

Implementation of Cybersecurity

How We Cover It Technically

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. Access Control Management . . . 3
   2.1. Functions and Components . . . 3
   2.2. Access Rights Lifecycle . . . 3
   2.3. Roles in the Access Rights Process . . . 4
   2.4. Recertifying Access Rights . . . 4
   2.5. Findings of a Review . . . 4
   2.6. Segregation of Duties . . . 5
3. Identity Management and Verification . . . 6
   3.1. Methods of Identity Management and Verification . . . 6
   3.2. Authentication Strength . . . 6
   3.3. Interim Rules for Authentication . . . 7
4. Privileged Access Management (PAM) . . . 8
   4.1. Privileged Access Management (2) . . . 8
5. Choosing an Access Control Model . . . 9
6. Single Sign-On (SSO) . . . 10
   6.1. Single Sign-On (SSO) (2) . . . 10
7. Access Control Policy . . . 11
8. Communication Network Security . . . 12
   8.1. Key Measures . . . 12
   8.2. Tools for Communication Network Security . . . 12
   8.3. Methods for Ensuring the Integrity of Communication Networks . . . 12
   8.4. Activity Recording and Protection of Data . . . 13
   8.5. Intrusion Detection System . . . 13
   8.6. Intrusion Prevention System . . . 13
   8.7. Monitoring, Testing, and Audit . . . 13
9. Protection against Malicious Code . . . 15
   9.1. Implementation . . . 15
   9.2. Implementation (cont.) . . . 15
   9.3. Roll-out of the Measure . . . 15
   9.4. Roles in Protection against Malicious Code . . . 16
   9.5. Removable Media and Code Execution . . . 16
10. Antivirus vs Anti-malware Systems . . . 17
   10.1. Detection Methods in Detail . . . 17
   10.2. Selecting an Anti-Malware Solution . . . 17
11. Email Security Solutions . . . 19
   11.1. Handling a Suspicious E-mail . . . 19
12. Handling a Malware Incident . . . 20

13. Ransomware . . . 21
13.1. Ransomware Prevention . . . 21
13.2. Ransomware Response . . . 21
14. Recording Events . . . 22
14.1. What Must Be Logged . . . 22
15. Process of Introducing Event Recording . . . 23
16. Collection and Evaluation of Cybersecurity Events . . . 24
16.1. Process of Collection and Evaluation . . . 24
16.2. Example: ELISA Security Manager . . . 24
16.3. Tools for Collection and Evaluation of Cybersecurity Events . . . 25
16.4. How a SIEM Works . . . 25
16.5. EDR and NTA . . . 26
16.6. Network Monitoring Tools . . . 26
16.7. Audit Tools . . . 27
17. Triage and Escalation of Alerts . . . 28
17.1. Severity Levels . . . 28
18. Evaluation Tool and False Positives . . . 30
18.1. Handling False Positives . . . 30
18.2. Detection Use Case . . . 30
19. Detection Quality . . . 32
20. Cryptographic Tools . . . 33
21. Terms . . . 34
22. Choosing an Algorithm . . . 35
22.1. Libraries and Certification . . . 35
23. Implementing Cryptographic Tools . . . 36
24. Key and Certificate Management . . . 37
24.1. Key Management Lifecycle . . . 37
24.2. Roles in Key Management . . . 37
24.3. Key Management Procedure . . . 38
25. End-to-End Encryption (E2EE) . . . 39
25.1. End-to-End Encryption (2) . . . 39
26. Application Security . . . 40
27. Processes in Application Security . . . 41
27.1. Processes in Application Security (2) . . . 41
27.2. Processes in Application Security (3) . . . 41
28. Penetration Testing . . . 42
28.1. Types of Penetration Test . . . 42
28.2. Methodologies and Standards . . . 42
28.3. Phases of a Penetration Test . . . 42
28.4. Rules of Engagement . . . 43
29. Ensuring the Availability of Information . . . 44

29.1. Measures by Availability Rating . . . 44
29.2. Roles in Ensuring Availability . . . 44
29.3. Tools and Procedures . . . 45
29.4. Tools and Procedures (cont.) . . . 45
30. Redundant Systems . . . 46
30.1. Redundant Systems (cont.) . . . 46
31. Data Backup . . . 47
31.1. Choosing a Backup Location . . . 47
31.2. Backup and Restoration Process . . . 47
31.3. Backup Schedule . . . 48
32. Data Recovery . . . 49
33. Distributed Systems . . . 50
33.1. Distributed Systems (cont.) . . . 50
34. Load Balancing . . . 51
34.1. Load Balancing (cont.) . . . 51
35. Monitoring and Problem Detection . . . 52
35.1. Monitoring and Problem Detection (cont.) . . . 52
36. Disaster Recovery Planning (DRP) . . . 53
36.1. Disaster Recovery Planning (cont.) . . . 53
37. Industrial, Control, and Similar Specific Systems . . . 54
38. OT and IT Compared . . . 55
39. Securing Specific Technical Assets . . . 56
39.1. Requirements of Section 27 . . . 56
40. Introducing Security in OT . . . 57
40.1. Roles in OT Security . . . 57
40.2. Maintenance-Window Record . . . 57
41. Digital Services . . . 59
42. Measures for Digital Services . . . 60
43. Obligations by Type of Service . . . 61
44. Handling an Illegal Content Notice . . . 62
44.1. Roles in Digital Services . . . 62
44.2. Notice and Action Record . . . 62
44.3. Products with Digital Elements . . . 63
44.4. Tools . . . 63

- Expected lecture date WS 2026: **Dec 1**

Chapter 1. Module Summary

- **Access control management**: functions and components, identity management and verification, authentication strength.
- **Authorization models**: role-based access control (RBAC), privileged access management (PAM), single sign-on (SSO), choosing an access control model.
- **Network security**: key measures and tools, integrity of networks, IDS and IPS, monitoring, testing, and audit.
- **Protection against malicious code**: implementation of the measure, antivirus vs. anti-malware, detection methods in detail.
- **Email security**: content filtering, anti-spam, authentication (SPF, DKIM, DMARC), encryption, handling of a suspicious e-mail, handling of a malware incident.
- **Recording events**: what must be logged, protection and retention of logs, introducing event recording.
- **Collection, evaluation, and detection of events**: the process (ELISA example), tools (SIEM, log management, IDS/IPS, EDR, NTA, SOAR), how a SIEM works, EDR and NTA, triage and escalation, severity levels, use cases, detection quality.
- **Cryptographic tools**: terminology, current tools, implementation, key and certificate management, E2EE.
- **Application security**: SDLC, SAST, DAST, IAST, penetration testing (types, phases, rules of engagement), secure authentication, encryption, patching, education.
- **Availability**: rating-driven measures, roles, backup and restore process, choosing a backup location, redundancy, load balancing, monitoring, disaster recovery planning.
- **Special systems**: industrial control (OT) vs. office systems (IT), IEC 61511 vs. ISO/IEC 27001:2022, measures and tools for digital services.

Chapter 2. Access Control Management

- Access Control Management is a process that ensures that only **authorized persons** have access to certain resources, information, or systems.
- Its goal is to ensure that the right people have access to the right resources at the right time and for the right reasons.
- Decree No. 409/2025 Coll., Section 13 (access management), Section 19 (identity management), and Section 20 (access rights management)

2.1. Functions and Components

- Identification of users and resources
- Definition of permissions
- Implementation of control mechanisms
- Monitoring and auditing
- Permission lifecycle management

2.2. Access Rights Lifecycle

Request

The manager or the user requests the resources and the operations needed for the job — described through **roles**, not individual systems. Decree No. 409/2025 Coll., Section 13(2)(a)

Approval

The role (data) owner approves the request. The approver must not be the requester — see segregation of duties below.

Provisioning

The administrator grants the rights through the access rights management tool, **only to the level strictly necessary for the work**; the user and administrator accounts of one person are kept separate. Decree No. 409/2025 Coll., Section 13(2)(b), Section 20

Use

The account is used under the assigned roles; its activity is recorded — see *Recording Events* in this module.

