Essay outline Michael Geiger:

benefits of the ASMIS:

* Enables a high volume of inquiries.
* Automation of appointments.
* Optimal coordination of medical specialists.
* Possibilities to record the number of inquiries and prognoses future need of specialist.
* Saving staff for reception.

potential problems:

* Technical failures prevent or make access more difficult.
* Security problems in data protection.
* Loss of information.

potential cyber threats to the system:

* Unauthorized access to user information through stolen access data (Spoofing).
* Malicious modification of the application that can lead to malfunction or failure (Tampering).
* Information theft (Information disclosure).
* Overload the application with traffic can lead to prevent legitimate use (DoS).
* Malicious attack on the system to steal or encrypt information (privilege escalation).

The greatest concerns when setting up the ASMIS should be in relation to the protection of sensitive data and a secure backup should the system be attacked and encrypted.

In order to protect the patient's sensitive data, the servers on which the ASMIS is located must be protected. On the other hand, the homepage has to be secure so that the information is not diverted and stolen.

A secure backup policy is recommended as the ASMIS enables the clinic to run smoothly. If the data were encrypted, work in the clinic would collapse, as doctors and patients would not know which appointments are to be kept.

Since this concerns particularly sensitive customer data and the medical system is a system-relevant system in which an intervention could endanger the health of the patient, it could be of interest to trace a potential attacker.

In order to be able to detect and trace an unauthorized intervention in the system at an early stage, it is advisable to implement a honey pot server that seduces the cyber criminal into hacking this server that is not relevant for the ASMIS and thus makes itself visible in the system. The honey pot server is equipped with tracking software, with which changes can be quickly identified and the attacker can be traced.

Finally, a secure password policy and education of the staff with regard to cyber security is recommended, so that spoofing is prevented and the weak point of people is as small as possible.



