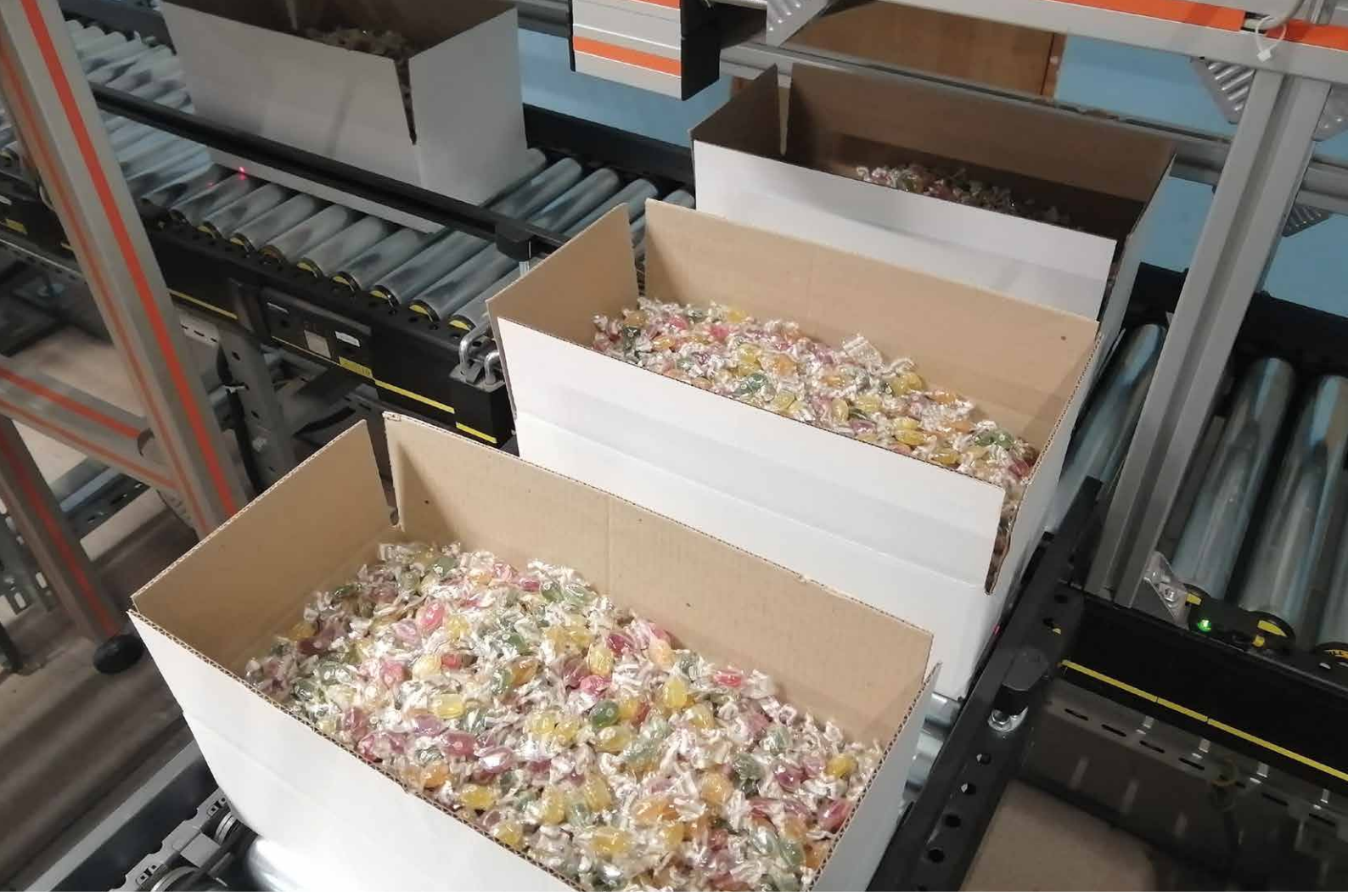

APROTECH

VPK production lines under Kaspersky protection

kaspersky BRING ON THE FUTURE

About the company

The private food production company Voznesensky Pischevoy Kombinat LLC (VPK, the Customer) was founded in 1996. The company's main line is the production and sale of confectionery, specializing in dairy sweets, jelly marmalade, mini caramels, and halva.

