Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Cserna Levente

SZEPARÁLT INFORMÁCIÓBIZTONSÁGI ZÓNA LÉTREHOZÁSA BIZTONSÁGI TESZTEK ELVÉGZÉSÉRE

KONZULENS

Bajor Péter

KÜLSŐ KONZULENS

Kiss Miklós

BUDAPEST, 2022

Tartalomjegyzék

HALLGATÓI NYILATKOZAT

Alulírott **Cserna Levente**, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy hitelesített felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Kelt: Budapest, 2022. 05. 29.

...…….
Cserna Levente

Összefoglaló

Az elmúlt évek során az autóipar jelentős átalakuláson ment keresztül. A gépjárműveket egyre inkább a *„négy keréken guruló számítógép”* jelzővel illetik, hiszen egyre összetettebb és bonyolultabb számítógép-vezérelt rendszerekkel vértezik fel ezeket, amelyek növekvő támadási felületet nyújtanak a kiberbűnözők számára. Az autóipari kiberbiztonság területén egyre komplexebb módszerekkel és eszközökkel kutatják és tesztelik a rendszerek vezérlőegységeit, amelyek során kritikus információk keletkeznek.

A Nemzetközi Szabványügyi Szervezet (International Organization for Standardization, ISO) és a Nemzetközi Elektrotechnikai Bizottság (International Electrotechnical Commission, IEC) által közösen kidolgozott ISO/IEC 27k szabványcsaládnak megfelelő információbiztonsági irányítási rendszer (Information Security Management System, ISMS) lehetővé teszi a kritikus információk hatékony védelmet azáltal, hogy szisztematikus megközelítést biztosít az információbiztonság kezelésére.

Jelen szakdolgozatban bemutatásra kerül az ISO/IEC 27k szabványcsalád szerinti információbiztonsági irányítási rendszer vállalati környezetbe való integrálása, beleértve az egyes implementációs lépések részletes ismertetését és az irányítási rendszer által keretbe foglalt fizikai infrastruktúra kialakítását és a hardverek konfigurálását.

Abstract

The automotive industry has undergone a major transformation in recent years. Vehicles are becoming associated with the term „computer on four wheels”, as they are equipped with increasingly complex and sophisticated computer-controlled systems, which provide a growing attack surface for cybercriminals. In the field of automotive cybersecurity, increasingly complex methods and tools are being used to research and test the control units of systems that generate critical information.

The Information Security Management System (ISMS), which complies with the ISO/IEC 27k family of standards and was developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), enables the effective protection of critical information by providing a systematic approach to managing information security.

This thesis presents the integration of an ISO/IEC 27k family of standards for information security management into an enterprise environment, including a detailed description of the implementation process as well as the physical infrastructure and hardware configuration that the management system will frame.

1 Bevezetés

„Az autója már nem egy mechanikus eszköz néhány számítógéppel a belsejében; ez egy számítógép négy kerékkel és motorral” – Bruce Schneier, biztonsági szakértő

Az autóipar a technológiai forradalomnak köszönhetően drámai fejlődésen ment keresztül. A gépjárművekbe integrált rendszerek egyre összetettebbé és kifinomultabbá váltak a fejlett számítógép-vezérelt rendszerek és kommunikációs technológiák térnyerésével. A korábban mechanikus és hidraulikus alapokon nyugvó komponenseket felváltották a korszerű elektromos és elektronikus megoldások, beleértve a kormányrendszereket is, amelyek a thyssenkrupp Components Technology Hungary Kft. fő fejlesztési profilját képezik. Tekintettel arra, hogy ezek a rendszerek létfontosságúak az emberi biztonság szempontjából, számos kiberbiztonsági kritériumnak kell megfelelniük, amelyeket a gyártók és az iparági szabályozások határoznak meg.

Az üzleti partnerek és a szabályozások elvárásainak való megfelelés olyan komplikált módszerek és eszközök használatát teszi szükségessé, amelyek jelentősen megnövelik a vállalat jelenlegi informatikai hálózatának kiberfenyegetettségét. Mindemellett a tesztelési és kutatási folyamatok során kritikus információk keletkeznek, amelyeknek biztosítani kell a bizalmasságát, sértetlenségét és rendelkezésre állását (Confidentiality, Integrity, Availability – CIA model). A szervezet kiberbiztonsági kockázatainak mérséklése, valamint az információk védelmének biztosítása érdekében egy szigorúan védett és elszigetelt zónára van szükség.

1.1 A kutatás motivációja

A thyssenkrupp személyautók elektromechanikus kormányrendszerének hardveres és szoftveres fejlesztésével foglalkozik. Ennek a rendszernek – biztonságkritikus mivoltának köszönhetően – magas szintű kiberbiztonsági és funkcionális biztonsági követelményeknek kell megfelelnie, amelyeket elsősorban nemzetközi iparági szabványok (ISO/SAE 21434, ISO/DIS 24089-DRAFT, ISO 26262-1, UNECE R155 és R156, GB 17675, GB/T 34590) fogalmaznak meg.

Ahhoz, hogy a kormányrendszer megfeleljen a szabványokban, gyártói követelményekben és jogszabályokban előírt kritériumoknak, az elektronikus

vezérlőegységeken (Electrical Control Unit, ECU) és a rendszer egyéb komponensein biztonsági teszteléseket kell végezni. A folyamatok célja az, hogy feltárják a kormányrendszer olyan hibáit és sérülékenységeit, amelyek hatással lehetnek a termék biztonságosságára. E tesztelések végrehajtására szeparált (izolált) információbiztonsági zónát szükséges létrehozni, amely megfelel az ISO/IEC 27001:2013 szabványban definiált információbiztonsági irányítási rendszer követelményrendszerének.

1.2 Kutatási célkitűzések

Szakdolgozatom elkészítésével elsődleges célom az volt, hogy különböző biztonsági tesztelési metodológiákhoz egy szeparált információbiztonsági zónát hozzak létre. Elsődleges célom teljesítésének érdekében több kisebb mérföldkövet tűztem ki:

1. Autóipari elméleti háttér ismertetése.
2. Információbiztonsági szabványok és fogalommeghatározások ismertetése.
3. Implementációs terv létrehozása szeparált információbiztonsági zóna létrehozásához.
4. Információbiztonsági irányítási rendszer kockázatkezelésének elvégzése.
5. Információbiztonsági szerepkörök, feladatkörök és besorolások kialakítása.
6. Izolált fizikai hálózatba tartozó eszközök konfigurációs irányelveinek kidolgozása.

1.3 Kutatási módszerek

Az 1.2 alfejezetben felsorolt kutatási célkitűzések teljesítésének érdekében több módszert alkalmaztam. Széles spektrumú hazai és nemzetközi irodalomkutatást és forráselemzést hajtottam végre, különös tekintettel az információbiztonsági és autóipari kiberbiztonsági szabványokra. Alkalmaztam a thyssenkrupp-nál kooperatív képzés keretében szerzett autóipari tapasztalataim, amelyek szorosan kapcsolódtak szakdolgozatom tárgyköréhez. Az irodalomkutatás és forráselemzés során megismert szabványok, illetve az autóiparban szerzett tudásom alapján kidolgoztam az információbiztonsági irányítási rendszerhez tartozó szerepköröket, besorolásokat és szinteket, illetve létrehoztam a rendszer üzemeltetéséhez és tanúsításához szükséges dokumentációkat.

2 Autóipari elméleti háttér ismertetése

Ebben a fejezetben a szakdolgozat témájának alapját képező autóipari terminológiát fejtem ki közérthető módon. Külön alfejezetekben tárgyalom az autóipar technológia fejlődését, az autóipari kiberbiztonság alapjait és az ehhez kötődő nemzetközi iparági szabványokat, illetve a szabványoknak való megfeleléshez szükséges biztonsági tesztelési módszereket.

2.1 Napjaink autóipara

A számítógépek világában zajló hardveres és szoftveres technológiai fejlődés óriási hatást gyakorol az autóipari szegmensre. A számítástechnika területén megjelenő innovációk új lehetőségeket teremtenek a mérnökök számára, hogy a gépjárművekkel való közlekedést még biztonságosabbá és kényelmesebbé tegyék. Emellett az olyan tényezők, mint a légszennyezés mérséklése, a növekvő felhasználói igények és a nemzetközi szabályozások megjelenése folytonos fejlődésre ösztönzik az autóipart. [1]

Az elmúlt néhány évtizedben exponenciálisan nőtt a gépjárművekbe integrált számítógép-vezérelt funkciók száma, illetve a korábban mechanikus funkciókat fokozatosan elektronikus megoldásokkal (X-by-wire) helyettesítik. A legkorszerűbb modellekben akár több mint száz elektronikus vezérlőegység és hasonló mennyiségű szenzor kooperációja felelős az egyes alrendszerek rendeltetésszerű működéséért. [2]

2.1.1 Elektromos és elektronikus rendszerek

A növekvő számítási teljesítmény és az elektronikus műszaki innovációk lehetővé teszik olyan elektromos és elektronikus rendszerek (Electrical and Electronic, E/E) és funkciók implementálását és működtetését, [3] amelyek tisztán mechanikus és hidraulikus technológiákkal megvalósíthatatlanok lennének. [1] Az elektromos és elektronikus rendszerek funkcionalitás szerint öt nagy tartományra (domain) bonthatóak: hajtáslánc, futómű, karosszéria, HMI (Human Machine Interface) és telematika. [1]

A hajtáslánc tartományba olyan rendszerek tartoznak, amelyek a gépjármű hosszirányú mozgásáért felelősek. Ide listázhatóak azok a komponensek, amelyek a motort és a sebességváltót vezérlik a járművezető utasításai és az egyéb rendszerek és szenzorok által szolgáltatott adatok alapján. [1]

A futómű tartomány azokat a járműbe ágyazott komponenseket tartalmazza, amelyek részt vesznek a kormányzásában, illetve az út és a jármű közötti interakcióban, mint például a blokkolásgátló-fékrendszer (Antilock Breaking System, ABS), az elektronikus stabilitás-vezérlés (Electronic Stability Control, ESC), illetve az elektronikus kormányrendszer (Electronic Power Steering, EPS). [1]

A karosszéria tartomány olyan rendszereket foglal magába, amelyek nem vesznek részt a jármű hossz- és oldalirányú mozgatásában, csupán a járművezető biztonságát és kényelmét biztosítják. Ebbe a kategóriába sorolhatók azok a komponensek, amelyek a nyílászárók, tükrök, fényszórók, ablaktörlők, ülések és a légkondicionáló vezérléséért felelősek, mint például az elektromos ablak- és ajtóvezérlés (Power Window and Door Control, PWDC), az intelligens tükör- és ablaktörlő szabályozás (Smart Mirrors and Wipers, SMW), illetve elektronikus üléspozíció-állítás (Electronic Seat Adjusment, ESA). [1]

A HMI tartomány azokat a rendszereket tartalmazza, amelyek az utasok és a gépjármű közti kommunikációt valósítják meg. Ide tartoznak a különböző analóg és digitális műszeregységek, kapcsolók és gombok, illetve a multimédiás rendszerek is. A telematikai rendszerek pedig a gépjárművek közötti kapcsolatért, illetve a jármű és a közúti infrastruktúra közötti információcseréért felelősek. [1]

Az előző bekezdésben említett elektronikus komponenseken felül megjelentek olyan fejlett vezetéstámogató-rendszerek (Advanced Driver-Assistance Systems, ADAS) is, amelyek tovább növelték az utasbiztonságot és a kényelmet. Ezek a rendszerek elsősorban a gépjárműbe integrált szenzorokra támaszkodnak, amelyek valós-idejű adatokat szolgáltatnak a jármű mozgásáról, illetve környezetéről. Ide tartozik például az adaptív sebességtartó automatika (Adaptive Cruise Control, ACC), a sávtartó asszisztens (Lane Keep Assist, LKA), illetve frontális ütközést elkerülő vészfékező rendszer (Automatic Emergency Braking, AEB) is. [3]

2.1.2 Járműfedélzeti kommunikáció

Az elektromos és elektronikus rendszerek működéséhez fejlett kommunikációs technológiák szükségesek, amelyek biztosítják a gyors és megbízható információcserét az egyes komponensek között. A kommunikációs hálózatok és protokollok kulcsfontosságú tényezők, [2] hiszen lehetővé teszik az ECU-k egymással, illetve más elektronikus alrendszerekkel és szenzorokkal való adatcseréjét. [3] A korábbi

gépjárművekben minden egyes elektronikus vezérlőegység között pont-pont összeköttetést alkalmaztak, amely hatalmas kábelmennyiséget igényelt és nagy mértékben növelte a gyártási költségeket. Emellett minden egyes elektronikus funkcióhoz dedikált ECU-t rendeltek, amely tovább növelte a belső hálózat komplexitását. [4]

Napjainkban az elosztott megközelítési módot alkalmazzák a gépjárműbe ágyazott elektronikus architektúrák megtervezésekor, annak érdekében, hogy csökkentsék a rendszer bonyolultságát és a gyártási költségét. [2] A különböző funkciókért felelős alrendszerek eltérő sávszélességet, hibatűrő képességet, késleltetési időt és biztonságot igényelnek, ezért több, eltérő tulajdonságokkal rendelkező kommunikációs protokollt alkalmaznak a fedélzeti hálózat kialakítására: CAN (Controller Area Network), FlexRay, LIN (Local Interconnect Network), AE (Automotive Ethernet), MOST (Media Oriented Systems Transport) és SENT (Single Edge Nibble Transmission). [1] A különböző hálózatok közti zavartalan kommunikációt átjárók (gateway) segítségével valósítják meg. A SAE (Society for Automotive Engineers) négy osztályt határozott meg a protokollok csoportosítása, az A, B, C és D osztályt. [4]

Az A osztályba azok a kommunikációs hálózatok tartoznak, amelyek 10 Kbps-nál alacsonyabb adatátviteli sebességgel rendelkeznek és egyszerűbb vezérlési utasítások továbbítására lettek kifejlesztve, mint például a karosszéria tartomány elektronikus rendszereinek irányítása. [4] Az A osztály fő képviselője a LIN, amely robosztus megoldást jelent kisebb hálózatok kialakítására, hiszen alacsony költség mellett magas szintű hibatűrési képességgel rendelkezik. [3]

A B osztályú hálózatok elsődleges feladata, hogy biztosítsák az ECU-k közti adatcserét. Ezek a protokollok, mint például az alacsony sebességű CAN, 10 és 125 Kbps közötti adatátviteli sebességre képesek. [3]

A C osztály azokat a hálózati típusokat tartalmazza, amelyek nagy sebességű, valós idejű kommunikációt tesznek lehetővé a hajtáslánc és futómű tartományok számára, mint például a nagy sebességű CAN (high-speed CAN). [3]

A D osztályba pedig azok a hálózati szabványok sorolhatóak, amelyek 1 Mbps-nál magasabb adatátviteli rátával rendelkeznek, mint az AE, FlexRay és a MOST. [4] Az AE-t a fejlett vezetéstámogató rendszerek esetén alkalmazzák, mivel rendkívül alacsony késleltetéssel, akár 100 Mbps adatátviteli sebességgel és fejlett biztonsági jellemzőkkel

rendelkezik. [3] A FlexRay egy magas komplexitású és költséges hálózati protokoll, azonban 10 Mbps adatátviteli sebességének és széleskörű hibatűrő funkcióinak köszönhetően elsősorban biztonságkritikus és valós idejű kommunikáció kivitelezésére alkalmazzák. A MOST protokollt nagy mennyiségű adat átvitelére tervezték, ezért tökéletes megoldást jelent a multimédiás rendszerek és a telematika számára. [3]

2.1.3 Vezeték nélküli kommunikáció

A vezeték nélküli kommunikációs technológiák fejlődése nagy hatást gyakorolt az autóiparra. Segítségükkel a járműtulajdonos képes távolról vezérelni a gépjármű bizonyos kényelmi és biztonsági funkcióit, beleértve a központi zárat, a nyílászárókat és az állófűtést, illetve csatlakozni tud a multimédiás rendszerhez. Továbbá a jármű kapcsolódni tud a gyártói infrastruktúrához és felhőszolgáltatásokhoz, amelyekről szoftver- és térképfrissítéseket, illetve egyéb információkat és beállításokat tud szinkronizálni. A jelenlegi tendenciák szerint a jövőben egyre szorosabb vezeték nélküli összeköttetés lesz a gépjárművek között, ami nagy mértékben hozzá fog járulni a biztonságos közúti közlekedéshez.

A technológia fejlődésnek köszönhetően napjaink korszerű gépjárművei képesek mozgás közben adatot küldeni és fogadni. Az ad-hoc járműhálózat (Vehicular Ad Hoc Network, VANET) decentralizált, hálós (mesh) topológiát valósít meg a gépjárművek között, melynek lényege, hogy a csomópontok közvetlenül cserélnek adatot, nem pedig egy bázisállomáson keresztül. [5]

Az autóiparban alkalmazott vezeték nélküli kommunikációs protokollok az adatcserében résztvevő felek szerint három nagy csoportra bonthatóak, a jármű-jármű (Vehicle-to-Vehicle, V2V), a jármű-infrastruktúra (Vehicle-to-Infrastructure, V2I), illetve a jármű-minden (Vehicle-to-Everything, V2X), utóbbi az előző kettőn felül még további csoportokat is magába foglal. [5]

A V2V kommunikáció első számú célja, hogy megelőzze a közúti baleseteket azáltal, hogy lehetővé teszi a mozgásban lévő gépjárművek közti adatcserét a haladási adataikra vonatkozóan. Ennek köszönhetően a gépjárművekbe olyan biztonsági funkciókat implementálhatnak, amelyek a közeli járművek sebességét, haladási irányát és pozícióját elemezve és a jelenlegi biztonsági rendszerekkel együttműködve képesek megelőzni a balesetek bekövetkezését. [5] A V2V esetén a vezeték nélküli adatcserét a WAVE (Wireless Access in Vehicular Networks) protokoll teszi lehetővé, amely dedikált

rövid hatótávolságú kommunikációt (Dedicated Short-Range Communication, DSRC) biztosít az IEEE 802.11p szabvány alapján. [3]A jelenleg alkalmazott biztonsági funkciók kizárólag az érzékelőkre támaszkodnak, amelyek sok esetben pontatlan és lassú reakciót eredményeznek. A jövő gépjárműveiben a V2V kommunikáció segítségével a veszélyes közúti szituációk időben észlelhetőek lesznek, ezáltal várhatóan nagy mértékben csökkeni fog a balesetek száma. [5]

A V2I kommunikáció DSRC segítségével lehető teszi, hogy gépjárművek adatot cseréljenek a közúti infrastruktúrával, beleértve többek között a közlekedési lámpákat, RFID-olvasókat (Radio Frequency IDentification), parkolóórákat és a közúti felfestéseket is. A V2I jelentősége egyre nő a fejlett önvezető gépjárművek térnyerésével, hiszen esetükben elengedhetetlen, hogy kommunikálni tudjanak a jelzőlámpákkal, illetve megfelelően érzékeljék a közúti felfestéseket és táblákat. [5] Ehhez természetesen a közúti infrastruktúra egységeinek (Roadside Unit, RSU) fejlesztésére is szükség van, amely nélkülözhetetlen lesz a teljesen önvezető járművek rendeltetésszerű működéséhez. [3]

A V2X egy gyűjtő fogalom, amely magába foglalja a jármű-gyalogos (Vehicle-to-Pedestrian, V2P), a jármű-útmenti infrastruktúra (Vehicle-to-Roadside, V2R), a jármű-eszköz (Vehicle-to-Device, V2D), a jármű-villamos hálózat (Vehicle-to-Grid, V2G), illetve a jármű-felhő (Vehicle-to-Cloud, V2C) kommunikációs megoldásokat. A V2P során a gyalogosokon és a kerékpárosokon (Vulnerable Road Users, VRU) van a hangsúly, akik valós idejű figyelmeztetést kaphatnak, amennyiben a közeledő jármű mozgási paraméterei alapján balesetveszélyes közlekedési szituációba kerülhetnek. A gyalogosütközésre figyelmeztető rendszer (Pedestrian Collision Warning, PCW) a gyalogosok mobiltelefonjába integrált Wi-Fi, Bluetooth, illetve NFC (Near Field Communication) vezeték nélküli kommunikációs technológiák segítségével képes előre jelezni a potenciális fizikai kontaktust. A V2R az úthálózatok mentén telepítésre kerülő RSU-kra támaszkodik, amelyekkel kétirányú kommunikációt megvalósítva képes adatot cserélni az aktuális forgalmi szituációkkal kapcsolatban. [5] A V2D azokat a vezeték nélküli kapcsolatokat foglalja magába, amelyek a vezető okos eszközei és jármű multimédiás rendszere között jönnek létre, leggyakrabban Bluetooth segítségével. A V2G kommunikáció lehetővé teszi a kétirányú adatcserét az elektromos járművek és a villamos töltőhálózat között. A V2C pedig a jármű és a gyártói felhőszolgáltatások közti

információcserét biztosítja, amely segítségével többek között vezeték nélküli szoftverfrissítés (Over-The-Air, OTA) és távoli diagnosztika végezhető el. [6]

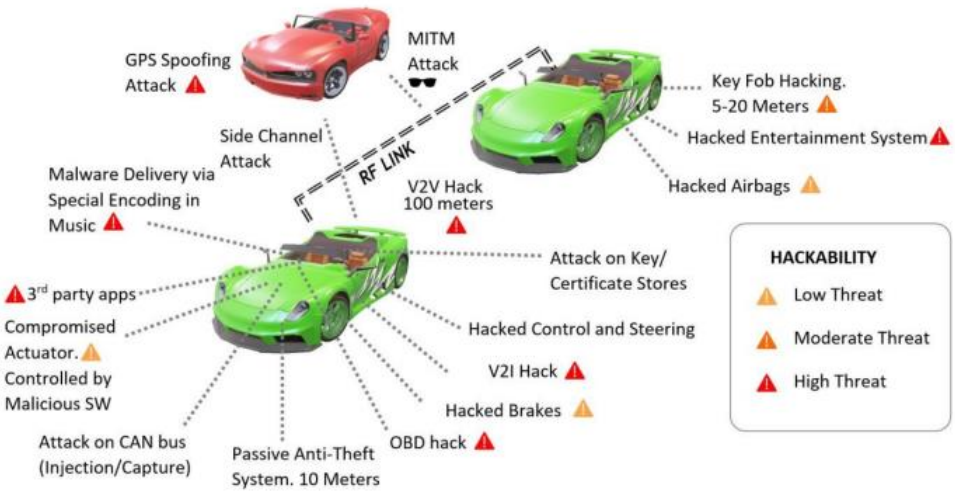
2.2 Autóipari kiberbiztonság

Az autóipari beágyazott rendszerek komplexebbé válása a sérülékenységek számának fokozatos növekedését eredményezte, mely tendencia a mai napig tart. A fejlett elektromos és elektronikus rendszerek, a vezetékes és vezeték nélküli kommunikációs technológiák térnyerése tovább növelte a gépjárművek bonyolultágát és új támadási felületeket létesített a kiberbűnözők számára.

A korábban mechanikus és hidraulikus mérnöki megoldásokkal kivitelezett komponenseket felváltották az elektronikus megoldások. Az olyan fő funkciókat, mint a hajtáslánc és futómű vezérlése, beleértve a motor, a fékek és a kormányrendszer vezérlését, már ECU-k végzik. Ha egy illetéktelen személy hozzáférést szerez egy adott elektronikus vezérlőegységhez és manipulálni tudja annak működését, az akár emberéleteket követelő balesetekhez is vezethet.

