Sabotageaufklärung im Logistikunternehmen

Ziel

Aufklärung von konzertierter Abschaltung großer Logistikanlagen mit Schadenswert in Höhe eines dreistelligen Millionenbetrags.
Ein Projekt von Digital Forensics in Zusammenarbeit mit Rhebo.

Herausforderungen

Das Unternehmen Digital Forensics wurde als Dienstleister für Netzwerkanalyse von einem international tätigen Logistikunternehmen beauftragt, ungeklärte Stillstände in Logistikanlagen aufzuklären.

Dabei waren bei drei seiner Endkunden die Steuerungssysteme auf einen Schlag ausgefallen. Die Wiederherstellung des Normalbetriebs dauerte mehrere Stunden bis Tage. Bei den Endkunden kam es dadurch zu hohen Konventionalstrafen sowie Wiederherstellungskosten im dreistelligen Millionenbereich. Da das Logistikunternehmen als Systemlieferant die Steuerungssysteme verantwortete, musste es diese Kosten tragen.

Eine erste Analyse konnte keine Fehler in der Anlagensoftware feststellen. Jedoch fielen für den entsprechenden Zeitraum aktive Fernwartungszugänge mit Kommunikation über das Protokoll VNC auf – ein Hinweis auf eine potentielle Sabotage der Anlagen.

Lösung

Digital Forensics entschied sich aufgrund des Anfangsverdachts auf Sabotage für ein Langzeitmonitoring der Steuerungskommunikation des Logistikunternehmens. Der Analysedienstleister integrierte die industrielle Anomalieerkennung Rhebo Industrial Protector im Netzwerk des Logistikunternehmens und analysierte fortlaufend und rückwirkungsfrei die gesamte Kommunikation innerhalb der Steuerungstechnik.

Rhebo Industrial Protector erkennt und meldet in Echtzeit jegliche Ereignisse im Netzwerk, die zu Störungen der Anlagen führen können. Solche Anomalien umfassen sowohl Sicherheitsvorfälle als auch technische Störungen, wie sie im Alltagsbetrieb industrieller Anlagen auftreten. Rhebo Industrial Protector unterstützt die Reduktion von Ausfallrisiken, die Erhöhung der Gesamtanlageneffektivität und damit die Sicherung der Anlagenverfügbarkeit.

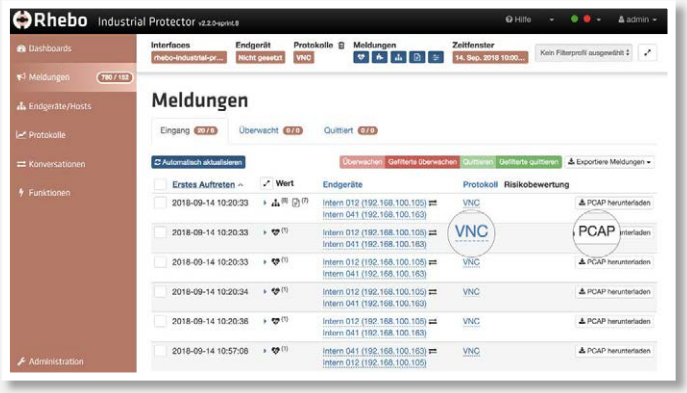
»Sabotage aus den eigenen Reihen ist nur sehr schwer nachweisbar, weil die Vorgänge innerhalb der gesicherten Zonen stattfinden. Mit Rhebo Industrial Protector konnten wir den Blick in die Steuerungstechnik öffnen und jeden Kommunikationsvorgang überwachen. Die Speicherung aller Anomaliedetails ermöglichte uns die sehr genaue Analyse und Rückverfolgbarkeit zur Workstation. Unser Kunde konnte mit den Ergebnissen gezielt an der Optimierung seiner Netzwerksicherheit arbeiten und das Risiko zukünftiger Sabotageakte – intern und extern – stark reduzieren.«

