IoT integration in Microsoft Dynamics ERP

Peter Porteleki

Multisoft Kft., Bartók Béla street 113., Budapest 1115, Hungary, peter.porteleki@multisoft.hu

Abstract

This article presents a software development project, that is based on integrating between Microsoft Dynamics ERP system, and other systems that are separate. Understanding customer needs, and the workflow of those separate systems, and creating an universal integrated product was essential to solving the specified requirements. This product provides device-independent interoperability between almost any hardware or software, making users life easier, business workflows more effective, eliminating third parties. The article provides a concrete example of this module and it's functions.

Keywords: ERP; IOT; Integration; Microsoft Dynamics; NAV; Navision; Business Central;

IoT integráció a Microsoft Dynamics ERP rendszerben

Porteleki Péter

Multisoft Kft., Bartók Béla út 113., Budapest 1115, Magyarország, peter.porteleki@multisoft.hu

Absztrakt

A cikkben egy vállalatirányítási rendszer a Microsoft Dynamics ERP és a különböző, általában szigetrendszerként működő hardverek és szoftverek közötti integráció kerül bemutatásra. A feladat megoldásához elengedhetetlen volt az ügyfelek igényeinek felmérése, és az egyes vállalatok által használt elszigetelt rendszerek működésének megismerése, valamint egy univerzális termék létrehozása, amely könnyen integrálható a különböző beállítottságú vállalatokhoz. Ezen termék eszközfüggetlen integrációt és átjárhatóságot biztosít a különböző rendszerek között, segítségével automatizmusok hozhatók létre, megkönnyítve ezzel a rendszert használók munkáját, ezáltal pénz, de főleg idő spórolható meg a harmadik fél kiiktatásával. A cikk egy konkrét példát felhasználva mutatja be a modult és annak funkcióit.

Kulcsszavak: ERP; IOT; Integráció; Microsoft; Dynamics; NAV; Navision; Business Central;

1. Bevezető

Néhány ügyfelünk részéről a közelmúltban felmerült az igény különböző egymástól elszigetelt rendszerek integrálhatóságára a Microsoft Dynamics NAV, illetve Business Central rendszerbe (Microsoft, 2020). Az ügyfeleink köre nagyon sokrétű, ezáltal az integrálásra váró rendszerek zöme teljesen eltér egymástól, mégis felmerült egy ötlet, hogy hogyan lehetne egységesíteni ezeket egy közös platform alá. A fejlesztés legfőbb célja ezen platform kialakítása volt, amelyet így minimális módosítással elérhetővé tegyünk a partnereinknek. Ezen modul egyaránt használható egy fős vállalkozások, valamint nagyvállalati környezetben egyaránt, függetlenül a különböző rendszerek földrajzi pozíciójuktól, az egyetlen dolog amire szükség van az az internetelérés. A múltban ügyfélspecifikusan már történtek hasonló irányban kutatások, és

fejlesztések, de ezek nem voltak egyszerűen átültethetők egy másik vállalathoz, így mindenképpen egy univerzális megoldást kellett találnunk, amelyhez könnyen megírható az ügyfélspecifikus kiegészítés. A cikkben ezen ügyfélspecifikus kiegészítés egy kártyás beléptető rendszer formájában kerül bemutatásra. (1. ábra)

1. ábra Kártyás beléptetőrendszer

1.1. A Protokoll kiválasztása

A tervezés során sok ötlet felmerült, hogy milyen protokoll az, amely elég univerzális ahhoz, hogy bármilyen egymástól független rendszerek között megvalósítható legyen a kommunikáció. Végül a saját okosotthon rendszerem tervezése alatt megszerzett tudás alapján az MQTT[1] (Eclipse Mosquitto, 2020) mellett döntöttem. Ezen protokoll nagyon rugalmas, valamint kis erőforrást igényel, nyílt forráskódú, publish-subscribe alapokon működő hálózati protokoll, amely üzeneteket közvetít az eszközök között, és alkalmas olyan környezetbe, ahol a hálózati sávszélesség erősen limitált. Az MQTT protokoll erősen hasonlít a Dynamics ERP rendszerében használható EventPublisher és EventSubscriber metódusokhoz, ahol bizonyos

[1] Message Queuing Telemetry Transport – Üzenetsorbaállító Telemetriai Transzport

eseményeket hozhatunk létre kód szinten, majd ezen eseményekre feliratkozva írhatunk funkciókat. Ez a hasonlóság nagyban megkönnyíti az MQTT integrációt.

1.2. MQTT Kliens a Dynamics-ben

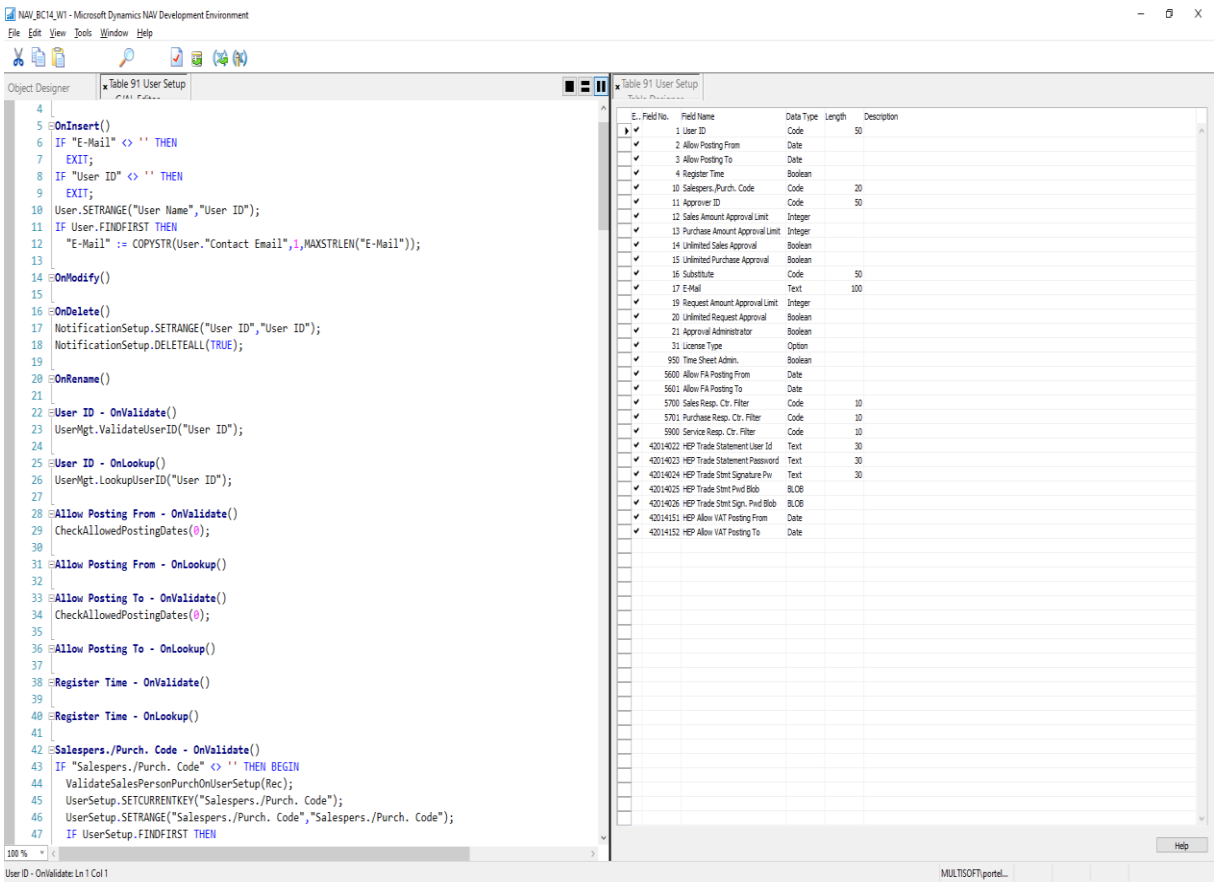
Hogy használni tudjuk az MQTT által nyújtott szolgáltatásokat szükségünk lesz egy kliens szoftverre, amin keresztül a kommunikáció megvalósítható a két rendszer között. A Dynamics NAV, illetve Business Central On-Premise változataiban használható külső .NET alapú könyvtár így a legkézenfekvőbb megoldás az volt, hogy keresni vagy írni kell egy ilyen kell egy ilyen könyvtárat. Ezt meg is találtam az M2MQTT (Paolo Patierno, 2015) személyében, amely akár módosítás nélkül használható a kitalált célra. Az MQTT brókerhez csatlakozva és a megfelelő topikokra feliratkozva, az ERP rendszer képes üzeneteket fogadni és küldeni a bróker irányába.

1.3. MQTT üzenet lista

Az ERP rendszerben, hogy a kliens által lekért és küldött üzeneteket átláthatóan kezelni tudjuk egy táblára van szükségünk, valamint egy Codeunit-ra, amely megadott időközönként lekérdezi az MQTT brókertől a friss üzeneteket és tölti az említett táblát. A Dynamics-ban az üzleti logika nem különül el élesen a különböző objektum típusoktól, így egy tábla, amely SQL szinten valóban egy SQL táblának felel meg, az ERP oldalon programkódot is tartalmazhat, akár a teljes táblára, akár az egyes mezőkre vonatkozóan. (2. ábra) Ezt a lehetőséget kihasználva két Triggert fogunk használni a táblánkban, erre a tervezés részben bővebben kitérünk.

1.4. Standard objektum kiegészítések

A Dynamics fejlesztők, néhány speciális objektum, kivételével hozzáférnek a teljes vállalatirányítási rendszer üzleti logikájának kódjához. Erre szükség is van mert sok esetben az ügyfél igényeinek megfelelően módosításokat kell eszközölni, de jelen esetben csak kiegészítjük a gyári objektumokat, valamint új objektumokat hozunk létre. A beléptető rendszer használatához, néhány új táblára is szükségünk van, amelyben definiáljuk a Kártyákat, a Kártyákhoz hozzárendelt Ajtókat, Egy Ajtók és Beléptetőkapuk tábla, valamint ki kell egészítenünk a Felhasználó táblát, hogy hozzárendelhessük az egyes felhasználókhoz a megfelelő kártyát/kártyákat.



