Cybersecurity for Local Government

New Funding Opportunities

The security study of local government websites conducted by the CSIRT NASK team in 2020 revealed **shocking data**. In over half of the examined sites, **vulnerabilities to attacks**, including serious errors, were discovered. These are increasingly being noticed and exploited by **cybercriminals**. Evidence of this is the clear upward trend in the number of reports registered by CSIRT NASK in the second half of 2022.

The Digital Poland Projects Center, in cooperation with the National Research Institute NASK, has commenced the acceptance of applications for the **"Cybersecure Local Government"** project. This initiative is targeted at **over 2.8 thousand local government units**, including municipalities, counties, and provinces. Funding is available for various purposes, such as **the development, implementation, and certification of procedures** related to information security management. Additionally, it covers **the acquisition, implementation, and configuration of systems, devices, and services** aimed at enhancing the level of cybersecurity.

The implementation of the project in a local government unit will contribute to, among other things:

- implementation or update of information security policies
- implementation of risk management measures in cybersecurity
- implementation of mechanisms and measures to enhance resilience to cyber threats

The deadline for submitting applications

from **July 19th** to **November 30th**, 2023

The amount of the grant

from **200,000** to even **850,000** PLN

Funding dependent on

the **population size** and **prosperity** of the unit

To ensure the required own contribution, which amounts to only **about 4%** for the entire project, only the wealthiest local governments will be obligated. Local governments will be able to settle actions carried out within the project between **June 1, 2023, and June 30, 2026.**

Information security management in the unit encompasses a broad range of activities related to the development and implementation of regulations, policies, and procedures. It also requires having the appropriate IT infrastructure. For over 20 years, **BTC** has been supporting public administration units in managing and ensuring the security of IT infrastructure.

These capabilities are enabled by the systems we implement:

- **eAuditor** - Comprehensive solution for managing, inventorying, monitoring, and ensuring IT security. The eAuditor software supports key processes in the organization and provides comprehensive support for IT departments.
- **Hyprovision DLP** - Professional data leak prevention system offering extensive control and blocking capabilities for servers. It prevents data loss and allows for the detection of suspicious activities.
- **Permission Management System** - Comprehensive software automating the processes of granting, verifying, and revoking permissions for IT systems. It contributes to increased IT security by ensuring the ongoing monitoring of permissions.
- **Whistleblower Module** - System dedicated to receiving reports of legal violations from whistleblowers, in accordance with the regulations of the Directive of the European Parliament and the Council of the EU. It is a secure channel for reporting irregularities in organizations.
- **eHelpDesk** - Solution for managing technical support processes. The system allows for supervising provided IT services and managing incidents to limit their negative impact on business.
- **RODOprotektor** - Solution for managing personal data in accordance with the GDPR. It supports data administrators and data protection officers in carrying out their daily tasks, allowing for oversight of authorizations and estimating potential threats.

Why choose the eAuditor system within the Cybersecurity for Local Government Program?

The eAuditor system meets all the requirements for ensuring the cybersecurity of local government IT systems. As part of the "Cybersecurity for Local Government" program, we propose implementing our solutions to **enhance the level of IT security** in local government entities.

Our clients appreciate that we provide IT departments with a comprehensive solution that, even in the basic configuration, enables: **ensuring IT security, IT management, IT inventory, and IT monitoring.**

indicators of security
for IT infrastructure (SOC)

secure remote connections
to computers in the local network and behind NAT using Real-Time Communication (RTC) technology

remote and mass encryption
of system and non-system partitions for SSD/HDD and USB using MS BitLocker.

monitoring permissions
MS ACL

Functionalities to ensure IT security

security policies DLP
(Data Loss Prevention)

Application Kiosk
as a method for secure software installation by employees

artificial Intelligence (AI)
in the process of classifying websites based on their content

Employee Panel
as an effective method of informing and training employees

Support for cybersecurity activities in the Local Government Unit (and Subordinate Units)

Selected items

Protection (OCH)	Action	Proposed solution
(OCH.1) Identity management, authentication, and access control	The Identity and Access Management system has been implemented in the Unit.	PAM - Permission Management System
	Remote access management to the resources of the Unit is operational.	eAuditor, Hyprovision DLP
	User accounts and their access rights to resources are managed by the Unit, following the principle of least privilege and separation of duties.	PAM - Permission Management System; eAuditor
	The integrity of the Unit's network is protected (e.g., through segmentation).	eAuditor, Hyprovision DLP
	Access verification to the Unit's resources is based on the use of multi-factor authentication (MFA).	eAuditor, Hyprovision DLP; PAM - Permission Management System
(OCH.2) Awareness and competence--building	Users with high privileges understand their roles and responsibilities in the Unit.	eAuditor LMS - Learning Management System
	The senior-level management in the Unit understands their roles and responsibilities.	eAuditor LMS - Learning Management System
	The cybersecurity and physical security personnel in the Unit understand their roles and responsibilities.	eAuditor LMS - Learning Management System
(OCH.3) Data Security	In the Unit, data at rest is protected.	Hyprovision DLP
	In the Unit, transmitted data is secured.	Hyprovision DLP
	The Unit's resources are formally managed during deletion, relocation, and disposal.	Hyprovision DLP
	The Unit maintains the appropriate capability to ensure availability of its data.	eAuditor, Hyprovision DLP
	Data leakage prevention mechanisms have been implemented in the Unit.	eAuditor, Hyprovision DLP
(OCH.5) Protective Technology	Event logs/records/inspections are defined, documented, implemented, and reviewed in accordance with the Unit's policies.	eAuditor, Hyprovision DLP
	Removable media are protected, and their usage is restricted according to the Unit's policies.	eAuditor, Hyprovision DLP
	The principle of least functionality is applied in the Unit when configuring systems, ensuring they have only the necessary capabilities.	eAuditor, Hyprovision DLP