2.2.1 Kiberfenyegetések és kihívások

Az autóipari beágyazott rendszerek összetettségének fokozódásával exponenciálisan nőtt a potenciálisan kihasználható sérülékenységek száma. A fedélzeti rendszert egyre több különböző hálózati protokoll alkotja, az ECU-k, szenzorok, vezetékes és vezeték nélküli interfészek száma nagy mértékben megnövekedett, illetve a járművek közti összekapcsoltság is fokozódik.



2.2.1-1. ábra: Gépjárművek elleni kibertámadások [7]

A 2.2.1-1. ábra jól szemlélteti, hogy a modern gépjárművek ellen melyek a legismertebb támadások. Az alábbiakban részletes tárgyalom a korszerű gépjárművek belső és külső kommunikációs rétegeivel kapcsolatos sérülékenységeket és támadási módszereket a kiberbűnözők laterális mozgásával megegyező sorrendben.

A vezetékes és vezeték nélküli interfészek egyfajta belépési pontként szolgálnak a támadóknak, ahonnan tovább haladhatnak a jármű belső hálózata felé. A gépjárművek összeszerelést követően egyetlen fizikai csatlakozási ponttal rendelkeznek, a fedélzeti diagnosztikai interfésszel (On-Board Diagnostics II, OBD-II), amelyen keresztül úgynevezett roncsolásmentes módon lehet a hálózatra csatlakozni. Roncsolásos hozzáférésnek nevezzük azt a csatlakozási módszert, amikor az illetéktelen személy közvetlenül az adatbusz fizikai kábelére kapcsolódva jut hálózati hozzáféréshez. Az OBD-II komoly sebezhetőségi pontot jelent, hiszen közvetlen hozzáférést tesz lehetővé a gépjármű belső kommunikációs hálózatához a legtöbb járműtípus esetén. [7]

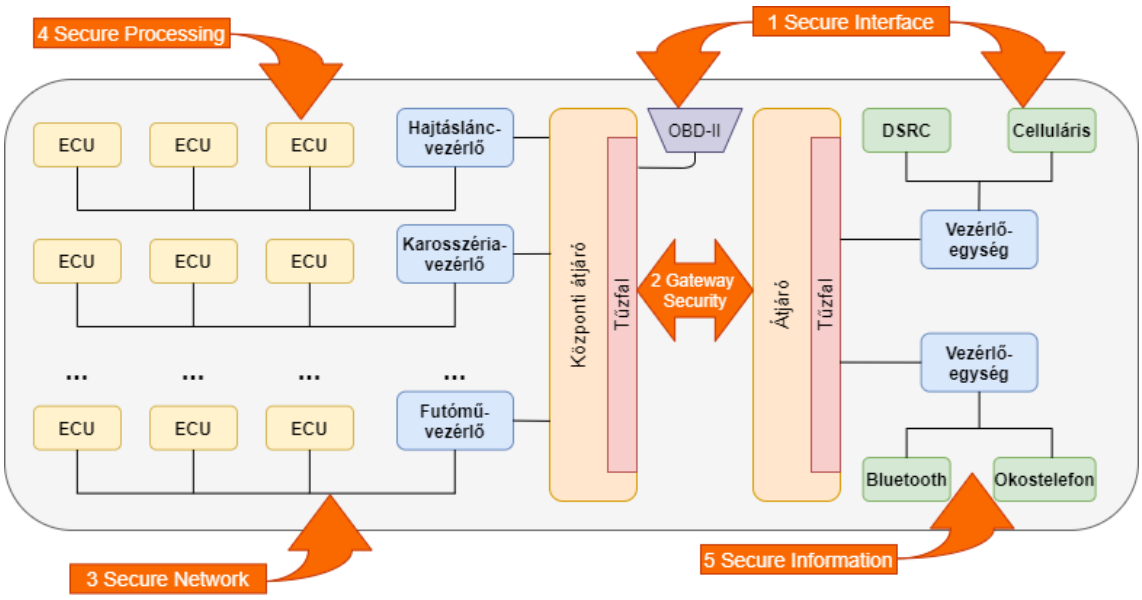
A vezeték nélküli kommunikációs technológiák térnyerése rendkívüli hatást gyakorolt az autóipari kiberbiztonság jelenére, hiszen lehetővé teszi a kiberbűnözők számára, hogy fizikai hozzáférés nélkül is támadást indíthassanak a gépjárművek ellen. A támadók képesek lehallgatni (lehallgatásos támadás, sniffing attack) a vezeték nélküli kommunikációt mind a fedélzeti rendszerek és a járműtulajdonos, mind a V2X csomópontok között. A távoli központi zár vezérlését megvalósító adó (távirányító kulcs) és az integrált fedélzeti vevőegység között lehallgatással megszerezhetik azt a digitális jelet, ami a jármű kinyitásához szükséges, majd a jel visszajátszásával (visszajátszásos támadás, replay attack) ki tudják nyitni az ajtókat (key fob hacking). A hitelesítési folyamat kijátszásával csatlakozni tudnak a jármű multimédiás rendszeréhez, ahonnan manipulálni tudják a szórakoztató elektronikák működését, illetve kártékony szoftvert telepíthetnek a rendszerre, amely a későbbi támadások során hátsó ajtóként (backdoor) funkcionálhat. V2V kommunikáció esetén a támadó képes lehallgatni a két csomópont közti adatcserét és manipulálni tudja az üzenetek tartalmát (közbeékelődéses támadás, Man-In-The-Middle attack). V2C tekintetében az OTA szoftverfrissítés kompromittálódása jelenthet komoly kockázatot, hiszen ezáltal rosszindulatú forráskód futhat le a vezérlőegységek processzorain (Central Processing Unit, CPU). [7]

A kommunikációs buszokkal kapcsolatos sérülékenységek kutatása és azok kihasználására irányuló módszerek kialakítása rendkívül népszerű a kiberbűnözők és a kutatók köreiben, hiszen az egyes alrendszereket vezérlő üzenetek ezen keresztül

áramlanak. A leggyakrabban előforduló támadási technikákat a CAN-en keresztül szemléltetem, amely nem támogatja az üzenetek (keretek) titkosítását, ezáltal a támadók le tudják hallgatni a rajta zajló adatforgalmat. Emellett üzenethitelesítési képességgel sem rendelkezik, emiatt a kiberbűnözők módosított üzeneteket tudnak injektálni a buszhálózatba (CAN-keret injekció, CAN-frame injection), illetve el tudják árasztani azt szolgáltatásmegtagadás céljából (szolgáltatásmegtagadással járó támadás, Denial of Service). A rosszindulatú támadók gyakran az utóbbi módszerek kombinációját alkalmazzák, miszerint lehallgatják a kommunikációt, visszafejtik (reverse engineering), hogy az egyes üzenetek mely funkciók vezérléért felelősek, majd visszajátszák a módosított üzeneteket a buszra. [3]

2.2.2 Autóipari kibervédelem

Az autóipari kibervédelem célja a gépjárművekkel kapcsolatos kockázatok kezelése. A beágyazott rendszerek kibervédelmének érdekében rétegzett architektúrát alkalmaznak, amely lehetővé teszi a robosztus és ellenálló kiberbiztonsági környezet kialakítását. [3] A 2.2.2-1. ábra jól szemlélteti a rétegeket, illetve azt, hogy az egyes rétegek mely alrendszerek és komponensek védelméért felelősek.



2.2.2-1. ábra: Védelmi rétegek [3] (szerk. a szerző)

Az első réteg (Security Interface) a gépjárműbe integrált fizikai és vezeték nélküli kapcsolódási pontok biztonságáért felelős. A beérkező üzenetek hitelesítésével és ellenőrzésével biztosítja a telematikai- és multimédiás rendszerek, a V2X kommunikáció és a fizikai interfészek, mint például az OBD-II biztonságát. [3] Ez a réteg kritikus

fontossággal bír, hiszen azokat a belépési pontokat védi, amelyeken keresztül illetéktelen személyek illegális módosítást hajthatnak végre a gépjármű bármely komponensén.

A második réteg (Gateway Security) az átjárók kiberbiztonságáért felelős. Az átjárók feladata, hogy biztosítsák az üzenetek strukturális konvertálását a heterogén hálózatban, illetve szegmentálják azt több kisebb funkcionális tartományra. Utóbbi rendkívül fontos, hiszen a biztonságkritikus komponenseket a lehető legnagyobb mértékben el kell szigetelni annak érdekében, hogy az illetéktelen személyek nehezen tudjanak hozzáférni. Emellett az átjárók ellenőrzik a beérkező üzenetek hitelességét és érvényességét mielőtt továbbítanák azokat a megfelelő célcsomópont felé. [3]

A harmadik réteg (Secure Network) elsődleges feladata az ECU-k közti kommunikáció védelme az egyes funkcionális tartományokon belül. Ennek érdekében a rétegben olyan funkciókat implementáltak, amelyek biztosítják a kommunikációban résztvevő csomópontok és a köztük áramló üzenetek biztonságát. A védelmi réteg motorindításkor és periodikus időközönként ECU-szintű validálást (ellenőrzést) végez abból a célból, hogy megerősítse a vezérlőegységek hitelességét. Emellett biztosítja az üzenetek bizalmasságát titkosítás révén, illetve gondoskodik a hitelességükről és a sértetlenségükről kriptográfiai tanúsítványok felhasználásával. Továbbá képes a gyanús, kompromittált csomagok kiszűrésére minta-alapú detekció segítségével. [3]

A negyedik réteg (Secure Processing) a biztonságos feldolgozásért felelős. A CPU-kon akár több millió sorból álló programkódok futnak le, amelyek potenciálisan tartalmazhatnak hibákat, sérülékenységeket és kompromittált kódrészleteket. A réteg feladata, hogy a mikrovezérlőkben implementált biztonságos indítási (safe booting) és valód-idejű védelmi mechanizmusok segítségével ellenőrizze az adott kódrészlet legitimitását és integritását. Továbbá az, hogy vizsgálja a fizikai vagy a vezeték nélküli interfészeken keresztül érkező firmware- és szoftverfrissítések hitelességét és sértetlenségét, mielőtt azok ténylegesen végrehajtódnának a processzorokon. [3]

Az ötödik és egyben utolsó védelmi réteg (Secure Information) a beágyazott rendszerben keletkező és tárolt információk biztonságáért felelős. A réteg feladata, hogy biztosítsa a szenzitív és bizalmas információk titkosságát, integritás-védelmét és rendelkezésre állását. A modern autóipari mikrokontrollerek hardveres biztonsági modullal (Hardware Security Modul, HSM) rendelkeznek, amely képes biztosítani a CIA modellt az érzékeny információk számára. [3]

2.3 Nemzetközi autóipari szabványok

Ebben az alfejezetben adatvédelmi okok miatt magasabb absztrakciós szinten ismertetem azokat a fő nemzetközi autóipari szabványokat, amelyek követelményeinek az autóipari vállalatok által fejlesztett kormányrendszereknek meg kell felelniük.

2.3.1 ISO/SAE 21434:2021

Az ISO/SAE 21434 a kiberbiztonság fontosságát és szerepét tárgyalja a sorozatgyártású gépjárművek elektromos és elektronikus rendszereinek megtervezésével kapcsolatban. A szabvány célja, hogy a kiberbiztonsági kritériumok megfelelő figyelembevételével lehetővé tegye az E/E rendszerek megtervezését, annak érdekében, hogy lépést tudjanak tartani a technológia fejlődéssel és az új támadási módszerekkel. További célkitűzése, hogy biztosítsa a teljes ellátási láncban (supply chain) való közös megértést azáltal, hogy részletesen tárgyalja a kiberbiztonsági tervezéssel kapcsolatos fogalmakat, célkitűzéseket, követelményeket és iránymutatásokat. Lehetővé teszi a szervezetek számára, hogy [8]:

- kiberbiztonsági irányelveket és eljárásokat hozzanak létre;
- kezelni tudják a kiberbiztonsági kockázatokat és fenyegetéseket;
- kiberbiztonság-kritikus gondolkodásmódot alakítsanak ki.

2.3.2 UNECE R155 (UN Regulation No. 155)

A UNECE R155 a gépjárművek kiberbiztonsági típusjóváhagyási folyamatával kapcsolatos követelményeket fogalmaz meg, mind a járműgyártó vállalatokkal (Original Equipment Manufacturer, OEM), mind a Jóváhagyó Hatósággal (Approval Authority) szemben. A típusjóváhagyás az a folyamat, amikor a hatóság ellenőrzi, hogy az OEM sikeresen implementálta-e a szabályozásokban szereplő követelményeket, beleértve a különböző tesztek végrehajtását és a szükséges dokumentációk és folyamatleírások létrehozását. [9]

A szabvány továbbá előírja, hogy az OEM-eknek Kiberbiztonsági Irányítási Rendszert (Cyber Security Management System, CSMS) kell létrehozniuk és üzemeltetniük, aminek keretében olyan eljárásokat kell alkalmazniuk, amelyekkel biztosítani tudják a gépjármű kiberbiztonságát a teljes életciklusa során. Az eljárások magukba foglalják a kockázatok értékelését és kezelését, a kiberfenyegetések észlelését

és nyomon követését, a sérülékenységek felismerését és azokat a folyamatokat, amelyeket a kiberbiztonsági tesztelés során alkalmaznak. [9]

2.3.3 UNECE R156 (UN Regulation No. 156)

Az UNECE R156 a típusjóváhagyást a szoftverfrissítéssel szembeni kiberbiztonsági követelmények teljesítéséhez köti. Általánosságban az OEM-eknek biztosítaniuk kell a frissítés integritás-védelmét, hitelességét és bizalmasságát, illetve a folyamat biztonságos végbemenetelét. Olyan eljárások alkalmazását írja elő, amelyek [10]:

- megelőzik az adatmanipulációt a frissítési folyamat kezdete előtt;
- biztosítják a frissítéskiszolgáló-rendszer fejlesztését;
- elvégzik a szoftver forráskódjának ellenőrzését és hitelesítését.

A sztenderd kiemelten kitér a vezeték nélküli szoftverfrissítésekkel szembeni elvárásokra. Olyan folyamatok implementálását várja el, amelyek biztosítják, hogy [10]:

- a menet közbeni frissítések nem veszélyeztetik a biztonságot;
- a fizikai beavatkozást igénylő frissítések nem zajlanak le szakértő jelenléte nélkül;
- sikertelen vagy megszakított művelet esetén a korábbi verzió visszaállítható legyen;
- a folyamat csak megfelelő akkumulátor kapacitás esetén kezdődhessen el;
- a felhasználó részletes tájékoztatást kapjon a frissítés paramétereiről és sikerességéről.

A szabvány előírja, hogy az OEM-eknek Szoftverfrissítés-kezelési Irányítási Rendszert (Software Update Management System, SUMS) kell létrehoznia. A SUMS a UNECE R156 szabványban foglalt szoftverfrissítési követelmények teljesítésének érdekében bevezetett szervezeti folyamatok és eljárások meghatározásának szisztematikus megközelítése. [10]

2.4 Az ECU-k kiberbiztonsági tesztelése

Ebben az alfejezetben ismertetem az E/E rendszerek és a vállalat által fejlesztett kormányrendszerek vezérléséért felelős ECU-k kiberbiztonsági tesztelésének indítékait, illetve a különböző tesztelési módszereket.

2.4.1 A tesztelés motivációi és szükségessége

A modern gépjárművek számos biztonságkritikus elektromos és elektronikus rendszerrel rendelkeznek. A hajtáslánc és futómű tartományok E/E rendszereinek funkcionális biztonsága és kiberbiztonsága kiemelt szereppel bír, hiszen ezek a rendszerek felelősek a gépjármű hossz- és oldalirányú mozgatásáért.

A thyssenkrupp által fejlesztett elektromechanikus kormányrendszerek a futómű tartományba tartoznak, ezért biztonság szempontjából kritikusnak számítanak. A kormányzásért és az aktív rásegítésért felelős elektromotor vezérlését egy ECU végzi, amely a kormányszög jeladó és a nyomaték szenzor jelei alapján határozza meg a megfelelő kormányzási utasításokat.

Ha az illetéktelen személyek jogosulatlan hozzáférést tudnak szerezni a vezérlőegységekhez és manipulálni tudják azok működését, az az ECU-k üzemzavarához vagy akár teljes leállásához vezethet. A tesztelési folyamatok célja, hogy feltárják a sérülékenységeket, beleértve a tervezési és implementálási hibákat az ECU-k fejlesztési fázisa során. Kritikus fontosságú, hogy a sebezhetőségek minél hamarabb azonosításra kerüljenek, hiszen a gyártási és üzemeltetési fázisokban a hibák javítása jóval költségesebb a fejlesztési szakaszhoz képest. A tesztelések eredményei alapján csökkenti lehet a sérülékenységek számát, illetve megfelelő ellenintézkedéseket lehet bevezetni annak érdekében, hogy az ECU-k kiberbiztonsága biztosítható legyen teljes életciklusukra nézve.

2.4.2 Tesztelés módszertanok

Lévén, hogy tökéletesen biztonságos rendszer nem létezik, a tesztelési folyamatok célja a sérülékenységek azonosítása, nem pedig a rendszer tökéletességének bizonyítása. Az elektronikus vezérlőegységek biztonsági tesztelésére számos módszertan létezik, amelyek mindegyike sajátos jellemzőkkel és megközelítéssel rendelkezik. A

kiberbiztonsági validációs folyamatok során e módszertanok segítségével győződnek meg az ECU-val szembeni kiberbiztonsági célok teljesüléséről.

A leggyakrabban alkalmazott tesztelési stratégiák a Black-Box, a Gray-Box, illetve a White-Box modellek, amelyek különböző nézőpontokból közelítik meg a kiberbiztonsági tesztelést. A szervezeten belüli tesztelési folyamatokat gyakran egy másik vállalat csapata által végzett független teszteléssel egészítik ki, melynek célja a tesztelési lefedettség növelése, illetve a kevésbé kritikus sérülékenységek azonosítása.

Black-Box módszertan

A „feketedobozos" módszertan során a tesztelő egy átlagos kibertámadó szerepét alakítja és nem kap előzetes információt az ECU-ról. A folyamatot végző szakember nem kap hozzáférést az architekturális dokumentációkhoz és a forráskódokhoz, amely arra ösztönzi, hogy a támadó fejével gondolkodjon. A módszertant alkalmazó tesztelőnek mind az automatizált szkennelési technológiákat, mind a manuális tesztelési eljárásokat ismernie kell ahhoz, hogy fel tudja térképezni az ECU belső működését. [11] Amennyiben külső vállalatot bíznak meg a módszer alkalmazásával, akkor az ECU-t fejlesztő szervezet semmilyen információt nem oszt meg a vezérlőegységre vonatkozóan. Alkalmazása ebben a felállásban nem célszerű, mivel magas költségek mellett alacsony eredménybeli megtérülést eredményez.

Gray-Box módszertan

A „szürkedobozos" módszertan esetén a tesztelő kizárólag a legszükségesebb információkkal rendelkezik az ECU-val kapcsolatban, beleértve az architekturális dokumentációkat, illetve az alacsony jogosultsági-szintű hozzáférési engedélyeket. A „feketedobozos" stratégiával szemben a Gray-Box megközelítés sokkal specifikusabban közelíti meg ECU-k egyes komponenseit és funkcióit, ezáltal jóval időhatékonyabb eljárás. [11]

White-Box módszertan

A „fehérdobozos" megközelítés esetén a tesztelő számára minden információ rendelkezésre áll az ECU-ra vonatkozóan. A metodológia elsősorban a statikus módszerekre támaszkodik, beleértve a funkciók manuális tesztelését, illetve a statikus kódelemzést. Mivel a White-Box tesztelés rendkívül kifinomult kódelemzéssel végezhető, a rendszer külső és belső sebezhetőségeinek átfogó értékelését teszi lehetővé. [11]

2.4.3 Tesztelési technikák

A leggyakrabban alkalmazott tesztelési eljárás a behatolási vizsgálat (penetration test), amelynek végrehajtását általában külső vállalatra bízzák. A módszer teljesítésére határozott időintervallum áll a tesztelő rendelkezésére, és amennyiben az időablakon belül nem talál sérülékenységeket, akkor a rendszer biztonságosnak tekinthető.

Emellett az elterjedt technikák közé tartozik a bemenet-érvényesítés (input validation), a sebezhetőségi vizsgálat (vulnerability scanning), a hibainjektálás (fault injection), illetve az oldalcsatornás támadás (side-channel attack) is.

Input validation

Bemenet-érvényesítés során a tesztelő különböző célzottan módosított üzeneteket fecskendez a kommunikációs hálózatba abból a célból, hogy vizsgálja az elektronikus vezérlőegységek reakcióit. Alapvető fontosságú, hogy az ECU-k megfelelően fel legyen készítve a rosszindulatú utasítások azonosítására és kezelésére, mielőtt tényleges végrehajtanák azokat.

Vulnerability scanning

A tesztelő a sebezhetőségi vizsgálat során ellenőrzi, hogy a vezérlőegység diagnosztikai és kalibrációs protokolljai megfelelően védve vannak-e hitelesítési és engedélyezési eljárásokkal. Kiemelten fontos, hogy ezekhez csak jogosult személyek férhessenek hozzá, hiszen ezeken keresztül alapvető módosításokat lehet végezni a vezérlőegységeken.

Fault injection

Hibainjektálás során a tesztelő a mikrokontroller feldolgozóegysége és egyéb perifériái ellen indít célzott támadást. Kivitelezésére a legelterjedtebb eljárás a feldolgozóegység tápfeszültségének pillanatnyi megszakítása, amely egyes kritikus utasítások átugrását eredményezheti.

Side-channel attack

Az oldalcsatornás támadás egy rendkívül speciális eljárás, amely során a mikrokontroller kívülről mérhető tulajdonságait vizsgálja a tesztelő, beleértve az áramfogyasztást, a hőmérsékletet, illetve az elektromágneses kisugárzást. A mért jellemzők elemzésével következtetni lehet a hardverben zajló folyamatokra, illetve bizonyos esetekben akár bizalmas információk is visszanyerhetővé válnak.

3 A zóna elméleti hátterének áttekintése

Ebben a fejezetben áttekintem az információbiztonság alapjait, beleértve azokat a kulcsfontosságú fogalommeghatározásokat, amelyek elengedhetetlenek a szeparált információbiztonsági zóna implementációs folyamatának közérthetőségéhez. Emellett a teljesség igénye nélkül ismertetem az ISO/IEC 27k szabványcsaládba tartozó sztenderdek tartalmát, illetve az ISMS létrehozásában betöltött szerepét. Továbbá részletekbe menően tárgyalom az irányítási rendszerek definícióját, illetve az ISMS folyamatainak kiépítése során alkalmazott négylépcsős modellt.

