ARC VIEW

DECEMBER 2019

Industrial Cybersecurity in the Era of Digitalization

By Thomas Menze

Keywords

Industrial Cybersecurity, Kapersky, IEC 62443, Ransomware, Anomaly Detection

Summary

The growing use of "off-the-shelf" technologies in industrial applications exposes owners/operators to constant barrage of threats that can only be mitigated with a comprehensive, holistic approach to cybersecurity. This ARCview explains the Kaspersky Industrial CyberSecurity (KICS) portfolio and how the individual components can be combined to form an effective overall solution against cyberattacks.

Recent Cyberattacks Emphasize the Need for Vigiliance

Recent attacks may mark the beginning of a major campaign. If you don't prepare yourself for the threat situation, you are very likely to become a victim.
- Arne Schönbohm, President, BSI

According to IT experts, a wave of cyberattacks hit European industry in autumn 2019. In Germany, the Federal Office for Information Security (BSI) observed that criminals are again causing "considerable damage" to companies, administrations and other organizations with Emotet malware.

The BSI is concerned that the recent attacks will mark the beginning of a major campaign: Soon, the attackers could paralyze significantly more systems. The danger is considerable, said BSI President Arne Schönbohm: "If you don't prepare yourself for the threat situation, you are very likely to become a victim."

Cybercriminals often use Emotet for the distribution of blackmail software, called Ransomware: They encrypt important files and demand a ransom for their release, which is usually paid in a crypto currency. The victims of this

trick in the past few months have included the aluminum producer Norsk Hydro, various hospitals and municipal administrations.

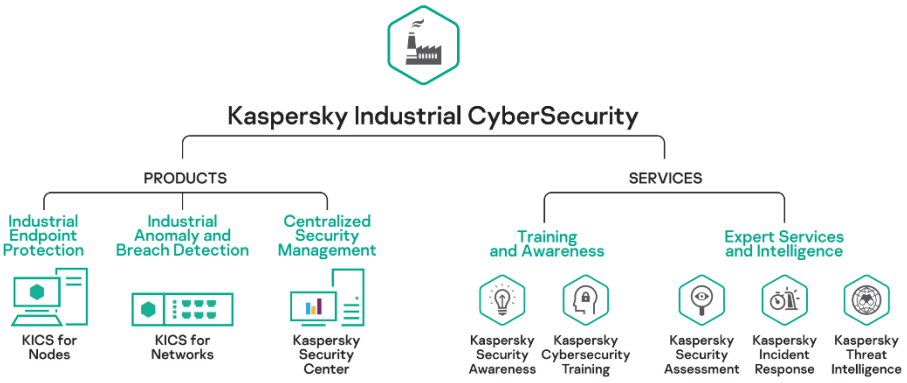
Emotet spreads fear and terror because the victims are targeted: They first find out which organizations own the infected systems and adjust the ransom demand to the expected willingness to pay. Some small towns in the USA, for example, transferred sums of around $500,000 to get their data back.

The industry is not defenseless against digital blackmail. Security updates and anti-virus software can stop the spread of programs like Emotet. Backup and recovery exercises can help you get back up and running quickly in an emergency. It is recommended to divide the enterprise networks into several zones to make the spread of the software more difficult.

Training of employees also plays an important role. Even with supposedly known senders, you should "only open file attachments of e-mails with caution".

