

MULTI-LAYERED CYBERSECURITY IN RESPONSE TO NATIONAL REQUIREMENTS

SECTOR:

Public, Local Government

ORGANIZATION PROFILE:

The municipality functions as a pivotal administrative hub, ranking among the largest within the country. The structure offers a significant array of electronic services tailored to the needs of the local population.

THE CHALLENGE:

Following a review and analysis of the inherited infrastructure, the municipality's leadership and IT team have concluded that there is a necessity for the implementation of contemporary security solutions. These solutions must align with the complexity of the provided electronic services, ensure the protection of citizens' personal data, and meet national requirements. Enhancing cybersecurity is of paramount importance to thwart potential cyberattacks and breaches that could have significant consequences for the trust and operational efficiency of the municipal administration.

DIAMATIX DEVELOPED THE FOLLOWING STREAMS FOR PROJECT COMPLETION:

- **Assessment Stage** - Thorough analysis of the existing IT infrastructure, formulation of a strategic framework, and design;
- **Project Management Stage** - Overseeing all project facets, including commercial, legal, and communications (internal and external);
- **Implementation Stage** - Integration of contemporary security solutions;
- **Procedures and documentation** - Developing procedures and policies according to the regulation
- **Managing & Operations** - Weekly reports, training, monitoring, and support for operational security;

TECHNOLOGICAL SOLUTIONS:

- **Network Security**

- Refreshing the existing network infrastructure with a new, high-capacity solution through the implementation of a next-generation Fortinet firewall. This fortifies network security against potential cyberattacks;
- Integration with our Security Operations Center (SOC) provides continuous monitoring, threat identification and investigation, incident management, and reporting;

- **Device & Data Protection**

- Comprehensive defense against malicious attacks, including malware and ransomware, coupled with multifactor authentication and automated vulnerability management through Acronis Cyber Protect;
- An integrated platform has been deployed for capturing and analyzing log files, identifying abnormal activities and potential threats, ensuring uninterrupted cybersecurity;
- Critical data is archived automatically, and cloud storage is facilitated via Diamatix Cloud.

- **Policies & Procedures**

- Developed by Diamatix's team, specific policies, procedures, and processes for network and information security cover key requirements such as access control, data and incident management, and system change management;

BUSINESS IMPACT:

The municipality invests in cybersecurity enhancements to safeguard citizens' personal data and ensure uninterrupted access to electronic services. This will contribute to bolstering trust in the municipal administration, optimizing operations, and adequately addressing national regulatory requirements to elevate the level of cyber resilience.

UTILIZED PRODUCTS AND SERVICES:

- Fortigate
- Acronis Endpoint Protection
- Diamatix Cloud Services
- Diamatix SOC
- Diamatix EDR
- Diamatix Professional Services
- Diamatix Managed Services