Review

All access rights and authorizations, including the division into groups and roles, are reviewed regularly — see *Recertifying Access Rights* below. Decree No. 409/2025 Coll., Section 13(2)(h)

Change or revoke

On a change of position the rights are changed **without delay**; on the end of the contractual relationship the account is **deactivated** and the rights removed without delay. Granting and revocation are documented. Decree No. 409/2025 Coll., Section 13(2)(i), (j), (k)

2.3. Roles in the Access Rights Process

Role	Responsibility
Requesting manager	States the business need; requests joiner, mover, and leaver changes
Role (data) owner	Approves requests for their resources; decides the outcome of every recertification finding
System administrator	Executes provisioning and revocation in the access rights tool; keeps the records
Security officer (cybersecurity manager)	Owns the access control policy; monitors the review cadence and the segregation rules
Auditor	Independently checks the documentation and review evidence; see *Cybersecurity Audit* in the last module

2.4. Recertifying Access Rights

- The **regular review of all access rights and authorizations, including the division into groups and roles** is a legal obligation; the campaign below turns it into a repeatable procedure. Decree No. 409/2025 Coll., Section 13(2)(h)
- The corresponding obligations are stated in *Access Control* in the previous module.

Scope

Decide which systems and roles are in this campaign; privileged accounts are always in.

Notify

Role owners receive the list of their users and the rights held.

Decide

The owner marks every right as **keep**, **change**, or **revoke** — no answer by the deadline means **revoke**.

Remediate

The administrator executes the decisions and records what changed.

Evidence

The campaign report — who decided, what changed, when — is kept for the auditor.

2.5. Findings of a Review

Finding	Action	Owner
Right exceeds the current job need	Revoke or downgrade to the level of the role	Role owner

Finding	Action	Owner
Account without an owner (contract ended, person left)	Deactivate immediately, then remove the rights	System administrator
Conflicting duties inside one role	Split the role; re-approve the pieces	Security officer
Review not completed in time	Repeat the campaign; record it as a finding for the audit	Security officer

2.6. Segregation of Duties

- No single person may **both authorize and execute** a sensitive action. Conflicting duties are split between different people, so that a mistake or an abuse by one is caught by another.
- Technical prerequisite: the user and administrator accounts of one person are separated, each with a unique identifier of its account type. Decree No. 409/2025 Coll., Section 13(2)(b)

Duties that must not be combined	Why
Requesting an access right and approving it	Self-granted privileges
Administering an account and auditing its activity	Covering one’s own tracks
Managing user accounts and managing the log records	Hiding account manipulation
Preparing a change and approving it for production	An unreviewed change reaches production

- Which security roles exist and how they are distributed — see *Organizational Security and Security Roles* in the third module.

Chapter 3. Identity Management and Verification

Component	Content
Identity management	Creating, updating, and deleting user accounts, including management of user attributes such as roles, groups, and permissions.
Authentication	The process of verifying a user's identity — *is the user who they claim to be* — usually through a password, biometric data, or multi-factor authentication (MFA).
Authorization	Determines which resources and applications a user can access based on their role and permissions.
Monitoring and auditing	Tracking and recording user activities to ensure security and compliance.

3.1. Methods of Identity Management and Verification

Identity management runs the whole account lifecycle: **registration** of the user and their identification data, assignment of **roles and permissions**, and **deletion** of the account. Verification then checks whether the user is who they claim to be — single-factor, two-factor, or multi-factor verification.

Roles and permissions

Defining what roles and permissions each user has in the system.

Monitoring and auditing

Tracking user activity and performing regular audits to ensure security.

3.2. Authentication Strength

Method	Factor types	Assurance	Typical use
Password alone	1 (knowledge)	Low	Interim state only — under the rules of the next slide
Password + one-time code from an application or token	2 (knowledge + possession)	Standard	Every user — the default requirement
Password + hardware token or smart card	2 (knowledge + possession)	High	Administrators and remote access
Continuous zero-trust authentication (behaviour and context)	continuous	Robust	Alternative allowed to multi-factor authentication

- Multi-factor means **at least two different factor types** — two secrets of the same type do not count. Decree No. 409/2025 Coll., Section 19(2)(a)

- The identity management tool verifies the identity **before** the activity starts, **limits the number of failed login attempts**, and requires **re-authentication after a period of inactivity**. Decree No. 409/2025 Coll., Section 19(1)

3.3. Interim Rules for Authentication

- Until the multi-factor requirement is met, authentication with **cryptographic keys or certificates** is used, and every account that does not comply is entered into a **register of exceptions** with a justification. Decree No. 409/2025 Coll., Section 19(2)(b), (3)
- Interim password tools must enforce: Decree No. 409/2025 Coll., Section 19(4), (5)
  - Minimum length of **12 characters** for user accounts, **17** for administrator accounts, **22** for technical asset accounts; at least **64** characters must be accepted
  - Mandatory change at least **once every 18 months**; no common or derived passwords (from the login name, e-mail, or system name); no reuse of the **last 12 passwords**
  - Default passwords changed immediately after the first login; one-time credentials for access recovery expire after **one use or at most 24 hours**

Chapter 4. Privileged Access Management (PAM)

Privileged account management

PAM solutions identify and manage accounts with high privileges that have access to sensitive systems and data. This includes creating, maintaining, and removing these accounts.

Secure authentication and authorization

PAM ensures that only authorized users can access privileged accounts. This is often done using multi-factor authentication (MFA) and other security measures.

Monitoring and auditing

PAM tools continuously monitor the activities of privileged accounts and record them for auditing purposes. This helps detect and respond to suspicious activity and ensures compliance with security policies.

4.1. Privileged Access Management (2)

Least Privilege Principle

This principle ensures that users only have the privileges they need to perform their tasks, minimizing the risk of abuse.

Just-in-Time (JIT) access

PAM can provide temporary access to privileged accounts only for the time necessary, further reducing the risk of unauthorized access.

Chapter 5. Choosing an Access Control Model

Model	Access is decided by	Strengths	Limits
DAC	The owner of the resource	Simple and flexible	Hard to audit; the owner can pass rights on
MAC	Security labels set centrally	Strongest separation	Rigid; administration is heavy
RBAC	The job role the user holds	Matches the organization; reviews work role by role	Roles must be designed; a wrong role spreads fast
ABAC	Attributes of user, resource, and context	Fine-grained and dynamic	The policy engine is complex; audits are harder

- The decree requires access to be **managed on the basis of groups or roles** — RBAC is therefore the default model here, enriched with attributes (ABAC) only where a role would become too coarse. Decree No. 409/2025 Coll., Section 13(2)(a)
- Which model applies where is recorded in the access control policy below; DAC and MAC appear only with a justification.
- The four models were introduced in *Access Control* in the previous module.

Chapter 6. Single Sign-On (SSO)

- Allows users to **log in once** and access multiple applications without having to re-enter their login details.

6.1. Single Sign-On (SSO) (2)

Federated identity

SSO is based on the concept of **federated identity**, which means sharing identity attributes between trusted but independent systems. When a user is authenticated by one system, they automatically gain access to other systems that have a trusted relationship with that system.

Authentication tokens

When a user logs in to a service using SSO, an authentication token is created and stored either in the user's browser or on a central SSO authentication server. This token serves as a digital key that confirms the user's identity when accessing other applications.

Protocols and standards

SSO uses various protocols and standards, such as SAML (Security Assertion Markup Language) and OpenID Connect, which enable the secure exchange of authentication information between systems.

Chapter 7. Access Control Policy

- One document carries the whole process; the auditor reads it first and then asks for the evidence behind it.

Template: access control policy (skeleton)

1. **Scope** — the systems, services, and roles the policy covers.
2. **Access model** — which model applies where (RBAC by default; DAC, MAC, or ABAC only with a justification).
3. **Rules for granting** — request, approval by the role owner, provisioning through the tool; least privilege; separate user and administrator accounts; four eyes for privileged rights.
4. **Authentication requirements** — multi-factor authentication per Section 19(2)(a) of the decree, the interim password rules, re-authentication after inactivity.
5. **Review cadence** — the recertification frequency for privileged and standard rights; the **no answer means revoke** rule.
6. **Segregation of duties** — the list of duty pairs that must not be combined.
7. **Exceptions** — who approves them, for how long, and with what compensating measures.
8. **Roles and responsibilities** — the five roles of the process above.
9. **Evidence** — records of granting and revocation, review campaigns, and the configuration of the management tools.