Kaspersky and Industrial CyberSecurity Portfolio

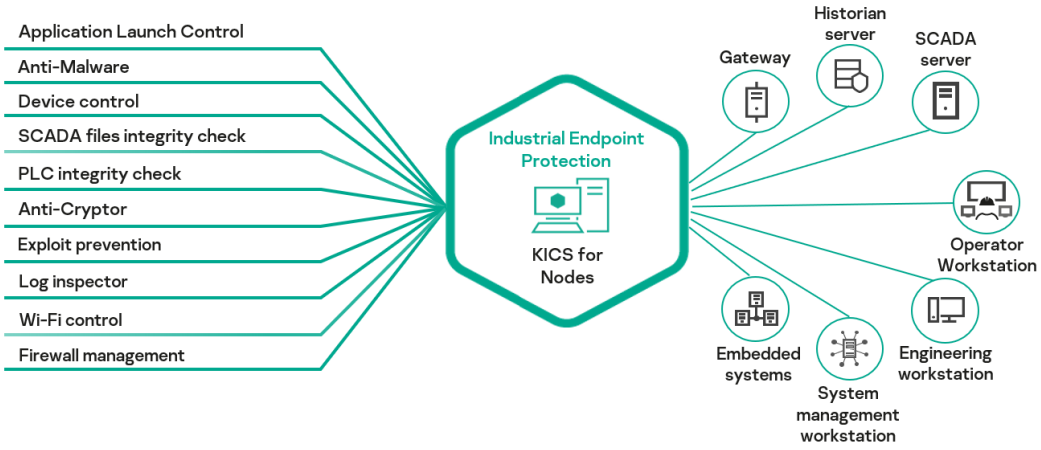
Security solutions that meet the specific requirements of industrial control systems and an industrial infrastructure can only be created by cybersecurity suppliers who understand the differences between OT applications and IT applications. Kaspersky claims to have the unique combination of threat intelligence, machine intelligence and learning, and human expertise to provide flexible protection against any type of threat in the industry. Today, Kaspersky offers a wide range of technologies and services around industrial cybersecurity solutions.



Kaspersky Industrial Cyber Security offering

KICS for Nodes

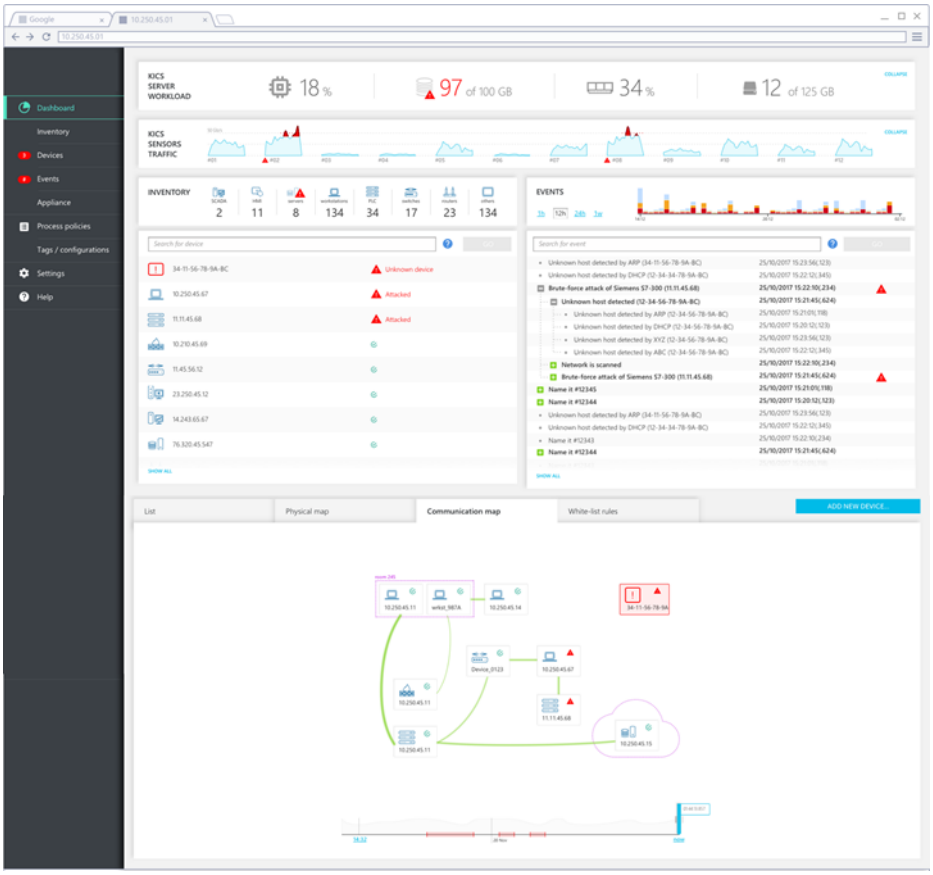
Kaspersky's cybersecurity solutions, developed for industry with the core competencies mentioned above, support users in all requirements around industrial cybersecurity. KICS for Nodes secures ICS/SCADA servers, human-machine interfaces and engineering workstations. As an Industrial Endpoint Protection solution, it secures industrial automation systems against human error, malware, targeted attacks or sabotage. KICS for Nodes supports a wide range of Windows OS, including older versions, and from 2020 is available for Linux machines.



