ҚазМұнайГаз
ПАВЛОДАР МҰНАЙ-ХИМИЯ ЗАУЫТЫ

Kaspersky implements industrial cybersecurity project at Pavlodar Oil Refinery

kaspersky

Kaspersky Industrial CyberSecurity

Pavlodar Oil Refinery

https://www.pnhz.kz/en/

Oil refinery

- Commissioned in 1978
- Part of the JSC NC KazMunayGas group
- Processing capacity of 5.1 million tons of oil a year

Pavlodar Oil Chemistry Refinery (POCR LLP) is the largest enterprise in the northeast of Kazakhstan for oil refining and production of oil products.

Pavlodar Oil Chemical Refinery (POCR LLP) is one of the three main oil industry enterprises in the Republic of Kazakhstan.

POCR manufactures a wide range of petroleum products, including motor gasolines of various octane ratings, diesel, fuel oil (mazut), hydrocarbon gas liquids, vacuum gas oil, commercial sulfur, various grades of bitumen (construction, paving, roofing) and petroleum coke.

The priorities for POCR today are to produce motor fuels that meet the K4 and K5 emission standards in sufficient quantities to satisfy the country's needs, upgrade the plant's technical operating life, introduce a two-year overhaul cycle, and begin producing aviation fuel to Jet A standard – that is opening new opportunities to the plant.

Challenge

Security of industrial facilities is a major talking point in Kazakhstan. In the second half of 2016, the country ranked 7th in the world for the number of industrial computers attacked.

One of the top priorities for POCR operations is to ensure industrial cybersecurity and improve the safety of enterprise automation.

Increasing the level of automation and the active adoption of IT into the industrial infrastructure raises the risks of cyberattacks against industrial facilities.

Security of industrial facilities is currently one of the most hotly discussed topics in Kazakhstan. This is hardly surprising: according to the Kaspersky ICS CERT report, in the second half of 2016 Kazakhstan ranked seventh in the world for the number of industrial computers attacked. In the first half of 2017, 45.9% of all industrial automation systems in Kazakhstan were targeted by attacks.

The plant therefore faced the necessity of ensuring the sufficient industrial security against cyberthreats.

Security

Monitoring the commands of programmable logic controllers (PLC) protects against cyberattacks that target key industrial control system assets.

Integrity control

Detection of unauthorized devices and connections helps ensure the integrity of the industrial network.

Risk management

Implementation of a specialized industrial cybersecurity solution helps enhance a risk management system on industrial enterprise.

The Kaspersky solution

POCR chose Kaspersky Industrial CyberSecurity – a portfolio of technologies and services designed to secure industrial layers and elements of organization – including SCADA servers, HMIs, engineering workstations, PLCs and network connections.

To ensure the cybersecurity of its infrastructure, POCR chose not only the endpoint security solution from the Kaspersky Industrial CyberSecurity portfolio but also protection on the industrial network level as well as training for employees. Such a comprehensive approach helps ensure continuity and stability of industrial processes.

Kaspersky Industrial CyberSecurity is specifically designed to protect critical infrastructures and industrial facilities. The solution uses a broad range of technologies to counter threats, including protection from malware, whitelisting and detection of anomalies in industrial network communications. It also controls device access, so clients can control connections to removable data storage devices and peripheral devices.

“The day-to-day business protection capabilities provided by Kaspersky have been complemented with technologies developed specifically for industrial environments, such as integrity checks and semantic monitoring of process management commands. Kaspersky Industrial CyberSecurity can also work in a special monitoring mode that detects cyberattacks, operational errors by employees and anomalies in industrial networks,” says Tatyana Pyatina, Kaspersky’s Head of Business Development in Kazakhstan.

"Kaspersky's task was to ensure the cybersecurity of industrial computers and the SCADA servers, as well as provide a tool to control the core parameters of the industrial processes. The solution was also to have no impact on the industrial process and require no changes to the SCADA configuration. This was accomplished in full by Kaspersky"

Semyon Tikhonenko,
Chief Information Security specialist at POCR

Results

Implementation of solutions from the Kaspersky Industrial CyberSecurity portfolio by Kaspersky experts in conjunction with suited security training has helped build a systematic approach at POCR to ensuring industrial cybersecurity, and provided reliable protection against cyberthreats.

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure operational technology layers and elements of your organization - including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers - without impacting on operational continuity and the consistency of industrial process.

Learn more at www.kaspersky.com/ics

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com
Cyber Threats News:
www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com

2019 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.

IIC MEMBER
industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

* World Leading Internet Scientific and Technological Achievement Award at the 3rd World Internet Conference

** China International Industry Fair (CIIF) 2016 special prize