Bilder: DLR, CC-BY 3.0

SECURITY INFORMATION AND EVENT MANAGEMENT FÜR
AIRBUS DEFENCE AND SPACE

Sicherheitsvorfälle erkennen und Gegenmaßnahmen einleiten

ConSecur
[security and consulting]

Columbus Modul

An der internationalen Raumstation ISS ist die Europäische Weltraumagentur (ESA) mit dem Columbus Modul beteiligt. Das Columbus Modul ist ein Labor-Modul für wissenschaftliche und medizinische Experimente, mit denen verschiedene Fragestellungen wie das Verhalten biologischer Reaktionen oder des Organismus bei längerer Schwerelosigkeit untersucht werden. Wie verhält sich der Organismus bei längerer Schwerelosigkeit?

Airbus Defence and Space / ESA

Die Airbus Defence and Space ist Teil des Airbus-Konzerns und das führende Verteidigungs- und Raumfahrtunternehmen Europas. Airbus Defence and Space betreibt mit dem DLR Teile der IT-Infrastruktur des Columbus-Moduls auf der Internationalen Raumstation (ISS) für die European Space Agency (ESA). Die IT-Infrastruktur besteht aus einem Bodensegment und einem Flugsegment.

Internetverbindung zur Internationalen Raumstation (ISS)

Die Kommunikation mit den Computersystemen der ISS erfolgt über eine verschlüsselte Internetverbindung. Das Besondere an dieser Verbindung ist das Weltall, da diese stündlich für Minuten unterbrochen ist. Während dieser Zeit befindet sich die ISS auf ihrer Flugbahn im Orbit außerhalb der Reichweite der Internetverbindung.

IBM QRadar

IBM® QRadar® Security Information and Event Management (SIEM) unterstützt Sicherheitsteams bei der präzisen Erkennung und Priorisierung von Sicherheitsbedrohungen. Die Lösung liefert intelligente Erkenntnisse, auf deren Grundlage Teams schnell reagieren können, um die Auswirkungen von Sicherheitsvorfällen zu verringern. QRadar konsolidiert Protokollereignisse und Netzwerkflussdaten von Tausenden von Geräten, Endpunkten und Anwendungen des gesamten Netzwerks, korreliert alle diese unterschiedlichen Daten und fasst zusammengehörige Ereignisse in einzelnen Alerts zusammen, um die Analyse und Behebung von Sicherheitsvorfällen zu beschleunigen.

ConSecur

Die ConSecur GmbH entwickelt passgenaue IT-Sicherheitskonzepte und Lösungen zur Erkennung, Abwehr und Analyse von Cyberattacken. So werden Schlagworte wie Künstliche Intelligenz, Industrie 4.0 und Internet der Dinge (IOT) zum Mehrwert für unsere Kunden. Wir verbinden die persönliche Nähe eines mittelständischen Unternehmens mit dem Leistungsspektrum eines Konzerns. Die Kernkompetenzen der ConSecur GmbH sind „Information Security Management (ISMS)“ und „Security Information and Event Management (SIEM)“. In den ConSecur Cyber Defense Centern Meppen und Bochum steht unseren Kunden unser gesamtes Security Wissen zur Verfügung. Wir unterstützen unsere Kunden beim Aufbau eines Cyber Defense Centers (CDC) vor Ort oder stellen unsere qualifizierten IT-Sicherheitsanalysten zur Verfügung.

Projektskizze

Airbus Defence and Space ist im Rahmen des Betriebs der Internationalen Raumstation von der Europäischen Raumfahrtagentur mit der Implementierung eines Security Incident and Event Management-Systems beauftragt worden. Ziel ist es, die IT-Infrastruktur des Columbus Moduls der internationalen Raumstation ISS sowie des zugehörigen Bodensegments, auf das europaweit verschiedene nationale Raumfahrtagenturen, User Operations Support Center sowie europäische Partner zugreifen, zu überwachen.

Das zuständige Programm der Airbus Defence and Space hat die ConSecur GmbH mit der Konzeptionierung und Implementation eines solchen SIEM Systems für das ISS Programm betraut.

Mit dem Ergebnis nach Abschluss des Projektes fühlt sich Markus Brachmann, zuständiger Projektleiter der Airbus Defence and Space, in seiner Einschätzung bestätigt.

„Eine große Stärke ConSecurs ist der Aufbau und Betrieb von SIEM Systemen."

MARKUS BRACHMANN,
AIRBUS DEFENCE AND SPACE

„Wir haben für dieses Projekt einen Partner gesucht, der sein Projektmanagement auf unsere Struktur innerhalb der Europäischen Raumfahrorganisation abstimmt."

