産業向けサイバーセキュリティにより セキュリティのギャップを解消

Plzeňský Prazdroj

https://www.prazdroj.cz/en/

Plzeňský Prazdroj 社

ビール会社

- 1842 年に設立
- プルゼニ（ピルゼン）、チェコ共和国
- 3 つの醸造所と 13 の配送センターに 2,000 人未満の従業員
- ピルゼン工場に 8 つのパッケージングライン

Plzeňský Prazdroj 社は、1842 年に設立され、チェコ共和国のプルゼニに本拠地を置くチェコのビール会社です。

Plzeňský Prazdroj 社は、Pilsner Urquell（ピルスナー・ウルケル）というブランドのピルスナーブロンドラガースタイルのビールを初めて生産したビール会社であり、現在世界で生産されているビールの 3 分の 2 以上は、このビールが原型となっています。それらのビールは、pils、pilsner、pilsener（ピルス、ピルスナー、ピルゼナー）などと呼ばれています。Plzeňský Prazdroj も Pilsner Urquell もいずれも大まかに訳すと「ピルゼンの水源」あるいは「ピルスナーの発生源」という意味になります。

Plzeňský Prazdroj 社は中央ヨーロッパ有数のビール会社です。そのブランドを通じて、Plzeňský Prazdroj 社はチェコ市場でどの企業よりも多くのビールを販売しています。1999 年から、同社は SABMiller グループ会社（当時は South African Breweries 社）の一部となりました。Anheuser-Busch InBev 社が 2016 年 10 月に SABMiller 社を買収することが許可される前に、規制当局と交わされた合意の一環として、Pilsner Urquell ブランドは（一部の地域を除く）2017 年 3 月 31 日にアサヒグループホールディングスに売却されました。

「当社の強いニーズは、予期しないあらゆるインシデントに備えること、世界有数のサイバーセキュリティ専門家によって、当社の OT インフラストラクチャを調査してもらい、産業ネットワークを保護するための導入計画を確立することにありました」