Events and Monitoring (CM)	Action	Proposed solution
Anomalies and Events (CM.1)	Detected events in the Unit are analyzed to detect the method, course, and purpose of attacks.	Hyprovision DLP
	Event data is collected from multiple sources in the Unit's IT infrastructure, then centrally correlated and analyzed.	Hyprovision DLP
Continuous Security Monitoring (CM.2)	The Unit's network is monitored to detect potential cybersecurity events.	Hyprovision DLP
	The physical environment of the Unit is monitored to detect potential cybersecurity events.	eAuditor, Hyprovision DLP
	The activity of the Unit's personnel is monitored to detect potential cybersecurity-related events.	eAuditor, Hyprovision DLP
	Malicious code in the Unit's software is detected.	eAuditor, Hyprovision DLP
	Unauthorized source code in the Unit's software is detected (e.g., ActiveX, JavaScript).	eAuditor, Hyprovision DLP
	The activity of external service providers for the Unit is monitored to detect potential cybersecurity threats.	eAuditor, Hyprovision DLP
	Continuous monitoring for unauthorized access, connections, devices, and software is conducted in the Unit.	eAuditor, Hyprovision DLP
	Cyclical vulnerability scanning is conducted in the Unit.	eAuditor, Hyprovision DLP

Response (RE)	Action	Proposed solution
Incident Response Planning (RE)	The incident response plan in the Unit is executed during or after the incident occurs.	Hyprovision DLP
	The personnel in the Unit are familiar with their roles and the sequence of operations in the event of needing to respond to security incidents.	eAuditor, Hyprovision DLP
	Incidents are reported in the Unit according to established procedures.	eHelpdesk
	Information about security incidents is shared within the Unit according to incident response plans.	eHelpdesk
	Voluntary exchange of information by the Unit with external entities is conducted to achieve a broader situational awareness in cybersecurity.	All systems - through APIs
	The Unit is connected to the S46 system.	All systems - through APIs
Incident Handling (OI)	Incidents are detected, reported, and handled within the Unit.	eAuditor, Hyprovision DLP, eHelpdesk
	Corrective actions are taken after incidents occur.	eAuditor, Hyprovision DLP, eHelpdesk
	New vulnerabilities identified in the Unit are either remediated or accepted, and the associated risks are documented.	eAuditor, Hyprovision DLP, eHelpdesk
Improvement (DS)	Incident response plans take into account drawing conclusions from detected and handled incidents.	eAuditor, Hyprovision DLP, eHelpdesk
	Incident response policies in the Unit are updated.	eAuditor, Hyprovision DLP, eHelpdesk

Essential functions to ensure IT security during remote work

Computer Management

- Dashboard – information about IT infrastructure
- Remote installation / uninstallation
- Remote desktop (RDP, RTC, VNC, UVNC)
- Remote management of Intel VPro / AMT
- Remote configuration
- Remote restart
- Remote execution of CMD scripts (several built-in scripts)
- Remote execution of PowerShell scripts (several built-in scripts)
- Technical support

Users

- Information about online users
- Login and logout times
- Work monitoring (active and inactive time)
- Monitoring of launched applications
- Monitoring of running processes
- Monitoring of printers and printouts
- Monitoring of websites based on content (machine learning)
- Monitoring of outgoing mail and attachments
- Remote employee training and monitoring of the training process progress

Device Monitoring

- Time of turning on, turning off, sleeping
- Computer location by IP (computer behind NAT)
- Connected external USB devices
- Monitoring and managing services
- Performance monitoring (RAM, HDD, CPU)
- Event log monitoring
- Employee process monitoring

Security

- Remote disk encryption (Bitlocker)
- BitLocker USB encryption
- Blocking unauthorized external USB devices
- Blocking launched websites
- Blocking running processes

Education and Communication

- Remote employee training
- Defining own training materials
- Ready instructional videos on security
- Automatic communication with users – sending any content with confirmation of receipt and reading
- Displaying urgent messages to users (Alert)
- Displaying messages to users

Do you want to learn more?

Fill out the form and schedule a free presentation!

Visit the eAuditor.eu website