3.1 Információbiztonságról általánosságban

Napjainkban szinte minden szervezet – iparágazattól és mérettől függetlenül – nagy mennyiségű információt gyűjt, dolgoz fel, tárol és továbbít. Az információ számos formát ölthet, többet között lehet digitális, kézzel fogható, illetve munkavállalói tudás formájában is megjelenhet. [12] Ezek az információk létfontosságúak a vállalatok működése szempontjából, hiszen minden belső és külső folyamatuk és tevékenységük ezeken alapszik. A rosszindulatú támadók körében egyre összetettebb és kifinomultabb módszerek jelennek meg az információk eltulajdonításával, manipulálásával és megsemmisítésével kapcsolatban. Emellett különböző környezeti behatások, mint például tűz, villámcsapás vagy hurrikán is hatással lehetnek az információk épségére. A szervezeteknek fokozott hangsúlyt kell helyezniük az információbiztonságra, hiszen ezek az információkkal kapcsolatos támadások és környezeti katasztrófák jelentős fenyegetést jelentenek a vállalat működésére, vagyonára és hírnevére nézve. [13]

Az adatok gyűjtése, feldolgozása, tárolása és továbbítása összetett folyamatokat igényel, melynek részei az emberek, a hardverek és szoftverek, adatkezelési eljárások, illetve a hálózatok. Ezek együttesen alkotják az információs rendszereket (Information System, IS). Az információbiztonság célja, hogy biztosítsa az adatok bizalmasságát, sértetlenségét és rendelkezésre állását az IS minden komponense esetén. [13] Emellett magába foglalja a megfelelő ellenőrzések (kockázatot mérséklő és/vagy megszüntető intézkedések) végrehajtását és kezelését, amelyek a kockázatok és fenyegetések széles körét veszik figyelembe, annak érdekében, hogy biztosítsák a hosszú távú üzleti sikert és folyamatosságot, illetve minimalizálják az adatbiztonsági incidensek hatását. [12]

3.2 Információbiztonsági terminológia áttekintése

Ebben az alfejezetem áttekintem azokat a kulcsfontosságú fogalmakat, amelyek az információbiztonság alapját képezik. Bemutatom a CIA és AAA modellek tagjait, illetve ismertetem az ISO/IEC 27000:2013 által definiált kockázatkezelési definíciókat.

3.2.1 A CIA modell

Bizalmasság (Confidentiality)

A bizalmasság, vagy másnéven titkosság célja az, hogy biztosítsa a kritikus információk védelmét az illetéktelen felhasználókkal szemben. Csak a megfelelő jogosultsági szinttel és kiváltsággal rendelkező felhasználók férhetnek hozzá a kritikus információkhoz, amennyiben az azokra való igényüket bizonyították. [13]

Sértetlenség (Integrity)

Egy adott információ sértetlensége, vagy másnéven integritása arra az állapotra utal, amikor az adat teljes és hiánytalan, illetve jogosulatlan módosításoktól mentes. Az információ integritásának megszűnéséről akkor beszélhetünk, ha az adat sérül, megrongálódik vagy megsemmisül, illetve ha tartalmát jogosulatlan entitás manipulálja. [13]

Rendelkezésre állás (Availability)

A rendelkezésre állás biztosítja a jogosult entitások számára, hogy egy adott információhoz időben és megbízhatóan férjenek hozzá, megszakítás vagy akadályoztatás nélkül. [13]

3.2.2 Az AAA modell

Hitelesítés (Authentication)

Egy nem hitelesített entitás feltételezett identitásának megerősítését hitelesítésnek nevezzük. Három gyakori hitelesítési eljárást vagy megközelítést szoktak alkalmazni:

- valami, amit tudsz (például egy jelszó vagy hitelesítési kód);
- valami, amivel rendelkezel (például RFID kártya vagy token);
- valami, ami vagy (például ujjlenyomat alapú azonosítás). [13]

Engedélyezés (Authorization)

Az engedélyezés az a folyamat, amely során egy hitelesített entitást összevetnek egy információs eszközökből és a hozzájuk tartozó hozzáférési szintekből álló adatbázissal (Access Control List, ACL). [13] Az engedélyezési folyamatra jellemzően a hitelesítés után kerül sor.

Elszámoltathatóság (Accounting)

Az elszámoltathatóság, más néven ellenőrizhetőség, garantálja, hogy a rendszerben történő valamennyi tevékenység – független attól, hogy engedélyezett vagy nem engedélyezett – visszavezethető legyen egy hitelesített személyhez. A rendszernaplók, adatbázisok naplói és az egyéb nyilvántartások ellenőrzése a legelterjedtebb módja az elszámoltathatóság biztosításának. [13]

3.2.3 ISO/IEC 27000:2013 kockázatkezelési fogalommeghatározásai

Kockázat (risk)

A kockázat a kiszámíthatatlanság hatása egy adott folyamat célkitűzéseire nézve. A hatás az előre jelzettől való bármilyen eltérést jelenti, akár pozitív, akár negatív irányba. A kiszámíthatatlanság vagy bizonytalanság az az állapot, amikor nem áll rendelkezésre kellő információ egy adott esemény bekövetkezésére vagy következményeire vonatkozóan. A kockázatot gyakran az esemény következményeinek és a bekövetkezés valószínűségének kombinációjaként szokták ábrázolni. [12]

Kockázatelemzés (risk analysis)

A kockázatelemzés az a folyamat, melynek célja a kockázat jellegének és természetének analízise, illetve a kockázati szint meghatározása. [12]

Kockázati kritérium (risk criteria)

Olyan küszöbérték, amelyhez képest az értékelendő kockázat jelentőségét és mértékét mérik. A szervezetek általában az üzleti céljaik és a saját kockázatvállalási hajlandóságuk szerint határozzák meg. [12]

Kockázat kiértékelés (risk evaluation)

A kockázatelemzést során eredményül kapott kockázati szintek összehasonlítása a kockázati kritériumokkal. [12]

Kockázat azonosítás (risk identification)

A kockázat felkutatásnak, észlelésének és jellemzésének folyamata, amely során azonosításra kerülnek a források, események és a lehetséges következmények. [12]

Kockázatértékelés (risk assessment)

Összetett folyamat, melynek építőkövei a kockázat azonosítás, a kockázatelemzés, illetve a kockázat kiértékelés. [12]

Kockázatmenedzsment (risk management)

A kockázatkezelés lényege a szervezet vezetésére és ellenőrzésére irányuló intézkedések összehangolása a kockázatokkal kapcsolatban. [12]

Kockázatkezelési folyamat (risk management process)

A kockázatkezelési folyamat a vezetési irányelvek, eljárások és tevékenységek rendszerszerű alkalmazása a kommunikáció, a konzultáció, a környezet meghatározása, illetve a kockázatok azonosítása, elemzése, értékelése, kezelése, nyomon követése és felülvizsgálata során. [12]

Kockázatkezelés (risk treatment)

A kockázatkezelés, másnéven kockázatkezelési stratégia egy olyan folyamat, amely módosítja a kockázatot, beleértve a kockázat forrásának mellőzését vagy megszüntetését, a valószínűség vagy a következmény megváltoztatását, a kockázat megosztását egy vagy több féllel, illetve a kockázat megtartását egy erre vonatkozó tudatos döntés révén. [12]

Ellenőrzés (control)

Kockázatmódosítást okozó ellenőrzési tevékenység, amely magába foglal minden olyan eljárást, eszközt, gyakorlatot és szabályzatot, amely kockázatmódosító hatást válthat ki. [12]

3.3 A zóna létrehozásának motivációi és szükségessége

Az elektromechanikus kormányrendszert vezérlő ECU-k biztonsági tesztelési folyamatai kiemelt jelentőséggel bírnak, hiszen a sérülékenységek és a különféle implementációs és tervezési hibák feltárásával lehetővé teszik a megfelelő ellenintézkedések bevezetését, ezáltal sokkal biztonságosabbá válik a rendszer működése. Ezen túlmenően a biztonságkritikus kormányrendszereknek számos nemzetközi iparági

szabványnak, előírásnak és gyártói követelménynek kell megfelelniük, és az ezen követelményeknek való megfeleléshez elengedhetetlenek a kiberbiztonsági tesztelési eljárások.

Az olyan tesztelési módszerekhez, mint például a penetrációs tesztek, speciális tesztkörnyezetek szükségesek, amelyek magukba foglalják az etikus hackeléshez szükséges hardveres és szoftveres eszközöket. Ezek használata nagy mértékben megnöveli a meglévő vállalati információs technológiai (Information Technology, IT) infrastruktúra kiberfenyegetettségét. Továbbá a tesztelési eljárások során keletkező információk rendkívül kritikusak és értékesek, ezért kulcsfontosságú a bizalmasságuk, sértetlenségük és rendelkezésre állásuk biztosítása. Amennyiben a rosszindulatú támadók megszereznék ezeket az adatokat, sokkal egyszerűbbé válna számukra a támadások végrehajtása.

A szeparált információbiztonsági zóna bevezetése tehát indokolt, hiszen izolált környezetet tud biztosítani az ECU-k tesztelési és kutatási folyamatainak, ezáltal minimálisra csökkenti a vállalat IT hálózatának kiberfenyegetettségét. Emellett biztosítani tudja a CIA modellt az információs eszközök számára, ezáltal elősegíti a vállalati vagyon megőrzését és a kormányrendszer biztonságát.

3.4 A zóna céljainak és funkcióinak ismertetése

Az alábbiakban felsorolásszerűen ismertetem a szeparált információbiztonsági zóna céljait, illetve a hatálya alá tartozó fizikai hálózati infrastruktúra funkcióit. A célok meghatározása során figyelembe vettem mind az ISO/IEC 27k szabványcsalád, mind a vállalat kiberbiztonsági osztálya által támasztott követelményeket és igényeket.

Az ISO/IEC 27k szabványcsalád szerinti célok [12]:

- érdekelt felek, üzleti partnerek és a szervezet által támasztott információbiztonsági követelményeknek való megfelelés;
- információbiztonsággal kapcsolatos szerepek, felelősségi körök meghatározása;
- hitelesítés, engedélyezés és elszámoltathatóság biztosítása a zóna felhasználóival szemben;

- szisztematikus megközelítés biztosítása az információs eszközökkel szembeni kockázatok azonosítására és kezelésére;
- információbiztonság kezelésének átfogó megközelítése, beleértve az incidensek aktív megelőzésére és felderítése irányuló folyamatokat;
- a zóna információs eszközeihez kapcsolódó ellenőrzések folyamatos nyomon követése, felülvizsgálata és fejlesztése.

A vállalat kiberbiztonsági osztálya által megfogalmazott célok:

- izolált környezet biztosítása a tesztelési folyamatok elvégzésére;
- bizalmasság, sértetlenség és rendelkezésre állás biztosítása az információs eszközök számára, különös tekintettel az ECU kutatási folyamata során keletkező kritikus információkra;
- ISO/IEC 27001 szerinti tanúsíthatóság, akkreditált tanúsító szervezet által.

A zóna hatálya alá tartozó hálózati infrastruktúra funkciói:

- kód aláírás (code signing);
- kriptográfia kulcsgenerálás és –menedzsment;
- „valódi” véletlenszám generálás;
- hardveresen gyorsított titkosítás;
- vállalat-specifikus hitelesítési eljárás.

3.5 ISO/IEC 27k szabványcsalád ismertetése

Ebben az alfejezetben bemutatom a szeparált információbiztonsági zóna követelményeit és irányelveit definiáló ISO/IEC 27k szabványcsaládot. Részletesen ismertetem azon tagjait, amelyek iránymutatásait az implementációs terv kidolgozása során követtem.

3.5.1 A szabványcsalád tagjai

Az ISO és az IEC által közösen létrehozott szabványcsalád az ISO/IEC 27k. A szabványcsaládba tizenkilenc sztenderd tartozik, amelyek négy kategóriára bonthatóak, a

szókincset ismertető, a követelményeket meghatározó, az általános útmutatást adó, és az ágazatspecifikus útmutatást közvetítő csoportokra. [12]

Az információbiztonsági irányítási rendszer kialakítása során az alábbi szabványok követelményeit és útmutatásait követtem [12]:

- ISO/IEC 27000 – ISMS áttekintése és szókincs;
- ISO/IEC 27001 – ISMS követelmények;
- ISO/IEC 27002 – Az információbiztonsági ellenőrzések gyakorlati kódexe;
- ISO/IEC 27003 – ISMS útmutató;
- ISO/IEC 27004 – Információbiztonság-menedzsment – Felügyelet, mérés, elemzés és értékelés;
- ISO/IEC 27005 – Információbiztonsági kockázatkezelés.

Az alábbi alfejezetekben adatvédelmi okok miatt magasabb absztrakciós szinten ismertetem a szabványcsalád azon tagjainak jellemzőit, amelyek az ISMS követelményeit és a létrehozásának útmutatásait tárgyalják.

3.5.2 ISO/IEC 27000:2018

Az ISO/IEC 27000 a szabványcsalád első eleme, melynek fő rendeltetése az ISO/IEC 27k tagjainak ismertetése és az ISMS-hez kapcsolódó terminológia áttekintése. Az ISO/IEC 27000 kimondja, hogy ISMS-szabványcsaládot alkotó sztenderdek célkitűzései a következők [12]:

- követelményrendszer definiálása az ISMS-sel és annak tanúsításával szemben;
- részletes útmutató biztosítása az ISMS létrehozásához, bevezetéséhez, fenntartásához és fejlesztéséhez;
- ISMS-re vonatkozó iparág-specifikus irányelvek meghatározása;
- ISMS megfelelőségértékelésével kapcsolatos folyamatok és elvárások meghatározása.

Emellett a szabvány részletesen tárgyalja az ISMS pontos definícióját és rendeltetését, implementálásának kritikus sikertényezőit, illetve az irányítási rendszerhez kapcsolódó kifejezéseket és fogalommeghatározásokat. Utóbbiakat a dolgozat 3.2.3. alfejezetében ismertettem a közérthetőség elérése érdekében. [12]

3.5.3 ISO/IEC 27001:2013

Az ISO/IEC 27001 a szeparált információbiztonsági zóna létrehozásának szempontjából a szabványcsalád legfontosabb tagja, hiszen az ISMS-el szembeni követelményrendszert ismerteti. Az akkreditált tanúsító szervezetek e szabvány szerint végzik ISMS megfelelőségértékelését, ezért kiemelten fontos a benne szereplő követelményrendszer teljeskörű implementálása.

A sztenderd a szervezet általános üzleti kockázatainak összefüggésében felvázolja az intézményesített ISMS létrehozására, működtetésére, felügyeletére, értékelésére, karbantartására és folyamatos fejlesztésére vonatkozó követelményeket. Meghatározza a szervezet, vagy annak egy kisebb egységére vonatkozó információbiztonsági intézkedések bevezetésének irányelveit a kitűzött célokhoz és igényekhez igazodva. A szabvány célja, hogy normatív előírásokat biztosítson az ISMS kialakításához és működtetéséhez, valamint a hatálya alá tartozó információs eszközök védelme érdekében bevezetett folyamatokhoz, beleértve a kockázatok kezelésére irányuló intézkedéseket. [12]

Az ISO 27001:2013 az alábbi témakörökkel foglalkozik részletekbe menően [14]:

- A szervezet és annak környezetének megértése.
- A vezetőség szerepe és elkötelezettsége.
- Támogatás a kompetencia szintekkel, kommunikációval és dokumentációval kapcsolatban.
- Operatív tervezés és ellenőrzés, beleértve a kockázatértékelést és –kezelést.
- Teljesítményértékelés, beleértve a folyamatos felügyeletet, elemzést és felülvizsgálatot.
- Folyamatos fejlesztés folyamata és korrekciós intézkedések.
- Ellenőrzési célok és ellenőrzések.

3.5.4 ISO/IEC 27002:2013

Az ISO/IEC 27002 iránymutatást nyújt a szervezeti információbiztonsági szabványokra és az információbiztonság-irányítási gyakorlatokra nézve. A szervezet információbiztonsági kockázati környezetét figyelembe véve segít a megfelelő ellenőrzések kiválasztásában és végrehajtásában, beleértve az általánosan elfogadott ellenőrzéseket és a szervezet saját irányelveit. [15]

A gyakorlati kódex célja, hogy egy keretrendszert biztosítson annak érdekében, hogy a rendszerek és az ellenőrzések közti interoperabilitás megfelelő legyen. Ajánlásokat ad arra vonatkozólag, hogy az ellenőrzéseket hogyan kell oly módon integrálni a rendszerbe, hogy az ISMS megfeleljen a tanúsítási folyamat során. [16]

Mindenképp megjegyzendő, hogy az ISO/IEC 27002 nem tartalmaz követelményeket az ISMS-re nézve, csupán ajánlásokat tesz az ideális ellenőrzések kiválasztására és létrehozására. Mindemellett néhány ellenőrzés már elavultnak számít a nagyléptékű információs technológiai fejlődés okán. [16] Ennek ellenére a szabvány a szeparált zóna kialakítása során rendkívül hasznosnak bizonyult, hiszen sokkal bőbeszédűbb módon fejti ki az ellenőrzések lényegét, illetve részletes útmutatót biztosít az implementációjukhoz.

3.5.5 ISO/IEC 27003:2017

Az ISO/IEC 27003 átfogó útmutatást nyújt az információbiztonsági irányítási rendszer szervezeti környezetben való megtervezésére és bevezetésére. Részletes irányelveket fogalmaz meg az ISO/IEC 27001:2013 összes követelményének implementálásával kapcsolatban, kivéve a teljesítményértékeléshez és a kockázatkezeléshez tartozó elvárásokat. [17]

A szabvány célja, hogy az ISO/IEC 27001 szűkszavú megfogalmazásait részletes magyarázatokkal egészítse ki. Fontos megjegyezni, hogy az ISO/IEC 27002-höz hasonlóan ez a sztenderd sem fogalmaz meg újabb követelményeket az ISO/IEC 27001-hez képest, viszont gyakorlati útmutatásokon és példákon keresztül jelentős mértékben hozzájárul az ISMS-el szembeni követelményrendszer teljesítéséhez.

3.5.6 ISO/IEC 27004:2016

Az ISO/IEC 27004 célja, hogy segítse a szervezeteket az információbiztonsági irányítási rendszer teljesítményének és hatékonyságának mérésében és értékelésében, annak érdekében, hogy megfeleljenek az ISO/IEC 27001:2013 követelményeinek. A teljesítményértékelési folyamatok fontos részét képezik az ISMS-nek, hiszen a mérési eredmények alapján hozhatóak meg a rendszer irányításával, vezetésével, működési hatékonyságával és folyamatosan fejlesztésével kapcsolatos döntések. [18]

A szabvány az alábbi témakörökhöz nyújt átfogó segítséget [18]:

- információbiztonsági teljesítmény felügyelete és mérése;
- ISMS hatékonyságának nyomon követése és mérése, beleértve a folyamatokat és ellenőrzéseket;
- felügyeleti és mérési eredmények elemzése és kiértékelése.

3.5.7 ISO/IEC 27005:2018

Az ISO/IEC 27005 a szervezeti környezetben alkalmazott információbiztonsági kockázatkezeléssel kapcsolatban fogalmaz meg iránymutatásokat. Egy olyan keretrendszert ismertet, amelyben számos ismert kockázatkezelési metodológia alkalmazható az iparágtól és a szervezeti környezettől függetlenül. [19]

A szabvány nem tartalmaz közvetlen útmutatást az ISO/IEC 27001:2013-ban ismertetett kockázatkezelési követelmények tekintetében, azonban hasznos módszereket ismertet a fenyegetések és kockázatok hatékony felmérésére és kezelésére. [19]

Fontos azonban megjegyezni, hogy az ISO/IEC 27001 rugalmasságot biztosít a kockázatkezelési metodológia megválasztásában, nem írja elő az ISO/IEC 27005 által ismertetett módszereket. A szervezet szabadon alkalmazhat bármilyen módszertant, az elvárás az, hogy a kockázatkezelési folyamat következetes és összehasonlítható eredményeket produkáljon, illetve a kiválasztott eljárás összhangban legyen a vállalat összetettségével és környezetével. [20]

3.6 Irányítási rendszerek

Ebben az alfejezetben részletesen ismertetem az irányítási rendszer és az információbiztonsági irányítása rendszer definícióját.

3.6.1 Irányítási rendszer

Az irányítási rendszerek keretrendszert biztosítanak az erőforrásoknak, annak érdekében, hogy a szervezet elérje a kitűzött céljait. A szervezeti struktúra, a különféle politikák, tervezési tevékenységek, felelősségi körök és szintek, eljárások és folyamatok és erőforrások mind-mind az irányítási rendszer részét képezik. [12]

Az irányítási rendszer az információbiztonság vonatkozásában lehetővé teszi a szervezet számára, hogy [12]:

- megfeleljen az üzleti partnerek és más érdekelt felek információbiztonsági előírásainak;
- fejlessze a terveit és tevékenységeit;
- elérje a kitűzött információbiztonsági céljait;
- megfeleljen az összes rá vonatkozó törvénynek, rendeletnek és iparági követelménynek;
- strukturáltan kezelje az információs eszközeit, annak érdekében, hogy lehetővé tegye a folyamatos fejlesztést és az aktuális szervezeti célokhoz való alkalmazkodást.

3.6.2 Információbiztonsági irányítási rendszer

Információbiztonsági irányítási rendszernek nevezzük azon szabályok és gyakorlatok átfogó rendszerét, amelyeket egy szervezet az információs eszközökkel kapcsolatos kockázatok kezelése érdekében hoz létre és tart fenn. Az ISMS célja az, hogy segítse a szervezetet az információbiztonsági hiányosságok feltárásában, illetve elősegítse a biztonsági incidensek megelőzését és minimalizálja azok hatását. [21]

Az ISMS bevezetése kritikus fontosságú az információs eszközök védelme szempontjából, hiszen lehetővé teszi a szervezet számára, hogy [21]:

- meggyőződjön arról, hogy az információs eszközei folyamatos védelmet élveznek a fenyegetésekkel szemben;
- strukturált és teljeskörű keretrendszert tartson fent az információbiztonsági kockázatok felismerésére és értékelésére, az

ellenőrzések kiválasztására és végrehajtására, illetve ezek teljesítményértékelésére és fejlesztésére;

- folyamatosan fejlessze az ellenőrzési környezetét;
- megfeleljen a jogi és szabályozási követelményeknek.

3.7 PDCA modell

A PDCA (Plan-Do-Check-Act) modell az üzleti folyamatok folyamatos fejlesztésének folyamatorientált megközelítése. A ciklus négy lépcsőből áll, a tervezésből, a megvalósításból, az ellenőrzésből és a cselekvésből. A tervezés fázis során definiálni kell a célokat, illetve azt, hogy ezeket milyen terv szerint lehet a leghatékonyabb módon elérni. A megvalósítás lépés során végre kell hajtani az előző fázisban meghatározott tervet. Az ellenőrzés lépésnél felül kell vizsgálni, hogy megvalósított terv végrehajtása elérte-e az első lépcső során meghatározott célokat. Amennyiben nem, azonosítani kell a hibákat és hiányosságokat, amelyek a célkitűzések nemteljesüléséhez vezettek és az utolsó fázisban reagálni kell rájuk javítások és teljesítménynövelések formájában. [22]

A PDCA egy iteratív modell, az ISMS létrehozásától egészen fennállásának végéig folyamatosan ismétlődik, hiszen az ISO/IEC 27001:2013 követelményként definiálja a folyamatos fejlesztést. Az első lefutáshoz képest, amely az ISMS létrehozására irányul, a fázisok némileg kiegészülnek, annak érdekében, hogy a fejlesztés vagy javítás eredménye mérhető legyen.