ヤン・シク氏（Jan Šik）、チーフエンジニア、Plzeňský Prazdroj 社

課題

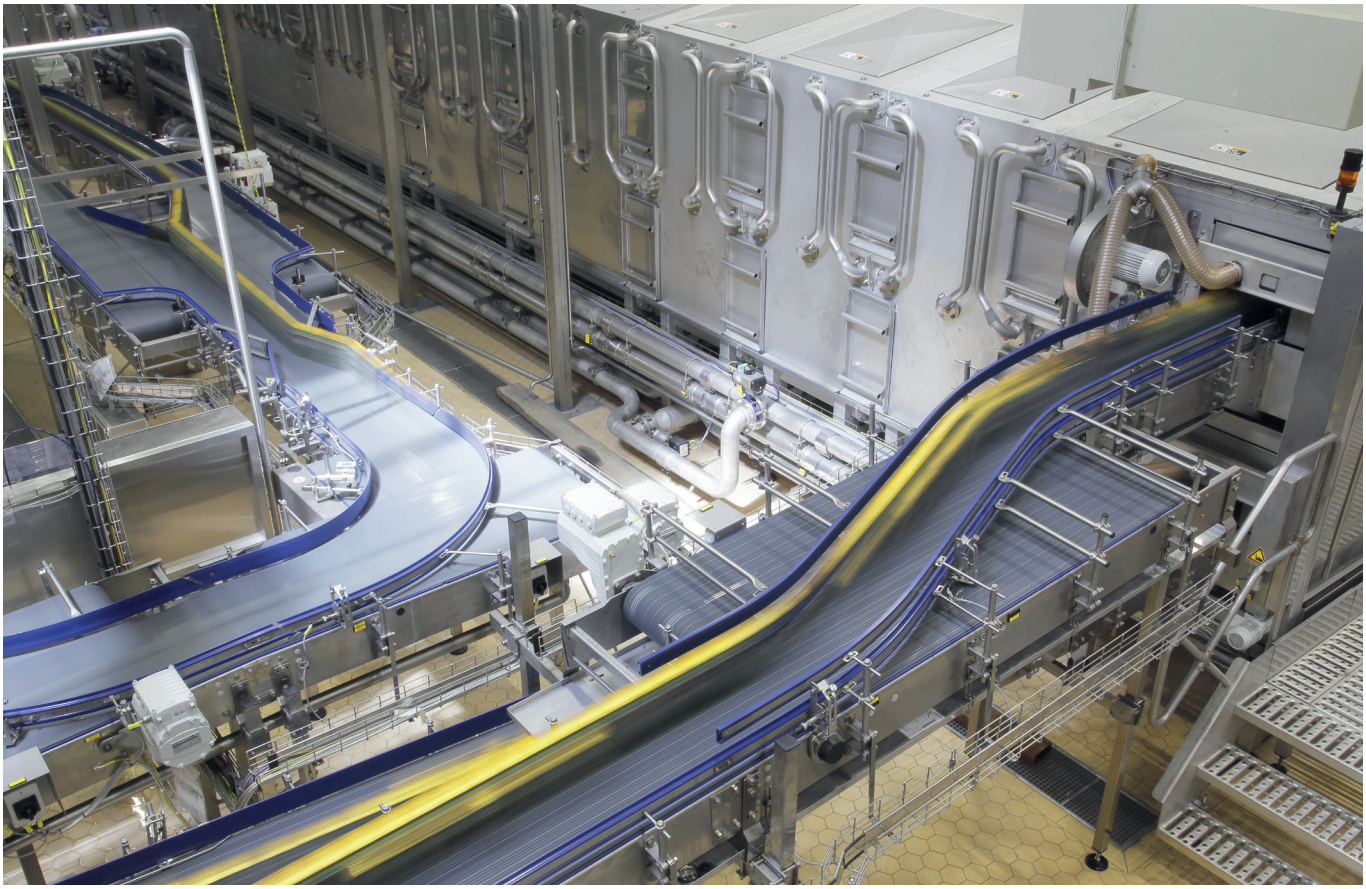
大規模な製造企業として、Plzeňský Prazdroj 社は IT と OT のサイバーセキュリティを非常に深刻に受け止めています。同社でいくつかの監査が実施され、興味深い調査結果が出されました。Plzeňský Prazdroj 社での技術開発が継続的なプロセスとなってすぐに、別の新しい評価を行う必要が生じました。

当時、同社は、標準の PC 群で実行されている個々のシステムから、すべてのシステムとデバイスを接続する仮想化サーバーベースのマスターシステムへと技術的なバックグラウンドを移行していました。

同社がサイバーセキュリティアセスメント（CSA）を行うことにした第一の動機は、製造システムの仮想化と、メインの OT ネットワークコンポーネントのアップグレードを含むプロジェクトの最終段階でインフラストラクチャを確認することにありました。第二の要因は、エンドポイントのセキュリティソリューションを重視した将来のプロジェクトに備えて主要トピックと要件を見据えて、標的型サイバー攻撃を受けた場合、または密接に関連する会社への攻撃によって「二次的な攻撃」を受けてしまった場合に、Plzeňský Prazdroj 社のすべての製造工場が影響を受けないようにするためでした。

産業向け CSA プロジェクトの目標は、製造ラインとすべての OT 関連ソフトウェアおよびハードウェアがサイバー攻撃に耐えられるようにすること、また同社が包括的な産業向けサイバーセキュリティの戦略を導入する準備を整えることでした。

CSA の実施前に、産業向けサイバーセキュリティのポリシーで最も困難なだった面は、OT インフラストラクチャの複雑さ（醸造とボトル詰めの 2 つの工程でまったく異なるインフラストラクチャを利用していたこと）、外部企業システムとの接続、そして新しい製造ラインを最近立ち上げたことです。



プロセスに影響を与えない
Kaspersky Industrial CyberSecurity の評価は産業プロセスの事業継続性または一貫性に影響を与えません。

深い専門知識
さまざまな業界と OT 機器に関する真の生きた経験により、Kaspersky Lab のエキスパートは、産業向けサイバーセキュリティサービスを効果的に提供することができます。

Kaspersky Industrial CyberSecurity は、トレーニングや評価からインシデント対応まで、お客様の OT セキュリティプロセスのどの段階でも価値をもたらす、技術とサービスのポートフォリオです。