VPK's produce is certified in accordance with international food quality and safety standards and certificates. The most important task of the enterprise is to ensure high-quality products. For this reason, VPK introduced a quality control system and installed all the necessary equipment to monitor the quality of products and incoming raw materials and to conduct related research.

Food industry

- Founded in 1996
- Moscow Region, Russia
- Total annual production > 14,000 tons per year

“It is important to note that industrial cybersecurity in Russia is relevant not only for critical infrastructures, but also for light industry and the food sector, which have a high level of automation. This project perfectly demonstrates that the market is maturing and there is a desire for secure, high-quality production.”

Alexey Petukhov,
KICS Business Development Manager, Kaspersky

Mission

VPK collaborates with reliable suppliers of industrial solutions for the food sector, including Siemens and B&R. Cybersecurity is front of mind for both the company founders and the IT team. Task prioritization led to the implementation of a commercial project to secure the business contours using Kaspersky solutions in early 2019.

The use of multivendor solutions in the industrial control system (ICS) environment, combined with organic growth in operational capacity, which involves the expansion of technological equipment and new connections, impose special requirements in terms of industrial cybersecurity to ensure sustainable business development. With a view to expanding the VPK production line, an agreement was reached to pilot the full-fledged solution Kaspersky Industrial CyberSecurity (KICS) in a real limited segment of the technological process.

The project covered the protection of VPK's key assets against various types of mass cyber attacks (ransomware, viruses, and exploits targeting old versions of operating systems; vulnerabilities in controllers), as well as resource access control for company engineers and specialists who start (sometimes remotely), configure, and operate industrial equipment.

One of the tasks of the pilot project was to determine the ICS segment for KICS deployment. This entailed selecting the most typical elements for monitoring and minimizing the work involved in deploying and configuring the solution. Collaboration between the Customer's IT team and experts from business partner Adaptive Production Technology (APROTECH) at the preparatory stage made it possible to engineer and deploy the solution in two days.

One of the additional requirements on the part of the Customer was the need for a simple and intuitive interface for detecting and interpreting events of interest in the context of industrial cybersecurity. Therefore, the pilot included skills transfer sessions on how to “teach” the main solution component the rules for creating whitelists of allowed elements and events.

Non-Intrusive solution

Kaspersky Industrial CyberSecurity does not affect the continuity of the company's technological processes.

Control and monitoring

Kaspersky Industrial CyberSecurity provides application launch policy and access to removable devices, as well as provides passive monitoring of network traffic of the automated control system.

Compliance

The implementation of a comprehensive solution for industrial cyber protection helps ensure compliance with regulatory requirements in the field of information security of industrial enterprises.

Solution

The initial stage of the project involved architecting and selecting the pilot segment. By agreement with the Customer, this architecture touched upon the main operational domains (production, packaging, storage). The number and composition of KICS components were selected in accordance with the ICS elements in use at the level of SCADA systems, controllers, and auxiliary software solutions.

KICS for Nodes provides cybersecurity for servers and workstations at the ICS level, while consuming fewer system resources and supporting the ability to install and update without a restart. The product is certified with the most common software and hardware components of industrial automation systems.

KICS for Networks is designed to monitor and protect industrial networks. The product does not interfere with production processes, since traffic is analyzed in passive mode. The extensive network integrity control and intrusion detection systems give the operator advance warning of deviations in production processes.

> “During the project, we saw in practice that cybersecurity issues, among other new types of risk, are a strong focus of VPK's owners. Even new scenarios for using industrial data are assessed in terms of business value, security, and cost.”

Andrey Suvorov,
CEO, APROTECH

Results

The integrated industrial cybersecurity approach adopted by the joint team of Kaspersky and APROTECH met all the expectations of VPK and nullified any risk of the deployment process having an impact on production. The project results demonstrated the effectiveness of the system at detecting incidents and reducing unscheduled downtime.

Currently, the system is functioning in pilot mode. It provides training in the new rules for using allowed elements and events, and full monitoring of industrial traffic and events at the level of operator computers. The decision to put the system into commercial operation will be based on the results of this work.

“Cooperation with colleagues from Kaspersky and APROTEH allowed us not only to prioritize company assets to enhance their cyber resistance, but to frame our initial plans for using trusted industrial data to increase production,” said Dmitry Goldobin, CEO, VPK.

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

Kaspersky ICS CERT:
https://ics-cert.kaspersky.com/
Cyber Threats News: www.securelist.com

#Kaspersky
#BringontheFuture

www.kaspersky.com

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

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

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