Closing security gaps – Kaspersky Lab delivers industrial cybersecurity assessment for Plzeňský Prazdroj

Plzeňský Prazdroj

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

Plzeňský Prazdroj

Brewery

- Founded in 1842
- Plzeň, Czech Republic
- >2,000 employees in 3 breweries and 13 distribution centers
- 8 packaging lines in Pilsen plant

Plzeňský Prazdroj a.s. is a Czech brewery founded in 1842 and headquartered in Plzeň, Czech Republic.

Plzeňský Prazdroj is the first brewery to produce the pilsener blond lager style beer, branded Pilsner Urquell, making it the inspiration for more than two-thirds of the beer produced in the world today, which are named pils, pilsner and pilsener. Both Plzeňský Prazdroj and Pilsner Urquell can be roughly translated into English as "the Fountainhead at Pilsen" or "the original source of Pilsner".

Plzensky Prazdroj is the leading brewing company in Central Europe. Through its brands, Plzensky Prazdroj sells more beer in the Czech market than any other company. From 1999, the brewery was part of the SABMiller group of companies (at the time, South African Breweries). As part of the agreements made with regulators, before Anheuser-Busch InBev was allowed to acquire SABMiller in October 2016, Pilsner Urquell – excluding certain geographical areas, – was sold to Asahi Breweries of Japan on March 31, 2017.

"Our strong need was to be ready for any unexpected incidents, examine our OT infrastructure and establish a deployment plan to secure the industrial network by the world's leading professionals."

Jan Šik, chief engineer,
Plzeňský Prazdroj

Challenge

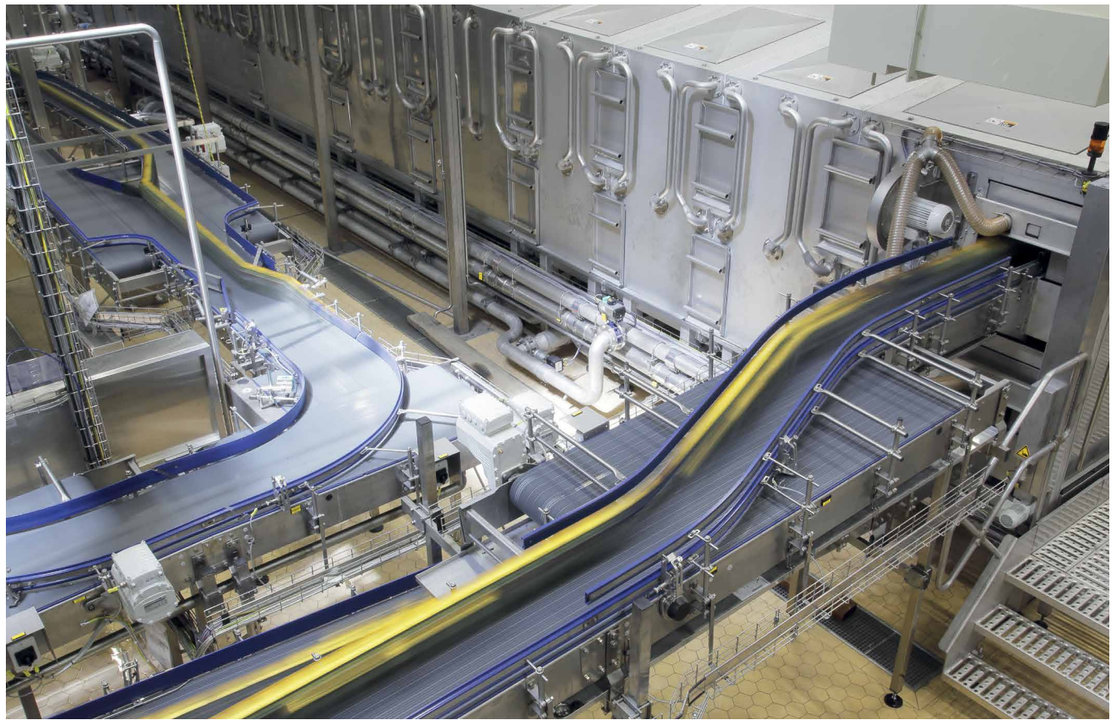
As a large manufacturing company, Plzeňský Prazdroj treats the cybersecurity of IT and OT very seriously. In recent years, some independent audits have been carried out at the company, with some interesting findings. As soon as the technology development on Plzeňský Prazdroj is a continuous process, the necessity for a new independent assessment emerged.