Chapter 8. Communication Network Security

Decree No. 409/2025 Coll., Section 18 (communication network security)

8.1. Key Measures

Communication network security rests on **encryption**, **authentication and authorization**, a **firewall** with **intrusion detection and prevention (IDS/IPS)**, **antivirus and antimalware programs**, **security updates and patches**, **port scanning**, **SIEM and event recording**, and **user training**.

8.2. Tools for Communication Network Security

User identity verification

Ensures that only authorized users have access to the network. See *Access Control Management* in this module.

Access control

Restricts access to the network and its resources to authorized users only. Models: **discretionary** (DAC), **mandatory** (MAC), **role-based** (RBAC), and **attribute-based** (ABAC) access control; the models are compared in *Choosing an Access Control Model* in this module.

Malware protection

Detects and blocks malware that could compromise data integrity. See *Protection against Malicious Code* in this module.

Activity logging

Monitors and records network activity, which helps in detecting and analyzing potential threats. See *Recording Events* in this module.

8.3. Methods for Ensuring the Integrity of Communication Networks

Authentication and authorization

Users must prove their identity (authentication) and have permission to access certain resources (authorization). This may include passwords, biometric data, or multi-factor authentication.

Network Access Control (NAC)

Controls access to the network based on predefined security policies.

Encryption

Data is encrypted during transmission and at rest. See *Cryptography* in this module.

8.4. Activity Recording and Protection of Data

Data loss prevention

Protects sensitive information from unauthorized access and leakage.

Log management and SIEM

Collection and analysis of logs from various sources to detect suspicious activities and generate alerts for suspicious activities. See *Recording Events* in this module.

Access rights control

Auditing and monitoring of user access to sensitive data and systems.

8.5. Intrusion Detection System

IDS

Function	Monitors and analyzes network traffic to detect potential attacks or intrusions.
Response	Passive; alerts administrators to detected threats, but does not interfere with operations.
Location	Typically deployed behind a firewall to monitor internal traffic.
Advantages	Low-cost implementation, no interference with network traffic.
Disadvantages	Potential delay in response to an attack, need for manual intervention by administrators.

8.6. Intrusion Prevention System

IPS

Function	Monitors, analyzes, and intervenes against suspicious traffic in real time.
Response	Active; can block or redirect traffic when a threat is detected.
Location	Deployed at the network entry point, often combined with firewall functionality.
Advantages	Fast response to attacks, automatic prevention.
Disadvantages	Higher implementation costs, potential false alarms may disrupt traffic.

8.7. Monitoring, Testing, and Audit

Penetration testing

Simulated cyber attacks against the network.

Vulnerability scanning

Automated tools that scan systems and networks for known vulnerabilities.

Audit of the network measures

See *Cybersecurity Audit* in the last module.

Chapter 9. Protection against Malicious Code

Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Section 21(2) (continuous and automatic protection against malicious code, control of removable media, automatic start-up, and code-execution rights) and Section 21(3) (regular and immediate updates of the tool and its detection rules)

9.1. Implementation

Scanning and detection

The software regularly scans files and applications on your device to identify potential threats. This includes checking files against a database of known malicious code and heuristic analysis that looks for suspicious behavior.

Reactive measures

If malicious code is detected, the software can isolate (quarantine) or remove it to prevent its spread and damage.

9.2. Implementation (cont.)

Database updates

Antivirus software regularly updates its database of known threats so that it can recognize and protect against the latest types of malicious code.

Real-time protection

Some tools offer real-time protection that monitors activity on your device and blocks suspicious actions immediately.

Security measures

As part of broader cybersecurity, various security measures can be implemented, such as a firewall, data encryption, and regular backups.

9.3. Roll-out of the Measure

Scope

The security officer and the administrators inventory the endpoints and decide which assets need protection — from the **asset evaluation** and the risk assessment.

Deployment

Administrators install **one centrally managed tool** on every relevant asset and check the coverage against the asset inventory. Decree No. 409/2025 Coll., Section 21(2)

Configuration

Policies are set: real-time protection, quarantine action, control of removable media, automatic start-up, and code-execution rights.

Updates

The tool, its settings, and its detection rules are updated **regularly and immediately**, and the update status is monitored. Decree No. 409/2025 Coll., Section 21(3)

Verification

A harmless test sample confirms on every asset class that detection and alerting actually work.

Review

Coverage, false-positive load, and update status are reviewed regularly and fed back into the risk assessment.

9.4. Roles in Protection against Malicious Code

Role	Responsibility
Security officer (cybersecurity manager)	Defines the scope from the asset evaluation; approves the policies; reviews coverage
System administrator	Deploys and configures the tool; monitors the update status
Analyst on duty	Investigates detections and decides on quarantine, cleanup, or escalation
Users and administrators	Keep the protection enabled and report blocked files and unusual behaviour of assets Decree No. 409/2025 Coll., Section 14(1)(f)
Auditor	Verifies the coverage and update evidence; see *Cybersecurity Audit* in the last module

9.5. Removable Media and Code Execution

- The tool must **control the use of removable media** and prevent the **automatic start-up** of media content; rules for the management of removable media are part of the security measures. Decree No. 409/2025 Coll., Sections 7 and 21(2)(b), (c)
- The **rights to execute code** and the communication between applications are restricted to what the work requires. Decree No. 409/2025 Coll., Section 21(2)(d), (e)

Rule	Practice
Removable media	Scan on insertion, no automatic start-up, only registered or encrypted media
Code execution	Application allowlisting on sensitive assets — only approved programs may run
Lost media	Reported and revoked; the content was encrypted
Related obligation	Limiting software that can bypass system or application controls — see *Access Privileges* in the previous module

Chapter 10. Antivirus vs Anti-malware Systems

	Antivirus	Anti-malware
Focus	Detects and removes **computer viruses**; the oldest tool category	Detects and removes a **wide range of malicious software** — viruses, spyware, ransomware, Trojans, adware
Methods	Virus signature databases and heuristic analysis; monitors changes in the system, directories, and system areas of the disk	Signatures and heuristics plus **behavioral analysis** in real time and **sandboxing**
Updates	Signature databases	Frequent updates of signatures and of the program itself, reacting to new and emerging threats

10.1. Detection Methods in Detail

Method	Principle
Signature detection	Comparison of file contents or traffic with signatures of known threats stored in a database. Precise, but blind to unknown threats.
Heuristic analysis	Detection of new or unknown threats based on analysis of file or program behavior; suspicious behavior is flagged as a potential threat.
Behavioral analysis	Monitoring of program behavior in real time — attempts to modify system files or to access sensitive data — with immediate response.
Sandboxing	Running a suspicious file in an isolated virtual environment and monitoring what it does: "detonation" reveals attempts to modify system files or to communicate with external servers.
Integrity check	Monitoring changes in the system, directories, and system areas of the disk; unexpected changes may indicate the presence of malware.
Automatic updates	Regular updates of signature databases and of the program itself are key to protection against the latest threats; without updates, new types of malware cannot be detected.

10.2. Selecting an Anti-Malware Solution

Criterion	What to check	Why
Detection coverage	Signature, heuristic, behavioral, and sandboxing methods combined	Signatures alone are blind to unknown threats

Criterion	What to check	Why
Central management	One console for policy, coverage, and update status of every asset	The law requires a **centrally managed tool** Decree No. 409/2025 Coll., Section 21(2)
Updates	Regular and immediate updates, including detection rules	Required by Decree No. 409/2025 Coll., Section 21(3)
Performance	Resource load during scans on production endpoints	A tool that slows down the work gets switched off
False positives	Ways to tune rules and whitelist without disabling protection	False alerts erode trust in the tool
Integration	Export of detections into the recording and detection tools	Detections must become events and alerts — see *Detection of Cybersecurity Events* in this module

Chapter 11. Email Security Solutions

Email security combines **content filtering** (detecting and blocking malicious attachments and links), **anti-spam filters** (content analysis, reputation databases, machine learning), **email authentication** (SPF, DKIM, and DMARC verify that a message comes from a trusted source and was not altered in transit), **encryption** (transport-layer TLS and end-to-end), and **advanced threat detection** (behavioral analysis of email traffic).