Kaspersky Industrial Enpoint protection

KICS for Networks

KICS for Networks monitors the OT communication protocols. The solution analyzes protocols in real time and detects anomalies. This helps operators to recognize attacks and to react in time. Furthermore, this solution is valuable for decrypting forensics after a cyberattack, based on the alerts, events list and asset map.



Kaspersky Network Monitoring solution

Efficiency of KICS

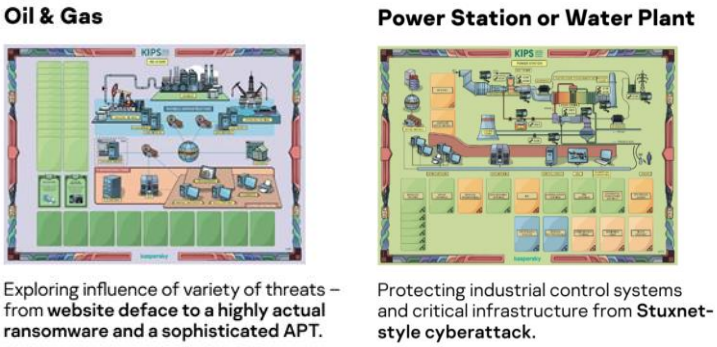
One of the main security benefits from using KICS is avoiding downtime. For a manufacturing facility, downtime often results in financial losses, including lost revenue, client dissatisfaction, and tarnished reputation. Any incident of unplanned downtime also requires investigation and additional efforts to restore operations.

One factor that prevented operators from using traditional endpoint antivirus software on workstations was the operating system, because the OS versions used were frequently incompatible with the available software. Another reason was the OS resource consumption and system overload. For the traditional endpoint antivirus solution to properly protect workstations, the information security team needed to upgrade operating systems. These constant upgrades are expensive and risky, because if an upgrade is not completed, the system remains an easy target for cyberattacks. Moving to

KICS for Nodes allows the organization to avoid the cost of software upgrades while ensuring the necessary level of protection.

Kaspersky Interactive Protection Simulation – KIPS

It is important to give users the opportunity to playfully learn and optimize cybersecurity decisions. This simulation explains the various automation components, their vulnerability to cyberattacks and the significance of the decisions made in case of emergency.



Kaspersky Interactive Protection Simulation examples

ICS Survey 2019

When it comes to securing the existing OT/ICS infrastructure, an important question is whether companies are regularly reviewing the security of their automation systems. According to a 2019 survey, nearly 70 percent said that they do. When asked how OT/ICS cybersecurity budgets will be used in the future, interviewees reported on average a 10-15 percent increase for operator awareness training, endpoint protection, and OT/ICS security audits.

If digital services are to be used increasingly in the future, then operators must be trained to deal with potential threats stemming from more connectivity. This is especially true when working with third party contractors that support OT networks.

As far as cybersecurity risks are concerned, systems need to be thoroughly reviewed, which requires major investment. The solution is systems that constantly monitor automation and document changes. Of course, operators will want a better understanding of communications in the OT network in the

future. This should allow early detection of attacks on the network to avoid major damage.

