Rhebo Industrial Network Continuity SUCCESS STORY

Sabotage investigation in logistics company

Aim

Investigation of concerted shutdown of large logistics facilities worth a triple-digit million euro loss.
A project of Digital Forensics in cooperation with Rhebo.

Challenges

The network analysis service provider Digital Forensics was assigned by an international logistics company to investigate unresolved shutdowns in several logistics systems.

At three of its end customers, the logistics control systems had failed in one single stroke. Restoring normal operation took several hours to days. This resulted in contractual penalties and recovery costs for the end customers in the three-digit million range. Since the logistics company was also provider of the control systems, it had to cover these downtime costs.

An initial analysis did not reveal any errors in the system software. However, active remote maintenance accesses with communication via the protocol VNC were found for the corresponding period – an indication of potential sabotage of the systems.

Solution

Based on initial indications of sabotage, Digital Forensics opted for long-term monitoring of the logistics company's control communication. The analysis service provider integrated the industrial anomaly detection Rhebo Industrial Protector into the logistics company's network to continuously analyze all communication within the Industrial Control System.

Rhebo Industrial Protector detects and reports in real-time any events in the network that could lead to plant disruption.

Such anomalies include both security incidents and technical malfunctions that occur in the daily operation of industrial plants. Rhebo Industrial Protector supports the reduction of downtime risk, increases overall equipment effectiveness and thus ensures plant availability.

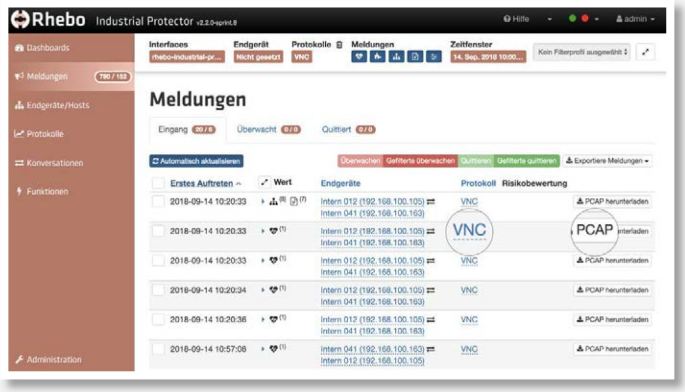
»Sabotage from in-house sources is very difficult to detect because the processes take place within the secured zones. With Rhebo Industrial Protector, we were able to open up a view into the control system and monitor every communication process. The storage of all anomaly details enabled us to perform a very accurate analysis and trace the incident to a particular workstation. With the results, our customer was able to work specifically on optimizing his network security and greatly reduce the risk of future acts of sabotage – internally and externally.«

Dr. Jens Pittler, Technical Director Digital Forensics

DIGITAL FORENSICS

Analysis

After several months of continuous monitoring, Rhebo Industrial Protector reported unusual communication at the suspicious remote access points. The events were recorded with all details as PCAP and were immediately evaluated by Digital Forensics. The analysis showed that »shutdown« commands were sent to the end customers from an internal corporate workstation. Due to the real-time notification of the events, the repeated sabotage action was stopped before the end customer facilities were affected.



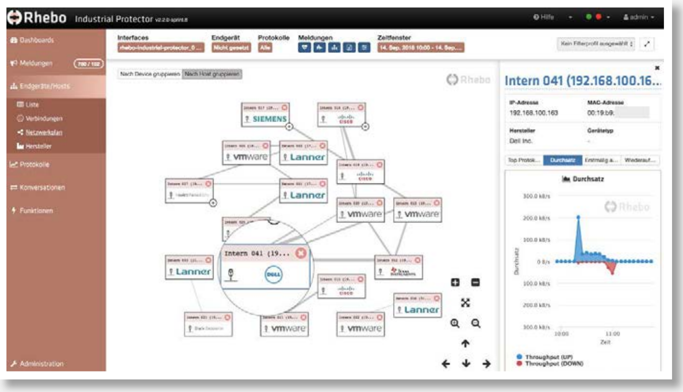
Interfaces	Endgerät	Protokolle	Zeitfenster
rhebo-industrial-pr...	Nicht gesetzt	VNC	14. Sep. 2018 10:00...

Meldungen

Eingang 20 / 6 | Überwacht 0 / 0 | Quittiert 0 / 0

Erstes Auftreten	Wert	Endgeräte	Protokoll	Risikobewertung
2018-09-14 10:20:33	(8) (7)	Intern 012 (192.168.100.105) ⇄ Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
2018-09-14 10:20:33	(1)	Intern 012 (192.168.100.105) ⇄ Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
2018-09-14 10:20:33	(1)	Intern 012 (192.168.100.105) ⇄ Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
2018-09-14 10:20:34	(1)	Intern 012 (192.168.100.105) ⇄ Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
2018-09-14 10:20:36	(1)	Intern 012 (192.168.100.105) ⇄ Intern 041 (192.168.100.163)	VNC	PCAP herunterladen
2018-09-14 10:57:06	(1)	Intern 041 (192.168.100.163) ⇄ Intern 012 (192.168.100.105)	VNC	PCAP herunterladen

Atypical VNC communication via remote maintenance access is reported and documented in real-time (Source: Digital Forensics).



Interfaces	Endgerät	Protokolle	Zeitfenster
rhebo-industrial-protector_0 ...	Nicht gesetzt	Alle	14. Sep. 2018 10:00 - 14. Sep....

Intern 041 (192.168.100.16...

IP-Adresse	MAC-Adresse
192.168.100.163	00:19:b9:
Hersteller	**Gerätetyp**
Dell Inc.	-

The network map identifies a specific workstation as the origin (Source: Digital Forensics).

Benefits

The workstation used for the sabotage was clearly identified. Though at that time several hundred people had access to the workstation via a universal password. It was therefore not possible to identify the attacker. For this reason, organizational and technical measures were defined and implemented in the group to avoid a repetition of such incidents. These included personalized access with individual passwords, strict security guidelines for remote maintenance and company-wide training on cyber security.

- ✓ CYBERSECURITY
- ✓ CONSOLIDATION OF SYSTEM SECURITY
- ✓ PLANT AVAILABILITY
- ✓ CUSTOMER TRUST
- ✓ DAMAGE AVOIDANCE
- ✓ COURT EVIDENCE OF SABOTAGE

About Digital Forensics

Digital Forensics GmbH is a german company specializing in forensic analysis of large-volume network traffic in industry and insurance. The company evaluates cases of damage and analyses cyber attacks. Knowledge of industry-specific protocols such as Profinet, OPC, S7 or IEC61850 as well as their evaluation form a focal point of the work.

About Rhebo

Rhebo is a german technology company specializing in the reliability of Industrial Control Systems and critical infrastructures by means of detailed monitoring of data communication within the industrial network. IT market analyst Gartner Inc. named Rhebo as the only German manufacturer of an industrial anomaly detection among the top 30 suppliers in the international »Market Guide for Operational Technology Security 2017«. The company is a member of Teletrust – IT Security Association Germany.