11.1. Handling a Suspicious E-mail

Report

The user reports the message **without clicking anything** — reporting suspicious behaviour is a duty of users, administrators, and contractors. Decree No. 409/2025 Coll., Section 14(1)(f)

Analyze

The analyst checks headers and links and runs the attachment in a sandbox (see *Detection Methods in Detail* above).

Block and withdraw

The mail administrator blocks the sender, URL, or attachment at the gateway and removes the message from the mailboxes.

Update

Filters, reputation lists, and detection rules are updated; the case feeds the awareness training.

Record

The handling is recorded as an event — see *Recording Events* in this module. If it led to a compromise, it continues as an incident — see *Managing Cybersecurity Events and Incidents* in the previous module.

Chapter 12. Handling a Malware Incident

Detect and confirm

The detection tool raises an alert; the analyst confirms it and assigns a severity — see *Triage and Escalation of Alerts* in this module.

Contain

The affected systems are isolated (network segment, account) and the spreading vector (mail, media) is blocked at the gateway — without destroying the evidence.

Eradicate

The malware is removed or the system is reinstalled; the entry point is closed and the credentials and rights of compromised accounts are changed.

Recover

Systems return from verified backups or clean images, with protection active and updated, before they are reconnected.

Learn

The cause, the records, and the handling are documented, the effectiveness of the solution is evaluated, and the detection rules are updated. Decree No. 409/2025 Coll., Section 14(1)(k), (l), (n)

- Who takes which responsibility and how the escalation works is given in *Managing Cybersecurity Events and Incidents* in the previous module.

Chapter 13. Ransomware

13.1. Ransomware Prevention

- **Isolated and verified backups** — backup environments are separated from the other environments, so that the malware cannot reach the backups together with the affected system. Decree No. 409/2025 Coll., Section 26(5)
- **Least privilege and separated administrator accounts** — see *Access Rights Lifecycle* in this module; one compromised administrator account would spread the attack everywhere.
- **Updates** — patches of systems and immediate updates of the protection tool close the entry points. Decree No. 409/2025 Coll., Section 21(3)
- **E-mail gateway filtering** — phishing is the main delivery vector; see *Email Security Solutions* above.
- **Restricted code execution** — no automatic start-up of media, allowlisting on sensitive assets (two slides above).

13.2. Ransomware Response

Containment first

Isolate the affected systems and segments from the network to stop the spread; detection keeps recording — see *Triage and Escalation of Alerts* in this module.

Identify the entry point

From the recorded events and detections, determine how the malware got in and which accounts were involved — see *Recording Events* and *Detection of Cybersecurity Events* in this module.

Recover only from verified sources

Restore from isolated, tested backups or clean images; confirm that the protection tool is active and updated before a system returns.

Report and evaluate

Handle it as an incident — see *Managing Cybersecurity Events and Incidents* in the previous module; document the cause and evaluate the handling. Decree No. 409/2025 Coll., Section 14(1)(k), (n)

Chapter 14. Recording Events

- Recording events in the information and communication system, its users, and administrators
- Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Sections 21 (detection), 22 (recording), and 23 (evaluation of events)

14.1. What Must Be Logged

Logged item	Typical content
User activity	Logon / logoff, failed authentication, password and privilege changes, use of privileged accounts
Application activity	Start and stop, access to records, configuration and security-relevant parameter changes
System activity	Service and system starts and stops, installation of software, changes to system time
Network activity	Sources and destinations of connections, source and destination addresses, ports, protocols, transferred volume
Security event	Alarms, warnings, detected incidents, actions of detection and evaluation tools

Logs must be stored in a place where they **cannot be modified by the users whose actions are being logged**, and their retention period must be set so that investigations remain possible.

Recording is followed by the **Collection and Evaluation of Cybersecurity Events** (see the next section), and the whole tooling is introduced by the process below.

Chapter 15. Process of Introducing Event Recording

Analysis of the current state

Evaluation of the current security of the information and communication system, identification of weaknesses and risks.

Proposed solution

Preparation of a feasibility study containing proposals for technical and organizational measures.

Implementation of technical measures

Introduction of tools for recording activities, including monitoring and logging of user and administrator activities, detection and evaluation of cyber security events, and protection of communication network integrity and user identity verification.

Control and audit

Regular checks and audits to ensure that the tools are functioning properly and effectively; see *Cybersecurity Audit* in the last module.

Training and awareness

Educating users and administrators about security procedures and the use of tools.

Chapter 16. Collection and Evaluation of Cybersecurity Events

Collection and evaluation is the step that follows recording: the events recorded under *Recording Events* are collected from the individual sources, correlated, evaluated, and turned into alerts and reports for the designated security roles.

Decree No. 409/2025 Coll., Sections 23 (detection of events) and 24 (collection and assessment of cyber security events); Act No. 264/2025 Coll., Section 14

16.1. Process of Collection and Evaluation

Data Collection

The tool gathers logs and events from various sources such as servers, network devices, applications, and databases. Agents like **NXLOG** are often used for this purpose, as they can collect data from text logs, Windows event logs, and other types of structured logs.

Correlation and Analysis

The collected data is analyzed and correlated in order to detect security incidents. ELISA uses advanced correlation mechanisms that enable the detection of events based on recurring patterns or unusual behavior, such as malware propagation or unusual user logins.

Risk Evaluation

The tool assigns each event a risk score that helps prioritize actions to address detected incidents. This allows for faster and more effective responses to security threats.

Notification and Response

Once suspicious activity is detected, the tool generates an alert and may automatically initiate response actions, such as blocking an IP address or isolating an infected system.

16.2. Example: ELISA Security Manager

User Interface

Data and analyses are presented in a clear user interface that enables easy searching and filtering of information.

Automation and Integration

The tool supports automated evaluation and integration with other security tools and systems, increasing its efficiency and ability to respond to incidents in real time.

Regular Updates

To remain effective, detection tools must be regularly updated with information about new threats and vulnerabilities.

16.3. Tools for Collection and Evaluation of Cybersecurity Events

Tool	Function
SIEM	(Security Information and Event Management) — collect, normalize, correlate, and analyze data from various sources
Log Management Tools	collect and manage logs from different systems and applications, enabling anomaly analysis and detection
IDS/IPS	(Intrusion Detection Systems / Intrusion Prevention Systems) — monitor network traffic and detect suspicious activities / take actions to prevent attacks
EDR	(Endpoint Detection and Response) — monitor and analyze activities on endpoint devices
NTA	(Network Traffic Analysis) — analyze network traffic and identify potential threats
SOAR	(Security Orchestration, Automation, and Response) — integrate and coordinate various security tools, automate repetitive tasks, and streamline workflows for handling incidents and threats

16.4. How a SIEM Works

Data collection

SIEM systems collect logs and events from various sources, such as servers, applications, network devices, firewalls, and other security tools. This data is centralized into a single repository.

Data normalization

The collected data is normalized, which means it is converted into a uniform format. This facilitates its analysis and correlation.

Event correlation

SIEM systems analyze normalized data and look for patterns and anomalies that may indicate security incidents. Correlation allows you to identify connections between different events and uncover potential threats.

Threat detection

Using predefined rules, machine learning, and behavioral analysis, SIEM systems detect suspicious activity and generate alerts based on identified threats.

Incident response

SIEM systems can be integrated with tools for orchestrating and automating security operations (SOAR), which enables automatic response to detected threats, such as isolating infected devices or blocking malicious traffic.

Reporting and auditing

SIEM systems generate reports and provide auditing tools, which help organizations meet regulatory requirements and improve their security posture.

16.5. EDR and NTA

EDR — continuous monitoring

EDR tools continuously monitor activities on endpoints and record data about these activities. This includes monitoring processes, files, networks, and user activities.

Data analysis

The collected data is analyzed using techniques such as machine learning and anomaly detection to identify suspicious activities that could indicate security threats.

Automatic response

EDR can automatically take actions to mitigate or eliminate threats, such as isolating an infected device or removing malicious software.

EDR — alerting and reporting

It generates alerts and reports for security teams to help them respond quickly to incidents and conduct further investigations.

Correlation and contextualization

EDR tools correlate data from various sources and provide context for a better understanding of security incidents. This includes identifying the origin of an attack, its scope, and its impact.