A tervezés lépcső az első bekezdésben leírtakhoz képest annyiban egészül ki, hogy meg kell határozni a javítások vagy a teljesítménynövelések alanyát, illetve azt, hogy milyen módon mérhető a változtatások eredménye. Utóbbi lehet bármilyen statisztikai mérőszám, lényeg, hogy a módosítás előtti és utáni állapot összehasonlítható legyen. Ez a harmadik fázis és a következő PDCA iteráció szempontjából is fontos, hiszen ez alapján ellenőrizhető a változtatás sikeressége, illetve sikertelenség esetén pedig a következő iteráció során fokozható a módosítások mértéke, vagy újabb változtatások eszközölhetőek. [23]

A megvalósítás fázis egyik iteráció során sem változik, azonban az ellenőrzés lépcső valamelyest kiegészül az első lefutáshoz képest. A célok tervszerinti elérésének

vizsgálatán felül a teljesítménymutatók összehasonlításával vizsgálni kell, hogy a fejlesztés vagy javítás elérte-e a kitűzött célját. Számos ilyen intézkedés nem eredményez változást vagy akár ront is a helyzeten, ezért fontos, hogy a mérési és a differenciálási folyamatok akkurátusan kerüljenek végrehajtásra. Az utolsó lépcső csupán annyiban egészül ki, hogy az előző iteráció során feljegyzett mérőszám értékét frissíteni kell a javítások vagy teljesítménynövelések utáni állapotra. [23]

Fontos megjegyezni, hogy az ISO/IEC 27001 2013-as változata csak a folyamatos fejlesztést definiálja követelményként, a PDCA modell használatát nem. A szabvány korábbi változataiban a ciklus alkalmazása követelményként szerepelt, azonban most már bármely más folyamatorientált modell használható. Ennek ellenére, a szeparált információbiztonsági zóna kialakítása során a PDCA ciklus fázisait követtem, hiszen a modell továbbra is hatékonynak számít.

3.8 A zóna szolgáltatásaihoz kapcsolódó elméleti háttér ismertetése

Ebben az alfejezetben közérthető módon ismertetem az ISMS által keretbe foglalt hálózati infrastruktúra funkcióihoz kötődő elméleti hátteret, beleértve a publikus kulcsú infrastruktúrát (Public Key Infrastructure, PKI), a kód aláírást (code signing), illetve a „valódi” véletlenszámok előállítására alkalmas generátort (True Random Number Generator, TRNG).

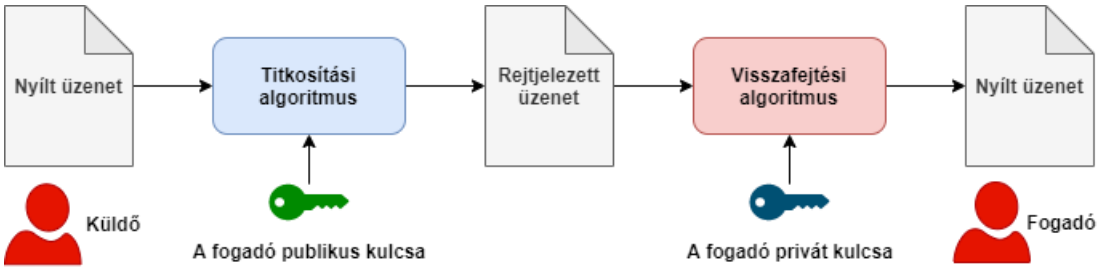
3.8.1 Publikus kulcsú infrastruktúra

A publikus kulcsú kriptográfia rendszer lényege, hogy a kódoláshoz és a dekódoláshoz két különböző kulcsot alkalmaz, a nyilvános és a titkos kulcsot, amelyek között matematikai kapcsolat áll fennt. A kulcsok fontos jellemzői, hogy minden kulcsnak csak egy párja van, illetve egymásból gyakorlatilag kiszámíthatatlanok. A publikus, vagy másnéven aszimmetrikus kriptográfiai rendszer hat építőelemből áll [24]:

- Nyílt szöveg: a rendszer bemenetét képező olvasható üzenet vagy adat, amelyet a küldő bizalmasan szeretne megosztani a fogadóval.
- Titkosítási algoritmus: olyan függvény, amely a bemenetet különböző transzformációkon keresztül átalakítja, mint például az RSA (Rivest-

Shamir-Adleman) és az ECDSA (Elliptic Curve Digital Signature Algorithm).

- Publikus és privát kulcsok: olyan kulcspár, amelynek tagjai között matematika kapcsolat áll fent és az egyiket titkosításra, a másikat pedig visszafejtésre használják. A titkosítási algoritmus által végrehajtott változtatások függnek a kulcs egyedi tulajdonságaitól.
- Rejtjelezett szöveg: A nyílt szöveg rejtjelezett változata, amely függ a titkosítási algoritmustól és a kulcstól.
- Visszafejtési algoritmus: Bemenete a rejtjelezett szöveg, amelyet az algoritmus a megfelelő kulcs felhasználásával visszaalakít az eredeti nyílt szöveggé.



3.8.1-1. ábra: A PKI összetevői és folyamata [24] (szerk. a szerző)

A 3.8.1-1. ábra jól szemlélteti a publikus kriptográfiai rendszer összetevőit és folyamatát. Általánosan elmondható, hogy a folyamat alapvető lépései a következők [24]:

1. A kommunikáló felek generálnak egy kulcspárt, amelynek egyik tagját egy nyilvánosan hozzáférhető adatbázisban vagy fájlban megosztják; ez képezi a publikus kulcsot. A másik tagját minden esetben titokban tartják, ez lesz a titkos kulcs.
2. Ha a küldő fél titkosított üzenetet szeretne eljuttatni a fogadó félnek, akkor a fogadó publikus kulcsával és a titkosítási algoritmussal rejtjelezi a nyílt üzenetet.
3. Amikor a fogadó fél megkapja az üzenetet, a saját privát kulcsával és visszafejtési algoritmussal visszaállítja az eredeti nyílt üzenetet.

A publikus kulcsú infrastruktúra lényeges előrelépést eredményezett a kriptográfia területén, hiszen kiküszöbölte a szimmetrikus kulcsú titkosítás során

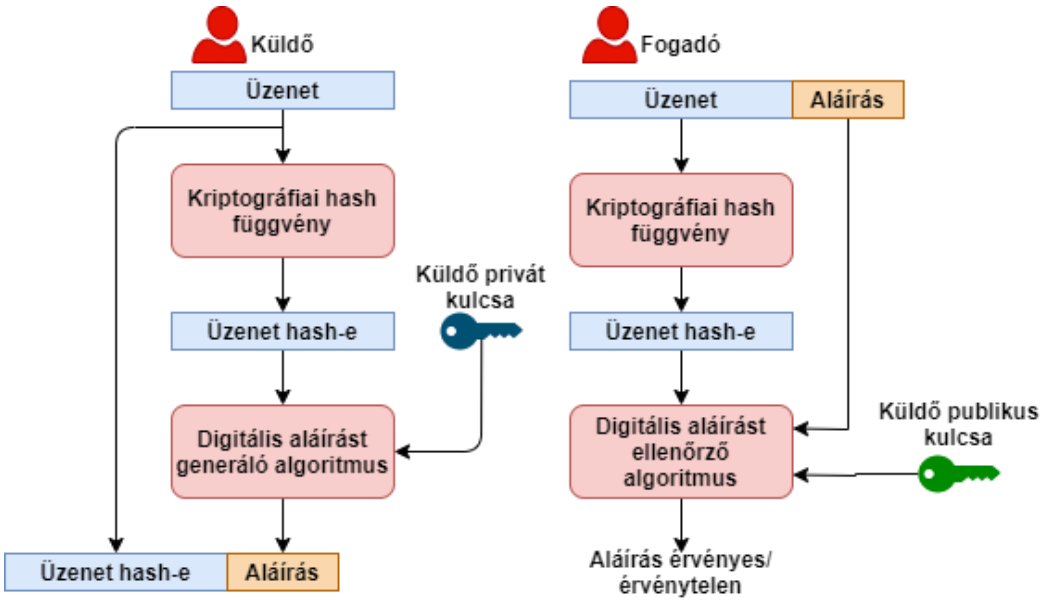
elkerülhetetlen kulcscserélési lépést. Mindemellett lehetővé tette az üzenetek hitelesítését és integritás-ellenőrzését a digitális aláírások segítségével, amelyet a 3.8.2. alfejezet ismertet. [24]

3.8.2 Kód aláírás

A kód aláírás egy olyan módszer, amely a digitális aláírás segítségével lehetővé teszi a forráskód sértetlenségének és hitelességének bizonyíthatóságát és ellenőrizhetőségét. Az eljárás megértéséhez fontos a digitális aláírás létrehozásának és jellemzőinek ismerete.

Digitális aláírás

A 3.8.1. fejezetben tárgyalt publikus kulcsú infrastruktúra tehát lehetővé teszi az üzenetek titkosságának biztosítását, azonban azok sértetlenségét és hitelességét nem garantálja. Erre a hiányra nyújt megoldást a digitális aláírási folyamat, amelynek elemeit és lépéseit a 3.8.2-1. ábra szemlélteti.



3.8.2-1. ábra: Digitális aláírás alkalmazása és ellenőrése [25] (szerk. a szerző)

Folyamatleírás a küldő oldal szerint [25]:

1. A küldő egy lenyomatképző (hash) algoritmus segítségével lenyomatot készít az üzenetről. A hash algoritmus egy egyirányú függvény (a bemeneti érték visszafejthetetlen a lenyomat alapján), amely bármilyen hosszúságú bemenetből kötött hosszúságú kimenetet állít elő. Fontos jellemzője, hogy ugyanazon bemenet mindig azonos lenyomatot

eredményez és az eltérő bemenetek mindig különböző lenyomatokat generálnak.

2. A digitális aláírást generáló algoritmus a küldő privát kulcsát és az üzenet lenyomatát felhasználva elkészíti az aláírást.
3. A küldő az eredeti üzenet mellé csatolja az elkészült digitális aláírást, majd elküldi a fogadónak.

Folyamatleírás a fogadó oldal szerint [25]:

1. A fogadó egy hash algoritmus segítségével lenyomatot készít az üzenetről.
2. A digitális aláírást ellenőrző algoritmus a küldő publikus kulcsát felhasználva dekódolja az aláírást.
3. Az digitális aláírást ellenőrző algoritmus összehasonlítja az 1. és 2. pontban eredményül kapott lenyomatokat. Amennyiben egyeznek, akkor az aláírás érvényes, ellenkező esetben pedig érvénytelen.

Tanúsítványok

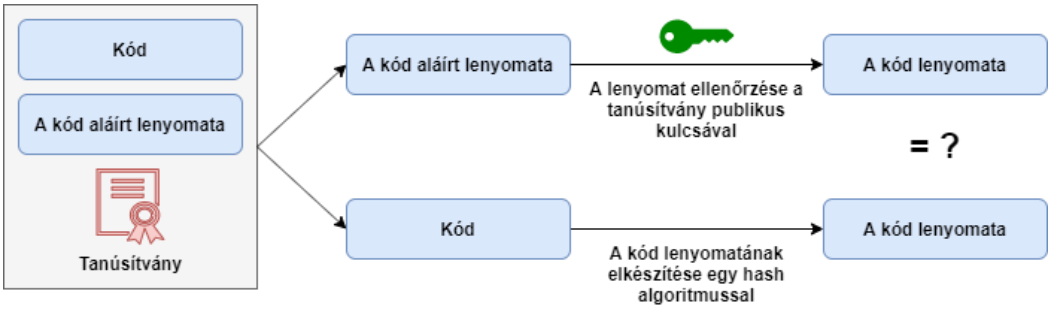
A PKI-vel kapcsolatban jogosan merülhet fel a kérdés, hogy mi biztosítja azt, hogy a feladó valóban a fogadó publikus kulcsát használta-e a folyamat során. Előfordulhat, hogy egy rosszindulatú támadó előzetesen kicseréli a fogadó publikus kulcsát a sajátjára a nyilvánosan hozzáférhető adatbázisban, ezáltal a saját magánkulcsával képes lesz dekódolni az üzenetet.

Annak biztosítása érdekében, hogy a titkosításhoz és az aláíráshoz használt nyilvános kulcs hiteles forrásból származzon, a Hitelesítés-szolgáltatók (Certificate Authority, CA) tanúsítványaira kell támaszkodni. A CA-k a személyazonosság ellenőrzését követően digitális aláírással látják el a publikus kulcsokat, hogy megerősítsék azok hitelességét.

Kód aláírás folyamata

A kód aláírás tehát a digitális aláírási folyamatot és a tanúsítványokat alkalmazza abból a célból, hogy biztosítani tudja az adott forráskód vagy forráskód részlet hiteles eredetét és sértetlenségét, illetve az aláíró fél letagadhatatlan mivoltát. A forráskód vagy forráskód részlet aláírását speciális kód aláíró tanúsítvány segítségével lehet

megvalósítani, amelyeket a Hitelesítés-szolgáltatók állítanak ki. A 3.8.2-2. ábra szemlélteti a kód aláírás folyamatát és építőelemeit.



3.8.2-2. ábra: A kód aláírás folyamata és komponensei [26] (szerk. a szerző)

Az E/E rendszereket vezérlő ECU-k tekintetében kiemelten fontos szerepet játszik a kód aláírás. Segítségével a különböző firmware- és szoftverfrissítések esetén ellenőrizhető, hogy a forráskód valóban hiteles forrásból származik-e, illetve, hogy nem manipulálták-e a kommunikációs folyamat során. Emellett a rendszerszintű ellenőrzések alkalmával a vezérlőegységek – a programkódok futtatását megelőzően - ellenőrzik azok aláírásait, hogy meggyőződhessenek azok sértetlenségéről és hitelességéről.

3.8.3 „Valódi” véletlenszám generátor

Napjaink fejlett kriptográfiai algoritmusainak működéséhez elengedhetetlenek a véletlenszámok. Többek között jelentős szerepet játszanak a titkos kulcsok és tanúsítványok generálásában, valamint számos hitelesítési és rejtjelezési műveletben. Kijelenthető, hogy véletlenszerűség nélkül nem létezne kriptográfia, hiszen minden művelet kiszámíthatóvá válna. [27]

A véletlenszerűséget nem lehet kizárólag számítógépes algoritmusok segítségével előállítani, ezért az analóg világban zajló folyamatok kiszámíthatatlanságát és bizonytalanságát is szükségszerű felhasználni. A véletlenszám generátorok a környezet kaotikus és megjósolhatatlan jelenségeit entrópia-forrásként (a rendezetlenség forrása) használják fel a véletlenszámok előállítására. A bemeneti entrópia-forrás alapján két fő generátortípus határozható meg [28]:

- álvéletlenszám generátor (Pseudo Random Number Generator, PRNG);
- „valódi” véletlenszám generátor.

Az álvéletlenszám generátor úgynevezett pszeudóvéletlen számok előállítására képes, determinisztikus működéséből adódóan. A PRNG kimenete egy véletlenszerű

bemenet (seed) és egy függvény együttes felhasználásával jön létre, ahol az előállított véletlenszám a seed (első lefutásnál) vagy előző kimenet (későbbi lefutásoknál) függvény szerinti transzformációja. Lényeges szem előtt tartani, hogy mivel a függvény egy előre meghatározott műveleti lánc, a seed az egyetlen olyan változó a PRNG alkotóelemei közül, amely véletlenszerűséggel rendelkezik. [28] A PRNG-k gyengesége abban rejlik, hogy a seed-et birtokló és az algoritmust ismerő kiberbűnözők képesek reprodukálni a teljes véletlenszám szekvenciát, ezáltal kompromittálni tudják a kriptográfiai folyamatokat.

A TRNG a véletlenszámok előállítására egy analóg, nem determinisztikus entrópia-forrást és egy feldolgozási (desztillációs) folyamatot alkalmaz. A generátor közvetlenül mintavételezi a forrást, a desztillációs eljárás segítségével kiszűri a nem-véletlenszerűséget okozó tényezőket, majd véletlen biteket állít elő a forrás változásainak megfelelően. [28] A leggyakrabban alkalmazott analóg változók például a hőmérséklet, az elektromos statikusság, a légörvények, illetve az akusztikus zajok. [27] Nyilvánvalóan sok egyéb környezeti jelenség is felhasználható, a lényeg, hogy a folyamatot eredendően kiszámíthatatlannak és megjósolhatatlannak minősítsék kutatások által. A TRNG-ket kriptográfiai felhasználásra alkalmassá teszi az a tény, hogy egyetlen determinisztikus lépést sem alkalmaznak működésük során, ezáltal a támadók nem tudják se visszafejteni, se megjósolni a véletlenszám szekvencia elemeit.

A szeparált információbiztonsági zónában alkalmazott HSM-ek integrált TRNG-vel rendelkeznek, amely nagy mértékben hozzájárul a zóna kriptográfiai technológiákon alapuló szolgáltatásainak kiberbiztonságához, beleértve a vállalat-specifikus hitelesítést, a kód aláírást, illetve a kulcsgenerálást.

3.9 A zóna fizikai infrastruktúrájához kapcsolódó elméleti háttér ismertetése

Ebben az alfejezetben magas absztrakciós szinten tárgyalom a szeparált információbiztonsági zóna fizikai infrastruktúrájához kapcsolódó elméleti hátteret, beleértve a switch, a tűzfal, a HSM, illetve a vállalati szerver általános jellemzőit és képességeit.

3.9.1 Switch

A hálózati switch elsőszámú feladata az adatcsomagok fogadása és továbbítása a helyi hálózatban (Local Area Network, LAN) elhelyezkedő csomópontok között. A switch-ek típustól függően mind az adatkapcsolati, mind a hálózati rétegben képesek kommunikálni. Mindemellett alkalmasak az adatcsomagok szűrésére és a hálózati torlódások, valamint a hurkok megszüntetésére.

3.9.2 Dedikált tűzfal

A dedikált tűzfal egy olyan hardver, amelyet a hálózat szélére (határára) telepítenek. Elsődleges feladata a hálózat védelme a bejövő és kimenő forgalom szűrésének segítségével. A tűzfal a vállalat által bevezetett átfogó biztonsági stratégia szerves részét képezi, hiszen a stratégia által definiált biztonsági irányelveket érvényesíti a hálózati forgalomra. [29]

A tűzfal a rajta áthaladó adatcsomagokat összehasonlítja egy tűzfalszabályzattal, amely alapján eldönti, hogy az adott csomag engedélyezésre vagy tiltásra kerül-e. A tűzfalszabályzat, másnéven hálózati-házirend kivételeket tartalmaz, amelyek az alapértelmezett tiltás/kivételes engedélyezés (default deny/allow by exception) filozófiáját követik. Amennyiben egy adatcsomag nem illeszkedik egy szabályra sem, akkor alapértelmezésként elutasításra kerül. [29]

A hálózati forgalom mellett a dedikált tűzfal útválasztási funkciókat is ellát. A csomagszűrés eredményei szerint meghatározza, hogy a forgalom mely interfész vagy hálózati szegmens irányába haladhat tovább. Mindemellett képes porttovábbításra (port-forwarding) és hálózati címfordításra (Network Address Translation, NAT), amelyekkel lehetővé teszi a hálózaton belüli IP-címek és portok elrejtését a nyílt interneten (Wide Area Network, WAN) elhelyezkedő hálózati csomópontok elől. Továbbá lehetővé teszi virtuális magánhálózatok (Virtual Private Network, VPN) kialakítását, amellyel biztosítja a hálózati erőforrások biztonságos távoli elérését és kezelését. [29]

3.9.3 Hardveres biztonsági modul

A HSM egy olyan speciális hardvereszköz, amely lehetővé teszi a kriptográfia kulcsok biztonságos tárolását és kezelését, illetve a kriptográfiai algoritmusok megbízható és gyors végrehajtását. A HSM-eknek rendkívül szigorú biztonsági

követelményeknek kell megfelelniük, amelyeket elsősorban az ISO/IEC 19790, az ISO/IEC 24759, a FIPS 140-2, illetve a Common Criteria (CC) szabványok fogalmaznak meg. [30]

Biztonsági követelmények

A kriptográfiai kulcsok és algoritmusok biztonságos kezelésén felül a HSM-nek sok egyéb biztonsági elvárásnak is meg kell felelnie, amelyeket elsősorban a nemzetközi szabályozások határoznak meg. A hardveres biztonsági modullal szemben támasztott követelmény közé tartozik:

- a fizikai HSM eszközzel szembeni mechanikai támadások észlelése és kivédése, beleértve a hamisítás elleni védelmet (tamper-resistance);
- védelem az oldalcsatornás támadásokkal szemben, beleértve minden időalapú viselkedésen vagy energiafogyasztási elemzésen alapuló fenyegetést;
- a szoftveres környezet védelme a kódmanipulációval és a kártékony harmadik féltől származó szoftverekkel szemben;
- kulcsgenerálás „valódi" véletlenszám generátor segítségével;
- a jelenlegi technológia fejlettségnek megfelelő kriptográfia műveletek és algoritmusok támogatása.

Tervezési alapelvek

A HSM fő tervezési alapelve, hogy rendelkezik egy úgynevezett belső biztonsági zónával, amely fizikailag és logikailag is különálló az egyéb komponenseivel és a külvilággal szemben. A biztonsági zónán belül helyezkednek el azok a hardver- és szoftverelemek, amelyek a kulcsfontosságú működési folyamatokért felelősek, beleértve a kriptográfiai tárterületet, az operációs rendszert, a firmware-t, a bootloader-t, illetve az érzékelőrendszert. [30]

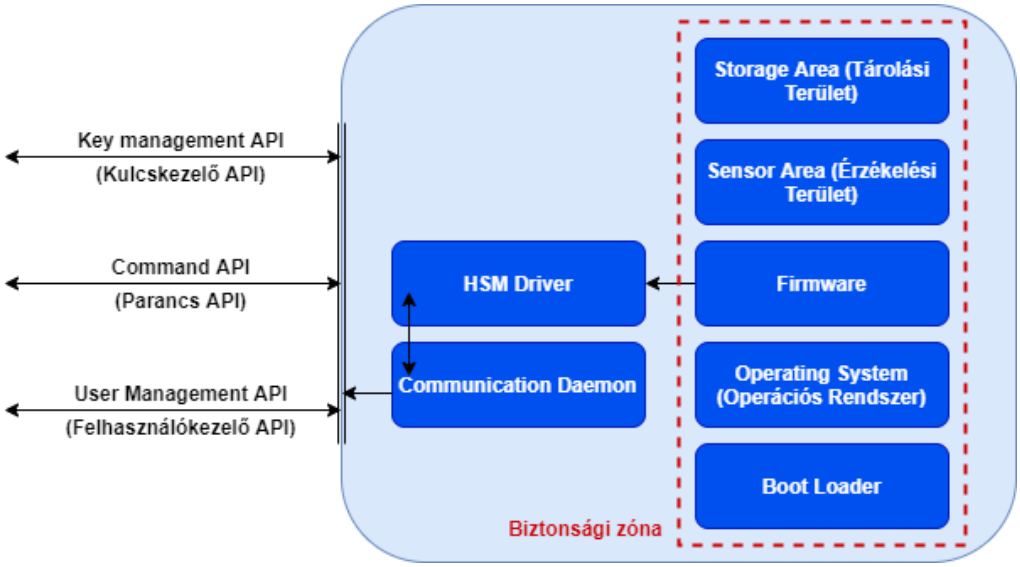
A HSM egyes funkcióit alkalmazásprogramozási interfészeken (Application Programming Interface, API) keresztül lehet kezelni, amelyekből három érhető el [30]:

1. Kulcskezelő API: lehetővé teszi a kriptográfiai kulcsok kezelését, beleértve a szállítási kulcsok előállítását és a HSM-ben tárolt kulcsadatok biztonsági mentését és helyreállítását.