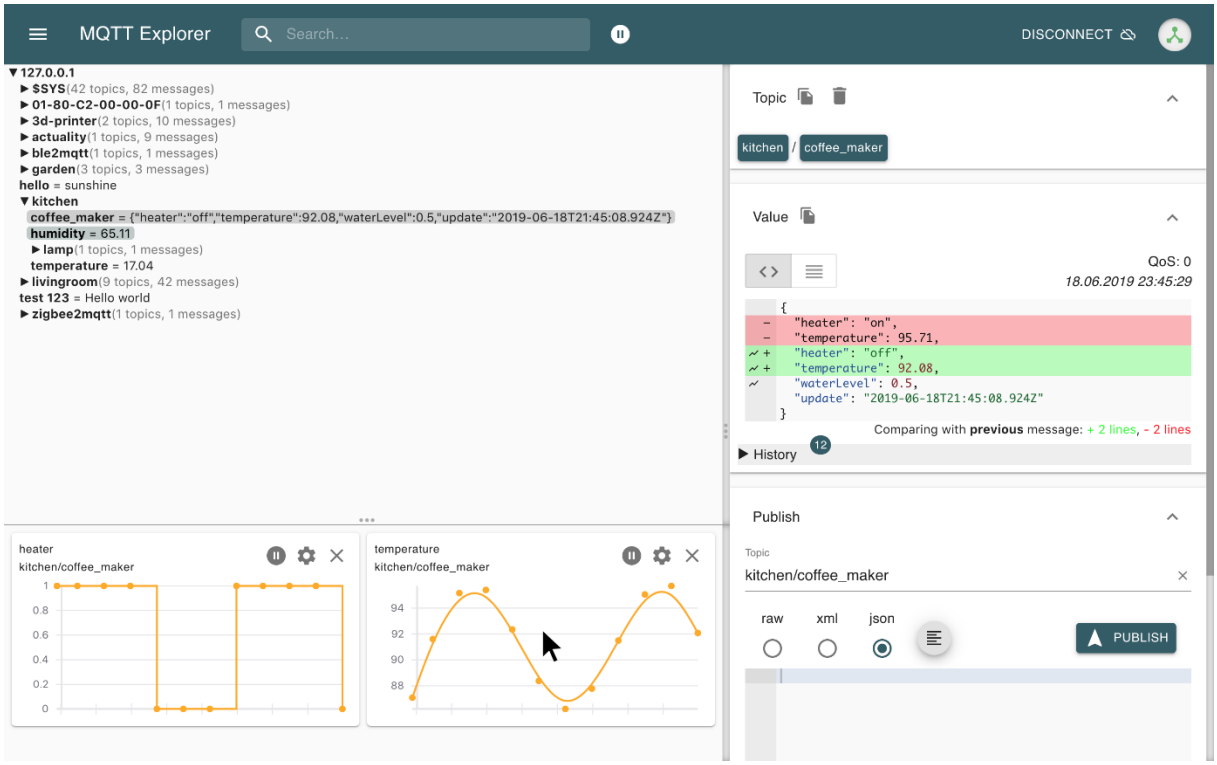
2. ábra User Setup tábla felépítése és üzleti logikája

2. Tervezés és Implementáció

A Dynamics ERP EventPublisher/Subscriber, valamint az MQTT Publish/Subscribe közti logikai hasonlóságok miatt a tervezés nem ütközött technikai bonyodalmakba. Alapvetően két részre lehet elkülöníteni a tervezési és implementációs fázist.

2.1. MQTT oldal

Ezen az oldalon, hacsak nincs speciális igényünk nincs szükség speciális tervezésre. A bróker szoftvert egy tetszőleges környezetbe feltelepítjük, vagy használhatunk a felhőben létrehozott ingyenes vagy fizetős szolgáltatást az igényeinknek megfelelően. Érdemes beszerezni emellé az MQTT Explorer (3. ábra) (Thomas Nordquist, 2020) vagy más, hasonló alkalmazást, amellyel közvetlenül kapcsolódhatunk a brókerhez, lekérdezhetjük az összes üzenetet, nyomon követhetjük az egyes topikokban a változásokat, feliratkozhatunk topikokra, valamint üzeneteket tehetünk közzé az egyes topikokban, megkönnyítve ezzel a tesztelést, valamint a rendszer monitorozását.



3. ábra MQTT Explorer

A hardvereket, jelen esetben a kártyás beléptető rendszert, valamint az ajtónyitó mechanikát csatlakoztatjuk az MQTT brókerhez a megfelelő topikba.

Például: /dooraccess/readers/reader1, valamint /dooraccess/doors/door1

Az első topikba beérkező üzenetet feldolgozzuk, majd amennyiben szükséges a megfelelő üzenetet a második topikba, amely az ajtó vezérlése elküldjük. Maguk az eszközök is tehetnek közzé üzenetet a saját topikjukba, így megoldható a nyitás után az automatikus zárás, ez lehetővé teszi egy adott ajtó aktuális állapotának lekérdezését is.

Az ajtónyitó hardver a megfelelő topikban egyetlen paraméterrel rendelkezik, amely az „Open” névre hallgat és két állapotot vehet fel, igaz vagy hamis annak megfelelően, hogy az ajtó nyitható vagy zárva van, nyitás után a beállított időtartamnak megfelelően automatikusan visszaállítja a zárt állapotot elkerülve az illetéktelenek belépését.

2.2. Dynamics oldal

Az alaprendszer használatához szükségünk van az MQTT Kliens könyvtárat példányosító Codeunitra, valamint ebben a könyvtárban iratkozunk fel az egyes topikokra, ezen felül szükség

van egy táblára a lekérdezett üzenetek tárolására, amellyel gyakorlatilag SQL oldalon reprodukáljuk az MQTT bróker aktuális, és múltbéli állapotait. Az MQTT kliens codeunitot szűk időközönként meghívjuk, hogy valós időben követhető legyen az üzenetek folyama. Szükség van még a Quality of Service[2] (QoS) definiálására. Ez a protokoll szempontjából szükséges, hogy a brókerbe beküldött üzenetünk a feliratkozók részére milyen fontossággal bírnak.

QoS-ből az MQTT három szintet támogat:

1. Legfeljebb egyszer (0)
2. Legalább egyszer (1)
3. Pontosan egyszer (2)

Ezen szintek használata a felhasználás jellegéből adódóik, és valóban azt fogalmazza meg hogy mennyire fontos az egyes topikokba beküldött üzenet nyugtázásának fontossága.

Például: ha hőmérséklet monitorozásra használjuk, ahol 30 másodpercenként beküldjük a megfelelő szenzorhoz tartozó topikba az aktuális hőmérsékletet, de erre az eseményre feliratkozott szoftverhez (amely például egy hőmérsékletet mutató kijelzőben működik) nem jut el, nem jelzünk hibát, és próbáljuk meg mindenképpen eljuttatni az üzenetet, hiszen 30 másodperc múlva jön a következő, friss értéket tartalmazó üzenet, így tanácsos a „0” szint használata. Azonban, ha olyan kritikus rendszerről beszélünk, ahol feltétlenül célba kell juttatni az üzenetet célszerű magasabb szintet használni, így a rendszer, noha rendelkezik frissebb bejegyzéssel az előző üzeneteket is elküldi a végeszközök számára.

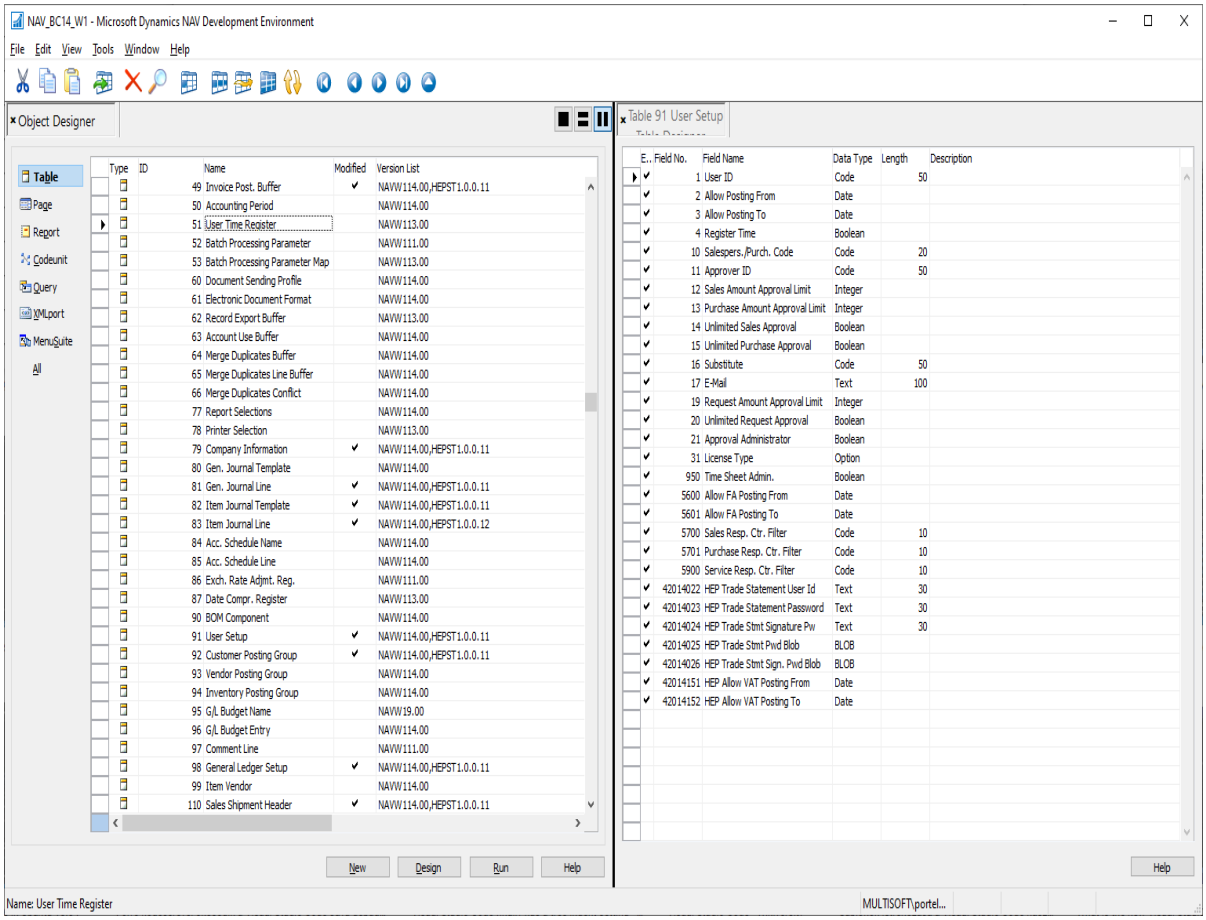
Jelen esetben a 0 szint használata megfelel az igényeinknek, mert egy kártyás beléptető rendszer esetén ha az üzenet valamilyen okból nem jut el a Dynamics oldalra, oda ahol a beléptetés authentikáció lezajlik, a felhasználó még egyszer meg fogja próbálni a belépést, valamint nem szükséges a régebbi üzeneteket eljuttatni az ERP felé, hiszen ez egy hálózati kimaradás esetén akár biztonsági kockázatot is jelenthet, az ajtók az ERP rendszer legközelebbi bekapcsolásakor kinyitja az ajtókat, noha az üzenet továbbítása és fogadása között akár napok telhetnek el, ezért is fontos jelen esetben hogy csak a legutolsó állapot kerüljön bejegyzésre.