NTA — anomaly detection

Using techniques such as behavioral analysis and machine learning, tools detect unusual patterns in network traffic that may indicate security threats or performance issues.

16.6. Network Monitoring Tools

Data collection

Network monitoring tools collect data from various network devices such as routers, switches, servers, and other components. This data includes information about traffic, performance, and device status.

Performance analysis

The tools analyze the collected data to identify performance problems such as high latency, packet loss, or bandwidth congestion. This analysis helps optimize network performance and prevent outages.

Availability monitoring

Network monitoring tools track the availability of network devices and services. If an outage or failure occurs, the tools generate alerts that enable a rapid response and minimize the impact on users.

Anomaly detection

Using techniques such as behavioral analysis and machine learning, the tools detect unusual patterns in network traffic that may indicate security threats or performance problems.

Alerting and notifications

Based on predefined rules and thresholds, the tools generate alerts and notifications for network administrators. These alerts help identify and resolve problems quickly.

Reporting and visualization

Network monitoring tools provide means for generating reports and visualizing data. This allows network administrators to better understand the state and performance of the network and to identify areas for improvement.

16.7. Audit Tools

Event collection and recording

Audit tools collect and record events from various sources such as operating systems, applications, databases, and network devices. These events may include user logins and logouts, password changes, access to sensitive data, and other important actions.

Centralized storage

The collected events are stored in a centralized repository, which enables easy access and management. Centralized storage also ensures that audit records are protected against unauthorized access and manipulation.

Data normalization and categorization

Audit tools normalize and categorize the collected data so that it is easy to analyze. Normalization involves converting different log formats into a unified format.

Event analysis and correlation

The tools analyze the recorded events and look for patterns and anomalies that may indicate security incidents or unauthorized activity. Correlating events from different sources makes it possible to identify relationships between individual actions.

Alerting and notifications

Based on event analysis, audit tools can generate alerts and notifications for security teams. These alerts help respond quickly to security incidents and other problems.

Reporting and audit

Audit tools provide means for generating reports and auditing activities in the system. This helps organizations meet regulatory requirements and improve their security posture.

Chapter 17. Triage and Escalation of Alerts

Alert received

The evaluation tool raises an alert for a detected cybersecurity event.

Validation

The analyst checks the context of the alert against the affected asset, recent changes, and known benign activity; alerts that turn out wrong are closed **with a reason recorded** — the law requires limiting false or unwanted evaluation. Decree No. 409/2025 Coll., Section 23(2)(a)

Classification

The validated alert is assigned a **severity level** (table below), considering the classification of the affected asset.

Assignment and escalation

The alert is routed to the responsible role within the response time of its severity; it escalates when the severity grows or when the finding exceeds the mandate of the role.

Handling

When an incident is confirmed, the alert is handed over to the incident handling process of the previous module; detection continues to collect evidence.

Closure

The outcome is recorded and fed back into rule tuning — see *Detection Quality* below.

Role	Duty in triage
Analyst on duty	Validates, classifies, and closes alerts; proposes rule changes
Security officer (cybersecurity manager)	Owns the severity scale and escalation rules; decides on escalation to top management
Asset / system administrator	Supplies context for the affected asset and carries out containment actions
Incident handler	Takes over confirmed incidents; ensures detection keeps recording evidence

17.1. Severity Levels

Level	Typical criteria	First response	Escalation
Critical	Confirmed compromise of a critical asset, active spread, service at risk	Immediate, continuous	Security officer and top management
High	Confirmed malicious activity on an important asset, no spread observed	Within hours	Security officer
Medium	Suspicious activity, probably an incident, limited impact	Within one business day	Analyst and asset administrator

Level	Typical criteria	First response	Escalation
Low	Isolated anomaly or probable false positive	Next review	Analyst

Four levels on purpose — they correspond to the four-level asset scale of Annex 1 to Decree No. 409/2025 Coll., so that one scale is used throughout the course.

Chapter 18. Evaluation Tool and False Positives

- The evaluation tool must **collect, search, and group** related records to detect events, **provide information continuously** and warn the selected security roles in time, and **evaluate events with the goal of identifying incidents**. Decree No. 409/2025 Coll., Section 23(1)
- It must **limit false or unwanted evaluation**, its settings and detection rules must be updated regularly, and so must the rules for alerting the security roles. Decree No. 409/2025 Coll., Section 23(2)
- The information gained this way is used to **optimize the information security management system**. Decree No. 409/2025 Coll., Section 23(3)

18.1. Handling False Positives

Identify

The analyst marks alerts that recur and are always wrong; a rising false-positive rate is itself a quality problem.

Analyze

The cause is found — a condition that is too broad, missing context, a changed asset, or an outdated use case.

Adjust

The analyst proposes a rule change and tests it against recorded history before it touches production.

Approve and deploy

The change runs through the regular change process; see *Change Management* in the previous module.

Verify

After deployment, the false-positive rate is monitored again and the result is recorded in the use case.

18.2. Detection Use Case

Table 1. Template: detection use case

Field	Content
Name and owner	One use case, one responsible analyst
Objective	The incident this use case should reveal
Asset and threat	Protected asset and threat category (Annex 3 to Decree No. 409/2025 Coll.)
Data source	Which log sources and feeds it consumes

Field	Content
Detection logic	Condition, correlation, and threshold that raise the alert
Default severity	Starting severity before validation
Immediate action	What the tool may do automatically (block, isolate, warn)
Status	False positives observed, date of the last tuning

Chapter 19. Detection Quality

Metric	Definition	Reviewed
Log source coverage	Share of assets in the coverage matrix that actually deliver records	Monthly
False-positive rate	False alerts divided by all alerts	Monthly
MTTD — mean time to detect	Detection time minus event time, where both are known	Per incident
MTTR — mean time to respond	Start of handling minus the alert time	Per incident
Rule freshness	Date of the last tuning of every use case	Quarterly

- Results feed the **risk assessment** and the **cybersecurity audit** of the last module — an untested or stale detection rule is a finding, not a protection.

Chapter 20. Cryptographic Tools

Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Section 25 (cryptographic algorithms): only currently robust algorithms, NÚKIB recommendations and methodologies, secure communication including e-mail, and management of cryptographic keys and certificates

Chapter 21. Terms

Encryption

The process of converting readable text (plaintext) into unreadable text (ciphertext) using a cryptographic algorithm and a key.

Symmetric Encryption

Uses the same key for both encryption and decryption.

Asymmetric Encryption

Uses a pair of keys – a public key for encryption and a private key for decryption.

Decryption

The reverse process of encryption, converting ciphertext back to plaintext using a decryption key.

Digital Signatures

Used to verify the authenticity and integrity of a message. A digital signature is created using a private key and verified with a public key.

Certification of Cryptographic Tools

Cryptographic tools must be certified to ensure they meet security standards and are suitable for protecting classified information.

Key Management

Involves generating, distributing, storing, and disposing of cryptographic keys. Proper key management is critical for the security of cryptographic systems.

Chapter 22. Choosing an Algorithm

Only currently **robust** algorithms may be used; anything weaker is at most a documented temporary exception while it is being replaced. Decree No. 409/2025 Coll., Section 25(1)

Algorithm	Type	Use today	Status
AES-256	Symmetric block cipher	Data at rest and in transit (disks, backups, TLS)	**Recommended**
ChaCha20	Symmetric stream cipher	Devices without AES hardware acceleration (mobile, IoT)	Recommended
RSA (at least 3072 bit)	Asymmetric	Digital signatures, key exchange, certificates	Recommended with an adequate key length
ECC (e.g., P-256)	Asymmetric	Signatures and key exchange on mobile and IoT	Recommended — shorter keys, the same strength
Diffie-Hellman / ECDH	Key agreement	Establishing the session key in TLS	Recommended with an adequate group
SHA-256 / SHA-384	Hash function	Data integrity and digital signatures	**Recommended**
DES, 3DES	Symmetric	Legacy systems only	**Must not be used in new designs**
MD5, SHA-1	Hash function	Legacy checks only	**Must not be used for security**
NIST post-quantum algorithms	Asymmetric	Protection against future quantum computers	Migration target — see *Implementing Cryptographic Tools*

22.1. Libraries and Certification

Libraries

OpenSSL, Crypto++, Bouncy Castle, or the Microsoft Cryptography API provide the implementations of the chosen algorithms.

