Proposal for the Procedure to Consolidate Cybersecurity Activities and Prepare for the NIS2 Directive:

1. Implementation of the Consolidation of Existing Data and Collection of New Required Information.

The outcome of this activity will be a cybersecurity consolidation document for the company, including a proposal for preparation for the NIS2 directive.

The document will include a budget, a timeline, and all activities necessary to ensure cybersecurity compliance with the NIS2 directive.

2. Regular performance of the activities of a cybersecurity manager, including:

- Management of various security incidents,
- Communication with the organization's IT and cybersecurity department,
- Cooperation with employees of contracted organizations,
- Coordination with IT service providers,
- Support in raising employee awareness about cybersecurity.

Task schedule:

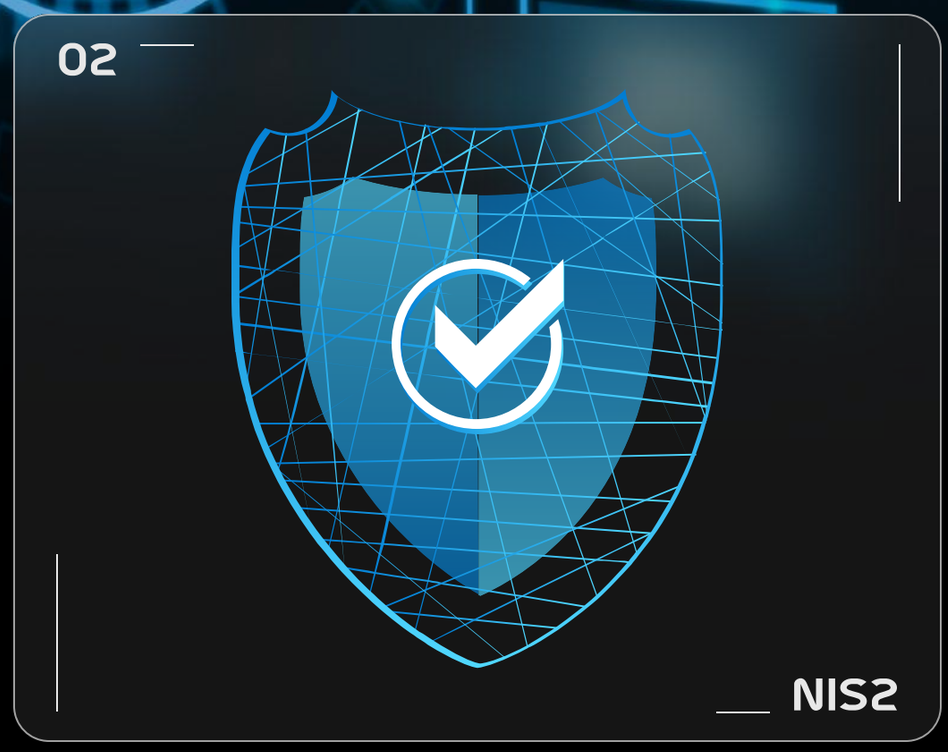
- Consolidation of existing documentation, updating of personnel matrices.
- Consolidation of supplier-customer relationships to ensure compliance.
- Monitoring of reports required for NIS2 compliance
- Providing information about security incidents to the national KB agency
- Establishment of a safety committee and development of a safety committee directive.
- Coordination of activities during security incidents.
- Analysis of software equipment for monitoring physical network devices with definition of threats and proposal of measures.
- Consolidation of organizational measures.
- Consolidation of technical measures.
- Consolidation of personnel measures – security policy and identity verification.
- Consolidation of process measures.
- Monitoring of external and internal threats.
- Penetration testing with reporting.
- Continuous network review with a proposal to update network segmentation based on the results.
- Identification of the current state and topology of the network, design of new segmentation and network rules between individual new segments, which will be designed based on the classification. Revision of FW and VPN profile rules, addition of IDS/IPS to individual network segments and their connection to SIEM.

Result: Consolidation report with draft recommendations.

List of activities required to prepare for compatibility with the NIS2 Directive in accordance with EU regulations

The following documentation needs to be processed:

- Development of a cybersecurity strategy in accordance with the NIS2 directive.
- Guidelines for security incident management, including defining procedures for resolving basic types of security incidents (e.g. malware, ransomware, phishing, spearphishing, vishing, DOS and DDoS, system unavailability, system or network intrusion, data and information leakage, etc.) and consolidating incident resolution procedures with a SIEM/SOC service provider.
- Guidelines for secure operation of information systems and networks.
- Guidelines for monitoring cyber incidents.
- Recovery plan guidelines, including detailed recovery plans (DRPs).
- Backup guidelines.
- Business continuity management (BCM) guidelines.
- Access rights management guidelines.
- Asset and risk management (AR/BIA) guidelines.
- Development of security projects for individual solutions.
- Guidelines for secure storage.
- Guidelines on the security of individual facilities, including security projects and DRP plans.



The technical part includes:

- Updating software and hardware equipment according to cybersecurity requirements.
- Deploying security solutions and updating them:
- Patch management.
- Central management of physical devices.
- Implementation of SIEM/SOC "as a service" including external support for resolving security incidents.
- Access management (2FA, VPN for suppliers).

Future-proofing:

Role of the Data Protection Officer (DPO):

Implementation in compliance with GDPR and personal data

- Public authorities and entities.
- Processing of data on a large scale.
- Processing of sensitive data.

DPO Responsibilities:

- Provision of information and advice.
- Monitoring compliance.
- Cooperation with the supervisory authority.
- Independence in performing tasks.

Implementation of the Cybersecurity Act:

- Activity of the responsible person – Anti-corruption auditor.
- Possibility of using an ethical hacker

Implementation method: Software solutions + professional activities of qualified persons.