[2] Jelen esetben a szolgáltatáson közzétett üzenetek prioritását jelöli

2.2.1. Táblák

Ahogy fentebb is említés esett róla, szükségünk van új táblák létrehozására a rendszerben. Az alaprendszer működéséhez egyetlen tábla is elegendő, amelyben az üzeneteket tároljuk. Ehhez a táblához két EventPublisher funkció hozzáadása is szükséges, amelyek a táblában végzett műveletnek megfelelően egy eseményt hoznak létre amire más objektumokból fel lehet iratkozni. A két Publisher az OnAfterModify, amely egy rekord módosítása után kerül meghívásra, illetve az OnAfterInsert, amely egy új rekord bekerülése után kerül meghívásra.

A tábla felépítése igen egyszerű, egy elsődleges kulcs, valamint egy üzenet fielddel rendelkezik, ennyi már elegendő az alapvető működéshez. (4. ábra)



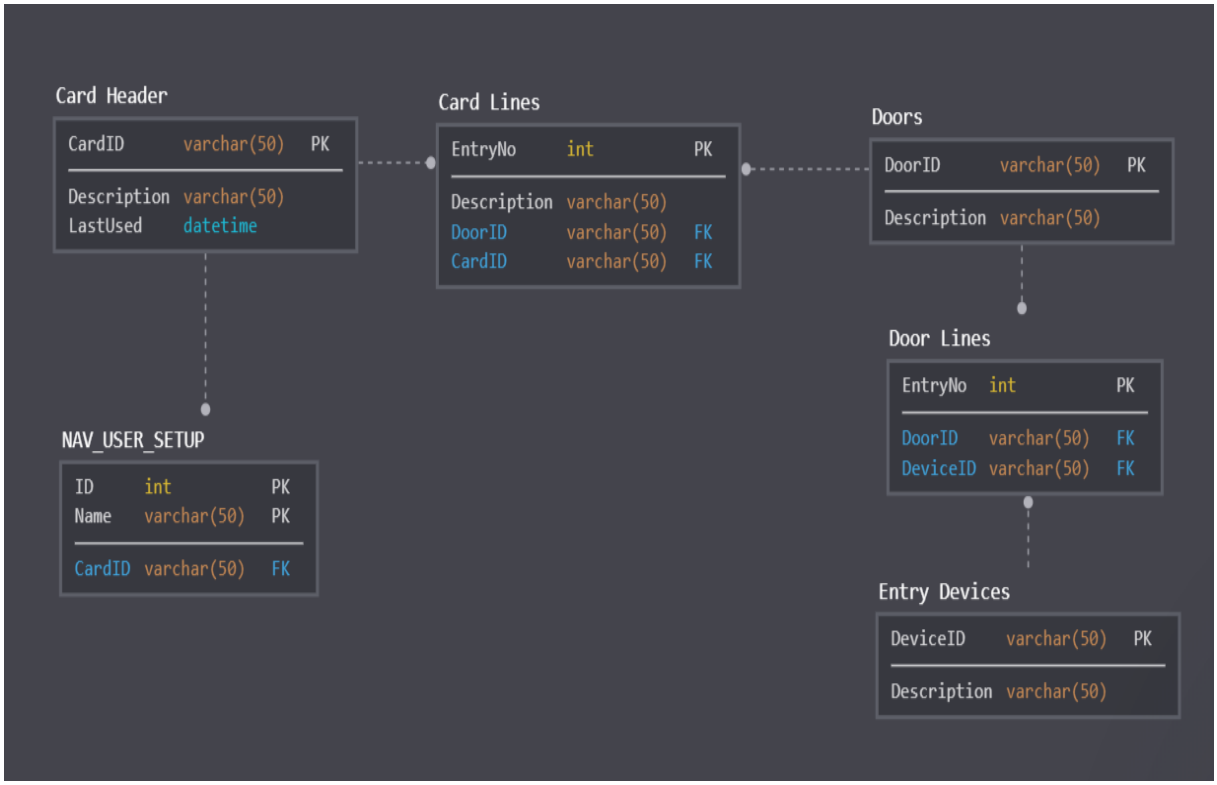
4. ábra Business Central C/AL Development Environment

A beléptetőrendszerhez szükségünk van még további táblákra, amelyek a következők:

1. Card Header: Az egyes kártyák alapvető adatait tartalmazza.
2. Card Lines: Az egyes kártyák által nyitható beléptető eszközöket tartalmazza

3. Doors: Az ajtókat tartalmazza
4. Door Lines: Az ajtókhoz tartozó beléptető eszközöket tartalmazza
5. Entry Devices: A beléptető eszközöket tartalmazza

Az adatbázis kapcsolatokat (5. ábra) általában papíron szoktam megtervezni és megrajzolni, később, amennyiben a projekt megkívánja a dokumentációba automatikus eszközökkel generálunk vizuális ábrákat.



5. ábra Adatbázis kapcsolatok

2.2.2. Pagek

A fent említett táblákhoz néhány oldal létrehozása is szükséges, hogy a felhasználó egyszerűen végezhessen módosításokat, egy-egy page az alapvető CRUD műveleteken kívül tartalmazhat más funkciókat is, de elsősorban az adatbázis kezelésére használatos, jelen esetben sincs szükség többre. Egy-egy oldal automatikusan kezeli az egyes táblák közti kapcsolatokat, leegyszerűsítve az adatok kezelését.

2.2.3. Code Unitok

Az MQTT kliens codeuniton kívül szükségünk van még a kívánt funkciónak megfelelő kód megírására.

Az ajtónyitáshoz szükséges codeunit működése nagy vonalakban:

A codeunitban feliratkozunk a táblában létrehozott OnAfterInsert eseményre (jelen esetben csak ezt használjuk mert minden üzenetet egyesével tárolunk, függetlenül attól, hogy melyik topikba érkezett). Így minden MQTT Üzenetek táblába történő íráskor lefut ebben a feliratkozóban megírt kód.

A codeunitban a táblán előzetesen elvégzünk egy szűrést, hogy kizárólag a /dooraccess/readers/ alá tartozó üzeneteket lássuk így bármely eszközön történő belépőkártya használatot látni fogunk.

Amennyiben a topikon belül az eszköz szerepel az adatbázisban pl. reader1 összehasonlítást végzünk, hogy a kártyák táblában található kártya aktivált-e, valamint van-e jogosultsága az adott ajtót kinyitni, amennyiben nem, úgy a felhasználót nem engedjük be, szükség esetén rögzíthetjük egy plusz táblába, hogy melyik ajtót mikor ki nyitotta ki/vagy épp nem nyitotta ki a kártyájával.

Amennyiben a kártya szerepel az adott ajtót nyitó kártyák között, az MQTT könyvtáron keresztül kiküldünk egy üzenetet az ajtónak megfelelő (/dooraccess/doors/ajtóneve) topikba, amelyben beállítjuk az állapotát nyitottra, így a felhasználó be tud lépni az ajtó által védett helyiségbe.

3. Tesztelés

A tesztelés az egyik legfontosabb eleme a szoftverfejlesztésnek, a legfőbb célja a hibák csökkentése, illetve megtalálása. A tesztelés tervezésekor úgy kell megválasztani a tesztelés módját, hogy a lehető legtöbb hibát kiszűrhessük, illetve kijavíthassuk. A kód írása közben a fejlesztő folyamatosan tesztel, eközben nálunk rendszerint egy független fejlesztő teszt codeunitokat ír, amelyek az automatizált tesztelést segítik. Ezen tesztek rendszerint pozitív, illetve negatív teszteket is tartalmaznak, jelen esetben az MQTT protokollon hardverek nélkül is követhetőek az üzenetek, szimulálhatóak a hardverek működései.

Hiba esetén nem kell végignéznünk a teljes forráskódot, mert az ERP rendszer, valamint a Visual Studio (Microsoft, 2020) is rendelkezik Debuggerrel[3], amely megállítja a program futását a töréspontokon, illetve a hibát kiváltó eseményről is információkkal szolgál.

Egy hiba felismerése és megtalálása esetén újbóli tesztekre van szükség, hogy meggyőződjünk a helyes működésről.

Mi általában csak a test codeunitokat szoktuk használni tesztelés céljából, ezeket úgy írjuk meg hogy a lehető legnagyobb részét lefedje a kódnak, valamint ügyfeleink általában rendelkeznek teszt rendszerrel, ahol az elkészült fejlesztéseket az ügyfeleink kipróbálhatják, az esetleg előforduló hibákat jelenthetik mielőtt az éles rendszerbe bekerülne.

4. Összegzés

A projekt alapvetően a saját hobbim kiterjesztése a munkámhoz céllal jött létre(ezt át kell fogalmazni kicsit furán hangzik: A projekt alapvetően azzal a céllal jött létre, hogy a saját hobbimat kiterjeszthessem a munkámra, viszont néhány ügyfél érdeklődése miatt folyamatos fejlesztés alatt áll, hogy később egy univerzálisan elérhető termék jöhessen létre. A legnehezebb ezen univerzális funkciók megtalálása, amely bárki számára egységes előnyöket nyújt, valamint a könnyű bővíthetőség megalkotása volt.

Természetesen előfordulhat, hogy az alaprendszert részben át kell tervezni egy egyéni igény miatt, de ez a rendszerbe integrálható hardverek, illetve szoftverek sokszínűsége miatt néha elkerülhetetlen, a platform által nyújtott lehetőségek tárháza gyakorlatilag végtelen.

Az egyes cégeknél dolgozóknak nagy segítség, hogy egyetlen rendszer használatát szükséges elsajátítaniuk a munkavégzésükhöz, és a munkakörüknek megfelelően azokhoz a modulokhoz férnek hozzá, amikhez jogosultságuk van. A külső rendszerek mély integrációjával egységes az egységes kezelőfelület mellett rugalmasan fejleszthető rendszert is kapunk, ami az ügyfél igényeinek megfelelően átalakítható, és személyre szabható.