Certification

Cryptographic tools intended to protect classified information must be certified, and the methods are taken from the NÚKIB recommendations and methodologies. Decree No. 409/2025 Coll., Section 25(1)(c)

Chapter 23. Implementing Cryptographic Tools

Needs identification

Determine which cryptographic tools are needed (encryption, digital signatures, authentication) and for which assets.

Algorithm selection

Choose only currently **robust** algorithms from the table above. Decree No. 409/2025 Coll., Section 25(1)

Library integration and configuration

Implement them through functional libraries (OpenSSL, Crypto++, Microsoft Cryptography API), configure them to the system specification, and test operation against attack scenarios.

Monitoring and maintenance

Monitor and update the tools and manage the keys over their whole lifecycle — see *Key and Certificate Management* below.

Chapter 24. Key and Certificate Management

If keys and certificates are used to protect technical assets and the communication network, only **currently robust** ones may be used, and their management must run through a dedicated tool. Decree No. 409/2025 Coll., Section 25(3)

24.1. Key Management Lifecycle

Generate

Create keys with a proper source of randomness and an adequate length for the chosen algorithm; generate new keys whenever the algorithm changes.

Distribute

Hand over keys and certificates only through a secure channel, and give each key only to the systems and persons that need it.

Store

Keep keys protected so that their **confidentiality and integrity** are preserved (a protected repository or an HSM), with access rights and no copies on workstations. Decree No. 409/2025 Coll., Section 25(3)(b)3

Change

Rotate keys regularly and immediately whenever a compromise is suspected or a person with access leaves.

Limit validity

Give keys and, in particular, certificates a limited validity and monitor their expiry. Decree No. 409/2025 Coll., Section 25(3)(b)1

Revoke

Revoke a certificate or key as soon as it is compromised, and publish the revocation so that the relying parties stop trusting it.

Dispose

Destroy keys and certificates that are no longer needed, irreversibly, so that they cannot be recovered. Decree No. 409/2025 Coll., Section 25(3)(b)1

Control and audit

Log every operation with a key, keep the audit trail, and let it be reviewed. Decree No. 409/2025 Coll., Section 25(3)(b)2

24.2. Roles in Key Management

Role	Responsibility
Key owner (asset owner)	Says what the key protects and how long the protected data must remain confidential

Role	Responsibility
Cryptographic administrator	Operates the management tool: generation, distribution, storage, rotation, revocation, and disposal Decree No. 409/2025 Coll., Section 25(3)(b)
Security officer	Approves the algorithm policy and the rotation cadence and keeps them in line with the NÚKIB recommendations Decree No. 409/2025 Coll., Section 25(1)(c)
Auditor	Reviews the audit trail of key operations and the exceptions — see *Cybersecurity Audit* in the last module

24.3. Key Management Procedure

Table 2. Template: key management procedure (skeleton)

Item	Content
Scope	Which assets, services, and communication the procedure covers.
Algorithm policy	The approved algorithms and key lengths and a link to the algorithm table above.
Generation	Source of randomness, key lengths, and who may generate keys.
Distribution and storage	The secure channel, the protected repository or HSM, and the access rights.
Rotation and validity	The rotation cadence, the validity of certificates, and the expiry monitoring.
Revocation	Who revokes, how, how fast, and how the revocation is published.
Disposal	How keys are irreversibly destroyed and how it is recorded.
Control and audit	What is logged, how often the trail is reviewed, and who reviews it. Decree No. 409/2025 Coll., Section 25(3)(b)2
Exceptions	Approval and a deadline for any temporarily weaker algorithm.

Chapter 25. End-to-End Encryption (E2EE)

Definition

A communication security method where data is encrypted on the sender's side and decrypted only on the recipient's side.

Security

Data remains protected during transmission, and only the sender and recipient can access the content.

Public Key Use

Data is encrypted with the recipient's public key before sending.

Protected Transmission

Encrypted data travels over the network safe from eavesdropping or tampering.

25.1. End-to-End Encryption (2)

Private Key Decryption

The recipient uses their private key to decrypt and read the original content.

Privacy Assurance

Ensures only the sender and recipient can read the message.

Common Usage

Used in messaging apps like WhatsApp, Signal, and others.

Difference from HTTPS

Unlike HTTPS, which encrypts data between the browser and the server, E2EE keeps it encrypted end-to-end between the communicating parties.

Chapter 26. Application Security

Chapter 27. Processes in Application Security

Secure Development Lifecycle (SDLC)

Implementing security measures at every stage of the application's development, from design through deployment and maintenance.

Static Application Security Testing (SAST)

Analyzing the application's source code to identify security vulnerabilities before the application is run.

Dynamic Application Security Testing (DAST)

Testing the application in its running state to reveal vulnerabilities that may appear during operation.

27.1. Processes in Application Security (2)

Interactive Application Security Testing (IAST)

Combining static and dynamic code analysis to provide a more detailed view of security vulnerabilities.

Penetration Testing

Simulating attacks on the application to identify and fix vulnerabilities.

Secure Authentication and Authorization

Ensuring that only authorized users have access to sensitive parts of the application.

27.2. Processes in Application Security (3)

Data Encryption

Protecting data in transit and at rest through encryption techniques.

Secure Data Storage

Ensuring that sensitive data is securely stored and protected from unauthorized access.

Regular Updates and Patching

Keeping the application up to date and fixing known vulnerabilities.

Education and Training

Providing regular training for developers and staff on the latest security threats and techniques.

Chapter 28. Penetration Testing

Penetration testing is a **controlled simulation of a cyber attack** against the information and communication system, carried out to reveal exploitable vulnerabilities before an attacker does. Unlike automated scanning it also verifies whether individual weaknesses can be combined into a realistic attack path.

Decree No. 409/2025 Coll., Section 24 (application security): penetration tests of the information and communication system focusing on important assets are performed before the assets are put into operation and in connection with a significant change.

28.1. Types of Penetration Test

Black-box

The tester has **no prior knowledge** of the target; the engagement mimics an external attacker.

Grey-box

The tester has **partial knowledge** (for example, valid user credentials or architecture documentation); the most common and cost-effective variant.

White-box

The tester has **full knowledge** of the source code, architecture, and credentials; it maximizes coverage rather than realism.

28.2. Methodologies and Standards

PTES

Penetration Testing Execution Standard — an end-to-end process from pre-engagement to reporting.

OSSTMM

Open Source Security Testing Methodology Manual — metrics-based testing of security, human, and communication channels.

OWASP WSTG

OWASP Web Security Testing Guide — the reference catalogue of web application test cases.

NIST SP 800-115

Technical Guide to Information Security Testing and Assessment.

28.3. Phases of a Penetration Test

1. **Pre-engagement and scoping** — define the target, the rules of engagement, the time window, and the **written authorization**.
2. **Reconnaissance** — passive and active information gathering about the target.

3. **Scanning and enumeration** — identify live hosts, open ports, services, and their versions.
4. **Exploitation** — attempt to verify and exploit the identified vulnerabilities.
5. **Post-exploitation** — determine the impact and the achieved level of access, then clean up.
6. **Reporting and remediation** — document the findings, their severity, and the recommended fixes; retest after remediation.

28.4. Rules of Engagement

- **Written authorization** signed by the asset owner before testing starts.
- **Defined scope** — in-scope and explicitly out-of-scope assets and time windows.
- **Emergency stop** — a contact and a procedure to halt testing immediately.
- **Data handling** — how any accessed data is stored and destroyed.
- **Legal limits** — testing must not exceed the mandate given by the owner.
- **Retest** — verification that the remediation actually closed the findings.

Chapter 29. Ensuring the Availability of Information

Decree No. 409/2025 Coll., Section 26 (ensuring the availability of the regulated service); Act No. 264/2025 Coll., Section 14

29.1. Measures by Availability Rating

The *availability rating* assigned to an asset in the first module (*Asset Management*) determines the target level of these measures: the worse the permitted unavailability, the stronger the redundancy and the faster the restoration.

