CASE STUDY

BRATISLAVSKÁ TEPLÁRENSKÁ

ENERGETICS

The managers of Bratislavská teplárenská gain a real overview of their sensitive corporate data

> „The new system allows us to work with sensitive data in a responsible way and in accordance with clearly defined rules."

Miloš Žitný
Bratislavská teplárenská
Head of the IT & Telecommunications Department

1. REQUIREMENTS

- Deploy a **Data Loss Prevention** (DLP) solution from Safetica in the company
- Ensure compliance of the company's processes and technologies with the new legislative requirements (GDPR and the Cyber Security Act)
- Use this opportunity to **update existing sensitive data processing procedures** to make them compliant with the legislation as well as with company management's expectations

2. SOLUTION

- Use the Safetica Auditor **to map the ways and forms** in which the data is processed, i.e., where the data comes from, how it is created and processed, and where it is transferred
- **Classify data** by content, origin, and other metadata
- **Create policies** for different groups of sensitive data
- **Provide training** to the client's IT team

3. OUTCOMES

- **Gaining an overview and control** over corporate data.
- The ability to immediately change and apply rules for working with sensitive information across the company
- **A notification system** that reminds users to heighten their caution regarding the data they are currently working with (the strong educational purpose of the solution)
- **Preventing unauthorized processing of sensitive data:** forwarding, copying, printing, or saving onto unknown USB sticks
- **New analyses and statistics** of the company's data flow

