Protecting Pilsner Urquell against cyber attacks

In times of Industry 4.0, the subject of cyber security is of elementary importance for producers in the food industry. The example of the Pilsner Urquell brewery shows how the first step towards further cyber safeguarding of industrial plants can be taken via a security audit by Kaspersky Lab without disturbing ongoing production operations.

The prestigious Czech brewery Pilsner Urquell, established in 1842, is the leading brewery enterprise in Central Europe. It employs a workforce of around 2,000 in three breweries, eight bottling/packaging lines and 13 sales and distribution centers. Pilsen, where the brewery company is based, is world-famous as the “birthplace” of Pilsener beer. More than two thirds of the beer produced throughout the world has been inspired by this beer type and is sold under the name ‘Pils’, ‘Pilsner’ or ‘Pilsener’. Pilsner Urquell is, so to speak, the original source of Pils beer.

From 1999 onwards the brewery belonged to the SABMiller Group, (at the time South African Breweries). In agreement with the regulatory authorities (before Anheuser-Busch InBev was allowed to take over SABMiller in October 2016), Pilsner Urquell – without specific geographical regions – was sold to the Japanese brewery group Asahi on 31 March 2017.

Technology development means a continuous process at Pilsner Urquell. A number of independent audits have been conducted in the company in the past years. When the IT Department wanted to change over from PC single-user solutions to a virtualized, server-based master system connecting all systems and items of equipment, the company saw a specific need for action – to examine relevant IT security aspects.

System conversion presents new challenges with regard to security

The main motivation for carrying out a cyber-security examination – also known as Cybersecurity Assessment (CSA) – consisted in examining the infrastructure in the end phase of the conversion project for IT security aspects. In addition, the project also includes virtualizing the production systems and upgrading the main network components of Operational Technology (OT). A further challenge is to determine the core themes and requirements of the future project as regards an endpoint security solution. The goal was quite clear – all production facilities of Pilsner Urquell were to be protected against possible targeted cyber-attacks and attacks against enterprises closely connected with the business. “What was important to us was to be prepared for all unexpected incidents, to review our OT infrastructure and to set up a plan for securing the industrial network together with the experts from Kaspersky Lab”, explains Jan Šik, Chief Engineer at Pilsner Urquell.

The objective of the industrial CSA project was to render the production lines and all OT-related software and hardware immune to cyber-attacks and to set up the company in such a way that a holistic, industrial cyber security strategy can be implemented.

Prior to conducting the security assessment (CSA), the greatest challenges with regard to industrial cyber security were the complexity of the OT infrastructure (two areas – brewery and bottling, each with quite different infrastructures), the connection to external business systems and the launch of the new production line which had recently taken place.

If you know your weaknesses, you can protect yourself

Pilsner Urquell decided on the industrial CSA by Kaspersky Lab, which consists of a minimal-invasive remote and on-site Cybersecurity-Assessment. The advantage of this is that Kaspersky Industrial CyberSecurity Assessment does not affect ongoing operations. Industrial processes can continue to run.

The experts from Kaspersky Lab began the industrial CSA process with an infrastructure audit and the development of a threat model. The industrial processes at Pilsner Urquell are divided above all into the fields of brewery and bottling. This involves two breweries and beverage tank sectors (cylindrically-conical fermentation tanks, CCT) and eight packaging lines within the production plant in Pilsen.

Kaspersky Lab examined the most critical areas of the infrastructure. For this specific attack-vectors were re-enacted in order to reveal gaps in security and subsequently examine the systems for malignant activities and anomalies.

In their examination of the company network and the associated industrial sectors, the experts discovered externally developed corporate software that revealed dangerous security gaps – security gaps through which the OT installations could be attacked very easily. In the industrial sector of the brewery the IT security experts even discovered a Zero-Day vulnerability for SCADA software. Furthermore, measures were taken to identify any uncontrolled external connections in and from the shop-floor level.

At the end of the infrastructure audit, Kaspersky Lab provided Pilsner Urquell with an overview of all the weaknesses and security gaps discovered, such as weak authentications, SQL injections and the like. This also included a detailed analysis of how these could be exploited. Furthermore, Pilsner Urquell received a description of the attack vectors discovered and confirmed that could be disastrous for the continuity of operations and integrity of the company's industrial processes.

Protect properly – analysis provides recommendations for action

Based on the results of the audit, in a next step the experts from Kaspersky Lab developed a threat model in order to develop recommendations for action which the company could implement. Such a final report plays a crucial role – it contains recommendations for future measures in the field of cyber security for specific industrial components and techniques in order to eliminate vulnerabilities. Recommendations for Pilsner Urquell were for example securing update and password guidelines, as well as strengthening the network and web application security.

"The analysis has provided us with important recommendations for the security life cycle and given us essential findings regarding the weaknesses in the security process. The final report from Kaspersky Lab has provided us with several possible improvements", summarizes Miroslav Zajíc, IT Analyst at Pilsner Urquell.

This strategic approach to industrial cyber security shows the company further paths to be taken in future regarding its own IT security. "On the basis of the CSA results, we now plan to implement the Kaspersky industrial cybersecurity solution for network connections and servers together with Kaspersky Lab", concludes Miroslav Zajíc.

Kasten Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity is a portfolio of technologies and services that offers comprehensive protection for each individual level of industrial systems, including SCADA-servers, HMI, Engineering-Workstations, PLC, network connections and staff. The solution increases the industrial security step by step in all areas, from human resources, via processes, right through to technologies. The continuity and consistency of industrial processes are not affected at all: https://www.kaspersky.de/enterprise-security/industrial-solution

Author: Denise Pflock, Corporate Communications Manager Europe bei Kaspersky Lab

Further information and contact

Kaspersky Lab GmbH
Ingolstadt
Denise Pflock
Phone: +49 (0) 841 98 18 90
kaspersky_de@berkeleypr.com
www.kaspersky.de