Dr. Jens Pittler, Technischer Leiter Digital Forensics

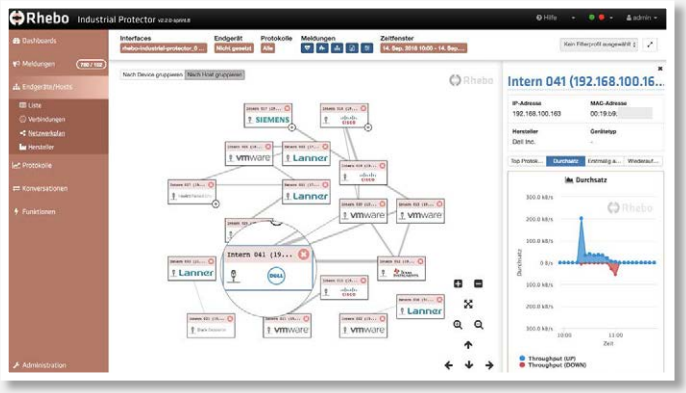
DIGITAL FORENSICS

Analyse

Nach mehreren Monaten kontinuierlicher Überwachung meldete Rhebo Industrial Protector ungewöhnliche Kommunikationsvorgänge an den verdächtigen Fernwartungszugängen. Die Vorgänge wurden mit allen Details als PCAP gespeichert und konnten durch Digital Forensics umgehend ausgewertet werden. Die Analyse zeigte, dass über eine interne Unternehmensworkstation »Shutdown«-Befehle an die Endkunden gesendet wurden. Aufgrund der Echtzeitmeldung der Vorgänge wurde die erneute Sabotagehandlung gestoppt, bevor die Endkundenanlagen betroffen waren.



Für den Fernwartungszugang untypische Kommunikation über VNC wird in Echtzeit gemeldet und als PCAP gespeichert (Quelle: Digital Forensics)



In der Netzwerkkarte wird eine interne Workstation als Ausgangspunkt identifiziert (Quelle: Digital Forensics)

Nutzen

Die für die Sabotage genutzte Workstation wurde eindeutig identifiziert. Problematisch war, dass zu diesem Zeitpunkt mehrere Hundert Personen über ein universelles Passwort Zugriff auf die Workstation hatten. Die Identifizierung des Täters war somit nicht möglich. Im Konzern wurden deshalb organisatorische und technische Maßnahmen definiert und umgesetzt, um eine Wiederholung solcher Vorfälle zu vermeiden. Dazu gehörten u.a. personalisierte Zugänge mit individuellen Passwörtern, strikte Sicherheitsrichtlinien für die Fernwartung und unternehmensweite Schulungen zur Cybersicherheit.

- CYBERSICHERHEIT
- FESTIGUNG DER SYSTEMSICHERHEIT
- ANLAGENVERFÜGBARKEIT
- VERTRAUEN BEIM KUNDEN
- SCHADENSABWENDUNG
- GERICHTSFESTE BEWEISE ÜBER SABOTAGE

Über Digital Forensics

Digital Forensics GmbH ist ein Leipziger Unternehmen mit Spezialisierung auf die forensische Analyse großvolumigen Netzwerkverkehrs in Industrie und Versicherungswirtschaft. Das Unternehmen evaluiert unter anderem Schadensfälle und analysiert Cyberangriffe. Kenntnisse industriespezifischer Protokolle wie Profinet, OPC, S7 oder IEC61850 sowie deren gezielte Auswertung bilden dabei einen Schwerpunkt der Arbeit.

Über Rhebo

Rhebo ist ein deutsches Unternehmen, das sich auf die Ausfall- und Störungssicherheit von Industrieunternehmen und Kritischen Infrastrukturen spezialisiert hat. Mit seinen Lösungen und Dienstleistungen überwacht und analysiert Rhebo die Datenkommunikation innerhalb der Steuerungstechnik, meldet Anomalien in Echtzeit und steigert so die Cybersicherheit und Produktivität von Industrial Control Systems und Leitsystemen. Rhebo ist einer der 30 Top-Anbieter für die industrielle Sicherheit in Gartners »Marktführer für betriebstechnische Sicherheit 2017«. Rhebo ist Mitglied im Teletrust – Bundesverband IT-Sicherheit e.V. sowie im Bitkom e.V.