Kaspersky for Business

KASPERSKY lab

Kaspersky Lab、Pavlodar Oil Refinery で産業用サイバーセキュリティプロジェクトを実施

ҚазМұнайГаз
ПАВЛОДАР МҰНАЙ-ХИМИЯ ЗАУЫТЫ

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

Pavlodar Oil Refinery

Pavlodar Oil Chemistry Refinery（POCR LLP）は、カザフスタン北東部最大規模の石油精製・石油製品製造会社です。

石油精製

- 1978 年設立
- JSC NC KazMunayGas グループ所属
- 年間 510 万トンの石油処理能力

Pavlodar Oil Chemical Refinery（POCR LLP）は、カザフスタン共和国の三大石油会社のうちの 1 社です。

POCR は、各種オクタン価の自動車用ガソリン、ディーゼル、燃料油（残渣油）、液体炭化水素ガス、減圧軽油、商用硫黄、各種グレードの歴青（建築用、舗装用、屋根用）、石油コークスなど、幅広い石油製品を製造しています。

現在の POCR の優先課題は、同国のニーズを満たすほどの十分な容量の、K4 および K5 排出基準に従った自動車用燃料を製造すること、プラントの技術的な動作寿命を延ばすこと、2 年間の総点検サイクルを導入すること、および Jet A 基準に沿った航空機燃料を製造することです。これらは、このプラントにとって新しい機会となるものです。

課題

POCR の業務における最優先課題の 1 つは、産業用サイバーセキュリティの確保と、エンタープライズオートメーションの安全性の向上です。

オートメーションのレベルを引き上げ、産業用インフラストラクチャに IT を積極的に導入すれば、産業用設備に対するサイバー攻撃のリスクが上昇します。

産業用設備のセキュリティは、カザフスタンで大きな話題となっています。同国は 2016 年後半に、攻撃を受けた産業用コンピューターの台数において世界第 7 位となったからです。

産業用設備のセキュリティは、現在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。これは驚くほどのことではありません。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 年後半に、攻撃を受けた産業用コンピューターの台数において世界第 7 位になりました。また、2017 年前半には、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% が攻撃の標的となりました。

そのため、同プラントは、サイバー脅威に対する十分な産業用セキュリティを確保する必要性に迫られていました。

セキュリティ

プログラマブルロジックコントローラー（PLC）のコマンドを監視することで、重要な産業用制御システムを標的としたサイバー攻撃から保護します。

整合性管理

不正な端末や接続の検知によって、産業用ネットワークの整合性を確保します。

リスク管理

産業用サイバーセキュリティソリューションの導入によって、産業に特化したエンタープライズのリスク管理システムを強化します。

Kaspersky Lab のソリューション

POCR が選択したのは、Kaspersky Industrial CyberSecurity です。この製品は、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す。

インフラストラクチャのサイバーセキュリティを確保するために、POCR は、Kaspersky Industrial CyberSecurity ポートフォリオのエンドポイントセキュリティソリューションに加えて、産業用ネットワークレベルでの保護を導入し、従業員向けトレーニングも導入しました。このような組織全体でのアプローチは、産業プロセスの継続性と安定性につながります。

Kaspersky Industrial CyberSecurity は、重要インフラや産業用設備を保護するように特別に設計されています。このソリューションは、マルウェアからの保護、ホワイトリスト、産業用ネットワーク通信における異常の検知など、幅広い技術を組み合わせて脅威に対抗します。また、端末における周辺機器へのアクセスを制御して、お客様がデータ保管用のリムーバブルデバイスや各種周辺機器との接続を管理できるようにします。

Kaspersky Lab のカザフスタンでの事業開発責任者である Tatyana Pyatina は「カスペルスキーが提供する日常業務の保護機能を補完する形で、整合性チェックやプロセス管理コマンドのセマンティックモニタリングなど、産業用環境向けに特別に開発された技術が利用されています。Kaspersky Industrial CyberSecurity は、サイバー攻撃、従業員による運用上のエラーなどの産業用ネットワーク内の異常を検知する、特殊な監視モードで動作します」と述べました。

「Kaspersky Lab の仕事は、産業用コンピューターおよび SCADA サーバーのサイバーセキュリティを確保すること、および産業プロセスの中心的なパラメータを制御するためのツールを提供することでした。また、このソリューションには、産業プロセスにまったく影響を及ぼさないこと、および SCADA 構成の変更を必要としないことも求められました。Kaspersky Lab はこれらの要件を完遂しました」

Semyon Tikhonenko 氏
最高情報セキュリティスペシャリスト、POCR

結果

Kaspersky Lab のエキスパートが Kaspersky Industrial CyberSecurity ポートフォリオのソリューションを実装し、さらに状況に適したセキュリティトレーニングを実施したことで、産業用サイバーセキュリティ確保ための体系的なアプローチを実現する体制を POCR が確立し、サイバー脅威に対する信頼できる保護を実現しました。

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity は、産業組織の運用技術の各層および各要素（SCADA サーバー、HMI パネル、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。詳細については、以下をご覧ください。
www.kaspersky.co.jp/enterprise-security/industrial

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

© 2018 AO Kaspersky Lab.All rights reserved.登録商標およびサービスマークは、それぞれの所有者に属しています。