Kivonat

A szakdolgozatom célja az egészségügyi informatikai rendszerek veszélyforrásainak, a támadók módszereinek, és eszközeinek feltérképezése. Megvizsgálom két egészségügyi intézmény informatikai rendszereit, bemutatom azok működését, valamint az alkalmazott informatikai biztonsági szabályozókat ismertetem, és a hiányosságokat feltárom.
Ismertetésre kerül az egészségügyi rendszerek elleni lehetséges támadók, és a támadások fajtáit. Célom javaslatot tenni a korszerű védelmi megoldások alkalmazhatóságára, melyek növelhetik egy egészségügyi rendszer biztonságát.
Amiért fontosnak tartom a fentieket megvizsgálni, mert bárki találkozhat az informatikai rendszerekben veszélyforrásokkal, amelyek komoly problémát jelenthetnek nem csak az egészségügyben, hanem akár a mindennapi életben is. Éppen ezért fontos tudni, hogy milyen lehetséges támadásoknak vannak kitéve ezek a rendszerek, és hogyan lehet ellene védekezni. Elengedhetetlen mindenki figyelmét felhívni arra, hogy milyen biztonsági követelményeket kell betartani.
Ilyen követelmény a CIA (Confidentality-Integrity-Availability) követelmények. Ez a bizalmasság, sértetlenség és rendelkezésre állás követelményeit tartalmazza. Bizalmasság magában foglalja a kódolást, rejtjelezést, titkosítást.
A nyílt hálózatok használata magával hozta azt az igényt, hogy az adatok sértetlensége biztosított legyen. Fontosnak tartom az aktív támadások lehetőségei ellen való védekezési formák megvizsgálását. Illetve elengedhetetlen megvizsgálni, hogy egy egészségügyi rendszernél milyen rendelkezésre állási időre van szükség, és miért.

Abstract

The purpose of my BSc thesis is the investigation of threatens of health informatics systems and the methods of attacks. This work examines the health informatics systems of two institutes and introduces the work of these systems and security regulators, furthermore tires to reveal deficiencies.

My thesis shows the attackers of health informatics systems and methods of attacks and recommends the application of most recent methods, which can improve the safety of health system.

It is important to examine these problems because anyone can meet security threat of informatics systems. These are serious problems of everyday life and emphasizing safety requirements is also important.
The most common criteria are the CIA (Confidentiality, Integrity and Availability) requirements.
Confidentiality consists of coding, ciphering and security.
Integrity is natural requirement in case of communication through open networks and protection of against active attacks. The investigation of availability parameters of health systems is also necessary.