KazMunayTeniz
産業用サイバーセキュリティを強化

КазМұнайТеңіз

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

KazMunayTeniz

KazMunayTeniz はカスピ海地域で海洋油田およびガス田を開発する代表的企業であり、
海洋油田およびガス田のプロジェクトを効果的に管理しています。

石油ガス開発企業

- 設立 - 2003 年
- オフィス所在地 - カザフスタン、アクタウ
- 所属 - JSC NC KazMunayGas グループ
- 専門 - 海洋油田およびガス田の生産

KazMunayTeniz は、カザフスタンの石油関連の国営企業である KazMunayGas の子会社であり、カスピ海とアラル海の沖合および沿岸部で石油ガス原料の探査と生産を専門に行っています。

同社の主な目的は、沖合水面下プロジェクトにおける請負業者の役割を果たすこと、およびカザフスタン共和国での石油ガス資源の効果的かつ合理的な開発によって、これらの資源を保護し、増やしていくことです。

KazMunayTeniz が扱うプロジェクトには、LUKOIL、Repsol、Rosneft、Shell、Oman Oil などの企業との合同プロジェクトが含まれています。

課題

海洋プロジェクトを進める際に KazMunayTeniz が最も優先することは、産業および環境の安全を確保することです。石油関連の業務はすべて、カザフスタンの労働保護法および環境保護法に厳格に従って実施され、起こりうる緊急事態を最小限に抑えて防止するための対策を常に講じています。

KazMunayTeniz はサイバーセキュリティの確保についても懸命に取り組んでいます。産業用設備の保護は、カザフスタンで現在最も広範に議論されている話題の 1 つであり、それには正当な理由があります。カスペルスキーの ICS CERT レポートによれば、カザフスタンは、2016 年に WannaCry の影響を受けた企業数の国別ランキングにおいて世界で 6 番目となり、2017 年の前半には、カザフスタンの産業用オートメーションシステムの 45.9% が攻撃を受けました。

産業用設備のセキュリティは、カザフスタンで最もよく議論されている話題の 1 つです。カザフスタンは、2016 年に WannaCry の影響を受けた企業数の国別ランキングにおいて、世界で 6 番目となりました。

「カザフスタンは、いまだ大部分で、サイバーセキュリティを確保するための技術を含む高度な IT 技術を外部から借りている状態にあり、いつ犯罪組織や個人の犯罪者による実験的攻撃、あるいは実際の攻撃の対象になってもおかしくありません。そうなれば、この国の重要インフラで予測不可能な事態が発生する可能性もあります」と、国家サイバーセキュリティプロジェクト「Cyber shield of Kazakhstan」のプログラムに記載されています。

サイバーインシデントと、それによる環境および事業への悪影響を防止するために、KazMunayTeniz は、産業用サイバーセキュリティおよび現在の脅威の状況についての従業員意識を高めることに決めました。

必要な知識
産業用オートメーションシステムに影響を及ぼすサイバーインシデントが増加し、その結果、産業用サイバーセキュリティについての従業員意識の向上がますます求められるようになっています。

効果的な教育
Kaspersky Industrial CyberSecurity トレーニングによって、産業界の効果的なサイバーセキュリティについての確かなスキルを短期間で習得することができます。

育成のための基礎
Kaspersky Industrial CyberSecurity ポートフォリオは、エンタープライズにおいて産業用サイバーセキュリティを確保するための体系的なアプローチの基礎を築きます。

Kaspersky Lab のソリューション

KazMunayTeniz の従業員は、Kaspersky Lab のエキスパートが実施する「Industrial Cybersecurity in Practice」トレーニングプログラムに、カザフスタンで初めて参加しました。

「Kaspersky Lab のトレーニングコースへの参加は、カザフスタンの重要なインフラストラクチャの保護を取り巻く現在の状況を考えれば、極めて重大でタイムリーな第一歩でした」と、KazMunayTeniz の IT スペシャリストである Nurlan Kulyshev 氏は言います。

Kaspersky Lab は KazMunayTeniz 従業員向けに、Kaspersky Industrial CyberSecurity ポートフォリオにある 2 日間のトレーニングコースを、石油業界特有の詳細事項に焦点を当てて実施しました。セッションでは、Kaspersky Lab のエキスパートが現在の脅威の状況、および産業界を標的としている攻撃に対抗するための最新の手法について説明しました。

コースの中で、実際の制御装置に対して起こりうる攻撃のデモを行うことで、参加者はサイバーインシデントの危険性を明確に理解しました。また、産業プロセスを進める中でそのような事態になるのを防止する方法について、必要な実践的アドバイスを受けました。

トレーニングでは、独自のインシデント対応計画を策定するために必要なあらゆるスキルを習得するのと同時に、マルウェア分析や基礎的なデジタルフォレンジックの実行方法について理解しました。

KazMunayTeniz の従業員はこのトレーニングについて、「効果的で、参考になり、極めて有効なものだ」と評価しています。

「Kaspersky Lab のトレーニングコースへの参加は、カザフスタンの重要インフラストラクチャの保護を取り巻く現在の状況を考えれば、極めて重要でタイムリーな第一歩でした」

Nurlan Kulyshev 氏、
IT スペシャリスト、KazMunayTeniz

今後の展望

Kaspersky Lab のエキスパートが実施する Kaspersky Lab の「Industrial Cybersecurity in Practice」トレーニングコースは、KazMunayTeniz で産業用サイバーセキュリティを確保するための体系的なアプローチの基礎を築いています。

カザフスタンの Kaspersky Lab 事業開発の責任者である Tatyana Pyatina は、KazMunayTeniz 従業員へのトレーニングはこの地域の石油ガス業界において成功したプロジェクトの一例であり、今後パートナーシップ関係を築いていくための良いスタート地点になると述べました。

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity は、産業界の運用技術の各層および各要素（SCADA サーバー、HMI 、エンジニアリング用ワークステーション、PLC、ネットワーク接続および産業プロセスなど）を保護するよう設計された技術とサービスのポートフォリオであり、事業継続性や産業プロセスの一貫性に影響を及ぼさないよう設計されています。
詳細は、www.kaspersky.co.jp/enterprise-security/industrial をご確認ください。

産業界のサイバー脅威に関する最新情報：https://ics-cert.kaspersky.com
サイバー脅威に関する最新情報：www.securelist.com

#truecybersecurity

www.kaspersky.co.jp