Digital Innovations and Technologies – a Priority Strategic Objective for **TMK-ARTROM S.A. Slatina**

A general trend among companies, regardless of the field in which they operate, is to postpone investments in technologies adapted to current security needs for a later date. This approach has proven to be very risky considering that last year's ransomware attacks on Romanian companies.

In a cyber threat landscape constantly changing, the best option for companies is to firstly lay the foundations of a robust infrastructure to cope with any kind of security threats.

TMK-ARTROM S.A. Slatina is one of the vigilant companies, with a history of over 25 years in Romania. TMK-ARTROM manufactures pipes for the automotive industry, deep-sea drilling tools, shale gas drilling tools, pipes for hydraulic cylinders, and counts well-established brands as its company's customers. TMK-ARTROM is part of the Russian group TMK, a company with a turnover of 3.3 billion euros in 2016, 42,000 employees and 27 factories in six countries.

For TMK-ARTROM, innovation and switching to digital technologies is a priority strategic goal. The company has invested in technologies and security solutions tailored to tackle the cyber-threat landscape over time. During the early years after the privatization of the plant and joining the TMK family, the organization aimed to strengthen and increase rolling capacities, sales volumes, and ensure the security of all production and technological equipment.

"For us, choosing Cisco was a natural decision. Cisco's equipment and technology have an undeniable reputation both worldwide and on the Romanian market. We talk about sustainable technology and a safe long-term investment. In addition, another major asset is the team of local experts who can provide support at all times. "

The company has established a solid and integrated infrastructure and implemented the first Cisco PIX firewall more than 10 years ago

In the ever-menacing context of cyber attacks invisible to most of the current security systems that have affected many institutions and companies in Romania, TMK-ARTROM has decided to increase security measures and to upgrade the infrastructure.

ETA2U, a Cisco partner with a wide experience and numerous certifications on the security area, was chosen to implement the security solution.

"The new security solutions have been deployed in just a few weeks. Cisco is a vendor providing customers with all the materials needed for an easy deployment. Direct support, both from Cisco and its partners has also helped to quickly and efficiently implement the project. Practically, the existing infrastructure has been implemented in several steps, each time providing a greater security and efficiency of internal operations by automation and minimizing the need for human intervention. The result is an intelligent network that provides support as an integrated platform and adapted to IT market trends. "

The security solution implemented at TMK-ARTROM is made up of 2100 series NGFW (Next-Generation Firewall) redundant devices with activated Intrusion Prevention System (IPS) and Advanced Malware Protection (AMP) licenses and URL filtering.

Email is a critical business tool that can expose organizations to a wide range of threats. According to the 2017 Cisco Security Report, 6% of the emails we receive are malicious. That's why any company should know how to identify the really important e-mails and those that pose a security risk. Thus, to provide advanced protection against e-mail threats, TMK-ARTROM decided to deploy ESA (Email Security) and WSA (Web Security) solutions, both protected with AMP (Advanced Malware Protection). By working with Talos, this solution manages to block infected attachments or mails containing malicious links. Last but not least, spam is no longer a problem for the company. Most of the spam messages are filtered through ESA and all access policies and roles assigned to users are being monitored.

All these solutions are part of an architecture integrated into the access platform ISE (Identity Services Engine), allowing visibility and control of all users and devices connecting to the corporate network, thus identifying, isolating and resolving threats quickly.

"Our challenge was changing the existing infrastructure with a modern, scalable, cost-effective and performing solution that can provide full security at all levels without obstructing productivity."

Florin Râmboiu, Product Manager ETA2U

"The proposed security solution has been extended to the entire LAN infrastructure by deploying an unified infrastructure using Cisco Nexus, delivering scalability and a high degree of resilience, easy server integration, storage and the next-generation of Cisco Catalyst switches with advanced capabilities of blocking and preventing cyber attacks. This helps to avoid threats right from the lowest levels of infrastructure and, at the same time, ensures greater resilience of the data network. "

Dan Iagar, Lead Consultant si Radu Mustață, Project Manager, ETA2U

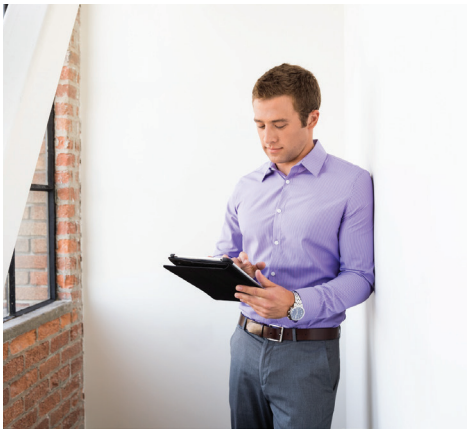
"These technologies give us the opportunity to automate the entire infrastructure so that the IT department can focus on innovation and operations support and not on troubleshooting or configuration and maintenance activities. Equally important, it offers us peace of mind and efficiency in delivering our services to users without interruptions and with the prospect of having an IT platform that can adapt to the technological trends of this decade. The company's processes have been steadily improving and the performance of the services has increased along with the level of security required in the institution. "

Cisco's security infrastructure and solutions serve both TMK-ARTROM and TMK-REŞIȚA, the Slatina plant's slab billet source, providing protection for all operational activities and safe information transfer.

Since its inception, TMK-ARTROM has put a significant focus on quality, one of the objectives being to continuously invest in improving the security system.

Cisco Security Architecture ensures the protection of the entire existing communications platform through Datacenter technologies - Nexus 3K / 9K and UCS C220 and C240, Collaboration - TP, CMS, BE6K, Switching - Catalyst 2K and 3K and Wireless APs of all ranges, 2504 controller.

"We are currently testing the DNS - Cisco Umbrella security solution, which provides us with an extra layer of security in the fight against ransomware attacks that we have encountered so often lately. Moreover, this solution allows the existing equipment to be freed from further filtering, provided that users or devices communicating on the Internet are blocked at the time of requesting the connection, if Cisco TALOS (Security Intelligence Operations) recognizes the IP address as having a low reputation or which can pose risks to users. "



In the context of the exponential growth of cyber attacks and network-connected devices, companies have to increasingly move towards an architectural approach on security. Cisco security solutions provide companies with in-depth control and the ability to extend protection beyond their perimeter.