2. Parancs API: hozzáférést biztosít a HSM kriptográfiai funkcióihoz, beleértve a kulcsok generálását, valamint a kulcsok importálását és exportálását.

3. Felhasználókezelés API: lehetővé teszi a felhasználók létrehozását és kezelését, illetve a hozzájuk kapcsolódó szerepkörök létrehozását.

A 3.9.3-1. ábra jól szemlélteti a hardveres biztonsági modul egyes belső komponenseit és külső interfészeit, amelyekről a korábbiakban szó esett.



3.9.3-1. ábra: A HSM komponensei és interfészei [30] (szerk. a szerző)

Fizikai védelem

A hardveres biztonsági modul átfogó fizikai védelemmel rendelkezik, annak érdekében, hogy megelőzze az illetéktelen személyek fizikai hozzáférését, illetve a természeti katasztrófák okozta adatvesztést. A teljeskörű biztonság érdekében a következő fizikai védelmi szinteket alkalmazza [30]:

1. Manipuláció elleni védelem: célja a hardver belső áramkörének védelme a külső, illetéktelen behatolásokból származó módosításokkal szemben. Általában az áramkör epoxigyantás bevonásával valósítják meg.

2. Manipulációs reakció: célja a fizikai behatolások érzékelése a HSM működésének teljes élettartama során. A legtöbb esetben az epoxigyantás fedőrétegbe egy elektromos vezetőhálózatot integrálnak, amely segítségével érzékelhetőek a mechanikai behatások.

3. Hőmérséklet-ellenőrzés: célja elsősorban a hőmérséklet csökkenésből eredő támadások érzékelése.
4. Feszültség-ellenőrzés: célja az üzemi feszültség meghatározott feszültségtartományban belül tartása.

3.9.4 Vállalati szerver

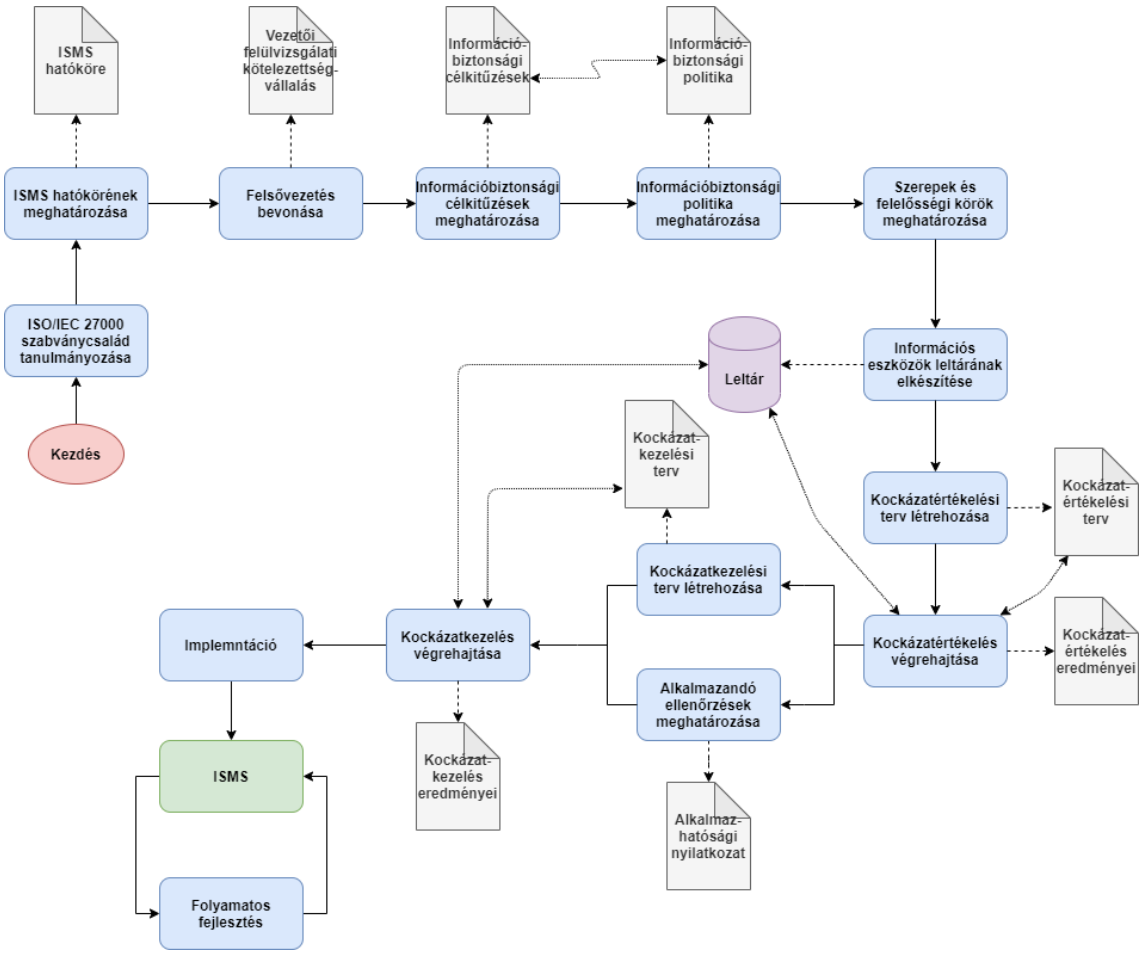
A vállalati szerverek olyan hardverek, amelyek funkcionalitásukat tekintve a személyi számítógépekhez (Personal Computer, PC) hasonlíthatók. A PC-kel ellentétben azonban a vállalati szervereket egy teljes szervezet vagy egy szervezeti csoport követelményeinek kielégítésére tervezték. Ennek megfelelően a belső hardverkomponenseik sokkal nagyobb teljesítménnyel rendelkeznek, beleértve a processzor számítási képességét és a különböző háttértárolók kapacitását. Továbbá a PC-khez képest magasabb hibatűrő képességekkel és alacsonyabb meghibásodási arányokkal bírnak, amelyek lehetővé teszi a vállalati-szintű kritikus szolgáltatások működésének folytonosságát.

4 Szeparált információbiztonsági zóna létrehozása

Ebben a fejezetben részletesen tárgyalom a szeparált zóna, avagy az információbiztonsági irányítási rendszer ISO/IEC 27k szerinti megvalósítási tervét. A 3.9.4-1. ábra szemlélteti a ISMS létrehozásának legfontosabb fázisait. Az alábbi lépések elvégzése a felső vezetőség feladatkörébe tartoznak, ezért nem kerülnek ismertetésre:

- információbiztonsági célkitűzések meghatározása;
- információbiztonsági politika (irányelvek) meghatározása.

Fontos megjegyezni, hogy jelen szakdolgozat a vállalati titoktartási kötelezettségek okán az implementációs fázisok során létrejött dokumentációk vázát, illetve fejléceit ismerteti.



3.9.4-1. ábra: Az ISMS létrehozásának fő lépései

4.1 Strukturált megvalósítási terv a PDCA modell szerint

A szeparált információbiztonsági zóna létrehozása során a PDCA modell fázisait követtem. Az alábbi alfejezetekben ismertetem, hogy a ciklus egyes lépcsőihez mely zónabeli folyamatok tartoznak.

4.1.1 Tervezés

Ez a fázis rendkívül fontos, hiszen a célkitűzések és megvalósításukra irányuló terv itt kerül meghatározásra. Fontos megjegyezni, hogy a PDCA ciklus első lefutásának (amely során létrehozásra kerül az ISMS) tervezési lépése speciális abból a szempontból, hogy néhány megvalósítás jellegű tevékenység is szerepelhet benne.

Ebbe a lépcsőfokba az alábbi folyamatok tartoznak [16]:

1. Irányítási keretrendszer létrehozása, beleértve az implementációs projekt létrehozását, a szervezet belső és külső környezetének meghatározását és az érdekelt felek követelményeinek azonosítását és felmérését.
2. ISMS hatókörének meghatározása az irányítási keretrendszer létrehozásának folyamatai szerint.
3. Folyamatos fejlesztés módszertanának és a dokumentáció stratégiájának megválasztása.
4. A felső vezetés támogatásának és elkötelezettségének megszerzése, az információbiztonsági irányelvek kidolgozása, illetve felelősségi körök meghatározása és az ennek megfelelő szerepek kiosztása.
5. Az információbiztonsági kockázatértékelés szisztematikus módszertanának, valamint az azonosított kockázatok elfogadhatósági kritériumainak meghatározása.
6. Kockázatértékelés elvégzése annak érdekében, hogy a információbiztonsági irányelvek és az ISMS alkalmazási körén belül meghatározásra kerülhessenek a szervezet kritikus információs eszközei, valamint az ezeket fenyegető veszélyek.
7. A feltárt kockázatok kezelési alternatíváinak azonosítása és értékelése, szükség esetén az alkalmazandó ellenőrzési célok és intézkedések meghatározása.

8. Alkalmazhatósági nyilatkozat (Statement of Applicability, SoA) és a kockázatkezelési terv létrehozása.

4.1.2 Megvalósítás

A megvalósítás fázisba azok a tevékenységek tartoznak, amelyek az előző lépésben meghatározott terveket hajtják végre a célkitűzések elérése érdekében. Ebbe a lépcsőfokba az alábbi folyamatok tartoznak [16]:

1. Kockázatkezelési stratégia és a kapcsolódó dokumentáció véglegesítése, beleértve az összes tervezett folyamatot és a vonatkozó alátámasztó dokumentumokat.
2. Kockázatkezelési terv és a kiválasztott ellenőrzések végrehajtása.
3. Megfelelő képzés szervezése az érintett személyek számára, annak érdekében, hogy elsajátítsák az információbiztonság-kritikus gondolkodásmódot.
4. A tevékenységek és az erőforrások kezelése az ISMS-sel összhangban.
5. Olyan folyamatok végrehajtása, amelyek biztosítják az információbiztonsági incidensek detektálását, valamint az azokra való gyors reagálást.

4.1.3 Ellenőrzés és cselekvés

Az ellenőrzés szakaszában a folyamatos fejlesztés elősegítésének eszközeként a teljesítményértékelés áll a középpontban, beleértve a nyomon követést, a felülvizsgálatot, a tesztelést és az ellenőrzést. Ezeknek a folyamatoknak az ISMS teljes hatókörére ki kell terjedniük, az eredményüket pedig alaposan dokumentálni kell annak érdekében, hogy a rendszer tanúsítható legyen az ISO/IEC 27001 szerint. [16]

A cselekvés fázis során a felső vezetőség a változó kockázati környezet fényében átvizsgálja az ellenőrzés lépés során keletkezett eredményeket, majd meghatározza a lehetséges javításokat és teljesítménynövelési lehetőségeket, amelyeket végre kell hajtani. [16]

4.2 Hatókör meghatározása

Az ISMS implementálásának első és egyben egyik legfontosabb lépése a hatókör meghatározása. A hatókör definiálja azt, hogy mi tartozik a rendszer ellenőrzése alá, beleértve többek között a szervezeti egységeket, helyszíneket, folyamatokat, illetve az érdekelt feleket és elvárásaikat. A hatókört a lehető legátfogóbb és legpontosabb módon kell dokumentálni, hiszen az üzleti partnerek ez alapján szerezhetnek bizonyosságot arról, hogy az ISMS lefedi-e a számukra releváns folyamatokat és erőforrásokat. Ahhoz, hogy a hatókört leíró dokumentum teljeskörű legyen, az ISO/IEC 27001:2013 implementációs segédlete a helyzetelemzés és a követelményelemzés végrehajtását javasolja. [21]

4.2.1 Helyzetelemzés

A helyzetelemzés célja az ISMS kontextusba helyezése a tágabb környezetében, annak hatókörének megfelelően. Az elemzésbe az ISMS szempontjából releváns szervezeti és technológiai összefüggéseken túlmenően az iparági, illetve helyspecifikus körülményeket is be kell vonni. Ezen felül vizsgálni kell a szervezet belső környezetét, beleértve a vállalat egyéb irányítási rendszereit és az ISMS vonatkozásában fontos vállalati részlegeket és érdekelt feleket. [21] Amennyiben a vállalat már rendelkezik egyéb irányítási rendszerrel, akkor az ISMS-t úgy kell integrálni a vállalati környezetbe, hogy az a másik rendszer kiterjesztése legyen az információbiztonsági irányításra. [16] Az analízis során a külső kontextust is vizsgálni kell, beleértve a szervezet fontos üzleti partnereit, beszállítóit és szolgáltatóit. [21]

4.2.2 Követelményelemzés

A követelményelemzés célja, hogy vizsgálja a külső és belső környezet analízise során dokumentált érdekelt felek igényeit és követelményeit. A külső érdekelt felek tekintetében rögzíteni kell a szervezet szempontjából releváns jogi és hatósági rendelkezéseket és egyéb szerződéses kötelezettségeket. A belső érdekelt felek esetén pedig fel kell mérni azoknak a személyeknek az elvárásait, akik az ISMS folyamatai felett döntéshozatali képességgel rendelkeznek. [21]

4.2.3 Megvalósítás

A megvalósítási folyamatot az ISMS külső és belső környezetéhez kötődő érdekelt felek azonosításával kezdtem. Megvizsgáltam, hogy a vállalat kiberbiztonsági

osztályán felül, mely vállalati egységek és személyek érdekeltek a szeparált zónában. Mindemellett felméretem, hogy milyen stratégiai és üzleti partnerek, beszállítók és szolgáltatók kötődnek az irányítási rendszerhez. A teljeskörű és pontos eredmények érdekében az ISO 31000:2009 szabványt használtam, amely részletesen ismerteti a külső és belső környezet definícióját és a lehetséges komponenseit.

A belső környezethez tartozó érdekelt felek közé sorolható:

- a vállalat kiberbiztonsági osztályának vezetője, illetve egyeneságú felettesei;
- minden vállalati munkatárs, aki részt vesz az ECU-k kutatási és fejlesztési folyamataiban, különös tekintettel a biztonsági tesztelésért, kód aláírásért és kriptográfiai kulcskezelésért felelős személyekre;
- minden olyan vállalati munkatárs, aki részt vesz az irányítási rendszer által keretbe foglalt fizikai infrastruktúra létrehozásban, kezelésében, karbantartásában és fejlesztésében;
- információbiztonsági tervezési csoport tagjai.

A külső környezethez tartozó érdekelt felek közé sorolható:

- azok az autóipari vállalatok, akik a zóna szolgáltatásait igénybe veszik;
- azok a szolgáltatók és beszállítók, akik részt vesznek a fizikai infrastruktúra kialakításában és karbantartásában.

Ezt követően felmértem, hogy az érdekelt feleknek milyen elvárásaik vannak az ISMS-el szemben. Utánajártam annak, hogy a vállat milyen tanúsítványokkal rendelkezik, különös tekintettel az információbiztonsággal és az irányítási rendszerekkel kapcsolatos sztenderdekre. Továbbá megvizsgáltam azt, hogy milyen vállalati szintű jogi és hatósági rendelkezések relevánsak az ISMS szempontjából. Mindemellett információkat gyűjtöttem a vállalati felépítésről, valamint a szeparált zóna fizikai infrastruktúrájának helyet adó helységekről.

4.2.4 Dokumentáció

Az előző fejezetben ismertetett folyamatok segítségével már pontosan meg lehet határozni az információbiztonsági irányítási rendszer hatókörét. Az ISO/IEC 27001:2013 előírja, hogy az ISMS hatókörét a lehető legátfogóbb és legpontosabb módon

dokumentálni kell, akár önálló okmányként, akár az információbiztonsági irányelvekről szóló irat részeként.

Az általam létrehozott dokumentáció az alábbi pontokra tér ki:

- a dokumentum célja;
- a vállalat általános ismertetése, beleértve az iparágazati elhelyezkedését, és az információbiztonsági célkitűzéseit;
- külső és belső környezet ismertetése, beleértve a szervezeti felépítést, a külső és belső érdekelt feleket és követelményeiket, és a releváns jogi és hatósági rendelkezéseket, valamint vállalat tanúsítványait és egyéb implementált irányítási rendszereit;
- ISMS hatókörének meghatározása, beleértve a fizikai helyszíneket is.

4.3 Felső vezetőség támogatásának megszerzése

Ennek az implementációs lépésnek a célkitűzése az, hogy elnyerje a felső vezetőség elkötelezettségét és támogatását az információbiztonsági irányítási rendszerrel kapcsolatban. Ez kulcsfontosságú, hiszen a vezetői elkötelezettség bizonyítása elengedhetetlen az ISO/IEC 27001:2013 szerinti tanúsítás során.

Ehhez a lépéshez is tartozik dokumentációs követelmény, amely során az igazgatóságnak egy nyilatkozat kell készítenie arról, hogy teljes mértékben támogatja a rendszer kialakítását és felelősséget vállal a folyamatok gyakori felülvizsgálatáért és az eredmények dokumentálásáért. [21]

4.3.1 A felső vezetőség meghatározása

Az ISMS terminológiájában a felső vezetés nem minden esetben egyezik meg a teljes vállalat irányításáért felelős személyekkel. [21] Amennyiben a hatókör nem terjed ki a vállalat egészére, akkor azokat az illetőket jelöli, akik a szervezet ezen részének irányításért és ellenőrzéséért felelősek. Az ISMS-ért illetékes vezetők feladata az, hogy irányítsák a rendszer belső folyamatait, illetve döntéseket hozzanak a hatókörbe tartozó erőforrások szervezésével, kezelésével, irányításával, felügyeletével és ellenőrzésével kapcsolatban. [12]

4.3.2 A felső vezetőség feladatköre

A ISMS-ért felelős vezetőségnek elkötelezettséget kell tanúsítaniuk a kitűzött információbiztonsági célok elérése érdekében. Ez magába foglalja [21]:

- a szükséges erőforrások biztosítását;
- a nem megfelelőségi esetek konzekvens kezelését;
- a folyamatos fejlesztés iránti ambíciót.

A vezetőség tagjainak számos fontos feladata van, többek között [21]:

- felelősség vállalása az érzékeny információk védelméért;
- információbiztonsági célkitűzések és az ezek elérésére irányuló terv kidolgozása;
- kritériumrendszer és a döntéshozatali alapelvek meghatározása a kockázatok kezelésének és értékelésének vonatkozásában;
- információbiztonsági elvárások beillesztése a vállalati folyamatokba és modellekbe;
- repetitív felülvizsgálatok végrehajtása a folyamatos fejlesztés érdekében.
- információbiztonsági stratégia és célkitűzések meghatározása, beleértve az ezekhez szükséges erőforrások biztosítását;
- információbiztonsági politika felülvizsgálata;
- szerepkörökhöz kötődő felelősségek felülvizsgálata, beleértve a vezetői szerepek kiosztását;
- folyamatok meghatározása a hatékony incidenskezelésre;
- főbb fenyegetések nyomon követése és hatásuk becslése az információs eszközökre.

4.4 Információs eszközök leltárának elkészítése

Az ISMS hatókörébe tartozó információs eszközök leltárának létrehozása (inventory of assets) elengedhetetlen előkövetelménye a kockázatkezelési folyamatok végrehajtásának. Az ISO/IEC 27001:2013 az ajánlott kockázatmódosító tevékenységek

ismertetése során tárgyalja az információs eszközökre vonatkozó követelményeket, beleértve a titkosságra, felelősségvállalásra és a fizikai adattároló hardverekre vonatkozó elvárásokat. [14] A leltár célja az, hogy biztosítsa az eszközök hatékony kezelését és nyilvántartását, mindemellett a kockázatkezelés alapjaként szolgáljon.

4.4.1 A leltár lehetséges elemei

Mindenekelőtt fontos meghatározni azt, hogy milyen típusú információs eszközök képezhetik az ISMS részét. Fontos, hogy minden hatókörbe tartozó eszköztípus azonosításra kerüljön, annak érdekében, hogy a majdani kockázatokfelmérés és hozzáférés-engedélyezés pontos eredményekre vezessen.

Releváns információs eszköznek tekinthető minden olyan hatókörbe tartozó elem, amely bármilyen szerepet vállal egy adott információ életciklusa során. A lehetséges eszköztípusok közé sorolhatóak az információk (bármilyen formátumú adatok), a szoftverek, a tárgyi eszközök, a szolgáltatások, az emberek, illetve az immateriális javak. [31]

4.4.2 Követelmények a leltárral szemben

Az ISO/IEC 27001:2013 előírja, hogy minden egyes információs eszközhöz tulajdonost kell párosítani. Az ISMS terminológiájában az információs eszköztulajdonos nem az a személy, aki birtokolja az adott elemet, hanem az, aki a legtöbbet használja vagy a legtöbb ellenőrzést gyakorolja felette annak teljes életciklusa során. Az eszközök sokrétűsége okán a szabvány nem várja el, hogy minden egyes eszközhöz konkrét személy legyen hozzárendelve, sok esetben a munkaköri pozíció vagy a vállalati osztály feltüntetése sokkal célravezetőbb. [31]

A tulajdonos megnevezésén felül elengedhetetlen az eszköz helyének, biztonsági besorolásának és a hozzáféréséhez kapcsolódó korlátozásainak dokumentálása. A birtokló feladata és felelőssége, hogy ezt a három tulajdonságot kezelje, fenntartsa, illetve rendszeresen felülvizsgálja. Az ISO/IEC 27001:2013 továbbá előírja, hogy az információs eszközökhöz olyan attribútumokat kell rendelni, amelyek szerint megfelelően osztályozhatók a kielégítő védelmi szint biztosítása érdekében. [31]

4.4.3 Megvalósítás és dokumentáció

A megvalósítási folyamatot az ISMS hatókörébe tartozó információs eszközök felderítésével kezdtem. A hatékony és teljeskörű vizsgálat érdekében felhasználtam a vállalati osztály már meglévő nyilvántartásait, beleértve a hardverekről, szoftverekről, licencekről és hálózati eszközökről vezettet listákat. Ezt követően meghatároztam azt, hogy mely eszközök számítanak információs eszköznek és ezek közül melyek tartoznak az ISMS hatókörébe. A szűrés eredményét felhasználva kialakítottam az információs eszközkategóriákat, amelyeket az adatbázis strukturált kialakítása során hasznosítottam. A kategóriák ismeretében felmértem, hogy az egyes csoportokhoz milyen attribútum-típusok kötődnek. Az általános kategória-specifikus jellemzőket az ISO/IEC 27002:2013 szabvány segítségével egészítettem ki annak érdekében, hogy az adatbázis a védelem megszervezése szempontjából releváns tulajdonságokat is tároljon az egyes csoportokra nézve.

A szeparált zóna alkalmazási körébe tartozó információs eszközöket az emberek, szoftverek, szerverek, analóg információk, digitális információk, laptopok, adattároló hardverek, hálózati eszközök és a szolgáltatások kategóriák szerint csoportosítottam. Az egyes csoportokhoz tartozó attribútum-típusokat tartalmazó fejléceket a 8.1-1. táblázatban ismertetem.