Felhasznált szoftverek

Microsoft (2020). Microsoft Dynamics Business Central 14.0 [Online] https://dynamics.microsoft.com/en-us/business-central/overview/ (2020.05.10)

[3] Forráskód elemző és hibakereső szoftver

Microsoft (2020). Microsoft Visual Studio Code [Online] https://code.visualstudio.com/ (2020.05.10)

Eclipse Mosquitto (2020). MQTT Broker 1.6.9 [Online] https://mosquitto.org/ (2020.05.10)

Thomas Nordquist (2020). MQTT Explorer 0.4.0-beta [Online] http://mqtt-explorer.com/ (2020.05.10)

Paolo Patierno (2015). M2MQTT Client 4.3.0 [Online] https://www.nuget.org/packages/M2Mqtt/ (2020.05.10)

Rövid szakmai életrajz

Porteleki Péter szoftverfejlesztő munkakörben dolgozik a Multisoft Számítástechnikai Kft.-nél. Felsőfokú tanulmányait a Dunaújvárosi Egyetem, mérnökinformatikus BSc képzésén, szoftverfejlesztés specializáción szerezte meg. Érdeklődési területe a programozás, gitározás.

Gamification vs Game Addiction

Gábor Kovács

Bethlen Gábor Technikum, 1157 Budapest XV., Árendás köz. 8, Hungary, gabor.kovacs@t-online.hu

Abstract

Gaming habits can be motivating in certain situations and to some extent, and can even have a positive effect on performance, but can also be a negative factor in certain situations. The article summarizes the role of gaming, game-based learning, and gEducation in education by contrasting the issue of game addiction, the probable causes of its development, and some of the symptoms of addiction. This draws attention to the fact that gamified learning is much more purposeful, active and educational for students, however, excessive game addiction can have disadvantages that can greatly impair a child's development, behavior and socialization.

Keywords: gamification; game addiction; z-generation

Játékosítás vs játékfüggőség

Kovács Gábor

Bethlen Gábor Technikum, 1157 Budapest XV., Árendás köz. 8, Magyarország, gabor.kovacs@t-online.hu

Absztrakt

A játékszokások bizonyos helyzetekben és mértékben lehetnek motiválók, és akár pozitívan is hathatnak a teljesítményre, azonban bizonyos helyzetekben és mértékben negatív tényezőként is jelentkezhetnek. A cikk a játékosítás, a game-based learning és a gEducation oktatásban betöltött szerepét foglalja össze azonban ezzel szembe állítva, összefüggésbe hozva a játékfüggőség kérdésével, a kialakulás vélhető okait és a függőség egyes tüneteit. Ezzel felhívva a figyelmet arra, hogy a játékosított tanulás sokkal célravezetőbb, aktívabb, műveltetőbb a diákok számára, azonban a túlzott játékfüggőség olyan hátrányokat hordozhat, amely nagyban ronthatja egy gyermek fejlődését, viselkedését, szocializációját.

Kulcsszavak: játékosítás; gamification; játékfüggőség; z-generáció

1. Bevezető

A játékszokások bizonyos helyzetekben és mértékben lehetnek motiválók, és akár pozitívan is hathatnak a teljesítményre, azonban bizonyos helyzetekben és mértékben negatív tényezőként is jelentkezhetnek (Balogh, 2019). Az évek során sok olyan tanulóval találkoztam, akiknek a szabadidejét a mindennapokban elsősorban a különböző platformokon futó játékokkal történő játszás tette ki. Jelen cikk a játékelmélet szakirodalmi hátterének feltérképezésén túl a játékfüggőség egyes tényezőit elemzi. A szakirodalmi áttekintés kiegészül a saját tapasztalaton alapuló véleményeimmel is. A cikk a (Kovács, 2020) diplomamunka alapján készült.

2. Játékosítás

Roger Caillois (1. ábra) francia szociológus nevéhez fűződik a játékok legáltalánosabb osztályozása. Az 1958-ban megjelent – „Les Jeux el les Hommes" című – könyvében írt arról, a játékok olyan szinten bonyolult és összetett részét alkotják az emberi tevékenységnek, hogy az egyes játékkatergóriák a valóságban nem fedik le a teljes játékuniverzumot, hanem összekapcsolódhatnak egy-egy játékon belül.

1. ábra Roger Caillois
Forrás: https://tinyurl.com/sj3b6fs

A kategóriából álló rendszer a következő: (Formann, 2017: 96-97)

- Agon. Versengésre épülő játék (például sakk).
- Alea. Szerencsén alapuló játék, ahol a játékos kockáztat (például rulett).
- Mimikri. Utánzáson alapuló játék, ahol a játékos valakit megtestesít (például színház).
- Ilinx. Teljes átélésre épülő játék (például hullámvasút).

A szociológus munkásságának egyik pontja, hogy ő fogalmazta meg szocioantropológiai álláspontból elkülönítve a játszás két dimenzióját (Formann, 2017: 96-97).

a. Play (paidia)

A gyermeki léthez kötődő, szabad, spontán játékot jelenti célok és kötött szabályok nélkül. A játékosnak kötetlen mozgástere van, fejleszti a gondolkodását, hiszen szerepel benne például a keresés, a kutatás, a felismerés, a felfedezés vagy a kísérletezés. A szabad játék lényege, hogy magáért a tevékenységért van, továbbá feloldja az esetleges szorongást és félelmet, illetve levezeti a túlterjedő energiákat.

b. Game (ludus)

Irányított és szabályoknak alávetett játékot jelent. Valamilyen cél érdekében jön létre, és eredménye számszerűsíthető. A játék során a játékosnak egy előre meghatározott pályán kell végig mennie, ami olyan választási lehetőségekkel van kikövezve, melyek következményeiből születik meg a játék eredménye. A játék konfliktusokkal tűzdelt, és ezek a játékosokat versenyzésre és problémamegoldásra ösztönzik.

A francia kutató a fent említetteken kívül kísérletet tett arra, hogy leírja az egyes játékok ismérveit és kritériumait.

Ezek a következők: (Formann, 2017: 99)

- Szabad cselekvés, azaz játszani nem kötelező.
- Elkülönülés, azaz a játéknak az idő és a tér szab határt.
- Bizonytalanság, azaz a játék végső kimenetelét nem lehet előre látni.
- Improduktivitás, azaz a játék nem állít elő javakat.
- Szabályozottság, azaz a játék hatálytalanítja az élet törvényeit.
- Nem létező valóság, azaz a játék a valós élethez képest valótlan tudatot hoz létre.

„A játék nem más, mint örömszerzés céljából különböző helyzetek és szerepek szabadon történő, szórakoztató felfedezése és kipróbálása, a szabályok korlátai és a véletlen eseményei között. A játéknak hat olyan kritériuma van, amelyből ha már egy nem teljesül, akkor az adott tevékenység nem számít játéknak.

1. Az örömszerzés célja alapvető feltétele a játéknak, e motiváció nélkül az adott tevékenység már nem játék, hanem inkább valamilyen képességfejlesztő aktivitás lesz.

2. A szabadon, szabad akaratból, saját döntésből történő játékos tevékenység egy másik alapfeltétele a játéknak, ellenkező esetben ez nem játék, hanem olyan munka, feladat, amely külső nyomásra, a kényszer erejével jön létre.

3. A játéknak szórakoztatónak és öncélúnak kell lennie.

4. A játék cselekménye és elsődleges funkciója a különböző helyzetek és szerepek felfedezése és kipróbálása. A játék igazi ereje abban rejlik, hogy az ember nem valós […] közegben, következmények nélkül próbálkozhat, kísérletezhet.

5. Egy játéknak a valós élet szempontjából mindig következmények nélkülinek kell lennie. Ez biztosítja ugyanis azt, hogy a játékos valóban ki merjen próbálni különböző helyzeteket, bátran kísérletezzen, és félelem nélkül, felszabadultan merüljön bele az egész játékba.

6. *A játékok világának talán legfontosabb szabálya, hogy vannak szabályai (Damsa 2014).*

Minden játék legismeretlenebb és talán legérdekesebb eleme a véletlen és a szerencse tényezője, […] jelentős szerepet töltenek be a játékok világában." (Formann, 2017: 99-101)

A játékosítás kifejezés közismerté válása, továbbá a játékosított rendszerek elterjedése 2011-hez köthető. A nemzetközi szintű piackutató és piacelemző cégek észlelték a jelenséget, és egymás után jelentették meg előrejelzéseiket a játékosítás jövőjéről. Ennek köszönhetően a játékosítás világviszonylatban jegyzett jelenség lett.

A játékosítás fogalomköre egy brit játékfejlesztő, Nick Pelling (2. ábra) nevéhez köthető. Ő használta először 2002-ben ezt a kifejezést (Formann, 2017: 105), mely az elektronikus eszközök játékszerű felhasználói felületekkel való felgyorsítását és élvezhetőségét reprezentálta (ennek ellenére a játékosítás nincs digitális technológia használathoz kötve). A gyakorlatban tanácsadóként működött közre játékszerű elektronikus eszközök tervezése terén.

