КазМұнайТеңіз
ТЕҢІЗ МҰНАЙ КОМПАНИЯСЫ OFFSHORE OIL COMPANY

Kaspersky ups the level of industrial cybersecurity at KazMunayTeniz

kaspersky

Kaspersky Industrial CyberSecurity

KazMunayTeniz

http://www.kazmunayteniz.kz/en/

Oil and Gas

- Founded in 2003
- Office in Aktau, Kazakhstan
- Part of the JSC NC KazMunayGas group
- Specializes in offshore oil and gas production

KazMunayTeniz is the leading offshore oil and gas company in the Caspian region, effectively managing offshore oil and gas projects.

KazMunayTeniz is a subsidiary of Kazakhstan's national oil company KazMunayGas and specializes in the exploration and production of raw hydrocarbons in offshore and coastal areas of the Caspian and Aral Seas.

The company's main objective is to perform the functions of a contractor in offshore subsurface projects, as well as effective and rational development of oil and gas resources in the Republic of Kazakhstan to ensure their preservation and growth.

KazMunayTeniz's portfolio includes joint projects with companies such as LUKOIL, Repsol, Rosneft, Shell, and Oman Oil.

Challenge

Security of industrial facilities is one of the most hotly discussed topics in Kazakhstan. In the second half of 2016, the country ranked 7th in the world for the number of industrial computers attacked.

The top priority for KazMunayTeniz when implementing offshore projects is to ensure industrial and environmental safety. All oil-related operations are conducted in strict accordance with Kazakhstan's labor and environmental protection laws and go hand in hand with measures to minimize and prevent possible emergencies.

KazMunayTeniz is committed to ensuring cybersecurity as well. Protection of industrial facilities is currently one of the most widely discussed topics in Kazakhstan, and for good reason: 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 industrial automation systems in Kazakhstan were attacked.

"As a country that is still, to a great extent, borrowing advanced IT technologies, including technologies to ensure cybersecurity, Kazakhstan could at any time find itself the subject of an experiment or real attacks by criminal organizations or individuals with unpredictable results for the country's critical infrastructure," according to the program of the state cybersecurity project "Cyber shield of Kazakhstan".

To prevent cyber-incidents and their negative impact on both the environment and business, KazMunayTeniz decided to increase employee awareness in the areas of industrial cybersecurity and the current threat landscape.

Necessary knowledge
The increasing number of cyber-incidents affecting industrial automation systems has resulted in a growing demand for greater employee awareness about industrial cybersecurity.

Effective education
Kaspersky Industrial CyberSecurity trainings allow participants to gain solid skills in effective cybersecurity for industrial environments within a short period of time.

Foundations for development
The Kaspersky Industrial CyberSecurity portfolio lays the foundations for a systematic approach to ensuring industrial cybersecurity at an enterprise.

The Kaspersky solution

KazMunayTeniz employees were the first in Kazakhstan to attend the Industrial Cybersecurity in Practice training program conducted by Kaspersky experts.

“Taking Kaspersky’s training course was a crucial and timely step, considering the current situation surrounding critical infrastructure protection in Kazakhstan,” said Nurlan Kulyshev, IT specialist at KazMunayTeniz.

Kaspersky conducted a two-day training course from the Kaspersky Industrial CyberSecurity portfolio for KazMunayTeniz employees, with a focus on oil industry specifics. During the sessions, Kaspersky experts described the current threat landscape and the latest methods for combating attacks that target industrial environments.

A demonstration of possible attacks on real controllers, conducted during the course, gave participants a clear insight into the danger of cyber-incidents, as well as the necessary practical advice on how to avoid such situations during the implementation of industrial processes.

During training, the participants received all the necessary skills to draw up their own incident response plan, as well as an understanding of how malware analysis and a simple digital forensics are conducted.

The employees of KazMunayTeniz evaluated the training as “effective, informative and extremely useful”.

> “Taking Kaspersky’s training course was a crucial and timely step, considering the current situation surrounding critical infrastructure protection in Kazakhstan”,”

Nurlan Kulyshev,
IT specialist at KazMunayTeniz.

Perspective

Kaspersky’s Industrial Cybersecurity in Practice training course, conducted by the company’s experts, has laid the foundations for a systematic approach to ensuring industrial cybersecurity at KazMunayTeniz.

Tatyana Pyatina, who is responsible for the development of Kaspersky’s business in Kazakhstan, described the training of KazMunayTeniz employees as an example of a successful project in the region’s oil and gas sector and a strong start for the further development of partnership relations.

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

#Kaspersky
#BringontheFuture

www.kaspersky.com

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