At the time, the technology background was changing from separate systems running on standard PCs to a virtualized server-based master system that connected all systems and devices.

Primary motivation for the company to do a cybersecurity assessment (CSA) was to check the infrastructure at the final stage of the project that included virtualization of the production systems and upgrade of the main OT networking components. Secondary factor was to prepare main topics and requirements for the future project focusing endpoint security solution and make sure that all production plants of Plzeňský Prazdroj company would not be affected in case of a targeted cyber attack or falling "victim" of attack on other closely related companies.

The goal of the industrial CSA project was to make sure the production lines and all OT related software and hardware were resistant to cyber attacks, and that the company was ready to implement a holistic industrial cybersecurity strategy.

The most challenging aspects for industrial cybersecurity policies before the CSA were the complexity of the OT infrastructure (two segments – brewing and bottling with completely different infrastructure), its connections with external business systems and the recent launch of a new production line.



Non-intrusive solution
Kaspersky Industrial CyberSecurity Assessment does not affect the operational continuity or consistency of the industrial processes.

Deep expertise
Real-live experience with a wide range of industries and OT equipment allows Kaspersky Lab experts effectively provide industrial cybersecurity services.

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services, that bring value on any stage of the customer's OT security process – from training and assessment to incident response.

The Kaspersky Lab solution

"Plzeňský Prazdroj chose Kaspersky Lab's industrial CSA, which provides a minimally invasive remote and on-premise cybersecurity assessment. Kaspersky Lab experts started the industrial CSA process with an infrastructure audit and threat model development. Plzeňský Prazdroj industrial processes are mainly divided on brewing part and bottling lines, including in total 2 brewhouses and CCT areas and 8 packaging lines in Pilsen plant. Kaspersky Lab experts examined the infrastructure's most critical segments emulating specific attack vectors, discovering vulnerabilities and scanning for malicious activity and anomalies.

Starting their assessment from the corporate network linked to industrial zone, Kaspersky Lab experts noticed some externally developed business software containing dangerous vulnerabilities that can help to access some of the OT devices through another IT system really simply. In the industrial segment of brewing part, Kaspersky Lab experts discovered a zero-day vulnerability of SCADA software.

Other activity was conducted at this stage to discover and describe all uncontrolled external connections from/to industrial floor.

At the end of this stage Kaspersky Lab experts provided Plzeňský Prazdroj a full list of discovered vulnerabilities and security gaps, including weak authentication, SQL injections, etc. along with a detailed analysis of how they could be exploited. In addition, Plzeňský Prazdroj received a description of detected and confirmed attack vectors that could damage the continuity or integrity of the company's industrial processes.

Based on research data from the first stages, Kaspersky Lab experts developed a threat model used as a basis for developing actionable recommendations. This final report is essential for a customer, as it includes recommendations for subsequent cybersecurity measures for specific industrial components and mitigation techniques for vulnerabilities. Recommendations for Plzeňský Prazdroj included ensuring update and password policy as well as hardening network and web application security.

"The analysis showed us significant recommendations for the security lifecycle and highlighted weaknesses in security processes. Several areas for improvements were noted and all findings were summarized in the final report", says Miroslav Zajíc, IT analyst at Plzeňský Prazdroj.

"The decision to cooperate with Kaspersky Lab was an easy one for a number of reasons. Their experience in the ICS cybersecurity domain, professionalism and the complexity of their solution, in comparison with other suppliers, has given us great value and ensured a bright future for our company's security strategy."

Ondřej Sýkora,
C&A manager,
Plzeňský Prazdroj

Perspective

Plzeňský Prazdroj affirms that Kaspersky Lab experts professionally organized and executed the industrial CSA and provided the basis for ensuring a strategic approach to industrial cybersecurity within the company.

"With Kaspersky Lab we are planning to follow up on the CSA results and recommendation and continuing discussing the deployment of Kaspersky Industrial CyberSecurity solutions for nodes and servers", says Ondřej Sýkora, C&A manager at Plzeňský Prazdroj.

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

All about ICS cybersecurity:
https://ics-cert.kaspersky.com
Cyber Threats News:
www.securelist.com

#truecybersecurity

www.kaspersky.com

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

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

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