Department of Informatics in Management

Managing enterprise IT infrastructure and security

Exercise 3

Selecting security controls

Rafał Leszczyna rle@zie.pg.edu.pl
Bartosz Woliński bwolinski@zie.pg.edu.pl

Gdańsk, 2022

Plan of lab exercises

Exercise	Points	Unit	Description
E1	*18*	1	Introduction to the lab; Explanation of the Exercise 1 (E1)
		2	Selection of the enterprise; Analysis of the enterprise and its IT infrastructure
		3	Reporting the results of the analysis of the enterprise and its IT infrastructure
E2	*30*	4	Impact assessment of the IT infrastructure assets
		5	Development of a threat repository; **Explanation of the Exercise 2.2**; Identification and analysis of organisation-specific threats; Risk evaluation
		6	
		7	Reporting the results of the risk assessment
E3	*18*	8	Explanation of the systematic approach to securing an enterprise IT infrastructure
		9	Justified choice of a security standard; Assignment of controls
		10	Reporting the results of the security controls assignment
E4	*12*	11	Identification and analysis of existing security policies; Definition of a proprietary policy; **Explanation of the Exercise 5 (E5)**
		12	
E5	22	*13*	Obtaining the data regarding security costs from the enterprise
		14	Analysis and processing of the data; Visualisation and reporting
		15	Model-based cost assessment; Reporting the results
EE	*4*	*E*	*Evaluation of a security/privacy solution (non-obligatory, extra points)*

*Red underline depicts the final dates for submitting the reports

***Italics* and grey/darker background indicate to the units in the form of consultations

Tasks

- Explaining the systematic approach to securing an enterprise IT infrastructure (a summary of the know-how obtained hitherto) [3 pts.]
- Choosing a security standard between ISO 27001:2018 and NIST SP 800-53 Revision 5, justifying the choice (comparison of strengths and weaknesses) [4 pts.]
- Selecting and describing security controls for 8 threats with the highest risk levels. Referring the controls to the threats. Indicating (potential) control areas which have not been addressed and explaining it [10 pts.]
- Updating the drawing of the IT infrastructure with proposed technical security controls (in MS Visio) [1 pts.]
- Preparing a report that comprises all the above information

Additional information

- Selecting and describing security controls
  - For each of the 8 threats, more than one security control
  - In addition, security controls common to several threats
  - Thus, two tables:
    - o With all the 10 individual threats:

	Threat	Security controls
1.	Loss of confidentiality of patient records due to a virus infection of the central medical server via USB	A.8.3.1 Management of removable media A.9.1.1 Access control policy A.11.1.1 Physical security perimeter A.11.1.3 Securing offices, rooms and facilities A.12.2.1 Controls against malware

Additional information

- o For common security controls:

	Security control	Threats
1.	A.5.1.1 Policies for information security	1. Loss of integrity of personnel data due to an unauthorised access of an employee to the accounting database 2. Loss of availability of personnel data due to an physical damage of the accounting server 3. …

- For each threat a common description of all security controls selected to protect from it (in own words)
- If applicable, indicating security control areas (clauses – A.5, A.6 etc.) from which no controls have been selected and explaining this

Assessment criteria

- Timeliness
  - Final report submitted after a deadline – each opened week reduction of 30% points
- Preparation to the exercises
- Team work, effort allocation
- Completeness and correctness of the results' content, consistency with the earlier analyses
- The presentation and the structure of the report

Literature, resources

1. ISO/IEC 27005:2018
2. NIST SP 800-53 Revision 5, mappings (ISO 27001 ⬄ NIST SP 800-53), other appendices: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
3. NIST Special Publications (all)
4. *Computer security handbook*, edited by Seymour Bosworth, M. E. Kabay and Eric Whyne. 6th ed. Wiley, 2014 – Part III Prevention: Technical Defenses, Part IV Prevention: Human Factors

Thank you!