Availability rating	Required behavior	Measures
Low	Unavailability up to approximately one week is tolerated; regular backups are sufficient.	Local or cloud backup, restoration verified in batches.
Medium	Unavailability must not exceed a working day.	Standard backup and recovery, monitoring, manual failover.
High	Unavailability must not exceed a few hours; any outage is addressed immediately.	Redundant systems, load balancing, automated monitoring, operator intervention or replacement of technical assets.
Critical	Unavailability is not permissible; even a few minutes is a serious threat.	Distributed and geographic redundancy, automated backup and restore, service restoration short-term and fully automated.

The **recovery time objective** (RTO — how long restoration may take) and the **recovery point objective** (RPO — how much data may be lost) follow from the same rating; see *Business Continuity Management* in the previous module.

29.2. Roles in Ensuring Availability

Role	Responsibility
Asset owner	Assigns the availability rating of the asset (first module) and accepts the residual risk
System administrator	Operates redundancy, monitoring, and failover; keeps the configurations and settings under control Decree No. 409/2025 Coll., Section 26(4)
Backup custodian	Runs the backups, protects them, tests restores, and documents the results Decree No. 409/2025 Coll., Section 26(3)

Role	Responsibility
Security officer (cybersecurity manager)	Approves the availability and backup rules; ensures the backup environment is separated and the backups are encrypted Decree No. 409/2025 Coll., Section 26(3), (5)
Continuity and crisis manager	Owns the disaster recovery plan; decides on failover and recovery priorities — see *Business Continuity Management* in the previous module
Auditor	Verifies the restore-test evidence and the disaster recovery drills; see *Cybersecurity Audit* in the last module

29.3. Tools and Procedures

Redundant Systems

Use of redundant systems and components to ensure that if one part fails, another can continue operating.

Data Backup and Recovery

Regular data backups and quick restoration in case of loss or damage.

Distributed Systems

Use of distributed systems that allow horizontal scaling and maintain service availability during outages.

29.4. Tools and Procedures (cont.)

Load Balancing

Use of load balancers to evenly distribute workloads across servers or nodes, improving availability and performance.

Monitoring and Problem Detection

Continuous system monitoring with rapid detection and resolution of issues affecting availability.

Service Takeover Planning

Preparing and regularly testing failover plans to quickly resume services during an outage.

Chapter 30. Redundant Systems

Hardware Redundancy

Use of multiple identical devices such as servers or drives, ready to take over if one fails.

Software Redundancy

Implementing software solutions that run applications on multiple servers simultaneously; if one fails, another takes over.

Geographic Redundancy

Hosting data and operations in different geographical locations to protect against regional outages or disasters.

30.1. Redundant Systems (cont.)

Network Redundancy

Using multiple network paths and ISPs to maintain connectivity if one link fails.

Automated Backup and Restore

Regular backups with automated restoration in the event of failure.

Chapter 31. Data Backup

Identifying Critical Data

Determine which data must be backed up, such as documents, databases, applications, or other critical assets; the scope follows from the availability rating of the asset.

31.1. Choosing a Backup Location

Location	Strengths	Weaknesses	Suits
Local (external drive, NAS)	Fast restore, full control, no transfer cost	Lost with the site (fire, flood) and reachable by ransomware	Low and Medium ratings; the first copy of the 3-2-1 rule
Cloud	Geographic redundancy, scalable, available during a local outage	Needs bandwidth, ongoing cost, dependence on the provider — see *Supplier Management* in the third module	Off-site copy for High and Critical services
Hybrid (local + cloud)	Local speed plus cloud resilience; meets the 3-2-1 rule	More complex and more expensive to operate	High and Critical services
Separated or immutable (offline, tape, WORM)	Malware cannot modify or delete the copies	Slower restore, extra process and handling	The separated backup environment required by Decree No. 409/2025 Coll., Section 26(5)

31.2. Backup and Restoration Process

Scope

Determine what must be backed up: the configurations and settings of the technical assets, and the information and data needed to restore the service after an incident. Decree No. 409/2025 Coll., Section 26(2)

Schedule

Backups run regularly and automatically (daily, weekly, monthly) to reduce human error; keep **three copies, on two different media, with one off-site** (the **3-2-1 rule**).

Protect

Backups are protected against modification and against loss of availability, and their confidentiality and integrity are ensured at least by encryption with currently robust algorithms. Decree No. 409/2025 Coll., Section 26(3)(c), (d) — see *Cryptographic Tools* in this module.

Separate

The backup environment is separated from the other environments, so that malware (in particular ransomware) cannot reach the backups together with the affected system. Decree No. 409/2025 Coll., Section 26(5) — see *Ransomware* in this module.

Test

Restores are tested regularly for integrity, availability, and recoverability, and the results of the tests are documented. Decree No. 409/2025 Coll., Section 26(3)(a), (b)

Recover

During an incident the recovery follows the disaster recovery plan; the integrity of the restored data is verified every time, and the records feed the evaluation.

31.3. Backup Schedule

Table 3. Template: backup schedule (skeleton)

Item	Content
Service or asset, availability rating	What is protected and how strict the requirements are.
RTO and RPO	Maximum restoration time and acceptable data loss.
What is backed up	Configurations, settings, data, applications.
Method and frequency	Full or incremental, and how often.
Retention	How long the individual copies and versions are kept.
Locations	On-site, off-site, and the separated backup environment.
Protection	Encryption, access rights, immutability.
Restore test	Cadence and the date and result of the last successful test. Decree No. 409/2025 Coll., Section 26(3)(a), (b)
Responsible and approver	The backup custodian and the person approving the schedule.
Evidence	Test reports, restore log, and the record of the last recovery.

Chapter 32. Data Recovery

Preparation

Identify which data to restore and from which backup location.

Initiating Recovery

Use backup software or manual methods to retrieve data, ensuring encryption and access verification.

Integrity Verification

Check data completeness and functionality after restoration.

Documentation and Plan Updates

Record the recovery process and update backup plans as needed.

Chapter 33. Distributed Systems

Architectural Design

Plan system topology, define nodes, and communication methods.

Data Replication

Implement data replication across nodes for availability.

Load Distribution

Use load balancers to prevent overload on individual components.

33.1. Distributed Systems (cont.)

Fault Tolerance

Configure automatic failover in case of node failure.

Geographic Distribution

Deploy nodes in multiple regions for disaster resilience.

Monitoring and Management

Track system health and performance for rapid response.

Chapter 34. Load Balancing

Hardware Load Balancer

High-performance, stable solutions such as Cisco or F5.

Software Load Balancer

Flexible, scalable options such as Nginx or HAProxy.

Distribution Algorithm

Choose between Round Robin, Least Connections, IP Hash, etc.

Health Checks

Monitor server health to route traffic only to functional nodes.

34.1. Load Balancing (cont.)

Routing Rules

Define traffic distribution policies.

Load Simulation

Test performance under various conditions.

Performance Monitoring

Continuously track availability and speed.

Updates and Optimization

Keep configurations updated for best results.

Chapter 35. Monitoring and Problem Detection

Monitoring Setup

- Tools – Nagios, Zabbix, Prometheus, Grafana.
- Configure tracking for CPU, memory, disk, network traffic, and application response.

Alerts

- Define thresholds for triggering alerts.
- Configure notifications via email, SMS, or other channels.

Data Analysis and Correlation

- Log Collection – Use ELK Stack or Splunk.
- Event Correlation – Identify problem patterns and root causes.

35.1. Monitoring and Problem Detection (cont.)

Incident Response

- Incident Response Team ready to act.
- Implement corrective and preventive measures.

Auditing and Testing

- Outage Simulations – Use chaos engineering.
- Security Audits – Ensure up-to-date protections.

Chapter 36. Disaster Recovery Planning (DRP)

Risk Analysis

Identify potential risks (natural disasters, technical failures, cyberattacks).

Prioritization

Determine critical services to restore first.

Recovery Procedures

Develop detailed recovery steps.

Resource Allocation

Assign personnel, hardware, software, and budget.

36.1. Disaster Recovery Planning (cont.)

Testing and Training

Run simulations and train staff.

Documentation and Updates

Keep DRP current with changes in infrastructure and risks.

Monitoring and Maintenance

Regularly assess DRP effectiveness.