4.5 Kockázatkezelési folyamat

A kockázatkezelés az ISMS középpontjában álló folyamat, melynek célja, hogy elősegítse az információbiztonsággal kapcsolatos kockázatok valószínűségeinek és következményeinek szisztematikus azonosítását (risk identification), elemzését (risk analysis), kiértékelését (risk evaluation) és értékelését (risk treatment) az ISMS hatókörében lévő információs eszközök számára. A kockázatkezelés hosszú távú célja az, hogy biztosítsa a vállalat felső vezetése által meghatározott biztonsági szintet az irányítási rendszer alkalmazási körén belül annak érdekében, hogy az üzleti célok, az üzletmenet folytonossága, illetve a jogi és szabályozási követelmények teljesülhessenek. [21]

Az ISO/IEC 27k szabványcsalád az ISMS hatókőrébe tartozó információs eszközökre vonatkozó kockázatkezelésre helyezi a hangsúlyt. Az ISO/IEC 27001:2013 szabvány követelményrendszerében nem szerepel egzakt kockázatkezelési módszertan, ezért a vállalat maga dönthet az alkalmazott eljárásról. Fontos azonban, hogy a választott

módszertannak tükröznie kell a vállalat kockázatvállalási hajlandóságát, illetve következetes és megismételhető eredményeket kell biztosítania, annak érdekében, hogy a teljesítmény mérhető legyen a későbbi eredményekkel való összehasonlítás által. [32] A két leggyakrabban alkalmazott megközelítés az eszközalapú és a forgatókönyv-alapú kockázatkezelés. [20] A kockázatkezelési stratégia kidolgozása és végrehajtása során az eszközalapú kockázatkezelést alkalmaztam, mivel ez a módszer szerepel az ISO/IEC 27005:2018 útmutatásaiban.

4.5.1 Kvantitatív és kvalitatív hatásvizsgálatok

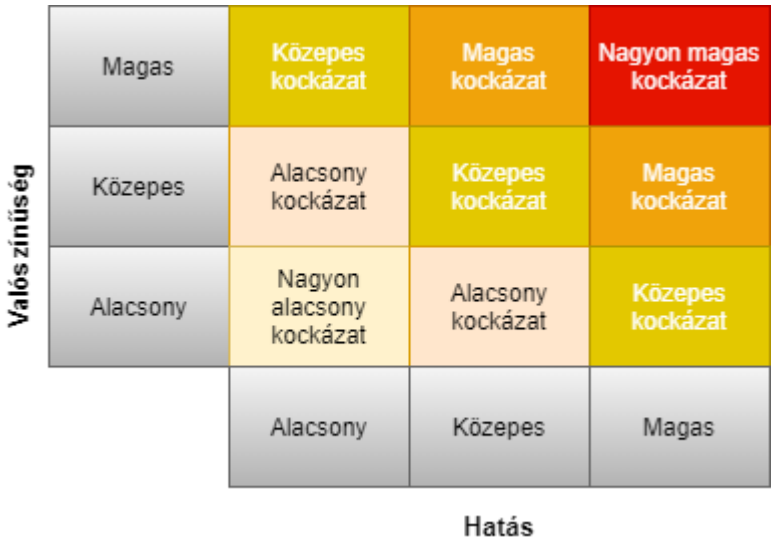
A kockázati hatás mennyiségi (kvantitatív) és minőségi (kvalitatív) jellegének értékelése egyaránt fontos szerepet játszik a kockázatkezelési folyamat kockázat kiértékeléssel és kockázatelemzéssel foglalkozó szakaszaiban. A két eljárás között a legfőbb különbség az, hogy a kvalitatív módszertannal ellentétben a kvantitatív megközelítés elsősorban matematikai adatokra támaszkodik, mint elsődleges bemenetforrás. [33]

A minőségi hatásvizsgálat elvégzésének legnagyobb előnye, hogy lehetővé teszi a kockázatok rangsorolását és azon területek azonosítását, amelyeken a sérülékenységek kezelése érdekében azonnali beavatkozásra van szükség. Mivel a kvalitatív hatásvizsgálat nem ad kézzelfogható, mérhető becsléseket a kockázati hatások nagyságrendjére vonatkozóan, így nehéz meghatározni a bevezetett ellenőrzések hatékonyságát a költség és haszon arányának fényében. Ez a módszertan különösen hasznos az immateriális információkhoz kapcsolódó kockázat kiértékelés során, hiszen például a hírnévvesztés vagy közbizalomvesztés nehezen számszerűsíthetőek. [33]

A mennyiségi hatásvizsgálat két adatcsoportot vesz figyelembe, egyrészt az esemény bekövetkezésének valószínűségét, másrészt az esemény bekövetkezése esetén várható kár számadatát. A kvantitatív megközelítés elsődleges előnye, hogy a kockázatok hatásában bekövetkező változásokat sokkal egyszerűbb nyomon követhetőek, ezáltal a bevezetett ellenőrzések eredményei könnyeben mérhetőek. Másrészt a módszertan hátránya, hogy sok esetben a bemeneti adatokat szubjektív döntések és számítások eredményezik, ezáltal egyes kockázatok felül-, illetve alulértékelté válhatnak. [33]

A kvalitatív módszertan a legelterjedtebb eljárás a kockázatok elemzésére és értékelésére. A szubjektív számadatok megjelenését kockázati skálák bevezetésével küszöbölik ki, de ennek ellenére elkerülhetetlen, hogy a minőségi hatásvizsgálat

tartalmazzon némi szubjektivitást. [33] A 4.5.1-1. ábra egy kockázatelemzés során gyakran alkalmazott mátrixot szemléltet, amely egy háromszintű kockázati skálát alkalmaz a valószínűség és a hatás mérésére.



4.5.1-1. ábra: Kockázatelemzési mátrix [33] (szerk. a szerző)

A kockázati szintet az alábbi egyenlet segítségével lehet meghatározni [33]:

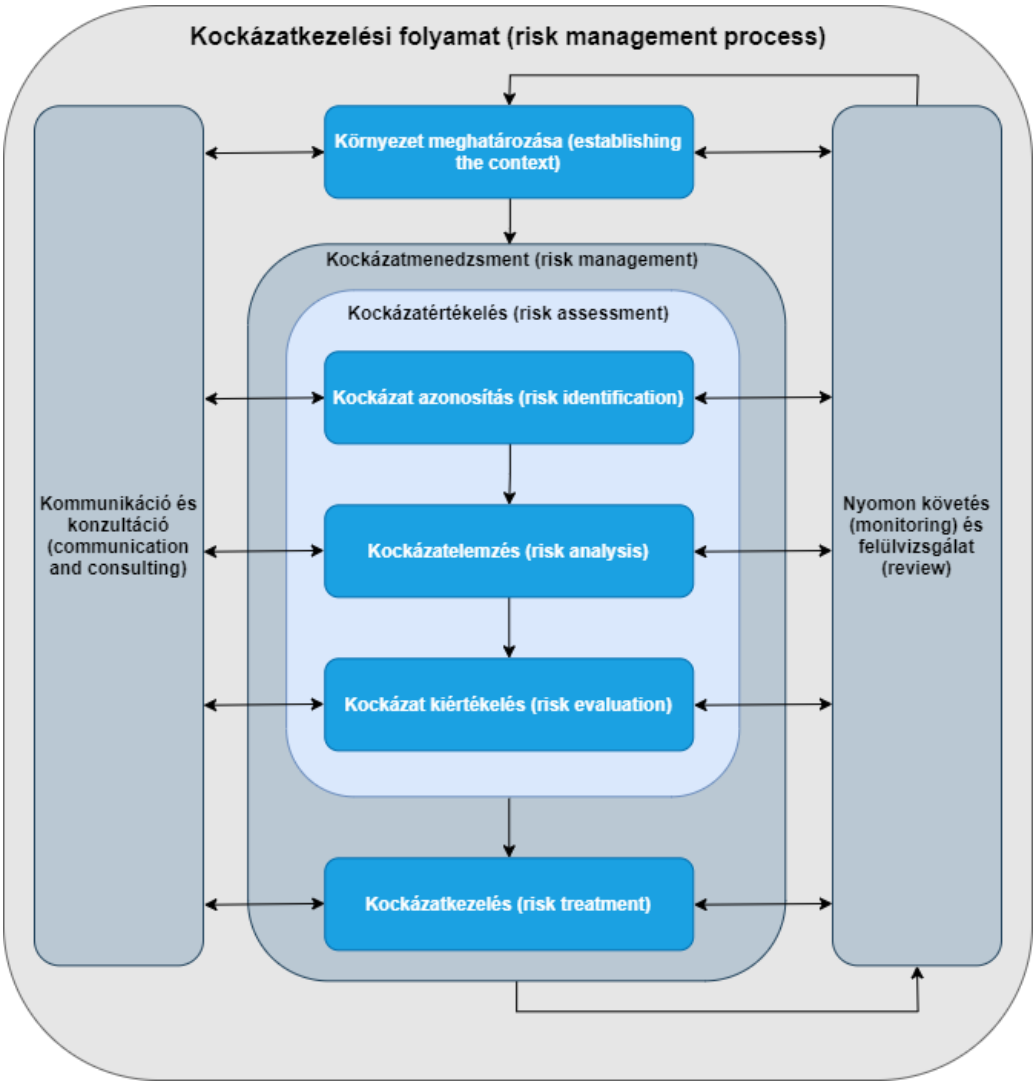
$$Kockázat = valószínűség * hatás$$

4.5.2 Az eszközalapú kockázatkezelés komponensei és lépései

Az eszközalapú kockázatkezelési módszertan lényege, hogy a kockázatok azonosítása és elemzése során figyelembe veszi az egyes információs eszközökhöz kapcsolódó fenyegetettségi modelleket és a hozzájuk kötődő sérülékenységeket. [33] Az eszközalapú módszertan szerint a kockázatok hatását értékelő egyenlet az alábbiak szerint egészül ki [33]:

$$Kockázat = (sérülékenység\ kihasználásának\ valószínűsége) * (sérülékenység\ kihasználásának\ teljes\ hatásköltsége)$$

Az eszközalapú kockázatkezelési folyamat egy rendkívül összetett és bonyolult eljárás, ezért az egyes lépéseit és komponenseit a 4.5.2-1. ábra segítségével ismertetem.



4.5.2-1. ábra: A kockázatkezelési folyamat komponensei és lépései [21] (szerk. a szerző)

A környezet meghatározása

A kockázatok és azok forrásainak teljeskörű azonosítása érdekében rendkívül fontos az ISMS környezetének átfogó elemzése és hatókörének pontos meghatározása. Jelen szakdolgozat 4.2. fejezetében részletesen tárgyaltam a szeparált információbiztonsági zóna hatókörének meghatározását, beleértve a helyzet- és követelményelemzéseket, amelyek a környezet felmérésének alapját képezik. A meghatározott alkalmazási kör fényében a 4.4. fejezetben felderítettem és nyilvántartásba vettem az információs eszközöket, amelyek a eszközalapú kockázatmenedzsment bemenetét képezik.

Kockázat azonosítás

Az ISMS hatókörébe tartozó információs eszközökhöz kötődő kockázatok azonosításához elengedhetetlen a velük kapcsolatos fenyegetések és sérülékenységek

ismerete. Az eszközalapú módszertant követve az első lépés a fenyegető veszélyek azonosítása, a második pedig a sebezhetőségek vizsgálata. Egy adott kockázat létezése a fenyegető veszély és a hozzá kapcsolódó sérülékenység együttes meglétéből származik, ezért fontos, hogy az elemzés során ezen összefüggést követve végezzük a vizsgálatot. [34]

Egy adott információs eszközzel szembeni fenyegetések érkezhetnek a vállalaton belülről, illetve kívülről egyaránt, továbbá egy adott fenyegetéshez akár több sérülékenyég is párosulhat. Az átfogó vizsgálati eredmények érdekében szisztematikus megközelítést kell alkalmazni, amely során a titkosság, a sértetlenség és rendelkezésre állás kategóriák mentén kell azonosítani egy adott információst eszközhöz kötődő kockázatokat. [34]

Kockázatelemzés

A kockázatelemzés célja az előző fázisban azonosított kockázatok valószínűségének és lehetséges hatásainak vizsgálata. [21] Az elemzés során a kvantitatív vagy a kvalitatív módszertanok segítségével meghatározásra kerülnek az egyes információs eszközökre vonatkozó kockázati szintek a bekövetkezési valószínűségük és várható hatásuk fényében.

Kockázat kiértékelés

A kockázat kiértékelés két bemenettel rendelkezik, az előző fázisban meghatározott kockázati szintekkel az egyes információs eszközökre nézve, illetve a vállalat kockázatvállalási hajlandóságának fényében meghatározott kockázatelfogadási kritériumokkal. A folyamat célja, hogy a két érték összehasonlításával megállapítható legyen az, hogy egy adott kockázat esetén szükséges-e bármilyen intézkedés bevezetése a kockázatkezelés során.

Kockázatkezelés

A kockázatkezelés célja a kockázatértékelés folyamatlánc során azonosított, elemzett és értékelt kockázatok megszüntetése vagy negatív hatásuk mérséklése. Az ISO/IEC 27001:2013 szabvány elvárja, hogy minden egyes ISMS-beli tevékenységet jól átlátható módon és precíz dokumentáció mellett kell végrehajtani, ezért ebben a fázisban egy kockázatkezelési terv létrehozása szükséges, amelyben minden egyes feltárt kockázat esetén a vállalatnak döntenie kell arról, hogy az adott kockázatot [35]:

- megszünteti azáltal, hogy nem folytatja az előidéző tevékenységet vagy folyamatot;
- megtartja, folyamatos felülvizsgálat és ellenőrzés mellett;
- mértékét az elfogadható szintre csökkenti ellenőrzések alkalmazásával;
- megosztja egy másik féllel megbízás révén.

Kulcsfontosságú, hogy a szervezet egy adott kockázat kezelése során mérlegelje azt, hogy megéri-e ellenőrzést alkalmazni a kockázat mérséklése vagy megszüntetése céljából, hiszen előfordulat, hogy egy adott ellenőrzés bevezetési és fenntartási költsége magasabb, mint a kockázatból származó várható anyagi veszteség [36].

Az ellenőrzések három nagy csoportra (típusra) bonthatóak, jellegük és célkitűzéseik szerint [36]:

1. Megelőző (preventive): célja a sérülékenység védelme, illetve a támadás meghiúsítása vagy hatásának mérséklése.
2. Detektív (detective): feladata a támadás felismerése, majd a megelőző vagy a reaktív intézkedés aktiválása.
3. Reaktív (reactive): célja a támadás hatásának mérséklése és a támadás utáni helyreállítási folyamatok elősegítése.

Az ellenőrzés típusok pedig tovább kategorizálhatóak az alábbi négy csoport szerint [36]:

1. Műszaki: azok az ellenőrzések, amelyek hálózati rendszerkonfigurációkat és szoftveres beállításokat és csomagokat érintenek.
2. Szervezeti: a szervezet felső vezetése által bevezetett ellenőrzések, amelyek elsősorban az általuk bevezetett információbiztonsági szakpolitikákból és eljárásrendekből származnak.
3. Fizikai: olyan ellenőrzések, amelyek a fizikai biztonságot kívánják biztosítani.
4. Emberi: a szervezet munkavállalóival kapcsolatos ellenőrzések.

4.5.3 Kockázatkezelési terv az ISO/IEC 27001:2013 szerint

A kockázatkezelési folyamat az ISO/IEC 27001:2013 követelményrendszerét alapul véve az alábbi lépésekből áll [32]:

1. az információbiztonságot fenyegető veszélyek és sérülékenyégek (kockázatok) azonosítása;
2. az ISMS hatókörébe tartozó információs eszközök bizalmasságát, sértetlenségét és rendelkezésre állását veszélytető kockázatok felderítése;
3. az azonosított kockázatok tulajdonoshoz rendelése;
4. annak vizsgálata, hogy a bizalmasság, a sértetlenség és a rendelkezésre állás megsértése milyen negatív hatásokat válthat ki;
5. annak meghatározása, hogy az egyes kockázatok milyen valószínűséggel valósulhatnak meg;
6. kockázati szintek kiszámítása;
7. a kockázatok értékelése a kockázatelfogadási kritériumok és a kiszámított kockázati szintek összehasonlításával;
8. kezelendő kockázatok azonosítása és rangsorolása.

A tervezet az eszközalapú megközelítést alkalmazza, hiszen az egyes információs eszközökből kiindulva vizsgálja a CIA modellt befolyásoló kockázatokat. A kockázati szintek kiszámítását a minőségi hatáselemzés segítségével végzi, amely során felméri a kockázatok potenciális bekövetkezésének a szervezetre gyakorolt hatását a CIA modell, illetve a szerződéses és jogi kötelezettségek fényében, majd kiszámítja a kockázat bekövetkezésének reális valószínűségértékét. A két számérték szorzata együttesen eredményezi a kockázati szintet, amelyet a kockázatelfogadási szinttel összehasonlítva megállapítható, hogy milyen intézkedésre van szükség. [32]

4.5.4 A szeparált zóna kockázatkezelésének megvalósítása

A szeparált információbiztonsági zóna kockázatkezelése során az eszközalapú megközelítést alkalmaztam. A folyamat bemeneteként a 4.4. fejezetben tárgyalt információs eszköz nyilvántartást (leltárt) használtam, amely osztályozva tartalmazza az ISMS hatókörébe tartozó információs eszközöket. Fontos megemlíteni, hogy jelen szakdolgozat az információs eszközök CIA modell szerinti értékelését mutatja be, amely

nem elegendő a szabványnak való megfeleléshez. Az értékelés során olyan egyéb szempontokat is figyelembe kell venni, mint például a szerződéses és jogi követelmények.

Első lépés

A kockázatkezelés első lépéseként megvizsgáltam, hogy a leltár által tartalmazott információs eszközök milyen fenyegetettségi vektorokkal és sérülékenyégekkel rendelkeznek. Ebben nagy segítségemre volt az ISO/IEC 27005:2018 szabvány függeléke, amelyben felsorolásszerűen ismertetik a létező fenyegetéseket és sérülékenységeket. Ezt követően az azonosított kockázatokat kockázattulajdonosokhoz rendeltem, a leltárban megjelölt információs eszköztulajdonosok és a releváns munkakörök szerint.

Második lépés

A második fázisban elvégeztem az információs eszközök értékelését a hozzájuk rendelt bizalmassági, sértetlenségi és rendelkezésre állási követelményeknek megfelelően. Ahogy a 8.1-1. táblázatban látható, minden egyes információs eszközkategória attribútum-típusai között szerepel a CIA modell. A bizalmassági, sértetlenségi és rendelkezésre állási követelményt egy ötszintű skála szerint határoztam meg, amely a nagyon alacsony, alacsony, közepes, magas és nagyon magas elemekkel rendelkezik. A skála értékeihez számadatokat is társítottam, rendre a nullát, az egyet, a kettőt, a hármat és a négyet. Egy adott információs eszköz értékét az alábbi képlet szerint számítottam ki:

$$\acute{E}rt\acute{e}k = \frac{C + I + A}{3}, ahol\ C, I, A\ \in (0, 4)$$

A képlet eredménye tehát egy olyan számérték, amely reprezentálja az adott információs eszköz értékét a CIA modell fényében. Egyes speciális eszközök esetén eltérő súlyozást alkalmaztam, illetve amennyiben a kapott érték nem egész szám volt, a kerekítés szabályai szerint jártam el.

Harmadik lépés

A harmadik fázisban az első lépés során azonosított fenyegetések és sérülékenységek, illetve a második lépésben kiszámolt információs eszközértékek segítségével meghatároztam a kockázati szinteket. Ehhez 4.5.4-1. ábra által prezentált

kockázatkezelési mátrixot alkalmaztam, amely az információs eszközök értékének figyelembevételével határozza meg a kockázati szintet.

	A fenyegetés előfordulásának valószínűsége	Alacsony			Közepes			Magas		
	A kihasználhatóság nehézségenek szintje	Alacsony	Közepes	Magas	Alacsony	Közepes	Magas	Alacsony	Közepes	Magas
Információs eszköz értéke	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

4.5.4-1. ábra: Kockázati szint meghatározására szolgáló mátrix [19] (szerk. a szerző)

A módszertan lényege, hogy a kockázati szint meghatározása során három faktort vesz figyelembe [19]:

1. a fenyegetés előfordulásának valószínűségét;
2. a fenyegetéshez kapcsolódó sérülékenység kihasználásának nehézségi szintjét;
3. az információs eszköz értékét.

Az első és a második vizsgált tényezőt egy háromszintű skála szerint határozza meg, melynek elemei az alacsony, a közepes, illetve a magas szintek. Az információs eszközök értékének szintjeit pedig a korábban ismertetett ötszintű skála segítségével ábrázolja. A mátrix eredményként egy nullától nyolcig terjedő számértéket közöl, amelyet az alábbi megfeleltetés szerint kell értelmezni [19]:

- Alacsony kockázat: 0-tól 2-ig;
- Közepes kockázat: 3-tól 5-ig;
- Magas kockázat: 6-tól 8-ig.

Negyedik lépés

A negyedik és egyben utolsó lépésben rangsoroltam a kockázatokat az első fázisban kiszámított kockázati szintek szerint, majd összehasonlítottam a kockázatvállalási kritériumokkal. Ennek megfelelően meghatároztam a megfelelő intézkedést, amelyeket a 4.5.2 fejezet kockázatkezelésről szóló bekezdésében ismertettem.

4.5.5 Dokumentáció

Habár ISO/IEC 27001:2013 szabvány nem írja elő a kockázatkezelés eredményeinek dokumentálását, mégis ennek megtétele erősen javallott. Az ISMS folyamatos fejlesztése során a kockázatokat gyakori időközönként felül kell vizsgálni és ellenőrizni kell, hiszen a kockázatkezelési folyamat több tényezője is változhat, amely más kockázatkezelési intézkedést eredményezhet.

A kockázatkezelési eredményeket táblázatos formában dokumentáltam. A nyilvántartásban használt attribútum-típusokat a 8.2-1. táblázat szemlélteti. A kockázatleltár egy adott kockázathoz tárolja annak egyedi azonosítóját, megnevezését, a kockázattulajdonost, a kapcsolódó információs eszközt, a kockázati szintet, a kockázatból várható anyagi veszteséget, a bevezetett kezelési intézkedést, az ellenőrzés típusát és kategóriáját, a kezelési intézkedés költségét, az elvárt kockázati szintet, illetve a létrehozás dátumát.

Az ISO/IEC 27001:2013 azonban követelményként említi, hogy létre kell hozni az alkalmazhatósági nyilatkozat. A SoA-ban a vállalatnak nyilatkoznia kell arról, hogy mely ellenőrzéseket alkalmazza és utasítja el a szabvány függelékében szereplő listából. Fontos, hogy minden esetben alaposan és részletesen meg kell indokolnia a döntését. A sztenderd nem definiál egzakt követelményt a dokumentum formájával kapcsolatban, ezért a táblázatos megvalósítási módot választottam. A 8.2-2. táblázat segítségével szemléltetem az általam kidolgozott alkalmazhatósági nyilatkozatot.

4.6 Szerepek és felelősségi körök meghatározása

Az emberek az ISMS szerves részét képezik, ezért kiemelten fontos meghatározni, hogy milyen hozzájárulást és szerepvállalást várnak el tőlük a rendszer létrehozása, fenntartása és folyamatos fejlesztése során. Ebben a fejezetben részletesen ismertetésre kerülnek az ISMS információs eszközeinek kezelésével kapcsolatos szerepkörök és a hozzájuk kötődő felelősségi körök.