Both facts lead to the conclusion that endpoint protection of an ICS component alone is no longer enough. Industrial Anomaly and Breach Detection solutions, such as KICS for Networks, already meet the previously mentioned requirements.

Review of the Existing Security Portfolio

Kaspersky complements security technologies with security training and service offerings. The aim is to optimize the human factor (secure behavior) and sensitize all employees to the topic of cybersecurity.This comprehensive Kaspersky range of technology and services also meets the requirements of the IEC 62443 standard in many respects. This standard recommends regular system audits, patch management and employee training.

The result is a holistic security portfolio that provides sustainable protection for industrial automation while consuming few resources. The security technology and the necessary processes are closely coordinated and reach a high level of protection.

Industry Outlook

The digitization of industry will continue. Key elements of digitization initiatives cover architecture of the digital factory with processes and operations traceability, together with digital twins of product, flexibility and efficiency. With this approach an asset owner gains insight to increase labor productivity and to optimize core industrial vertical and horizontal chains.

This requires more sensors and distributed computer systems to collect and pre-process the data. The number of interfaces within the system and to the internet will increase. All these interfaces are vulnerable, and sensor data can be manipulated.

In the future, intelligent, self-learning systems will be needed to ensure the integrity of automation systems. Only in this way can the required future cybersecurity be achieved.

In the future, software functions such as machine learning and anomaly detection will be used together with cybersecurity solutions. This software will

also detect other anomalies such as faulty devices and human errors and thus avoid costly plant downtime, which will have a further positive effect on the efficiency of the methods used.

Kaspersky Solutions for Future Security Challenges

Kaspersky is constantly assessing future challenges with asset owners to enhance security solutions. Some of these challenges are described below.

Cyber-Immunity concept

Industry develops and changes every year. Today, industry is facing challenges that nobody could imagine five years ago. Cyberthreats are growing in frequency and complexity.

According to Kaspersky, the current cybersecurity situation requires a drastically different approach - a transition from cybersecurity to "cyber-immunity," which implies that the cost of a cyberattack should exceed the cost of damage that it can inflict.

Kaspersky OS

The closer integration of machines, products and processes generates data and creates the basis for digital business models. However, the data integrity and secure data exchange are mandatory. Compared with office IT, industrial security requires high plant availability and real-time functionality. An important factor is the reaction time to detect malicious communication. At the Hanover Fair 2019, Kaspersky presented with partners the first industrial gateway with a “secure by design” architecture. This architecture based on Kaspersky OS. KasperskyOS is designed on a reliable microkernel that implements the only way of communicating and can be used on various platforms. This also ensures in digital business models that the communication between the individual components cannot be manipulated. This ensures authentication in the various digital business models.

KICS & MLAD: Insight into Condition-Based Monitoring

Asset owners are constantly looking for opportunities to increase the productivity of production sites by improving uptime of components and fail-free production. Kaspersky has developed Machine Learning for Anomaly

Kaspersky Anomaly Detection Software

Detection (Kaspersky MLAD), an application designed to provide security for a cyber-physical system (ICS, Internet of Things, Industrial Internet of Things) based on detection and interpretation of anomalies by employing machine learning methods in telemetry from the operating technologies of the protected facility.

Conclusion

As a trusted IT security provider and partner to leading industrial companies, Kaspersky works with leading industrial automation suppliers. The goal is to develop specialized methods and collaborative frameworks to protect industrial systems from cyberthreats, including targeted attacks.

Kaspersky Industrial CyberSecurity enables the combination of different protection methods within the framework of coordinated security solutions. A holistic approach to industrial cybersecurity, from the prediction of potential attack vectors to special detection technologies to the rapid defense against cyberincidents, is ultimately the prerequisite for secure plant operation. This security offer also includes various training programs, helping to level-up the awareness and professional skills of operators..

For further information or to provide feedback on this article, please contact your account manager or the author at tmenze@arcweb.com*. ARC Views are pub-lished and copyrighted by ARC Advisory Group. The information is proprietary to ARC and no part of it may be reproduced without prior permission from ARC.*