Kaspersky Lab のソリューション

Plzeňský Prazdroj 社は、Kaspersky Lab の産業向け CSA を選びました。この CSA では、最低限の侵襲でリモートとオンプレミスのサイバーセキュリティ評価を行います。Kaspersky Lab のエキスパートは、インフラストラクチャの監査と脅威モデルの開発から、産業向け CSA のプロセスに着手しました。Plzeňský Prazdroj 社の産業プロセスは主に醸造とボトル詰めラインの 2 つに分割され、ピルゼン工場には合わせて 2 つの醸造エリアと円筒円錐型タンク（CCT）エリア、8 つのパッケージングラインが存在します。Kaspersky Lab のエキスパートは、具体的な攻撃経路の再現、脆弱性の発見、そして悪意ある活動と異常のスキャンを行って、このインフラストラクチャの最も危険なセグメントを調査しました。

産業用ネットワークにつながる企業ネットワークから評価を開始した Kaspersky Lab のエキスパートは、外部で開発されたあるビジネスソフトウェアに気付きました。そのソフトウェアには、別の IT システムからいとも簡単に OT 機器の一部にアクセスできてしまう可能性のある、危険な脆弱性が含まれていました。また、醸造工程で使用されている SCADA ソフトウェアのゼロデイ脆弱性を発見しました。

並行して実施されたアセスメント作業により、工場の内外へつながる、管理されていない接続がすべて発見されました。

Kaspersky Lab のエキスパートは、弱い認証、SQL インジェクションなどを含む、見つかった脆弱性とセキュリティ上のギャップを記載した完全なリストと共に、それらをどのように悪用できるかを示した詳細な分析結果のレポートを Plzeňský Prazdroj 社に提供し、同社の産業プロセスの継続性または完全性にダメージを与える可能性があるとして発見され、確認された攻撃経路の詳述情報も提供しました。

第 1 段階での調査データに基づき、Kaspersky Lab のエキスパートは、実用的な推奨事項を策定するための脅威モデルを作成しました。この最終レポートには、特定の産業用コンポーネントに対する今後のサイバーセキュリティ対策、そして脆弱性を軽減する手法に関する推奨事項が含まれています。Plzeňský Prazdroj 社への推奨事項には、セキュリティアップデートとパスワードポリシーを徹底することのほか、ネットワークと Web アプリケーションのセキュリティを強化することなどが含まれています。

「この分析結果は、セキュリティライフサイクルに対する重要な推奨事項を当社に示し、セキュリティプロセスにおける弱い部分を明らかにしてくれました。最終レポートには改善の余地のあるいくつかの領域が記載されており、すべての調査結果がまとめられていました」と Plzeňský Prazdroj 社の IT アナリストであるミロスラフ・ザイーツ氏（Miroslav Zajíc）は話します。

展望

Plzeňský Prazdroj 社は、Kaspersky Lab のエキスパートが産業向け CSA を専門的に計画および実施し、同社内での産業向けサイバーセキュリティへの戦略的アプローチを確実に実現するための基盤を提供したことを認めています。

Plzeňský Prazdroj 社の C&A マネージャーのオンドジェイ・シーコラ氏（Ondřej Sýkora）は、次のように述べています。「Kaspersky Lab と共に、当社は CSA の結果と推奨事項を実行に移すことを計画しており、工場内の端末やサーバーに Kaspersky Industrial CyberSecurity を導入することを引き続き検討していきます」

「Kaspersky Lab と協力したことで、ICS サイバーセキュリティ分野での豊富な経験、専門性と、ソリューションの高度さは、当社に大きな価値をもたらし、また当社のセキュリティ戦略の明るい未来を保証してくれました」

オンドジェイ・シーコラ氏（Ondřej Sýkora）、
C&A マネージャー、
Plzeňský Prazdroj 社

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity は、企業における運用技術の層や要素（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エンジニアまで）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、www.kaspersky.co.jp/enterprise-security/industrial を参照してください。

ICS サイバーセキュリティについて：
https://ics-cert.kaspersky.com
サイバー脅威のニュース：
www.securelist.com

#truecybersecurity

www.kaspersky.co.jp

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* 第 3 回 World Internet Conference で World Leading Internet Scientific and Technological Achievements（インターネット科学技術における世界有数の功績賞）を受賞

** China International Industry Fair（CIIF）2016 で特別賞を受賞