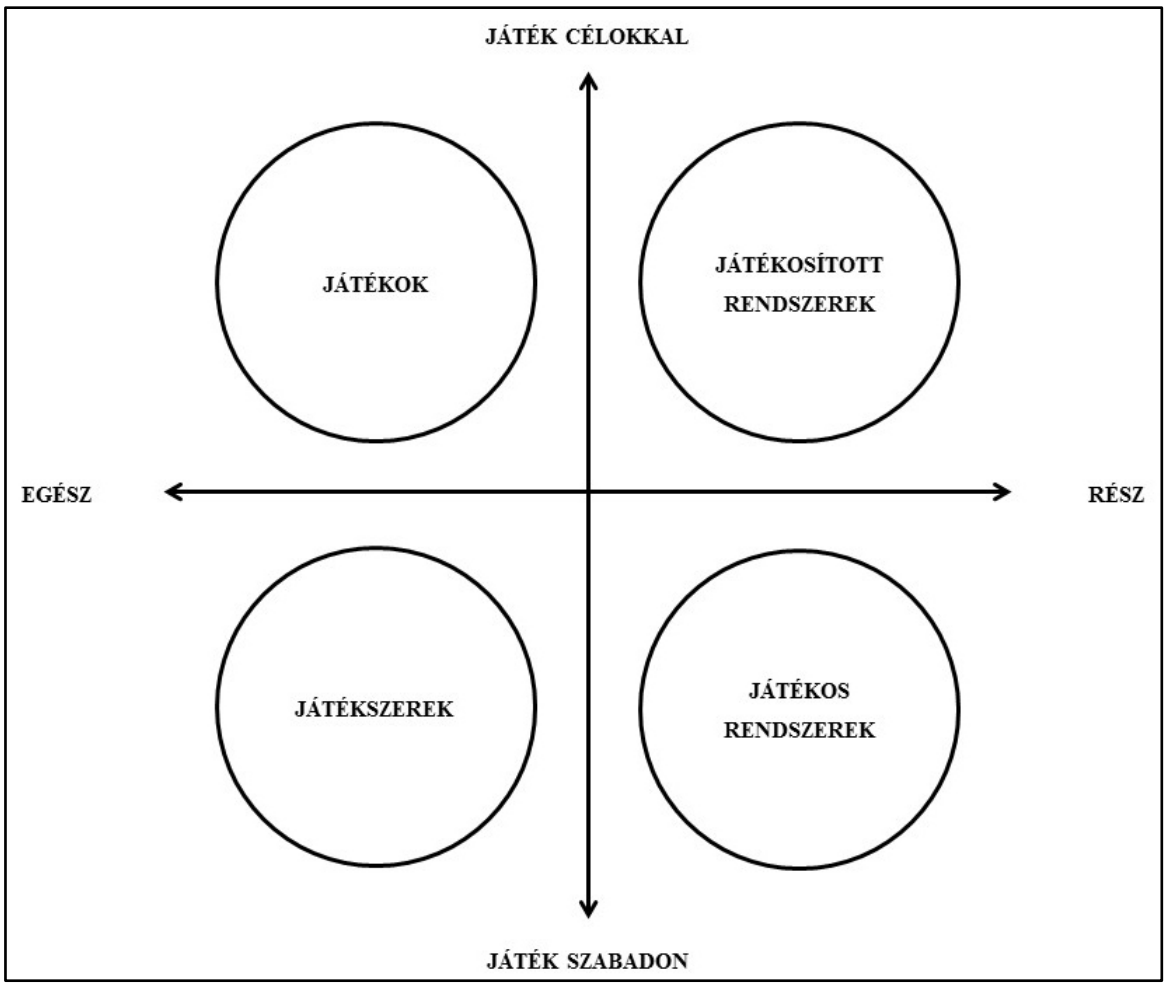
2. ábra Nick Pelling

Forrás: https://tinyurl.com/qpn365m

A kifejezés a 2010-ben vált széles körben ismertté Jesse Schell és Jane McGonigal előadásai során (Formann, 2017: 106). Az első játékosítás témájú konferenciát 2011-ben rendezték, melynek San Francisco adott otthont. A konferencia célja az volt, hogy a téma képviselőit megismertessék egymással, és ezen keresztül a játékosítás beépüljön a köztudatba.

„A gamification a játékélményhez szükséges játékelemek, játékmechanizmusok és játékdinamikák alkalmazását jelenti az élet – játékon kívüli – területein azzal a céllal, hogy az adott folyamatokat érdekesebbé és hatékonyabbá tegye. Burke (2014) megfogalmazásában is jól látszódott, hogy a gamifikáció kifejezést sokan a digitális eszközökkel végzett játékosítás vonatkozásában használják, miközben számos offline környezetben megvalósuló gamifikáció is létezik. Gondoljunk többek között a szerepjátékok eszköztárával történő játékosításra." (Formann, 2017: 111)

Sebastian Deterding és csoportja 2011-ben meghatározta a játékosítás fogalmát, mely a mai napig a legelfogadottabb definíciónak számít. Kidolgoztak egy olyan modellt (3. ábra), mely kétdimenziós rendszerbe helyezi a játékosítás fogalmait (Formann, 2017: 113).



3. ábra Deterding modellje

Forrás: Formann, 2017: 114 alapján szerkesztve

Az ábráról az alábbiak olvashatók le:

- Játékszerek (toys). Funkciója öncélú, célja a szabad szórakozás.
- Játékos rendszerek (playful design). Funkciója öncélú, kötött szabályok alapján történik.
- Játékok (games). Funkciója a játékon kívüli eredmény elérése, célja a tanulás.
- Játékosított rendszerek (játékosítás). Funkciója a játékon kívüli eredmény elérése, célja a felhasználó motivációjának biztosítása.

Véleményem szerint a játékosítás jó eredménnyel alkalmazható az élet különböző területein, ugyanis ezek a módszerek pozitív hatásokat eredményezhetnek. Kiváló példa lehet erre az oktatás, hiszen az elmúlt évek során az információs technikai forradalom a tanárokat és az oktatási intézményeket is kihívások elé állították. Gondoljunk például arra, hogy a diákok és a tanárok digitális tudásszintje sok esetben eltér, ami egyfajta szakadék kialakulásához vezethet.

Az oktatás világában a komoly játékok és a játékosított rendszerek két különböző kategóriát képeznek, melyek ismertetését az alábbiakban mutatom be (Formann, 2017: 127-130).

a. Játékalapú tanulás (game-based learning)

Elsősorban a komoly játékok területeit képviseli, mivel a játék fontos szerepet tölt be a pszichológiai fejlődésben. A digitális korban felnövő generációk fejlesztéséhez evidens lehet az ilyen jellegű tanulás alkalmazása. Olyan programok, weboldalak tartoznak ebbe a csoportba, melyek használata során a tanuló úgy érzi, hogy játszik, miközben valójában tudását bővíti.

b. Játékosított tanulás (gEducation)

A számítógépes játékok megjelenésével kezdték el kutatni a játékosított tanulást. Az oktatási környezetben megjelenő projektek lehetnek mikro- vagy makroszintűek. Előbbi eseténben a tanár a saját óráit játékosítja, még utóbbi során az egész rendszer átjárja a játékosítás. Természetesen a játékosított tanulás esetén pedagógiai szemléletváltás szükséges.

3. Játékfüggőség

Hétköznapi szóhasználatban a függőség szót ragaszkodás, hozzászokást jelent. Magának a jelenségnek nincs önmagában pozitív vagy negatív értéke. Amennyiben a függőségbe való eljutás sérül, akkor szenvedélybetegségek (addikciók) és kóros állapotok (autisztikus magtartás) alakulhatnak ki (Wikipédia, 2020).

A szenvedélybetegségeket kétféle csoportba soroljuk: (Balogh, 2019)

- Kémiai addikció. Ide sorolható az alkohol-, a drog-, a nikotin- és a gyógyszerfüggőség.
- Viselkedésre ható addikció. Ide sorolható a játékszenvedély, internet- és játékfüggőség, munkamánia, szex- és pornográfia függőség – továbbá ebbe a csoportba tartoznak a különböző rögeszmék (vásárlási-, lopási- és hazudozási mánia), evéskényszer, anorexia, társfüggés.

A számítógép- és a játékfüggőség nemre- és életkorra való tekintet nélkül bárkinél szinte bármikor kialakulhat.

A kialakulás okai széles skálán mozognak: (Balogh, 2019)

- Genetikai hajlam.
- Családi hajlam.
- Társadalmi és környezeti hatások.
- Gyermekkori feldolgozatlan traumák.
- Felnőttkori krízisek.
- Életkori változások és váltások.

A gyermekeket leginkább a számítógép függőség veszélyezteti (4. ábra), de ma már nem csak a számítógépek, hanem a táblagépek, játékkonzolok és okostelefonok túlzott használata is függőséget okozhat. Tapasztalataim szerint a függőség valójában egy segélykiáltás a gyermek részéről, hogy érzelmi szempontból elhagyottnak érzi magát, úgy véli, valamit nem kap meg és ezt a hiányt akarja pótolni. Sajnos a függőségben élő gyermekek nincsenek tisztában a cselekedeteik és a lelki állapotuk összefüggésével.

4. ábra A számítógépfüggőség egyik formája (Szabó László Róbert karikatúrája)
Forrás: https://tinyurl.com/vzlnf3v

Eddigi sokéves tapasztalataim szerint a függőség tünetei a gyermek részéről:

- Sok időt képes eltölteni a számítógépe előtt, és kevésbé lesz együttműködő.
- Elhanyagolja a családját, érzelmileg instabil lesz, és agresszívvá válik.
- A tanulmányi eredménye romlik, és elvonási tünetek jelentkeznek nála.
- Megfeledkezik alapvető egészségügyi szükségleteiről.

Azon gyermek, aki a virtuális világban találja meg a számításait, annak társas kapcsolatai megváltoznak, szocializációs nehézségei lesznek a való világban, befelé fordul és csak a virtuális társaival találja meg az összhangot.

4. Összefoglalás

Véleményem szerint a játékosítás jól használható a különböző tanórákon. A Z generáció tagjai számára a frontális oktatás nehezen kivitelezhető, számukra a játékosított tanulás sokkal célravezetőbb, hiszen ha aktív résztvevőként bevonjuk őket a tanóra folyamatába, azzal elérhető, hogy nagyobb kedvvel tanulják az adott tárgyat. Azonban a túlzott játékfüggőség olyan hátrányokat hordoz, amely nagyban ronthatja egy gyermek fejlődését, viselkedését, szocializációját. A játékfüggőség tehát lehet káros, amit meg kell előzni, és ebben fontos szerepet kap a szülői minta, kommunikáció a gyerekkel, következetesség, az alternatív tevékenység, mint például a természet vagy akár pszichológusi segítség (Gősi, 2016). Elmondható tehát, hogy fontos az ekvivalens gyermek-szülő partnerkapcsolat, továbbá a gyermeknek éreznie kell, hogy a szülő a javát akarja.

Mivel a játékosítás nagyon jól használható az oktatásban, készítettem egy szófelhőt (5. ábra), melyben feltűntettem néhány fontos fogalmat. A későbbiekben a pedagógiai munkámban egyre több helyen kívánom alkalmazni a játékosítást a tanóráim során. A szakirodalmat böngészve az is világossá vált, hogy az üzleti életben is egyre nagyobb szerepet kap a téma.

5. ábra Összefoglaló szófelhő

Irodalomjegyzék

Balogh Mária (2019). Van-e kiút a mindennapi függőségek fogságából?, Webbeteg.hu, Debrecen, 2019. Retrieved from: https://tinyurl.com/yckjpf4u (utoljára megtekintve: 2020.04.25.)

Formann Richárd (2017): Játékoslét – A gamifikáció világa. Typotex, Budapest.

Gősi Rozi (2016). Tabletfüggő gyerekek – Néztem, ahogy a párnának vágja a készüléket. NLC, Budapest. Retrieved from: https://tinyurl.com/v93387h (utoljára megtekintve: 2020.01.12.)

Kovács Gábor (2020): A kilencedik osztályos szakgimnáziumi tanulók informatikai tudása és a számítógépes játékszokásaik, diplomamunka, Budapesti Műszaki és Gazdaságtudományi Egyetem.

