das nicht so schmackhaft, aber wohl genauso wichtig ist: Öl. Die in Bayern ansässige Raffinerie BAYERNOIL, die von der deutschen Regierung als kritische Infrastruktur („KRITIS") eingestuft wurde, musste ihre Netzwerksicherheit aufrüsten, um die strengen Leistungs- und Audit-Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu erfüllen. BAYERNOIL wandte sich an Forcepoint und den zuverlässigen Vertriebspartner Software Symbiose, um ein Sicherheitskonzept zu entwickeln, das auf Forcepoint NGFW basiert. Das Ziel war, neue Cloud-Anwendungen zu schützen, eine Netzwerksegmentierung einzurichten und die Berichterstellung zu verbessern – alles, um die BSI-Vorgaben zu erfüllen und das Geschäft voranzutreiben.

KUNDENPROFIL:
Die größte Raffinerie im bayerischen Raum produziert aus ca. 10,3 Millionen Tonnen Rohöl pro Jahr hochwertige Flüssiggase, Kraftstoffe, Benzin, Kerosin, Diesel, Heizöl und Bitumen.

BRANCHE:
Öl und Gas

HAUPTSITZ:
Deutschland

PRODUKTE:
Forcepoint NGFW mit Forcepoint One Endpoint

In Deutschland werden Energieunternehmen, Transportunternehmen, Lebensmittelverarbeitungsbetriebe und Ölraffinerien als kritische Infrastrukturen („KRITIS") eingestuft, für die ausgereifte Cyber-Sicherheitstools erforderlich sind. Betreiber kritischer Infrastrukturen wie die Ölraffinerie BAYERNOIL müssen dem BSI nachweisen, dass sie die im IT-Sicherheitsgesetz von 2015 festgelegten Standards einschließlich ISO 27001 im Rahmen der Nationalen Strategie zum Schutz kritischer Infrastrukturen des Landes einhalten können und müssen etwaige Sicherheitsvorfälle an das BSI melden.

Nachdem Marcus Waatsack, IT-Manager bei BAYERNOIL, die behördlichen Anforderungen des BSI an getrennte Netzwerke, hohe Performance und detaillierte Audits vorgelegt wurden, setzte er sich mit Franz Hermann, CEO von Software Symbiose, einem zuverlässigen Lösungsanbieter, zusammen, um sich über mögliche Optionen zu informieren. Waatsack wollte außerdem einen Teil der lokalen Infrastruktur von BAYERNOIL auf die Cloud-basierten Anwendungen Microsoft Office 365 und Citrix File Services umstellen. Die Netzwerksicherheitsarchitektur musste weiterentwickelt werden, um eine hohe Sicherheit zu gewährleisten und sowohl die gesetzlichen als auch die Leistungsanforderungen zu erfüllen.

Die Entscheidung darüber, welchen Weg Sie zur Einhaltung der BSI-Vorschriften und hin zu einer Hybrid-Cloud einschlagen wollten, fiel Waatsack und Hermann leicht. Bereits einige Jahre zuvor wurde bei BAYERNOIL Forcepoint Next Generation Firewall (NGFW)-Appliances als Grundlage für die Netzwerksicherheit eingesetzt, sodass Waatsack bereits mit den Funktionen vertraut war. BAYERNOIL entschied sich für ein Upgrade auf die neueste Forcepoint NGFW-Appliance mit einer einheitlichen Endpunktlösung, die von Software Symbiose implementiert wurde. „Die Technologie von Forcepoint war für unser Unternehmen einfach perfekt, und wir waren absolut von ihrer Leistungsfähigkeit überzeugt", erinnert sich Waatsack. „Warum sollten wir die Firewall ändern, wenn unsere Leute dafür geschult waren und wir der Technologie vertraut haben? Wir waren überzeugt, dass Forcepoint die richtige Wahl ist, um unsere aktuellen und zukünftigen Herausforderungen zu lösen."

One Endpoint ermöglicht einen auf den Menschen fokussierten Netzwerkrand

BAYERNOIL führte sofort ein Pilotprojekt durch, in dem Forcepoint One Endpoint-Agenten auf mehreren Client-Systemen installiert wurden, die mit der neuen Forcepoint NGFW-Appliance verbunden waren. Das BAYERNOIL-Team beobachtete dann die Protokolle und passte die Richtlinien über das Forcepoint Security Management Center (SMC) an. One Endpoint bietet Einblick in Anwendungen und Geräte, die versuchen, sich über die Forcepoint NGFW mit dem Netzwerk von BAYERNOIL und dem Internet zu verbinden. One Endpoint identifiziert Benutzer durch Informationen, die an NGFW geliefert werden, so dass der Zugriff unabhängig davon, von wo aus sich Benutzer anmelden, anhand der Gruppenzugehörigkeit verwaltet werden kann anstatt anhand einer spezifischen IP-Adresse. Wenn BAYERNOIL neue Sicherheitsfunktionen von Forcepoint hinzufügt, kann One Endpoint verwendet werden, um weitere Lösungen anzubinden.

Das SMC von Forcepoint ermöglichte auch einen nahtlosen Übergang von der vorherigen Netzwerksicherheitsplattform zur neuen: Waatsacks Team konnte die Hardware im laufenden Betrieb austauschen, Richtlinien für autorisierte Benutzergruppen und Aktionen ganz einfach aktualisieren und unsichere URLs und Apps einschränken. Die Forcepoint NGFW erkannte automatisch einen erlaubten Browser oder eine erlaubte Anwendung und blockierte die Ausführungs- oder Verbindungsversuche von nicht autorisierter Software im Netzwerk von BAYERNOIL.

