Computer security audit

Purpose

1. Increasing the level of security of the court's IT systems.
2. To make users aware of the importance and necessity of taking care of the security of IT systems.

Assumptions

1. In good practice, it is about controlling the security of workstations and computer devices, but this does not mean that the security of only these elements (workstations and devices) is checked. In fact, it is a *security control of the entire IT system through the prism of computer workstations*.
2. The detail of the audit and the benefits it will bring depend on the structure of the audit lists and the reliability of the answers provided.
3. The aspect of user awareness is a derivative of the inspections carried out.
4. Regular inspections and self-checks of the security of workstations and equipment meet the basic training objectives and will allow users to familiarize themselves with issues such as, m.in. basic concepts related to AI security, b. basic security needs and objectives of AI security policy, c. consequences of threats and security breaches, d. functioning of the security system, e. duties and responsibilities of AI users, f. consequences of unauthorized action (including disciplinary sanctions).

Create a tool

1. An audit list – or checklist – is a set of questions to which the user answers, most often in a binary way: "yes"/"no", ("is"/"is not"; "fulfilled"/"not fulfilled") with the possibility of answering "not applicable". Sometimes the audit letters allow for the answer: "partially fulfilled".
2. The advantage of audit lists is that *they immediately draw attention to the occurring problems*, system elements and phenomena that are important for the security of the system. Which, in turn, should be the starting point for further action.
3. The use of lists to determine the level of security of the system consists in the appropriate construction of a *pattern* that determines the ideal state and the maximum number of points that the controlled system can achieve. The standard is therefore a reference for the results obtained.
4. Then, a number of points for positive and negative answers is assigned to individual questions (most often "1" for "yes"/"is"/"fulfilled" and 0 for "no"/"not available"/"not fulfilled"). Further levels of assessment (e.g. satisfactory, satisfactory, unsatisfactory) are also determined, to which the system will be included depending on the number of points obtained.
5. After answering all the questions on the list, the points should be added up and the result compared with the pattern.

6. The result can be presented graphically, which often makes it easier to analyze.

Description of the functioning of the practice

1. Good practice assumes that security checks of workstations and computer equipment are carried out using the audit list (checklist) method.
2. The data obtained during the audit is analyzed, which allows to detect weaknesses in the system and implement appropriate safeguards.

Benefits

1. The benefits in terms of work organization include:a) increasing the security of the IT system,b) identifying the strengths and weaknesses of the IT system security,c) improving the functioning of the IT system,d) increasing the ability to control the IT infrastructure,e) adapting the functioning and securing of the IT system to the law and ISO standards,f) reducing the number of crisis situations resulting from a breach of system security It.
2. The benefits in terms of the employee include:a) increasing the safety of the workplace,b) increasing knowledge about issues related to the safety of AI,c) increasing awareness of the occurrence of threats,d) receiving feedback on the level of security of one's own workplace (including on one's own conduct affecting the security of the system),e) using the potential of employees, m.in. in terms of tracking irregularities and occurrence of IT security incidents,f) increasing the motivation to comply with security rules when using the IT system.
3. The benefits in financial terms include:a) reduction of costs related to the removal of the effects of threats and breachesb) of IT system security, m.in.- reduction of system unavailability costs,- reduction of repair costs,- reduction of data recovery costs.c) reduction of training costs, due to the increase in user awareness of IT system security.

Cost of implementation

Implementation costs are primarily *personnel costs* – costs of IT services (mainly for the development of audit lists, supporting tools and conducting inspections) and costs of user work incurred for self-control of their workstations and devices:

1. The cost of developing and subsequently updating audit lists and a security assessment template.
2. The cost of analysing the results of the inspection and assessing the level of safety.
3. The cost of developing IT tools to support inspections, analysis of results and assessment of the level of security.
4. The cost of training people responsible for the functioning of the practice.
5. The cost of conducting security inspections of computer workstations and devices:- by employees of the IT department,- by users of workstations and devices.

Other necessary expenditures/activities

To carry out security inspections of workstations and computer devices, an IT tool supporting this process is necessary, e.g. an online form with the ability to save results in a database.