Wikipédia (2020) Függőség. Retrieved from: https://tinyurl.com/yczc3z7n (utoljára megtekintve: 2020.04.25.)

Rövid szakmai életrajz

Kovács Gábor 1998 óta informatika szakos tanárként dolgozik. Az elmúlt években az alap- és középiskolai oktatás mellett a felnőttképzésben is tevékenykedett, az összes egykori- és jelenlegi iskolatípusban tanított (általános iskola, szakmunkásképző intézet, szakközépiskola, szakgimnázium, technikum, gimnázium, szakképző iskola). Számos állami- és magánkézben levő felnőttképző tanfolyamon adta át tudását különböző korosztálynak. Felsőfokú tanulmányait a Gábor Dénes Főiskolán, a Debreceni Egyetem Műszaki Főiskolai Karán, illetve a Budapest Műszaki és Gazdaságtudományi Egyetem Mérnöktanári mester szakán szerezte (ez utóbbit kitüntetéses jeles – summa cum laude – eredménnyel). Érdeklődési területe a fotózás, a videózás és a zene.

Security perimeter of school networks

János Csordás

Szentistvántelepi Általános Iskola, Martinovics u. 9., Budakalász, 2011, Hungary,
csordas.janos@szentistvantelepi-iskola.hu

Abstract

Perimeter security of IT systems is becoming more complex, more expensive, and next-generation firewalls are in most cases unavailable to some institutions. The article is about school security perimeter. I will cover the possibilities provided by open source solutions, the functions and shortcomings of the available environments, and describe how perimeter security can be implemented with the available tools. The article highlights information security vulnerabilities and suggests how school administrators can reduce risks.

Keywords: security perimeter; next-generation firewall; open source solutions; cybercrime; HuEDU; OpenLab

Az iskolai hálózatok határvédelme

Csordás János

Szentistvántelepi Általános Iskola, 2011 Budakalász, Martinovics u. 9.
csordas.janos@szentistvantelepi-iskola.hu

Absztrakt

Az informatikai rendszerek határvédelme egyre komolyabb kihívásokat jelent, anyagi okokból az újgenerációs tűzfalak a legtöbb esetben elérhetetlenek egyes intézmények számára. A cikk a határvédelem lehetőségeit járja körül az iskolák tekintetében. Kitérek a nyílt forráskódú megoldások által biztosított lehetőségekre, a rendelkezésre álló környezetek funkcióira, hiányosságaira, körüljárom azt a témát, hogy miképpen lehet a határvédelmet megvalósítani a rendelkezésre álló eszközökkel. A cikk az információbiztonsági hiányosságokra kíván rámutatni, javaslatot tesz arra, hogy az iskolák rendszergazdái hogyan csökkenthetik a kockázatokat.

Kulcsszavak: határvédelem; újgenerációs tűzfalak; nyílt forráskódú rendszerek; kiberbűnözés; HuEDU; OpenLab

1. Bevezető

Egyre gyorsabban változó világunkban az informatika egyre jelentősebb kihívás elé állítja az intézményeket. A kiberbűnözés valóságos iparággá vált, a szervezett online bűnözés visszaszorításához egyre nagyobb erőfeszítésekre van szükség.

Az Europol Európai Kiberbűnözői Központja (EC3) minden évben közzéteszi az internetes szervezett bűnözéssel kapcsolatos fenyegetések értékelését (IOCTA) és kiemelt stratégiai jelentését. Az IOCTA kulcsfontosságú ajánlásokat fogalmaz meg a bűnüldöző szerveknek, a politikai döntéshozóknak és szabályozóknak annak érdekében, hogy hatékony és összehangolt

módon reagálhassanak az EU kormányait, vállalkozásait és polgárait érintő számítógépes bűnözésre.

A legfrissebb, 2019-es IOCTA-jelentés[1] (Internet Organised Crime Threat Assessment 2019) szerint a kiberbűnözés elleni harc legfontosabb prioritásai:

- kiberbűncselekmények
- gyermekek szexuális zaklatása
- fizetési csalás

elleni harc. Az első prioritásként megjelölt cél egy gyűjtőfogalom, amely minden, változatos és akár szolgáltatásként[2] bárki számára igénybe vehető „High-tech" bűncselekményt magában foglal[3].

A kiberbűnözés elleni harc komoly kihívásokat jelent, a védelem feltételinek megteremtése nem elhanyagolható költségeket ró a szervezetek költségvetésére. A legnagyobb veszélyben természetesen azok az intézmények vannak, amelyeknek nincsenek megfelelő forrásaik a határvédelem feltételeinek megteremtésére. A kórházak mellett a közoktatási intézmények a kiberbűncselekményeknek leginkább kitett szervezetek.

2. Információbiztonság a közszférában

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról rendelkezik (továbbiakban Ibtv.). A jogszabály a nemzet érdekében kiemelten fontos a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon védelme érdekében fogalmaz meg rendelkezéseket, mivel *„Társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme."*[4]

Az információbiztonsággal kapcsolatos operatív feladatok elvégzésére a Nemzetbiztonsági Szakszolgálat (NBSZ) került kijelölésre, a szervezeten belül 2015-ben került létrehozásra a Nemzeti Kibervédelmi Intézet (NKI). Az NKI ellátja:

[1] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2020. 04. 18.)
[2] https://www.exploit-db.com/ (2020. 04. 18.)
[3] https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime (2020. 04. 18.)
[4] https://net.jogtar.hu/jogszabaly?docid=a1300050.tv (2020. 04. 18.)

- *„az eseménykezelési feladatokat a létfontosságú információs rendszerek és rendszerelemek, valamint*
- *az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvényben meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében az eseménykezelési, valamint a hatósági felügyeletet."*[5]

3. A NIIF program

A Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program a magyarországi kutatói és oktatási hálózat fejlesztése és működtetése érdekében jött létre. A program a teljes magyarországi kutatási, oktatási és közgyűjteményi közösség számára biztosít országos nagysebességű számítógép-hálózati infrastruktúrát, valamint erre épülő szolgáltatásokat.

A program céljainak megvalósítása érdekében életre hívott intézet 2016-ban beolvadt a Kormányzati Informatikai Fejlesztési Ügynökségbe (KIFÜ).[6]

4. Határvédelem az iskolákban

4.1. Az iskolai végpontok védelme

2015 szeptemberétől az iskolai végpontokon a Zone-based Policy Firewall került bevezetésre, az eszközöket a KIFÜ felügyeli. Az új tűzfalon a következő zónák kerültek kialakítása:

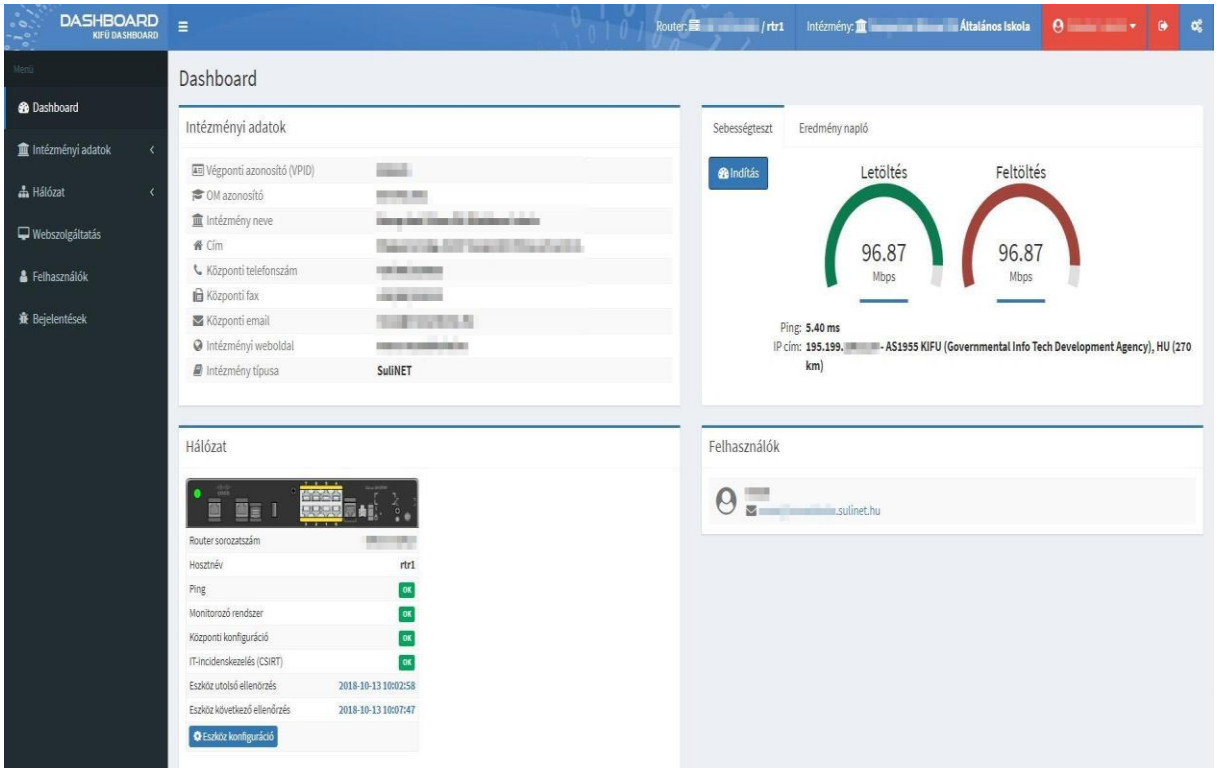
[5] https://nki.gov.hu/intezet/tartalom/magunkrol/ (2020. 04. 18.)

[6] https://kifu.gov.hu/content/kif%C3%BC-lett-jogut%C3%B3dja-nemzeti-inform%C3%A1ci%C3%B3s-infrastrukt%C3%BAra-fejleszt%C3%A9si-int%C3%A9zetnek%C2%A0 (2020. 04. 18)

- Privát (Privát + Wifi)
- Védett
- Publikus
- Internet

Az első zóna a Privát és a Wifi szegmenst együtt kezeli. A Wifi szegmens az iskolákban megvalósított eduroam szolgáltatást teszi lehetővé[7], mely a felhasználókat Radius szerverrel, MS-CHAPv2 EAP-módszerrel autentikálja, így biztonságos hálózati hozzáférést biztosít az arra jogosultaknak. Nevéből adódóan a Privát, valamint a Védett szegmens eszközei privát IP címekkel konfigurálhatók statikusan, vagy a router-en beállított DHCP szolgáltatás segítségével. A Publikus zónában a 195.199.0.0/29-es tartomány használható általában. Ezeket a publikus IPv4 címeket kizárólag manuálisan lehet beállítani.