4.6.1 Az ISO/IEC 27001:2013 követelményei

Az ISO/IEC 27001:2013 szabvány az eszköz- és kockázattulajdonoson, illetve a felső vezetésen felül nem definiál egyéb, kötelezően meghatározandó szerepköröket az ISMS-re nézve. Azonban elvárja, hogy a rendszer létrehozásával, fenntartásával és

folyamatos fejlesztésével kapcsolatos szerepeket és felelősségi köröket meg kell határozni. A szabványhoz kapcsolódó implementációs segédlet kifejezetten javasolja a vezető információsbiztonsági tisztségviselő (Chief Information Security Officer, CISO) és/vagy az információbiztonsági tisztségviselő (Information Security Officer, ISO) szerepkörök alkalmazását. A vállalat felelőssége, hogy megbizonyosodjon arról, hogy a folyamatba részt vevő valamennyi személy megkapta-e a megfelelő képzést és oktatást, amely a pozíció betöltéséhez szükséges tudással ruházza fel őket. Mindemellett ajánlja, hogy az esetleges összeférhetetlenségek, valamint a felelősségi körök egyértelmű megszervezésének és meghatározásának garantálására a RACI (Responsible, Accountable, Consulted, Informed) diagram optimális megoldást jelenthet. Továbbá a feladatkörök meghatározása és szerepekhez rendelése során követni kell a feladatok egyértelmű elkülönítésének (Segregation of Duties, SoD) elvét. [21]

4.6.2 Információs eszközökkel kapcsolatos szerepkörök ismertetése

A szerepkörök meghatározása nagy mértékben függ a szervezet és az ISMS hatókörébe tartozó vállalati infrastruktúra és személyzet méretétől és számosságától. Mindemellett a szervezet felépítése, az információbiztonsággal foglalkozó személyek száma és a rendelkezésre álló erőforrások is befolyásolják a kiosztható szerepeket és felelősségeket, hiszen a biztonsági célok eléréséhez képzett személyek szükségesek. [37]

Felső vezetőség

A felső vezetőség támogatása kulcsfontosságú az ISMS szempontjából. Tagjainak elkötelezettsége nélkül a projekt kivitelezhetetlen lenne, hiszen ők biztosítják a kellő erőforrásokat a rendszer létrehozásához, karbantartásához és folyamatos fejlesztéséhez. A felső vezetés pontos meghatározását és feladatkörét korábban, a 4.3. fejezetben részletesen kifejtettem.

Vezető információbiztonsági tisztségviselő

A vezető információbiztonsági tisztségviselő felelős a szervezet információbiztonságával kapcsolatban felmerülő problémák és kérdések megválaszolásáért. Fő feladata, hogy iránymutatást adjon a felső vezetőség számára az információbiztonsági feladataik és az ISMS-ben betöltött szerepük megfelelő ellátásához. Mindemellett a felelősségi körébe tartozik többek között [37]:

- információbiztonsági folyamatok koordinálása és ellenőrzése;

- a felső vezetőség támogatása az információbiztonsági irányelvek kidolgozásakor;
- képzési és oktatási folyamatok megszervezése;
- információbiztonsági koncepciók és iránymutatások kidolgozása;
- ellenőrzések végrehajtásának kezdeményezése és nyomon követése;
- kritikus biztonsági incidensek kezelése.

A CISO részt vesz minden olyan projektben, amely jelentős hatást gyakorol az információfeldolgozás módjára, beleértve az új alkalmazások és informatikai rendszerek bevezetésének folyamatait. Jelenlétével biztosítja, hogy a projektfejlesztések különböző fázisai az információbiztonsági célkitűzések és irányelvek figyelembevételével valósuljanak meg. [37]

Adatvédelmi felelős (Data Protection Officer, DPO)

Az adatvédelmi felelős elsőszámú feladata, hogy felügyelje és ellenőrizze az ISMS hatókörébe tartozó folyamatokat adatvédelmi szempontok szerint. Figyelembe kell vennie minden olyan jogi és hatósági rendelkezést, amely adatvédelmi előírásokat határoz meg és releváns a vállalat szempontjából. Fontos, hogy az adatvédelmi felelős áthatóan ismerje a terület-specifikus adatvédelmi törvényeket, valamint a szervezet egyedi szabályait és előírásait. [37]

Információbiztonsági irányító csoport (Information Security Management Team)

A csoport célkitűzése, hogy koordinálja és felügyelje a védelmi intézkedéseket az információbiztonság vonatkozásában. Tagjai olyan személyek lehetnek, akik kellő információbiztonsági és IT-üzemeltetési tapasztalattal és kompetenciákkal rendelkeznek. A kollektíva tagjainak feladatai közé sorolható többek között [37]:

- információbiztonsági célok, eljárások és irányelvek kidolgozása;
- információbiztonsági procedúrák folyamatos felügyelése és ellenőrzése;
- képzési és oktatási programok megtervezése;
- információbiztonsági óvintézkedések nyomon követése és hatékonyságuk ellenőrzése.

Területi IT biztonsági felelős (Area IT Security Officer)

A területi IT biztonsági tisztviselő felelős azért, hogy az összes üzleti folyamat, alkalmazás és informatikai rendszer megfeleljen a legmagasabb szintű biztonsági és védelmi előírásoknak. A területi jelző arra utal, hogy a szerepet betöltő személy nem a teljes szervezetért felelős, hanem annak csak egy részéért. Fontos, hogy a tisztséget betöltő munkavállaló széleskörű IT-üzemeltetési rálátással rendelkezzen. A teljesség igénye nélkül a pozícióhoz az alábbi feladatkörök rendelhetők [37]:

- biztonsági irányelveknek megfelelő védelmi intézkedések kiválasztása és végrehajtása;
- IT-rendszerspecifikus információk összegyűjtése és kezelése;
- naplófájlok rendszeres időközönkénti ellenőrzése és értékelése.

Kockázattulajdonosok

A kockázattulajdonosok azok a személyek, akiket egy adott kockázat kezelésével bíznak meg, annak érdekében, hogy felelősséget vállaljanak érte és folyamatosan felülvizsgálják azt. Ez a kötelezettség azzal jár, hogy a kockázattulajdonosoknak aktívan részt kell venniük a kockázatkezelési folyamatokban, beleértve a kockázatkezelési terv jóváhagyását és a folyamat után fennmaradó kockázatok kezelését. [38]

Információseszköz-tulajdonosok

Ahogyan a 4.4.2. fejezet is említi, az ISO/IEC 27001:2013 szabvány elvárja, hogy minden információs eszközt tulajdonoshoz kell rendelni. Azonban fontos megjegyezni, hogy minden információs eszköz jogi tulajdonjogával a felső vezetés rendelkezik. Az információseszköz-tulajdonos feladatkörébe tartozik [39]:

- eszköznyilvántartás kezelése és naprakészségének biztosítása;
- az eszközök érzékenységi szintjének meghatározása a CIA modell szerint;
- ellenintézkedések és ellenőrzések bevezetése és folyamatos felügyelete a CIA modell teljesülése érdekében;
- hozzáférés-engedélyezés kezelése.

4.6.3 Üzletmenettel és vészhelyzetekkel kapcsolatos szerepkörök ismertetése

Az üzleti tevékenységek folyamatosságának fenntartása rendkívül fontos a vállalatok számára. A kockázatkezelés gyakorlata sok esetben csak a kockázatok súlyosságát képes mérsékelni, teljesen felszámolni nem tudja azokat. A fennmaradó kockázatok okozta incidensekre a szervezeteknek előrelátóan fel kell készülniük annak érdekében, hogy a kritikus üzleti folyamatok az incidensek hatására is kielégítően működhessenek. [40]

Mindemellett a különböző környezeti behatások és katasztrófák is befolyással lehetnek az üzleti folyamatokra és az IT infrastruktúra rendeltetésszerű működésére. A vállalatoknak ezen körülményekre is fel kell készülniük, beleértve a magas hibatűrő képességű és redundáns informatikai rendszerek implementálását és a megfelelő vészhelyzeti tervek kialakítását. [40]

Vészhelyzeti tervezési felelős (Contingency Planning Manager, CPM)

A vészhelyzeti tervezési felelős elsőszámú feladata, hogy átfogóan irányítsa, vezesse és ellenőrizze a vészhelyzeti tervezéshez kötődő procedúrákat. Emellett folyamatosan felügyelnie kell az ISMS tevékenységeire veszélyt jelentő fennmaradt kockázatokat, illetve ki kell dolgoznia az ezen veszélyek kezeléséhez szükséges ellenőrzési, irányítási és felügyeleti intézkedéseket. [40]

Üzletmenet-folytonossági felelős (Business Continuity Planning Manager, BCPM)

Az üzletmenet-folytonossági felelős fő feladata annak biztosítása, hogy a fontos üzleti folyamatok megfelelő rugalmassággal rendelkezzenek ahhoz, hogy az incidensek bekövetkezése ellenére is hatékonyan működjenek. [40]

IT katasztrófa utáni helyreállítási felelős (IT Disaster Recovery Planning Manager, IT DRPM)

Az IT DRPM elsőszámú feladata egy átfogó helyreállítási program kidolgozása, amely tartalmazza a helyreállítási terveket és folyamatokat. A szerepkör célja, hogy felkészítse a fizikai infrastruktúrát a katasztrófahelyzetekre és biztosítsa annak helyreállítását a lehető legrövidebb időn belül.

4.6.4 A RASCI mátrix bemutatása

A RASCI (Responsible, Accountable, Supportive, Consulted, Informed) egy mátrix, amelyet a projektben résztvevő valamennyi érdekelt fél szerepének és felelősségi körének meghatározására használnak. A mátrix a felelős, elszámoltatható, támogató, konzultált és informált összerendelési típusokat alkalmazza a szerepek felelősségi körökhöz párosítása során. A módszertan segítségével [41]:

- kiküszöbölhetőek az összeférhetetlenségek és az ütközések;
- a felelősségek elosztása megfelelően dokumentálható;
- a szervezeti hierarchia átláthatóan ábrázolható.

Az alábbiakban az ISMS terminológiájában ismertetem az egyes összerendelési típusok jelentését:

- felelős: az adott szerep a fő felelőse a tevékenyégek végrehajtásának;
- elszámoltatható: ha az adott tevékenység vagy ellenőrzés meghiúsul, akkor ez a szerepkör számon kérhető miatta;
- támogató: az adott szerepkör aktívan segíti az adott tevékenységek tervezését és/vagy végrehajtását és/vagy irányítását;
- konzultált: az adott szerepkör útmutatást és iránymutatást nyújt az adott tevékenységekben aktívan résztvevő szerepköröknek;
- informált: adott szerepkört informálni kell az adott tevékenységek állapotáról és eredményeiről.

4.6.5 Megvalósítás

Az ISO/IEC 27001:2013 implementációs segédlete ugyan a RACI mátrix használatát javasolja, azonban a megvalósítás kezdeti fázisban, kellő információsgyűjtést követően a RASCI változat mellett döntöttem. Ez a módszertan segít a kötelezettségek, felelősségek és feladatok szerepkörhöz rendelésében, amellett, hogy biztosítja az összeférhetetlenségek és ütközések elkerülését.

Elsőként az ISMS hatókörét figyelembe véve meghatároztam a szükséges szerepköröket. A döntés során figyelembe vettem az ISMS hatókörét, amely jelen esetben nem terjed ki a teljes vállalatra. A 4.6.2. és a 4.6.3. fejezetekben ismertetett szerepkörök

mindegyikét implementáltam, hiszen ezek elegendőek az ISO/IEC 27001:2013 szabványban ismertetett ellenőrzések lefedéséhez. Fontos megjegyezni, hogy az általam delegált szerepek nem feltétlenül lennének elegendőek a feladatokörök hatékony ellátásához, amennyiben az ISMS alkalmazási köre a teljes vállalatot magába foglalná.

A megvalósítás utolsó fázisában a RASCI mátrix segítségével elvégeztem a szerepek feladatkörhöz rendelését. A feladatkörök teljessége érdekében az ISO/IEC 27001:2013 függelékében szereplő listát alkalmaztam, amely tartalmazza azokat az ellenőrzéseket, amelyekkel szemben az adott szerepkör felelős, elszámoltatható, támogató, konzultált és informált viszonyt tarthat fennt. A létrejött dokumentáció struktúráját a 8.3-1. táblázat szemlélteti.

5 A fizikai infrastruktúra kialakítása

Ebben a fejezetben részletesen ismertetem a szeparált információbiztonsági zóna által keretbe foglalt fizikai infrastruktúrát, beleértve a hardveres és szoftveres komponenseket egyaránt. Magas absztrakciós szinten tárgyalom az egyes elemek általános jellemzőit és funkcióit és meghatározom a hálózatban betöltött szerepüket. Mindemellett – a vállalati üzleti titkok megsértése nélkül – ismertetem a konfiguráció során követett irányelveket.

5.1 Hardverek komponensek ismertetése

Ebben az alfejezetben a hálózati infrastruktúra kialakítására során alkalmazott hardverek kerülnek bemutatásra, beleértve a switch-et, a tűzfalat, a HSM-et és a szervert. A 3.9. fejezetben ismertetett általános jellemzőkön felül ismertetem azokat a tulajdonságokat és funkciókat, amelyek az adott hardverkategóriában speciálisnak számítanak, illetve relevánsak a szeparált zóna működésének és szolgáltatásainak szempontjából. Emellett részletezem, hogy az egyes fizikai eszközök milyen rendeltetésekkel bírnak a szeparált információbiztonsági zónában.

5.1.1 Felső kategóriás switch

Hardver-specifikus jellemzők

Az általunk használt switch egy felső kategóriás, nagy teljesítményű eszköz, amely beágyazott biztonsági funkciókkal is rendelkezik, többek között MAC-hitelesítéssel és hozzáférés-engedélyezéssel. Közel ötven bemeneti csatlakozója és négy gigabájt memóriája kiválóan alkalmassá teszi nagyvállalati környezetben való alkalmazásra. A zóna fizikai infrastruktúrájának kialakítása során két switch-et használtunk fel, amelyek kizárólag adatkapcsolati-rétegbeli kommunikációra állítottunk be.

Zónában betöltött szerep

A hálózati infrastruktúra komponenseinek elhelyezkedése nem egy helységre korlátozódik. Az eszközök két különböző terem között oszlanak meg, a szerverterem és a labor között. A két helyszínt összekötő optikai összeköttetés végpontjain találhatóak a

switch-ek, amelyekhez a hálózat egyéb eszközei kapcsolódnak. A switch-ek feladata, hogy:

- biztosítsák az optikai összeköttetésen átmenő adatcsomagok (keretek) továbbítását a megfelelő végpontok felé;
- biztosítsák a szolgáltatásminőséget (Quality of Service, QoS), beleértve a torlódáskezelést és a forgalom priorizálást;
- hitelesítsék a hálózati eszközöket a MAC címek segítségével;
- biztosítsák a hozzáférés-engedélyezést hozzáférés-szabályozási listák (Access Control List, ACL) segítségével;

5.1.2 Tűzfal

Hardver-specifikus jellemzők

A szeparált információbiztonsági zóna fizikai hálózatának határán egy olyan felső kategóriás tűzfal helyezkedik el, amely magas áteresztőképességgel rendelkezik és a dedikált tűzfalak csoportjába tartozik. Alkalmazási szintű tűzfal révén képes az ISO-OSI modell mind a hét rétege szerint vizsgálni a forgalmat, ezáltal sokkal mélyrehatóbb és szélesebb körű adathalmaz alapján tud szűrési döntéseket hozni. Mindemellett az általunk alkalmazott tűzfal képes többek között:

- a bejövő és kimenő titkosított forgalom szűrésére, nyomon követésére és naplózására;
- az ismert és ismeretlen támadások észlelésére és automatikus elhárítására;
- a teljes hálózati forgalom és a konfigurációs módosítások naplózására;
- felhasználói csoportok létrehozására és kezelésére;
- centralizált és távoli kezelhetőség biztosítására.

Zónában betöltött szerep

A tűzfal a szeparált információbiztonsági zóna első védelmi vonalaként funkcionál. Dedikált tűzfal révén rendkívül fejlett és kiterjed képességekkel rendelkezik, ezért központi szerepet tölt be a hálózatban. A tűzfal elsőszámú feladata a hálózati biztonság biztosítása a zóna hálózatába tartozó fizikai és virtuális csomópontok számára, amely az alábbi feladatköröket foglalja magába:

- a hálózati forgalom szűrése mind a bejövő, mind a kimenő adatcsomagok esetén;
- hozzáférés-engedélyezés a legkisebb kiváltság (least privilege) elvének érvényesítésével;
- hálózati címfordítás és porttovábbítás megvalósítása;
- VPN hozzáférés biztosítása;
- támadások észlelése (Intrusion Detection) és elhárítása (Intrusion Prevention);
- hálózati események nyomon követése és naplózása.

5.1.3 Hardveres biztonsági modul

Hardver-specifikus jellemzők

Az ISMS által keretbe foglalt fizikai infrastruktúra központi elemei a HSM-ek. Az általunk alkalmazott eszközök megfelelnek a FIPS 140-2 Level 3 szabályozásnak, hiszen [42]:

- szabotázsvédelemmel (hamisításállósággal) rendelkeznek;
- a kritikus biztonsági paramétereket (Critical Security Parameter, CSP) kezelő interfészeik elkülöníthetőek, mind logikailag, mind fizikailag;
- biztosítják a privát kriptográfia kulcsok titkosítását azok importálása és exportálása során.

Emellett teljesítik a Common Criteria EAL4+ szabvány követelményeit is, amely átfogó tesztesetek teljesítésével garantálja az eszköz hamisítás elleni védelmi képességeit. Ezen túlmenően a kriptográfiai algoritmusok széles skáláját támogatják, mind a szimmetrikus, mind az aszimmetrikus módszerek esetében.

Zónában betöltött szerep

A HSM-ek felelősek a szeparált zóna külső és belső felek számára nyújtott szolgáltatásainak biztosításáért, beleértve a vállalat speciális ECU-khoz kapcsolódó hitelesítési eljárását, a kriptográfiai kulcsgenerálást és –kezelést, illetve a kód aláírást.

5.1.4 Felső kategóriás vállalati szerver

Hardver-specifikus jellemzők

A szeparált információbiztonsági zóna szolgáltatásainak és alapvető funkcióinak kiszolgálására két vállalati szervert alkalmaztunk. Az általunk használt modellek állványra (rack) szerelhető, felső kategóriás eszközök, amelyek kiemelkedően magas számítási teljesítménnyel és széleskörű bővíthetőségi lehetőségekkel rendelkeznek. Emellett fejlett biztonsági funkciókkal is bírnak, többek között biztosítják a firmware illetéktelen manipulációjával szembeni védelmet és firmware frissítések digitális aláírásainak ellenőrzését.

Zónában betöltött szerep

A szerverek kiemelkedően fontos szerepet töltenek be a zóna hálózatában, hiszen az egyes szolgáltatásokat megvalósító virtuális gépek (Virtual Machines, VM) ezek erőforrásait használják, beleértve a DNS (Domain Name System), az NTP (Network Time Protocol), a DHCP (Dynamic Host Configuration Protocol), a RADIUS (Remote Authentication Dial In User Service) vagy TACACS+ (Terminal Access Controller Access-Control System), az FTP (File Transfer Protocol) és a proxy virtuális szervereket. A szerverek feladata, hogy biztosítsák a megfelelő erőforrásokat a virtuális szerverek rendeltetésszerű működéséhez, illetve magas hibatűrést és rendelkezésre állást nyújtsanak a szolgáltatások folytonosságának érdekében.

5.2 Szoftver komponensek ismertetése

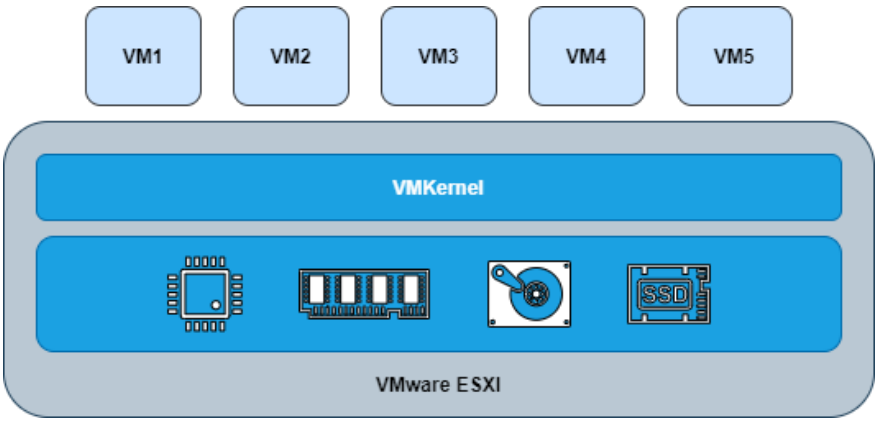
Ebben az alfejezetben bemutatom a szeparált információbiztonsági zóna során alkalmazott fő szoftveres komponenseket, beleértve a VMware ESXi-t, illetve a VMware vCenter-t.

5.2.1 VMware ESXi

Általános jellemzés

A VMware vSphere termékcsalád központi eleme az ESXi (Elastic Sky X) hypervisor, amely képes közvetlenül a rendszer egy adott hardverén működni (bare-metal), operációs rendszer szükségessége nélkül. A hypervisor egy olyan szoftver, amely lehetővé teszi a virtuális gépek létrehozását és működtetését, valamint több VM egyidejű

futtatását egy gazdarendszeren, az erőforrások hatékony megosztása mellett. [43] A 5.2.1-1. ábra jól szemlélteti az ESXi egyes komponenseit és architekturális felépítését.



5.2.1-1. ábra: A VMware ESXi komponensei és felépítése [44] (szerk. a szerző)

A virtuális gépek és a hardver komponensek között elhelyezkedő réteg a VMKernel, amely a processzor ütemezés, a memóriakezelés és a virtuális kapcsolók adatfeldolgozásának biztosítása révén kezeli a virtuális gépek hozzáférését a fizikai erőforrásokhoz. [44]

Zónában betöltött szerep

A VMware ESXi hypervisor-ok elsőszámú feladata a két vállalati szerver erőforrásainak maximális kihasználása. A különböző hálózati szolgáltatások és protokollok, beleértve a DNS-t, NTP-t, DHCP-t, a RADIUS-t vagy TACACS+-t, az FTP-t és proxy-t, dedikált virtuális gépeken futnak. Az ESXi-k feladata, hogy biztosítsák a VM-ek létrehozását és a hozzájuk kapcsolódó fizikai erőforrások megfelelő elosztását.

5.2.2 VMware vCenter

Általános jellemzés

A VMware vCenter szerver elsőszámú feladata, hogy centralizált kezelési felületet és keretrendszert biztosítson az összes ESXi fizikai csomópont és a hozzájuk tartozó virtuális gépek számára. A vCenter központi szerepet játszik minden VMware vSphere implementációban, hiszen lehetővé teszi a rendszergazdák számára, hogy központosított módon telepítsék, kezeljék, felügyeljék és automatizálják a virtuális infrastruktúrát. [44]

A vCenter széleskörű konfigurációs és kezelési funkciókkal rendelkezik, beleértve a virtuális gépekhez kötődő sablonokat, a szerepköralapú hozzáférés-

szabályozást és az erőforrás-elosztás-szabályozást, amelyek nagy mértékben csökkentik az adminisztrátorokra háruló felelősségeket. [44]

Zónában betöltött szerep

A VMware vCenter feladata, hogy megkönnyítse a zóna hálózati adminisztrátorainak feladatait azáltal, hogy centralizált felületet biztosít a virtuális csomópontok folyamatos felügyeletére és kezelésére.