Chapter 37. Industrial, Control, and Similar Specific Systems

Act No. 264/2025 Coll., Section 14 (list of security measures); Decree No. 409/2025 Coll., Section 27 (industrial, control, and similar specific technical assets)

Chapter 38. OT and IT Compared

Criterion	OT — industrial control systems	IT — office systems
Primary objective	Safety of physical processes and uninterrupted production	Confidentiality and integrity of data and services
Availability	Critical: downtime stops production or endangers people	Planned maintenance windows are acceptable
Patching and updates	Only in validated maintenance windows, with a vendor-approved version and a safety review	Routine and continuous
Lifetime	Decades; legacy protocols and components remain in use	Three to five years
Impact of failure	Physical damage, injury, loss of production	Data loss or service outage
Threats	Physical-process threats, unsafe commands, manipulated measurements	Data theft and disruption of services
Standards	IEC 62443 (OT security) and IEC 61511 (functional safety)	ISO/IEC 27001:2022
Network	Traditionally isolated and segmented, with special protocols; connectivity is a new risk	Open, standardised, and internet-connected

Chapter 39. Securing Specific Technical Assets

39.1. Requirements of Section 27

Letter	Requirement	How it is met in practice
a)	Limit physical access to the assets	Locked cabinets and rooms and access records — see *Physical Security* in the previous module.
b)	Limit the access authorizations	Minimal accounts for operators and engineers, kept separate from the IT accounts — see *Access Control Management* in this module.
c)	Segmentation and separation of the OT network from other environments	Separate zones and VLANs, firewalls between OT and office networks, and no direct routing to the Internet — see *Communication Network Security* in this module.
d)	Limit remote access and management, including communication outside the entity's network	A jump host and multi-factor authentication, vendor access only in agreed windows, and no direct vendor links.
e)	Protect the individual assets against known vulnerabilities and threats	An asset inventory, firmware updates in maintenance windows, disabled unused services, and passive monitoring and detection.
f)	Availability and recovery of the OT assets	Backups of controller and configuration data, tested recovery, and spare parts — see *Ensuring the Availability of Information* in this module.

Chapter 40. Introducing Security in OT

Inventory

List the OT assets, their protocols, their owners, and their role in the physical process.

Assess

Evaluate the risk together with the **safety impact**: which failures can endanger people or production.

Segment

Separate the OT network from the office and Internet environments and define the allowed flows.

Restrict

Limit the operator and engineer accounts and the remote and vendor access.

Protect and monitor

Patch and update only in validated maintenance windows, take configuration backups, and monitor passively.

Test and practise

Rehearse recovery and the incident procedure, which includes a **safety stop** of the process where needed.

40.1. Roles in OT Security

Role	Responsibility
Process or safety owner	Decides on changes with a safety impact and approves the maintenance windows.
OT engineer or administrator	Operates and patches the control systems and performs the safety review.
Security officer	Sets the rules and runs the risk assessment.
Vendor or supplier	Supplies updates and remote support under contract — see *Supplier Management* in the third module.
Auditor	Verifies the evidence: the change records and the recovery drills.

40.2. Maintenance-Window Record

A **significant change** triggers penetration testing of the affected application. Decree No. 409/2025 Coll., Section 24(5)(a)3; see *Change Management* in the previous module

Table 4. Template: maintenance-window record (skeleton)

Item	Content
System or asset	The controller, the station, or the device being changed.
Window	Date, start, and end of the maintenance window.
Change or update	What is applied and the approved version from the vendor.
Safety validation	Who validated the change and the result of the safety review.
Backup taken	The configuration backup created before the change.
Rollback plan	How the original state is restored if the change fails.
Persons and approver	Who performs the change and who approved it.
Result	The outcome after the change, verified against the expected behaviour.
Evidence	The record and the logs of the change and the test.

Chapter 41. Digital Services

Regulation (EU) 2022/2065 (Digital Services Act); Regulation (EU) 2024/2847 (Cyber Resilience Act); Directive (EU) 2022/2555 (NIS2); Regulation (EU) 2016/679 (GDPR)

Digital services are the online platforms, marketplaces, and digital infrastructure whose obligations follow mainly from the **Digital Services Act** (DSA), while their security and data obligations follow from the **Cyber Resilience Act**, **NIS2**, and the **GDPR**.

Chapter 42. Measures for Digital Services

Area	Obligation	Legal basis
Content moderation	Mechanisms for reporting and removing illegal content (notice and action).	DSA, Article 16
Personal data protection	Personal data is protected and processed lawfully; a data protection officer and the security of processing.	GDPR, Articles 32 and 37
Transparency	Transparency about content moderation and, for the largest platforms, about recommendation and advertising; transparency reports.	DSA, Articles 15 and 27
Product safety	Products with digital elements sold online must meet safety and security requirements and come with updates; online marketplaces must collect information about the sellers.	CRA; DSA, Article 30
Protection against disinformation	Platforms combat disinformation and manipulative content, in particular during a crisis.	DSA, Article 36

Chapter 43. Obligations by Type of Service

Type of service	Examples	Main obligations
Intermediary and hosting service	Internet access, DNS, CDN, web hosting	Points of contact, terms and conditions, transparency reports, and the duty to act on illegal content once it is known; for hosting also notice and action. DSA, Articles 11-16
Online platform	Marketplace, social network, app store	In addition: internal complaint handling, trusted flaggers, statements of reasons, and traceability of traders. DSA, Articles 17-30
Very large online platform or search engine (VLOP / VLOSE)	A large social network or search engine with at least 45 million average monthly recipients in the EU	In addition: systemic risk assessment and mitigation, an independent audit, an advertising repository, and data access for researchers. DSA, Articles 33-40
Micro and small enterprise	A start-up below 50 persons and up to EUR 10 million turnover	Reduced obligations. DSA, Article 19

Chapter 44. Handling an Illegal Content Notice

Receive

A user, a trusted flagger, or an authority submits a notice with the location of the content and the reason why it is considered illegal. DSA, Article 16

Assess

The provider verifies the notice diligently and in good faith against the law and its own terms and conditions.

Act

The content is removed or access to it is disabled; the affected user is informed of the decision and the reasons (a statement of reasons). DSA, Article 17

Appeal

The user can use the internal complaint-handling system and, for platforms, out-of-court dispute settlement.

Record

Every action is logged, repeated infringers are tracked, and the data feeds the transparency report.

44.1. Roles in Digital Services

Role	Responsibility
Compliance officer	Owns the obligations of the DSA and the relationship with the authorities.
Content moderator	Assesses the notices and applies the terms and conditions.
Data protection officer	Guards the personal data processing under the GDPR. GDPR, Article 37
Security officer	Ensures the security of the service and of the processing. GDPR, Article 32
Auditor or external assessor	Carries out the independent audit for the largest platforms. DSA, Article 37

44.2. Notice and Action Record

Table 5. Template: notice and action record (skeleton)

Item	Content
Notice	ID, date, and the source (user, trusted flagger, authority).
Content	The location of the content (URL or asset) and its type.

Item	Content
Reason	The alleged illegality and the terms and conditions involved.
Assessment	Who assessed the notice, when, and on what basis.
Action	Remove, disable access, or keep, with the date and the reason.
User informed	The statement of reasons sent to the affected user.
Appeal	The complaint or counter-notice and its outcome.
Repeat offender	The counter updated for repeated infringers.
Evidence and reporting	The retained evidence and the entry for the transparency report.

44.3. Products with Digital Elements

Products with digital elements must be secure by design, handle vulnerabilities, provide security updates for the declared support period, and report an actively exploited vulnerability within 24 hours (early warning), 72 hours (notification), and 14 days (final report). Regulation (EU) 2024/2847 (Cyber Resilience Act), Article 14; see *Application Security* in this module

44.4. Tools

Digital services rely on the same measures as the rest of this module: firewalls and segmentation (*Communication Network Security*), protection against malicious code (*Protection against Malicious Code*), encryption and key management (*Cryptographic Tools*), access control and multi-factor authentication (*Access Control Management*), and event recording and detection (*Recording Events* and *Detection of Cybersecurity Events*). Service-specific additions are protection against volumetric attacks (DDoS mitigation and rate limiting) and content filtering and verification.