„Das Upgrade von der Forcepoint NGFW 1000 Series auf die 3000 Series-Appliance verlief besser als erwartet", so Waatsack. „Wir konnten die Hochverfügbarkeitsfunktionen von Forcepoint nutzen, um jeweils einen Firewall-Knoten in einem Aktiv-Aktiv-Cluster zu installieren und die Hardware komplett auszutauschen, ohne dass es zu einem Netzwerkausfall kam."

Herausforderungen

Deutsche IT- und Sicherheitsrichtlinien für kritische Infrastrukturen einhalten.

Migration zu Cloud-Anwendungen unterstützen.

Netzwerksegmentierung und Netzwerkzonen einrichten.

Vorgeschriebene Audit-Anforderungen erfüllen.

Strategie

Forcepoint NGFW bereitstellen.

Segmentierung für verbesserte Sicherheit und Compliance

Neben der detailgenauen Transparenz erleichterte das NGFW SMC dem Team von Waatsack auch die Segmentierung von Netzwerken, um die Anforderungen der Regierung gemäß KRITIS und ISO 27001 zu erfüllen. Mit Forcepoint NGFW können Administratoren das Netzwerk von BAYERNOIL in separate Segmente mit unterschiedlichen Zugangsberechtigungen unterteilen. Da Datenverkehr und Benutzerzugriff physisch getrennt sind, erhöht Forcepoint das Schutzniveau und verhindert, dass böswillige Personen im Netzwerk Schaden anrichten, selbst wenn ein Segment kompromittiert wird.

Die SMC-Kontrollen von Forcepoint helfen Waatsacks Team auch dabei, Audit-Anforderungen zu erfüllen. Die Sicherheitsanalysten können Berichte abrufen, die zeigen, dass die Netzwerksegmentierung durchgesetzt wird, und können bei Bedarf wöchentlich, monatlich oder vierteljährlich erforderliche Kontrollpunkte für das Incident Management erfüllen.

„Die Berichterstellung ist für uns während des Auditprozesses sehr wichtig geworden", erklärt Waatsack. „Wir konnten bisher den Datenverkehr und die Benutzer nicht physisch von unserem Netzwerk trennen. Jetzt sind wir dazu in der Lage und können die strengen Richtlinien des BSI erfüllen. Die Benutzerfreundlichkeit ist wirklich entscheidend. Wir brauchen eine Software, die einfach zu bedienen ist, damit wir unsere Ziele erreichen und dann auch halten können."

Mit großen Schritten auf dem Weg in die Cloud

Die Verbesserung der NGFW-Leistung legte nicht nur die Messlatte für die Sicherheit höher, sondern half dem Unternehmen auch dabei, einige Anwendungen, die strikt lokal waren, nahtlos in die Cloud zu verlagern, einschließlich der Umstellung auf Office 365. Da Microsoft seine IP-Adressen und Domänennamen als Teil der Office 365-Anwendungsdienste dynamisch aktualisiert hat, konnte die Forcepoint NGFW mühelos mithalten.

„Die detailgenaue Steuerung ist eine Notwendigkeit", so Waatsack. „Vorher konnten wir Microsoft-Anwendungen wie Teams nicht unterstützen, weil es problematisch war, die Kommunikation mit Office 365-Ressourcen aufrechtzuerhalten, die aus Sicherheitsgründen ständig wechselten. Dies hat sich alles zum Besseren gewendet, da Forcepoint NGFW die Schnittstelle zwischen den Netzwerk- und Sicherheitsanforderungen der Cloud-Anwendung und des Anwenders abdeckt. Wir können einige Einschränkungen lockern, damit unsere Mitarbeiter produktiv bleiben, aber trotzdem sicher sind."

Zukunftssicher mit Cyber-Sicherheit von Forcepoint

Forcepoint unterstützt BAYERNOIL dabei, sich auf eine Zukunft in der Hybrid-Cloud vorzubereiten. Laut Herrmann bietet Forcepoint BAYERNOIL einen völlig neuartigen Ansatz für die Cyber-Sicherheit. Dabei werden die Netzwerksicherheit, Data Loss Prevention (DLP), Web-Sicherheit und Cloud Access Security Broker (CASB) integriert, um eine ganzheitliche Lösung zu bieten, die jederzeit für eine stärkere Ausweitung in sichere Cloud-Dienste bereit ist.

„Forcepoint versteht, dass unsere Anforderungen ziemlich einfach sind: Anwendungen schnell einrichten und ihre Ausführung sicherstellen", fasst Waatsack zusammen. „Bei unserer aktuellen Hybrid-Cloud-Strategie brauchen wir die Unterstützung unserer Sicherheitspartner, um BAYERNOIL mit Funktionen wie CASB, DLP oder Dynamic Edge Protection zukunftsfähig absichern zu können. Das ist ein Weg, auf dem wir uns mit Partnern wie Forcepoint und Software Symbiose sicher fühlen können."

„Forcepoint versteht, dass unsere Anforderungen ziemlich einfach sind: Anwendungen schnell einrichten und ihre Ausführung sicherstellen."

MARCUS WAATSACK, IT-MANAGER

Ergebnisse

- Physikalisch getrennte Netzwerksegmente, um den Datenverkehr und den Zugriff nur auf autorisierte Benutzer zu beschränken.
- Nutzung eines einheitlichen Endpunkts zur Optimierung der Informationen über Benutzer, Apps und Zugriffe im Netzwerk.
- Verbesserte Netzwerkleistung, um erstmalig Cloud-Dienste zu ermöglichen.
- Erstellung verifizierbarer Audit-Trails, unterstützt durch automatisierte Berichte.