5.3 Eszközök konfigurálásának irányelvei

A szeparált zóna hálózati eszközeinek, szoftvereinek és szolgáltatásainak konfigurációja során kiemelten fontos, az ISMS implementációs fázisai során meghatározott információbiztonsági célok és irányelvek érvényesüljenek. Ebben az alfejezetben részletesen ismertetem azokat az irányelveket, amelyeket az eszközök konfigurációja során követni szükséges.

5.3.1 Irányelvek a leltár alapján

Az információseszköz-nyilvántartás hiánytalanul listázza azokat a szoftvereket, hálózati eszközöket, szervereket és szolgáltatásokat, amelyeknek a konfigurációját el kell végezni. Egy szoftver esetén nyilvántartja többek között az eszköz függőségeit, karbantartási állapotát, illetve a kapcsolódó szolgáltatásokat. Ezeket mind figyelembe kell venni a szoftverek konfigurációja során, hiszen:

- a függőségek esetén meg kell győződni arról, hogy a szükséges szoftvercsomagok telepítésre kerültek és a meghatározott verziószámmal rendelkeznek;
- a karbantartási státusz alapján ellenőrizni kell, hogy a szoftver verziója az elvárt vagy a legfrissebb;
- a kapcsolódó szolgáltatások esetén meg kell győződni arról, hogy az adott szoftver megfelelően nyújtja/kiszolgálja az adott szolgáltatást.

A hálózati eszközök és a szerverek esetén a leltár releváns attribútum típusai az operációs rendszer, a kapcsolódó szolgáltatások, a szoftveres és hardveres függőségek, a redundancia követelmény, a karbantartási állapot, illetve az IP-cím, melyek alapján az alábbi konfigurációs szempontok fogalmazhatóak meg:

- a szoftveres függőségeknél ellenőrizni kell, hogy a szükséges szoftvercsomagok telepítve vannak és az elvárt verziószámmal rendelkeznek; a hardveres függőségeknél pedig azt, hogy megfelelő-e a kommunikációs kapcsolat az eszközök között;
- amennyiben van redundanciára vonatkozó követelmény, akkor a meghatározott redundancia-modell, például aktív-készenléti (active-standby) szerint kell a konfigurációt elvégezni.

Mindemellett a leltár minden egyes információs eszközhöz tárolja annak tulajdonosát, akit ugyancsak figyelembe kell venni a konfiguráció hozzáférés-engedélyezés fázisa során.

5.3.2 Irányelvek a kockázatkezelési folyamat alapján

A kockázatkezelési folyamat során azonosításra kerülnek az információs eszközökkel kapcsolatos fenyegetések és sérülékenységek és meghatározásra kerülnek a kockázati szintek. A kockázati besorolások alapjaiban meghatározzák az eszközök hálózaton belüli elhelyezkedését, illetve az egyes szerepkörökhöz tartozó hozzáférési-szinteket és kiváltságokat. A hálózati architektúrát külön dokumentálni kell, beleértve az összes hardver- és szoftverkomponens tervezett konfigurációs beállításait. Kiemelten fontos, hogy a konfigurációs tervnek tükröznie kell a kockázatkezelési folyamat eredményeit, beleértve a bevezetett műszaki ellenőrzéseket, mind a megelőző, detektív és reaktív intézkedési típusok esetén.

Az ISO/IEC 27002:2013 szabvány javasolja, hogy az ISMS által keretbe foglalt fizikai hálózatban olyan intézkedéseket kell bevezetni, amelyek lehetővé teszik a szolgáltatások, a felhasználók és az információs rendszerek egyértelmű elkülönítését. [15]

Hálózati szegregáció irányelvei

A switch-ek és tűzfal segítségével a hálózat egyszerűen szegmentálható több helyi hálózatra, vagy virtuális helyi hálózatra (Virtual Local Area Network, VLAN). A hálózati szegregációs folyamatra az alábbi irányelveket határoztam meg:

- a hálózati szegregáció során elegendő alhálózatot kell kialakítani ahhoz, hogy az információs eszközök kellően izolált hálózati szegmensbe kerülhessenek a kockázati kitettségük szerint (oszd meg és uralkodj elv);

- a magas kockázati szintű elemeket tartalmazó alhálózatokba csak a minimálisan szükséges kommunikációs üzenetek juthatnak be;
- a távoli hozzáférés és az egyéb publikus internet felől érkező hálózati adatforgalmat különösen kritikusan kell kezelni, megfelelő titkosítás és hitelesítés mellett;
- az alhálózatok közti adatforgalmat szigorúan ellenőrizni és naplózni kell;
- az információs rendszerekhez felülvizsgálati tervet és útmutatót kell létrehozni, amely szerint a konfigurációs beállításokat és szűréseket felül kell vizsgálni;
- az információs rendszerek kockázatkezelését új sérülékenységek és fenyegetések megjelenése vagy kockázati szint változása esetén újból el kell végezni.

Hozzáférés-szabályozás irányelvei

Az ISO/IEC 27001:2013 szabványnak való megfelelés érdekében a szervezetnek egyértelműen meg kell határoznia a hozzáférés-szabályozással kapcsolatos igényeit, majd ezeket a szabályokat be kell építenie a hálózati beállításokba. [45] A kockázatértékelés eredményei egyértelműen rámutatnak arra, hogy ki férhet hozzá egy adott információs rendszerhez. Az alábbiakban ismertetem azokat az irányelveket, amelyek figyelembe vettem a hozzáférés-ellenőrzési konfigurációs beállítások kidolgozása során:

- az információs eszközök hozzáférés-szabályozási folyamatához meghatározott feladatköröknek egyértelműen el kell különülnie (a feladatok elkülönítésének elve);
- minden szerepkörhöz a lehető legalacsonyabb kiváltságfokozatot kell rendelni, amely mellett a szerepkörhöz kapcsolódó tevékenységeket el lehet végezni (legkisebb kiváltság elve);
- a szerepkörök hozzáférés-engedélyezése során többfaktoros hitelesítést és forgalomtitkosítást kell alkalmazni;
- a hozzáférési jogokat rendszeresen felül kell vizsgálni, és ki kell korrigálni vagy vissza kell vonni amennyiben egy munkavállaló szerepköre megváltozik vagy munkaviszonya megszűnik;

Firmware- és szoftverfrissítéssel kapcsolatos irányelvek

A szeparált zónához kapcsolódó firmware- és szoftverfrissítéseket két kategóriára bontottam, az új funkciókat tartalmazó és a biztonsági problémákat kezelő frissítésekre. Mindkét kategória esetén érvényesek az alábbi irányelvek:

- a szoftverek és firmware-ek frissítésére ütemterveket kell létrehozni, amelyben a hosszú távú támogatással rendelkező, stabil verziókat kell előnyben részesíteni;
- a frissítési folyamatok megkezdése előtt meg kell győződni arról, hogy az eljárás üzembiztos és nem okoz szolgáltatásbeli degradációt;
- amennyiben a szolgáltatásbeli kiesés elkerülhetetlen, meg kell határozni annak elfogadható idejét és fel kell készülni a lehetséges következményekre és hatásokra;
- a frissítést követően az újonnan telepített firmware- vagy szoftververziót tesztelésnek kell alávetni a megfelelő működés ellenőrzése és biztosítása érdekében;
- szoftverfrissítési folyamatokat lehetőség szerint virtualizációs és konténerizációs technológiákkal kell elősegíteni és automatizálni a hatékonyság és a gyorsaság érdekében;
- a sikeres és sikertelen frissítéseket naplózni kell egy központi adatbázisba.

6 Értékelés

Szakdolgozatomban betekintést nyújtottam az autóipar jelenlegi technológia fejlettségébe, illetve ismertettem az aktuális fenyegetéseket és kockázatokat az iparági kibertérben. Áttekintettem a nemzetközi iparágazati szabványokat, illetve a különféle védelmi rétegeket és tesztelési metodikákat, amelyek az E/E rendszerek és az ezeket vezérlő ECU-k kiberbiztonságát hivatottak növelni.

Jelen dolgozat középpontjában a szeparált információbiztonsági zóna kialakítása áll, amely elszigetelt és kontrollált környezetet biztosít a különböző tesztelési eljárások számára. Részletesen bemutattam az információbiztonsági irányítási rendszer megvalósítási tervezetét az ISO/IEC 27k szabványcsalád szerint, kiemelvén azokat a fontos implementációs fázisokat, amelyek a feladatom részét képezték, beleértve a kockázatkezelést, illetve a szerepek és felelősségi körök kialakítását. Mindemellett ismertettem az irányítási rendszer által keretbe foglalt fizikai hálózati infrastruktúrát, melynek fő elemei a switch-ek, a szerverek, a tűzfal, illetve a HSM-ek.

A kutatómunka során elmélyültem a témakörhöz kapcsolódó szakirodalomban és sikerült kibővítenem a tudásom mind a nemzetközi szabványokkal, mind az információbiztonsági irányítási rendszerrel kapcsolatban. Emellett hasznosítani tudtam a Budapesti Műszaki és Gazdaságtudományi Egyetem üzemmérnök-informatikus szakán szerzett tudást, különös tekintettel a *Hálózatok alapjai és üzemeltetése*, a *Számítógép-hálózatok a gyakorlatban*, illetve a *Gyakorlati hálózatbiztonság* tantárgyak ismeretanyagára.

A szeparált információbiztonsági zóna kialakítása során megtanultam értelmezni és hatékonyan feldolgozni a nemzetközi szabványok követelményrendszereit, illetve elsajátítottam azokat a dokumentációs készségeket, amelyek az ISMS tanúsíthatóságához szükségesek. Bízom benne, hogy az általam elvégzett munka hasznosnak fog bizonyulni a rendszer további implementációs lépései és folyamatos fejlesztése során.

7 Irodalomjegyzék

[1] N. Navet és F. Simonot-Lion, „Vehicle Functional Domains and Their Requirements," in *Automotive Embedded Systems Handbook*, Boca Roton, London, New York, CRC Press Taylor & Francis Group, 2009, pp. 1-1 - 1-22, ISBN-13: 978-0-8493-8026-6.

[2] N. Navet és F. Simonot-Lion, „Preface," in *Automotive Embedded Systems Handbook*, Boca Raton, London, New York, CRC Press Taylor & Francis Group, 2009, pp. vii-xiii, ISBN-13: 978-0-8493-8026-6.

[3] S. Kim és R. Shrestha, „In-Vehicle Communication and Cyber Security," in *Automotive Cyber Security*, Springer Nature Singapore Pte Ltd., 2020, pp. 127-178, ISBN: 978-981-15-8053-6.

[4] N. Navet és F. Simonot-lion, „A Review of Embedded Automotive Protocols," in *Automotive Embedded Systems Handbook*, Boca Roton, London, New York, CRC Press Taylor & Francis Group, 2009, pp. 4-1 - 4-31; ISBN-13: 978-0-8493-8026-6.

[5] F. Arena és G. Pau, „An Overview of Vehicular Communications," *Future Internet*, pp. 1-13, 2019.

[6] „rgbsi," rgbsi, Interneten elérhető: https://blog.rgbsi.com/7-types-of-vehicle-connectivity. [Hozzáférés dátuma: 2 május 2022].

[7] E.-R. Zeinab, S. Karthikeyan, F. S. Daisy, J. P. Siby és R. Prakash, „Cybersecurity challanges in vehicular communication," *Vehicular Communications Vol. 23*, pp. 1-28, 2019.

[8] *ISO/SAE 21434:2021, Road vehicles — Cybersecurity engineering*, International Organization for Standardization, 2021.

[9] *UN Regulation No. 155 - Cyber security and cyber security management system*, United Nations, 2021.

[10] *UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system,* United Nations, 2021.

[11] H. Poston, „INFOSEC," Infosec Institute, Inc., 11 augusztus 2020. Interneten elérhető: https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/. [Hozzáférés dátuma: 22 május 2022].

[12] *ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary,* Switzerland: International Organization for Standardization, 2018.

[13] M. E. Whitman és H. J. Mattord, „Introduction to Information Security," in *Principles of Information Security Sixth Edition*, United States, Cengage Learning, 2017, pp. 1-47, ISBN: 978-1-337-10206-3.

[14] *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements,* Switzerland: International Organization for Standardization, 2013.

[15] *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls,* Switzerland: International Organization for Standardization, 2013.

[16] A. Calder és S. Watkins, „ISO27001," in *IT Governance An International Guide to Data Security and ISO27001/ISO27002 7th Edition*, Great Britain, United States, Kogan Page Limited, 2020, pp. 37-54, ISBN: 978-0-7494-9696-8.

[17] *ISO/IEC 27003:2017 Information technology - Security techniques - Information security management systems - Guidance,* Switzerland: International Organization for Standardization, 2017.

[18] *ISO/IEC 27004:2016 Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and*

evaluation, Switzerland: International Organization for Standardization, 2016.

[19] *ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management,* Switzerland: International Organization for Standardization, 2018.

[20] A. Calder és S. Watkins, „The risk assessment and Statement of Applicability," in *IT Governance An International Guide to Data Security and ISO27001/ISO27002 7th Edition*, Great Britain, United States, Kogan Page Limited, 2020, pp. 89-114, ISBN: 978-0-7494-9696-8.

[21] G. Funk, J. Hermann, A. Holl, N. Jeliazkov, O. Knörle, B. Krsic, N. Müller, J. Oetting, J. Rozek, A. Rupprich, T. Dr. Sattler, M. Schmid és H. Schrader, *Implementation Guideline ISO/IEC 27001:2013,* Berlin, Germany: ISACA Germany Chapter e.V., 2016.

[22] S. G. Watkins, „ISO27001 and the management system requirements," in *An Introduction to Information Security and ISO27001*, United Kingdom, IT Governance Publishing, 2008, pp. 19-23, ISBN: 978-1-905356-69-0.

[23] S. v. Otterloo, „ICT Institute," ICT Institute (ICTI BV), 8 február 2017. Interneten elérhető: https://ictinstitute.nl/pdca-plan-do-check-act/. [Hozzáférés dátuma: 9 május 2022].

[24] W. Stallings, „Asymmetric Ciphers," in *Cryptography and Network Security,* England, Pearson Education Limited, 2017, pp. 283-312, ISBN: 1-292-15858-1.

[25] W. Stallings, „Digital Signatures," in *Cryptography and Network Security*, England, Pearson Education Limited, 2017, pp. 420-440, ISBN: 1-292-15858-1.

[26] „SECTIGO Store," SECTIGO, Interneten elérhető: https://sectigostore.com/page/what-to-know-about-code-signing-certificates-for-individual-developers/. [Hozzáférés dátuma: 28 május 2022].

[27] J.-P. Aumasson, „Randomness,” in *Serious Cryptography A Practical Introduction to Modern Encryption*, San Francisco, No Starch Press, Inc., 2018, pp. 55-78, ISBN: 1-59327-826-8.

[28] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray és S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, National Institute of Standards and Technology, 2010.

[29] M. J. Stewart és D. Kinsey, „Firewall Fundamentals,” in *Network Security, Firewalls, and VPNs Third Edition*, Burlington, MA, Jones & Bartlett Learning, 2021, pp. 442-560; ISBN: 9781284183658.

[30] A. Philipp, Hardware Security Modules (HSM) for Dummies, Weinheim: WILEY-VCH Verlag GmbH & Co. KGaA, 2015.

[31] A. Calder és S. Watkins, „Asset management,” in *IT Governance An International Guide to Data Security and ISO27001/ISO27002 7th Edition*, Great Britain, United States, Kogan Page Limited, 2020, pp. 139-155, ISBN: 978-0-7494-9696-8.

[32] A. Calder és S. G. Watkins, „The ISO 27001 risk assessment,” in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 87-93, ISBN: 978-1-78778-137-5.

[33] A. Calder és S. G. Watkins, „Risk assessment methodologies,” in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 27-43, ISBN: 978-1-78778-137-5.

[34] A. Calder és S. G. Watkins, „Threats and vulnerabilities,” in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 106-113, ISBN: 978-1-78778-137-5.

[35] A. Calder és S. G. Watkins, „Risk management," in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 16-26, ISBN: 978-1-78778-137-5.

[36] A. Calder és S. G. Watkins, „Risk treatment and the selection of controls," in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 147-158, ISBN: 978-1-78778-137-5.

[37] *BSI-Standard 100-2 IT-Grundschutz Methodology Version 2.0,* Germany: Bundesamt für Sicherheit in der Informationstechnik, 2008.

[38] A. Calder és S. G. Watkins, „Roles and responsibilities," in *Information Security Risk Management for ISO 27001/ISO 27002 Third edition*, United Kingdom, IT Governance Publishing, 2019, pp. 55-64, ISBN: 978-1-78778-137-5.

[39] M. Kamat, *Guideline for Roles & Responsibilities in Information Asset Management,* ISO 27001 security ISO 27001 Implementer's Forum, 2009.

[40] D. G. Hinson PhD és L. Kowalski, *Roles and responsibilities for contingency planning version 1,* ISO 27001 security, 2008.

[41] R. Sasha, „GOODCORE," GoodCore Software Limited, 11 szeptember 2019. Interneten elérhető: https://www.goodcore.co.uk/blog/a-guide-to-the-raci-rasci-model/. [Hozzáférés dátuma: 17 május 2022].

[42] r. ciphertex, „CIPHERTEX data security," Ciphertex, 29 december 2020. Interneten elérhető: https://ciphertex.com/what-is-fips-140-2-level-3/. [Hozzáférés dátuma: 24 május 2022].

[43] VMware, Inc., „VMware," VMware, Inc., Interneten elérhető: https://www.vmware.com/topics/glossary/content/hypervisor.html. [Hozzáférés dátuma: 24 május 2022].

[44] N. Marshall, M. Brown, B. G. Fritz és R. Johnson, „Introducing VMware vSphere 6.7," in *Mastering VMware vSphere 6.7*, United States, Canada, SYBEX A Wiley Brand, 2019, pp. 1-23, ISBN: 978-1-119-51294-3.

[45] A. Calder és S. Watkins, „Access Control," in *IT Governanace A Manager's Guide to Data Security and ISO 27001/ISO 27002 4th edition*, Great Britain, United States, Kogan Page Limited, 2008, pp. 226-243, ISBN: 978-0-7494-5271-1.

8 Függelék

8.1 Információs eszközök leltárának attribútum-típusai

8.1-1. táblázat: A leltárban szereplő egyes információs eszközkategóriákhoz tárolt attribútum-típusok

Szolgáltatások	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Típus	Kapcsolódó hardver
Hálózati eszközök	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Típus	Gyártó vállalat
Adattároló hardverek	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Helyszín	Gyártó vállalat
Laptopok	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Helyszín	Gyártó vállalat
Digitális információk	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Helyszín	Tárolási mód
Analóg információk	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Helyszín	Tárolási mód
Szerverek	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Típus	Gyártó vállalat
Szoftverek	Egyedi azonosító	Megnevezés	Tulajdonos/ felelős	Letétemények	Típus	Fejlesztő vállalat
Emberek	Egyedi azonosító	Név	Vállalati osztály	Munkaköri beosztás	Felettes	Elvárt képességek

Kapcsolódó szoftver	Hely	Függőségek	Redundancia követelmény	Ellenőrzési periódus	Felülvizsgálati állapot	Titkossági követelmény	Sértetlenségi követelmény
Széria szám	Hely	Rack/Slot szám	Operációs rendszer	Kapcsolódó szolgáltatás	Szoftveres függőségek	Hardveres függőségek	Redundancia követelmény
Széria szám	Hely	Hatókörön kívüli használat	Tárolási kapacitás	Biztonsági másolat	Biztonsági másolat helye	Ellenőrzési periódus	Tárolt információk
Széria szám	Hely	Megosztott meghajtók/adatok	Operációs rendszer	Kapcsolódó szolgáltatás	Hatókörön kívüli használat	Szoftveres függőségek	Karbantartási állapot
Adattároló megnevezés	Biztonsági besorolás	Biztonsági másolat	Titkosítási módszer	Másolat helye	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény
Adattároló megnevezés	Biztonsági besorolás	Biztonsági másolat	Másolat helye	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény	
Széria szám	Hely	Rack/Slot szám	Operációs rendszer	Kapcsolódó szolgáltatás	Szoftveres függőségek	Hardveres függőségek	Redundancia követelmény
Széria szám	Verzió szám	Licenc adatok	Kapcsolódó szolgáltatás	Függőségek	Karbantartási állapot	Technikai segítségnyújtás	Titkossági követelmény
Titkossági követelmén	Sértetlenségi követelmény	Elérhetőségi követelmény					

Elérhetőségi követelmény							
Karbantartási állapot	IP cím	Technikai segítségnyújtás	Felülvizsgálati periódus	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény	
Titkosítási módszer	Technikai segítségnyújt	Felülvizsgálati periódus	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény		
Redundancia követelmény	IP cím	Technikai segítségnyújtás	Tárolt információk	Felülvizsgálati periódus	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény
Karbantartási állapot	IP cím	Technikai segítségnyújtás	Tárolt információk	Felülvizsgálati periódus	Titkossági követelmény	Sértetlenségi követelmény	Elérhetőségi követelmény
Sértetlenségi követelmény	Elérhetőségi követelmény						

8.2 Kockázatkezelési dokumentációk

8.2-1. táblázat: A kockázat nyilvántartásánál használt attribútum-típusok

Kockázat azonosító	Kockázat megneve-zése	Kockázat tulajdonosa	Kapcsolódó információs eszköz	Várható anyagi veszteség	Kockázati szint	Kezelés típusa és kategóriája	Kezelés
12732	Elektromágneses sugárzás okozta információ vesztés	IT hálózati mérnök	Szerver	15 500 000 HUF	Magas	Árnyékolás	Megelőző/Fizikai

Kezelés költsége	Elvárt kockázati szint	Dátum
1 400 000 HUF	Alacsony	2022.02.30

8.2-2. táblázat: Alkalmazhatósági nyilatkozat részlete

ISO/IEC 27001:2013 A függelék - Ellenőrzések		Jelenlegi ellenőrzések	Indoklás	A kiválasztott ellenőrzés és a kiválasztás oka				Megjegyzés
Záradék	Szakasz	Ellenőrzés		Kockázat -kezelés	Szerződéses követelmény	Jogi követelmény	Üzleti követelmény	
8 Eszköz-kezelés	8.1.1	Ellenőrzés	Jelenleg nincs ilyen.	Indoklás	X			
	8.1.2	Ellenőrzés	Van ilyen jellegű.	Indoklás				
	8.1.3	Ellenőrzés	Jelenleg nincs ilyen.	Indoklás			X	

8.3 Szerepekkel és felelősségi körökkel kapcsolatos dokumentáció

8.3-1. táblázat: RASCI mátrix a szerepek és felelősségi körök ábrázolására

ISO/IEC 27001:2013 A függelék - Ellenőrzések			Szerepkörök					
Záradék	Szakasz	Ellenőrzés	CISO	DPO	IT DRPM	Kockázat-tulajdonos	Információseszköz-tulajdonos
8 Eszköz-kezelés	8.1.1	Ellenőrzés	R	R	C	S	A
	8.1.2	Ellenőrzés	S	A	A	C	I
	8.1.3	Ellenőrzés	I	C	R	A	A