A tűzfalon konfigurált zónák, wifi felhasználók és szolgáltatások a KIFÜ dashboard-on, webes felületen kezelhetők.



1. ábra - A Sulinet Dashboard felülete[8]

[7] http://sulinet.niif.hu/eduroam (2020. 04. 25.)

[8] A kép forrása: https://sulinet.niif.hu/sites/sulinet.niif.hu/files/dashboard_foablak.jpg (2020. 04. 28.)

A zónákra vonatkozó szűrési szabályok listája a NIIF honlapján megtekinthető,[9] mivel azonban alapvetően nem a tűzfal beállításainak elemzése és értékelése a cikk témája, erre a kérdésre a nem térek ki. Információbiztonsági szempontból itt csupán annyit említenék meg, hogy a zóna alapú tűzfal állapot követő, így a forgalomirányító a csomagok információit miután kiolvassa, a válaszcsomagokat akkor is visszaengedi, ha visszafelé minden tiltva van. A PPTP illetve az IPSEC VPN-hez az ESP, GRE protokollokat a router vizsgálat nélkül engedi át, viszont csak az egyik irányba, így a forgalmat mindkét irányba engedélyezni kell, azaz a TCP 1723-as portot az internet felől ki kell nyitni. Továbbá megjegyzendő, hogy a PPTP VPN csupán a publikus szegmensből engedélyezett.

4.2. Opcionális határvédelem

A fentiekben említett forgalomszabályozás egységesen került bevezetésre az egyes iskolákban. Sajnos a 21. században a szervezeti infrastruktúra védelmére rendelkezésre bocsátott eszközök, amelyek kizárólag ACL szabályok segítségével engedik vagy tiltják a forgalmat komplex védelmet egyáltalán nem biztosíthatnak, sem a behatolás detektálására, sem a támadás elhárítására nem alkalmasak. Emiatt az Ibtv. rendelkezései, amely szerint biztosítani kell a *„kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos" védelmét",* az iskolák esetén egyre kevésbé teljesülhetnek.

A teljesség igénye nélkül az alábbi támadási formákkal szemben védtelenek teljességgel az említett szervezetek:

- adathalászat
- adatszivárogtatás
- csatolmányba rejtett rosszindulatú programok letöltése
- social engineering (szélhámosság)
- célzott támadás
- szolgáltatásmegtagadással járó támadás

Mivel az iskolák rendszergazdái is tisztában vannak a lehetséges veszélyekkel, a védelmet igyekeznek kiterjeszteni, a határvédelmet (általában ingyenes eszközökkel) kiegészíteni. Évekkel ezelőtt a Microsoft Internet Security and Acceleration Server (ISA Server), illetve a

[9] http://sulinet.niif.hu/tuzfal (2020. 04. 28.)

Microsoft Forefront Threat Management Gateway (Forefront TMG) ingyenesen állt rendelkezésre az iskolák számára, segítségükkel grafikus felületen is definiálható szabályokkal, viszonylag egyszerűen volt lehetőség a hálózati forgalom további szűrésére. Sajnos a TMG-vel a Microsoft évekkel ezelőtt kivonult a piacról, 2020. április 14-én a kiterjesztett support is végleg lejárt.

Emiatt egyre több rendszergazda igyekezett a TMG-t más megoldásra cserélni, a Linux disztribúciók a legtöbb helyen, ahol addig korábban egyáltalán nem kaptak szerepet, a Microsoft termékek helyére léptek. Az állami ösztönzők ezt a folyamatot felkarolták, a nyílt forráskódú szoftverek bevezetésének támogatását tűzték ki célként, így közös igényből született meg az OpenEDU és a HuEDU program.

A cikk további részében ezeket a megoldásokat mutatom be.

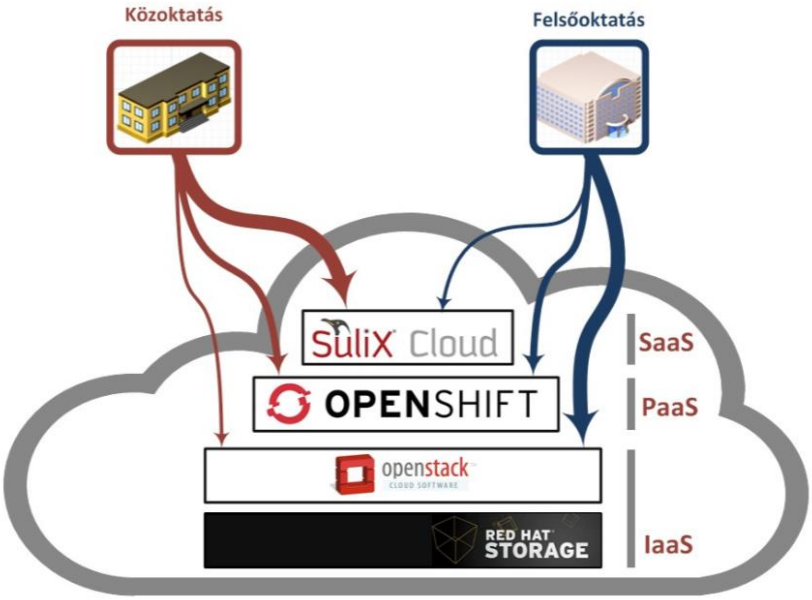
4.3. SuliX és az OpenLab

Az ULX Kft. az OpenEdu program keretében a közoktatást és a felsőoktatást látja el szoftverekkel és támogató szolgáltatásokkal. Szoftverek tekintetében a support-on kívül ez a SuliX Professional Network Edition és a SuliXerver ingyenes biztosítását jelenti. A SuliX disztribúció a Redhat/Fedora EPEL csomagforrásaiból készült. A Network Edition a desktop operációs rendszernek speciális, intézményi használtra szánt szolgáltatásokat tartalmazó verziója. A SuliXerver egy „kulcsrakész” szoftvermegoldás. A SuliXerver az alábbi funkciókat kínálja:

- tanuló- és tanárkezelés
- hozzáférések korlátozása (tanulókra vonatkozik)
- dolgozatírás, érettségi
- SuliX Learning
- webszerver
- biztonsági mentés
- SuliX Active Class (rugalmasan alakítható oktatási környezet)
- fájlszerver
- levelezés
- csoportmunka
- távoli adminisztráció
- több internetkapcsolat kezelése

- tartalomszűrési és tűzfal funkciók. *„A SuliXerver globális és teremszintre leosztott tartalomszűrési valamint tűzfalfunkciókat tartalmaz, amely a tanárok által rendszergazdai beavatkozás nélkül is irányítható.”*
- desktop-ok központi kezelése
- szoftver- és hardverleltár
- cloud integráció
- Active Directory funkció[10]

A SuliX az azt használó intézmények számára skálázható megoldást jelent, a felhő infrastruktúra modellek mindegyikét támogatja.



2. ábra - A SuliX Cloud általános rendszerarchitektúrája[11]

4.4. HuEDU és az OpenLab

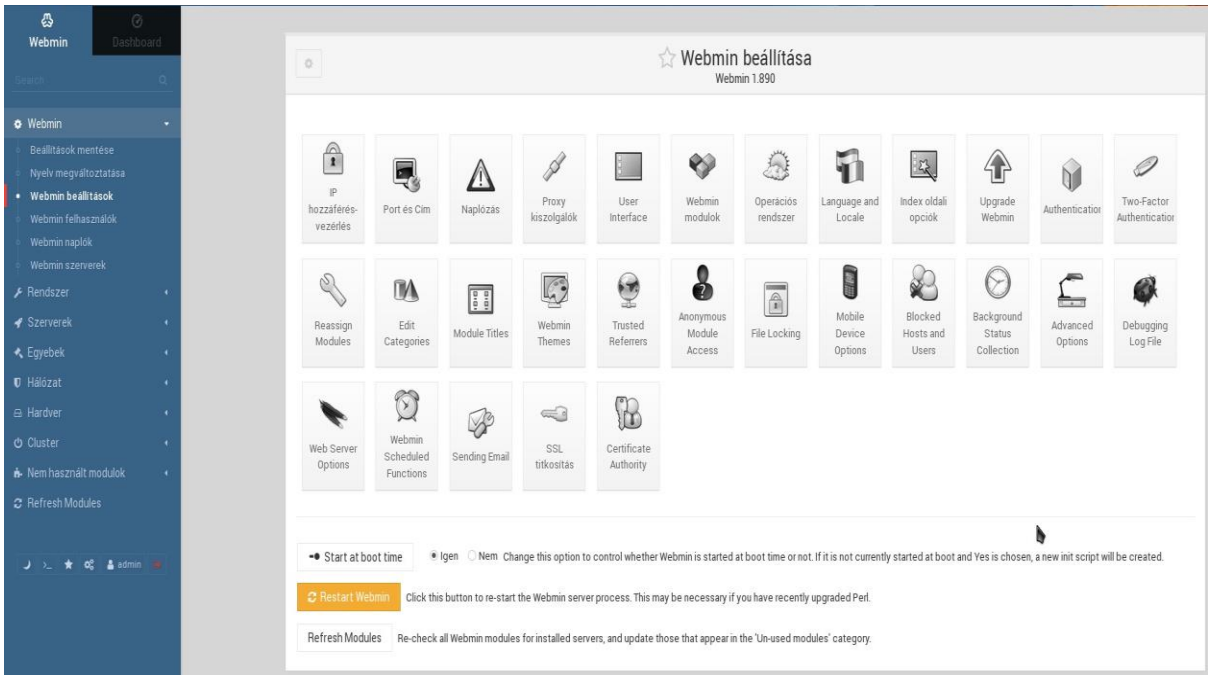
A HuEDU a magyar kormány és a Novell között létrejött megállapodás, amelynek fő célja *„a nyílt forráskódú modellben rejlő lehetőségek kihasználása”*[12]. A HuEDU projekt keretében készült el az openSUSE Linux disztribúció. 2009-től 2012-ig számos felhasználó és oktatási intézmény számára elérhetővé vált az örökös alapinfrastruktúra licenc a program keretében. 2013-ban a kormányzat látva a kezdeményezés sikerét, támogatását kibővítette egy nyílt forráskódú alkalmazáscsomagra, így született meg az OpenLAB. Szoftverek tekintetében az OpenLAB is egy szerver oldali és egy munkaállomás oldali programcsomagból áll. Az

[10] http://www.sulix.hu/ (2020. 04. 28.)
[11] https://docplayer.hu/5146938-Informatikai-celrendszertol-a-komplex-oktatasi-intezmenymenedzsmentig.html (2020. 04. 20.)
[12] https://tisztaszoftver.hu/download/huedu_kozoktatas_flyer.pdf (2020. 04. 20.)