Ausgangssituation

Airbus Defence and Space betreibt für die European Space Agency (ESA) zusammen mit dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) und anderen europäischen Partnern die IT-Infrastruktur des Columbus Moduls auf der internationalen Raumstation ISS sowie Teile des Bodensegments. Die Projektpartner wollen die Kommunikation dieser IT-Infrastruktur, die aus einem Boden- und aus einem Flugsegment besteht, auf ein neues Sicherheitsniveau bringen. Das geplante aktive Security Monitoring wird ein Zusammenspiel von Maschine und Mensch sein: Sicherheitsvorfälle in der IT-Infrastruktur werden durch das SIEM als solche identifiziert und Gegenmaßnahmen vom Analysten-Team der SIEM-Mannschaft eingeleitet.

Die Entscheidung für ConSecur als externer Partner für Aufbau und Betrieb des geplanten SIEM, das auf IBM® QRadar® basiert, hat Airbus Defence and Space nach einem Auswahlverfahren aus Überzeugung getroffen.

„Wir haben für dieses Projekt einen Partner gesucht, der unsere Anforderungen versteht, und der sein Projektmanagement auf unsere Struktur innerhalb der Europäischen Raumfahrorganisation abstimmt", sagt Markus Brachmann. Über die konzeptionellen und technischen Herausforderungen hinaus bewertet Markus Brachmann insbesondere den permanenten Dialog mit allen beteiligten europäischen Partnern in der Projektvorbereitung sowie kurze Kommunikationswege in der Projektumsetzung als kritische Kernaufgabe.

Diese Flexibilität hat sich Markus Brachmann für dieses Projekt gewünscht.

„Was wir für dieses wichtige Projekt nicht wollten ist eine Lösung, die nach Auftragsabschluss unserer Auffassung nach buchstäblich über den Zaun gekippt wird."

Markus Brachmann,
AIRBUS DEFENCE AND SPACE

Projektdurchführung

In dem initiierenden Kickoff-Workshop am Airbus-Standort Bremen haben ConSecur und Airbus Defense and Space den Projektablauf visualisiert und für alle Aktionen konkrete Zeitabschnitte hinterlegt. Zum offiziellen Projektbeginn haben Airbus Defence and Space und ConSecur alle europäischen Partner nach Oberpfaffenhofen eingeladen, um an einem Tisch Projektziel und Projektablauf vorzustellen, eine gemeinsame Wissensgrundlage zu schaffen und um die Unterstützung der internen nationalen Administratoren zu werben.

„Uns ist klar gewesen, dass wir nur dann erfolgreich sein werden, wenn wir in diesem sensiblen Sicherheitsbereich schon im Vorfeld mögliche Unsicherheiten auflösen sowie nationale Interessen konsequent respektieren und für den Projekterfolg harmonisieren“, sagt Markus Brachmann rückblickend.

CHRISTOPH KRONABEL,
CONSECUR PROJEKTLEITER

Befugte Zugriffe von Anomalien unterscheiden

Das geplante SIEM soll befugte Zugriffe von Anomalien automatisch unterscheiden können. Diese Automatisierung basiert auf einem Regelwerk, in dem alle legitimen Zugänge aus den verschiedenen Logquellen der europäischen Partner hinterlegt und gleichzeitig Muster für Anomalien vordefiniert worden sind. Die Anbindung dieser Logquellen bezeichnet Markus Brachmann als „hohe koordinative Aufgabe“ und als ersten Meilenstein auf dem Weg zu einem effizienten Security Monitoring.

Zusammen mit Markus Brachmann hat ConSecur Projektleiter Christoph Kronabel Regeln für Anomalien definiert, hinter denen sich unbefugte Zugänge bzw. Angriffe auf die IT-Infrastruktur verbergen können.

Zu diesen Mustern zählen zum Beispiel Anmeldungen außerhalb der Bürozeiten oder Zugriffe aus Staaten, zu denen einzelne europäische Partner keine Beziehungen unterhalten. Ereignisse wie diese werden im operationellen Betrieb des SIEM automatisch eine Kette von Alarm-Reaktionen auslösen, die Security-Analysten alarmieren, die entsprechende Gegenmaßnahmen einleiten, um den versuchten Systemzugriff unterbinden.

Bilder: DLR, CC-BY 3.0

Fazit

In der Umsetzung ist es gelungen, auch alle externen Partner erfolgreich in das Regelwerk einzubinden. Die ESA gestattet verschiedenen europäischen Universitäten, zu Lehr- und Forschungszwecken gesicherten Zugriff auf das Netz der internationalen Raumstation.

Nach der erfolgreichen Projektumsetzung arbeiten Airbus Defence und Space und ConSecur an der nächsten Ausbaustufe. Die Zielsetzung ist, das implementierte SIEM in den operationellen Betrieb zu überführen, den Analysten aus den ConSecur-Cyber-Defense-Centern in Meppen und Bochum sicherstellen.

AIRBUS
DEFENCE & SPACE

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de

www.ConSecur.de