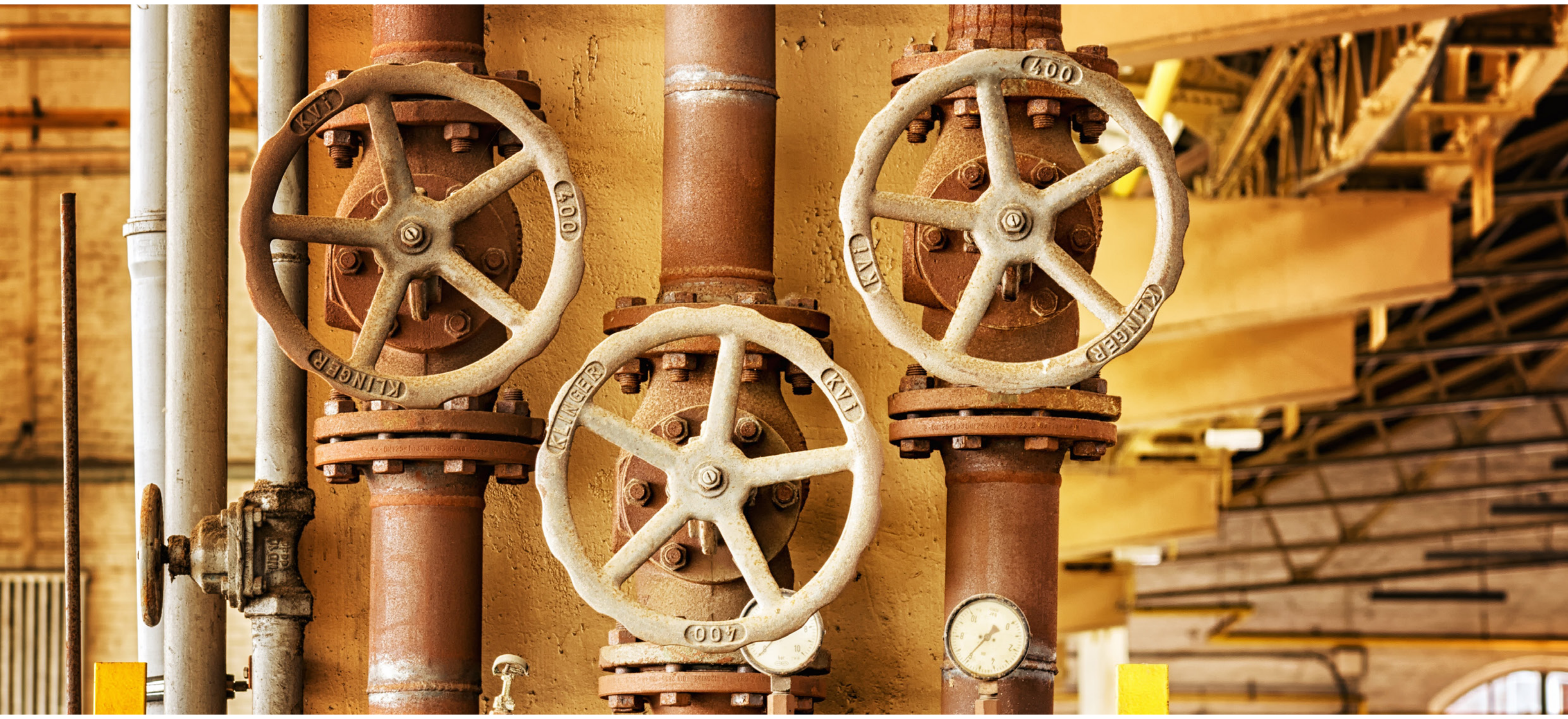
CASE STUDY

BRATISLAVSKÁ TEPLÁRENSKÁ

ENERGETICS

Background

Bratislavská teplárenská, a.s. (BAT) has been one of the Soitron's major customers for many years. The cooperation on this new project was triggered by the Cyber Security Act passed in 2018. According to the act, specific companies providing "essential" or "digital" services must ensure the enhanced security of their data. Simply put, this includes companies that are of strategic importance for the functioning of the country, such as banks, telecommunication companies, energy companies, hospitals, chemical producers, heavy industry, transport, water, and energy distribution companies. This includes BAT. This heat producer and distributor had already tried a different DLP system in the past. They were not happy with it, and this is why they were looking for a new supplier. There were two reasons why they chose Soitron: they had prior experience with Soitron, and we are a certified Gold Partner of Safetica Technologies, the developer of the renowned Safetica DLP software package. This was exactly what BAT was interested in. There is a lot of data that BAT needs to protect, including the personal data of its own employees, customer information and consumption data, financial data, and sensitive industrial documents such as design diagrams, drawings, and proposals. More than 250 workstations – desktops and laptops – had some degree of access to the data. The data was constantly being sent back and forth, distributed over the internal information system, copied (both digitally and physically), and transferred onto removable media (typically USB sticks).



Solution

BAT is one of a few Soitron customers who knew exactly what they wanted from the very beginning. Having tested multiple trial versions of solutions from various developers, they chose the Safetica DLP package to prevent data leaks. Soitron's role was to ensure the smooth deployment of the technology and scaling the necessary hardware, performing pilot testing, and setting up and optimizing Safetica before it was deployed across the company. The client decided right away that they would not just stand by with their arms crossed and watch the implementation. On the contrary, a working group was formed at BAT with representatives from across the entire company structure. Its members diligently and openly communicated with other employees at all levels, actively collected feedback from them, and organized training sessions.

The Safetica solution comprised of two essential modules. The first module – Safetica Auditor – was used to obtain an initial image of company data flows. It ran at selected terminals for approximately three months.

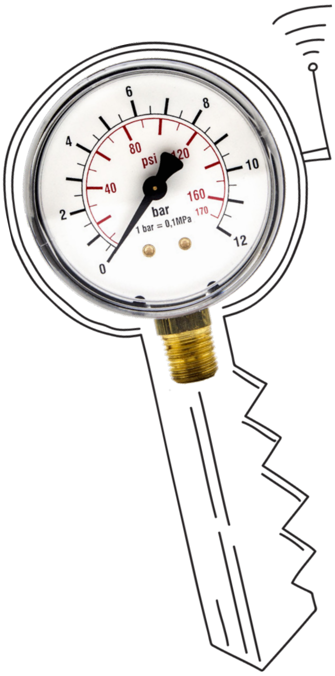
The results of the initial audit were first presented to the heads of departments, whose job was to compare them with reality, i.e., to verify whether or not the Auditor's findings were correct. In addition, they verified the data content, as the module only focused on monitoring the data flows.