OpenLAB kiszolgáló szintén egy „kulcsrakész” szoftvermegoldás, amely openSUSE alapokon az alábbi funkciókat kínálja:

- egyszerűen kezelhető webes felület az adminisztrátorok és oktatók számára
- Moodle e-learning és tananyag kezelő rendszer
- Integrált laborfelügyelet (Veyon)
- GLPI + FusionInventory hardver és szoftver leltár
- továbbfejlesztett behatolás védelem (fail2ban)
- órai fájlok kezelése
- Postfix/Cyrus/Roundcube levelezőszerver
- hálózati alapszolgáltatások: DNS, DHCP, Tűzfal
- integrált kiszolgáló felügyelet (Webmin)
- Samba4 alapú fájlszolgáltatás
- Samba4 Acitve Directory (teljes értékű tartományvezérlő modern Windows kliensek számára)
- Squid/SquidGuard proxy, hálózati korlátozások[13]

A szerver operációs rendszer GUI-val nem rendelkezik, az igényeknek megfelelő konfigurálás konzolon illetve webes felületen, Webmin-ben valósítható meg.

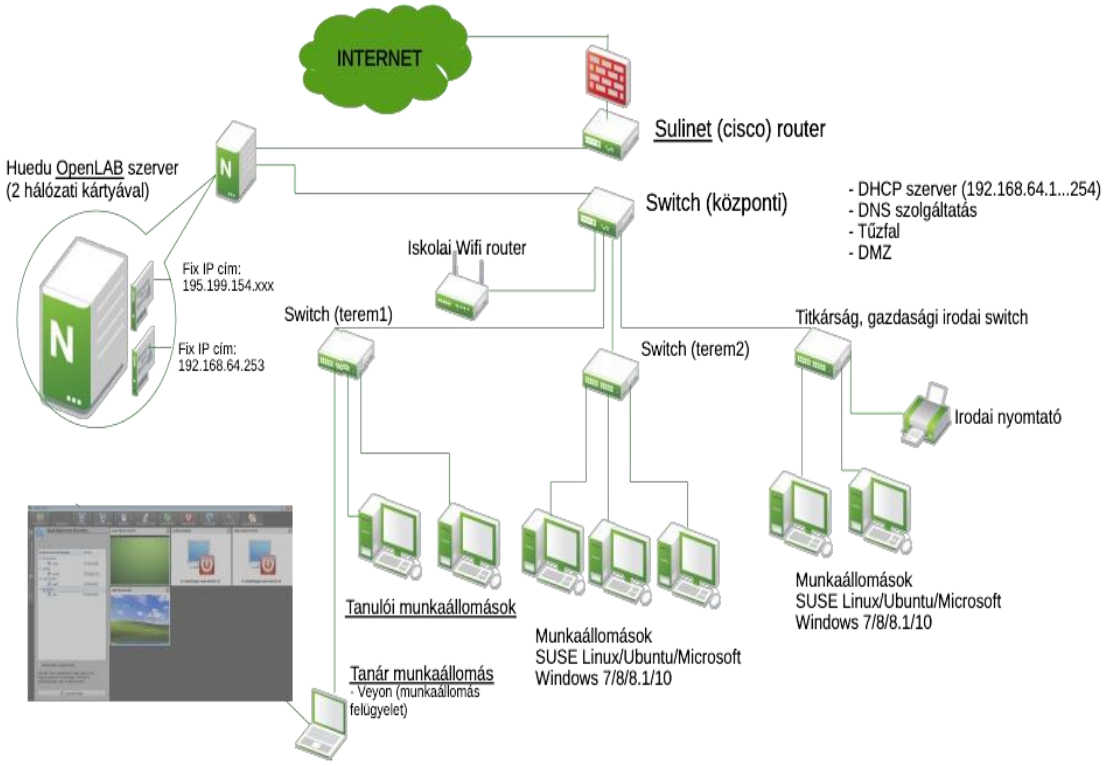


3. ábra - Kiszolgáló adminisztráció az OpenLAB-ban[14]

[13] http://huedu.hu/wp-content/uploads/2019/04/OpenLAB_telepitesi_dokumentacio.pdf (2020. 04. 20.)

[14] A kép forrása: http://huedu.hu/wp-content/uploads/2019/01/OpenLAB_alkalmazasok.pdf (2020. 04. 20.)

Az OpenLAB szervernek a méglévő infrastruktúrába történő integrálására többféle forgatókönyv is létezik, alább annak a megoldásnak a topológiáját mutatom be, amely alkalmas lehet a helyi hálózat szofisztikáltabb védelmének megvalósítására.



4. ábra - Gateway-ként működő OpenLAB kiszolgálóval megvalósított topológia.[15]

5. Újgenerációs tűzfalak

A digitális kor információbiztonsági kihívásainak, így a kiberbiztonság fokozottabb igényeinek megfelelően már évtizedekkel korábban megfogalmazódott az igény a kifinomultabb határvédelem megteremtésére. A drasztikusan növekvő fenyegetésekre válaszképpen született meg a „Next-generation firewall" koncepciója. Az újgenerációs tűzfalak kombinálják a hagyományos tűzfal szerepköröket más hálózati szűrési funkciókkal, így például az alábbiakkal:

- Deep Packet Inspection (DPI)
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- TLS/SSL encrypted traffic inspection
- website filtering

[15] http://huedu.hu/wp-content/uploads/2019/04/OpenLAB_telepitesi_dokumentacio.pdf (2020. 04. 20.)

- QoS management
- antivirus inspection
- identity management (pl. LDAP, RADIUS, Active Directory)

Az újgenerációs eszközök, illetve szoftverek piacán számos gyártó cég terméke fellelhető (pl. CheckPoint, PaloAlto, Cisco, Fortinet).

5.1. IDS/IPS

Az újgenerációs tűzfalak egyik legelterjedtebb funkciója Intrusion Detection Systems (IDS) és/vagy Intrusion Prevention Systems (IPS).

Az IDS elemzi a hálózati forgalmat és detektálja az ismert kibertámadások szignatúráit, naplózza a gyanús eseményeket és támadásokat. Az IPS ezen felül képes beavatkozni, megállítani a behatolási kísérletet[16]. Mindkét rendszer alapvetően cyberthreat adatbázisra támaszkodik, azaz csak ismert támadási formákat képes felismerni, így például egy Zero-day sérülékenység kihasználó exploit-ot – AI funkcionalitás nélkül – sem detektálni, sem blokkolni nem tud. A legtöbb esteben az újgenerációs tűzfalak éppen ezért vannak felvértezve más eszközökkel, rendszerkekkel is.

6. Összegzés

A közoktatási intézmények sajnos nem rendelkeznek megfelelő eszközökkel a megfelelő határvédelem kialakítására, a kereskedelmi forgalomban beszerezhető újgenerációs tűzfalak beszerzésére és üzemeltetésére nincsen lehetőségük. Az elmúlt években a kormányzat a nyílt forráskódú megoldások támogatására helyezte a hangsúlyt, azonban ezek a rendszerek, legyen szó akár az OpenEDU vagy a HuEDU programról csak korlátozottan terjedtek el a magyar iskolákban.

A rendelkezésre bocsátott kiszolgálók tulajdonságait szemügyre véve, egyértelmű, hogy a fejlesztés mindenkori irányát alapvetően az intézmények adminisztrációs feladatainak digitalizálása, modernizálása ihlette, és amennyiben a nyílt forráskódú kiszolgálók valamelyike gateway-ként került vagy kerül bevezetésre valamelyik intézményben, alapvető funkcióit tekintve egy újgenerációs tűzfal feladatait egyáltalán nem láthatja el.

Számos olyan kezdeményezés van azonban, amely lehetőséget biztosít újgenerációs tűzfal „építésére” nyílt forráskódú alapokon. Ilyen például a Snort vagy a Suricata IDS/IPS engine,

[16] https://www.varonis.com/blog/ids-vs-ips/ (2020. 04. 25.)

ezek telepítése és konfigurálása legyen szó akár a SuliX, akár az OpenLAB rendszerről megteremthetné az újgenerációs határvédelem minimális feltételét. Jóllehet ezeknek a rendszereknek az üzemeltetése, monitorozása, a naplóállományok kezelése, feldolgozása, esetlegesen elemzése újabb kihívásokat jelentene az érintett intézményeknek, az automatizált elhárítás lehetősége önmagában jelentősen hozzájárulna az Ibtv.-ben megfogalmazott elvek arányos érvényesüléséhez.

Kétségkívül mindez abból a megfontolásból indul ki, hogy az On-Premises megoldásoknak van és lesz is létjogosultsága, ez pedig ellentmondani látszik annak, hogy a Cloud Computing – szélsőséges esetben a SaaS modell implementálása - egyre nagyobb tért nyer a helyi megoldások rovására. 2020-ben, a COVID-19 krízis következtében az oktatás kényszerű és a váratlan helyzetben központi koncepció nélküli digitalizációja a használatba vett különféle virtuális kollaborációs környezetek révén a felhőbe költöztette az iskolai adminisztráció jelentős részét. Bár kényszer szülte megoldásokról van szó, az oktatás digitalizációja elkerülhetetlen, kollaborációs környezetre szükség van, ez pedig annak a ténynek az elfogadásával is jár, hogy az adatok egy részét az intézményeknek meg kell osztaniuk egy harmadik féllel. Viszont az adminisztratív működéshez szükséges adatok jelentős részének a felhőben való elhelyezését semmi sem indokolja, éppen ezért van szükség a fent részletezett On-Premise megoldásra, lehetőséghez mérten a helyi hálózatok körültekintő határvédelmére.

Irodalomjegyzék

EUROPOL (2019). Internet Organised Crime Threat Assessment (IOCTA) 2019. Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2020. 04. 18)

OFFENSIVE Security (2020). Exploit database. Retrieved from https://www.exploit-db.com/ (2020. 04. 18)

Rövid szakmai életrajz

Csordás János információbiztonsági területen dolgozik a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.-nél. Felsőfokú tanulmányait a Dunaújvárosi Egyetem végezte, rendszerinformatikus oklevelet szerzett. Az információbiztonság területén belül érdeklődési köre alapvetően az adatbiztonsággal kapcsolatos kérdésekre irányul. Gyakorlati feladatain kívül az információbiztonság területén oktatói feladatokat is ellát a közoktatási rendszerben.