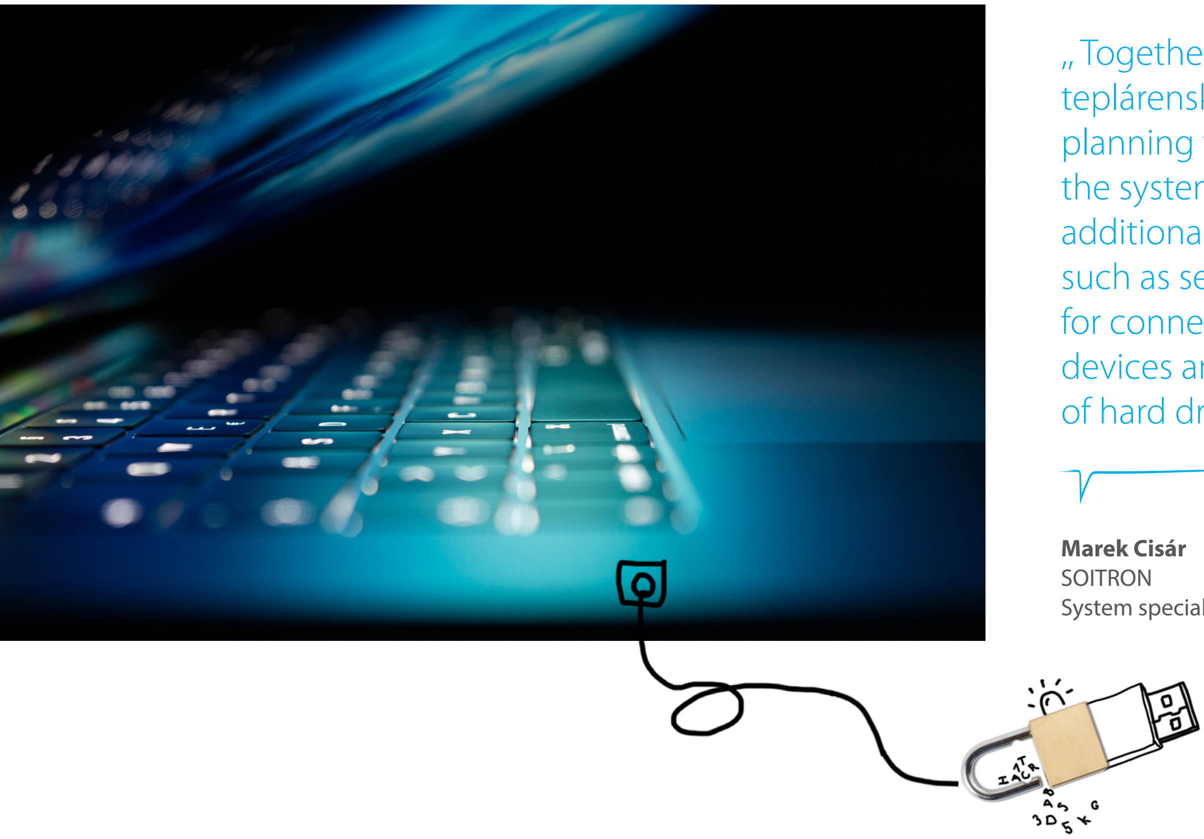
The initial analysis allowed for the following:

- The effective classification (sorting and labelling) of the data
- A revision of the policies for data processing by various user groups (who can access, process, distribute, and copy the data, and under what conditions)

The second module – Safetica DLP – ensured compliance with these policies. Before launching the live operation, the client's IT team took care of distributing the Safetica DLP software to all workstations connected to the company's network. The policies are applied in two different ways: (1) employees are notified whenever they work with sensitive data, and (2) they are prevented from processing the data in an unauthorized way.

In terms of hardware, Safetica did not require any major investments. The only system requirements were one dedicated virtual server and hardware performance to be increased by approximately five percent. Once the data is properly classified and policies are defined, the whole system rollout can be done in a matter of hours or no more than a few days. Safetica, the solution developer, was available during the entire deployment, but as it turned out they did not have to address any serious problems.





„Together with Bratislavská teplárenská, we are already planning to extend the system to include additional functionalities, such as setting policies for connecting additional devices and the encryption of hard drives and USB sticks."

Marek Cisár
SOITRON
System specialist

Outcome

Today, BAT employees are unable to send, copy, print, or save onto USB drives any sensitive data without it being recorded and evaluated by the Safetica DLP system.

The data is clearly categorized and processed under strict supervision in compliance with clearly defined rules. This protects customers, employees, and the credibility of the BAT brand. In addition, BAT's IT team and management have gained a comprehensive overview of how sensitive data is handled in the company: where it comes from, who processes it and how it is processed, and where it is sent. This can be the basis for taking any further measures, or for changing classifications or policies. On top of that, BAT has got a much better idea of what the value of specific business applications is for them based on how often they are used and for what operations.

BRATISLAVSKÁ TEPLÁRENSKÁ, a.s.

Bratislavská teplárenská, a.s.

The core business of Bratislavská teplárenská includes heat production, base-load and peak-load power generation, heat purchasing and distribution, and electricity distribution. In the process of heat and power cogeneration, the company ensures the cost-effective operation of centralized heat supply systems (CHP). It supplies heat for hot service-water heating and production for the vast majority of residential and administrative buildings; schools; health care, cultural, and sports facilities managed by customer organizations; and industrial customers. Presently it covers approximately 55% of the total heat demand in Bratislava, the capital of Slovakia.

www.batas.sk

SOITRON, s.r.o., member of SOITRON Group

Soitron is a Central European integrator operating in the IT market since 1991. The company's philosophy is to constantly move forward, and that is why it is a leader in implementing unique technologies and innovative solutions. It offers its clients products and services in the field of robotization and process automation, artificial intelligence, the Internet of Things (IoT), IT infrastructure, communication and cloud solutions, IT security, IT services and outsourcing, IT advisory and applications, and IT department digitalization. Its product portfolio includes smart police car solutions – Mosy and cyber security services – Void Security Operations Center. Soitron, s.r.o. is a part of the Soitron Group and employs more than 800 international experts. The group brings together professional teams in Slovakia, the Czech Republic, Romania, Turkey, Bulgaria, Poland, and the UK.

www.soitron.com