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:

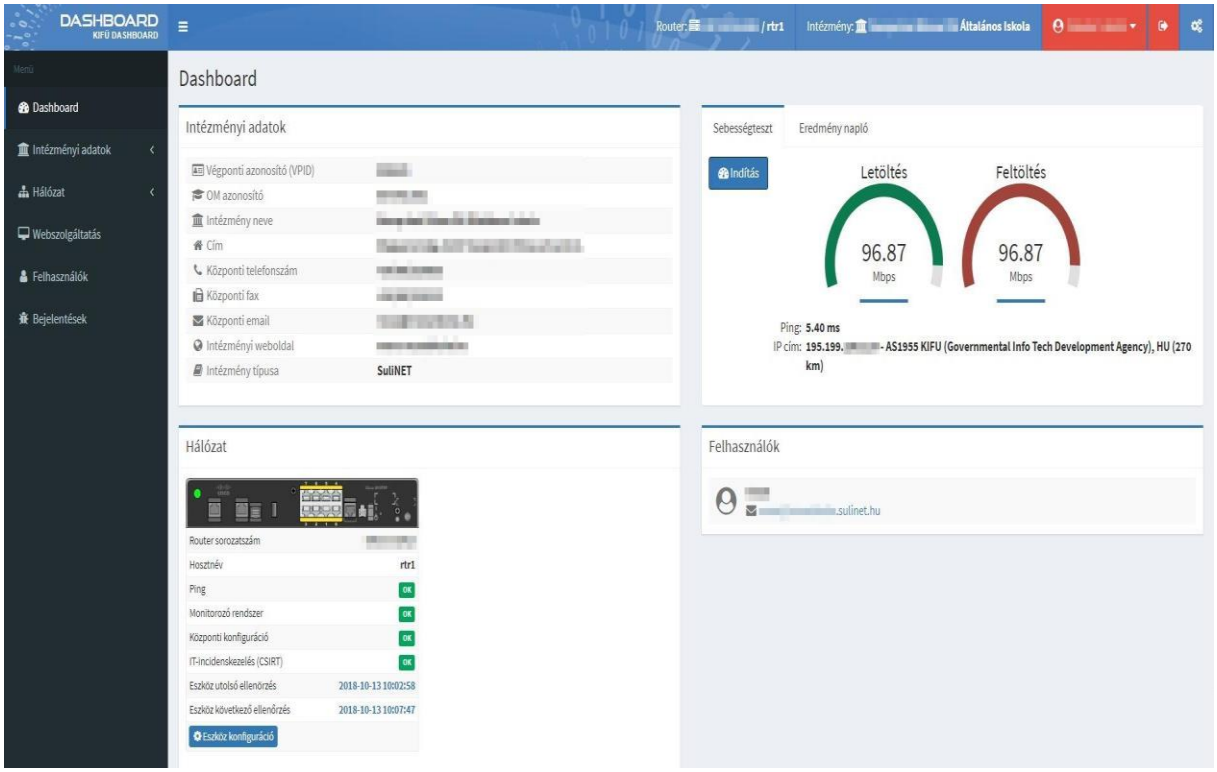
[5] https://nki.gov.hu/intezet/tartalom/magunkrol/ (2020. 04. 18.)

[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.

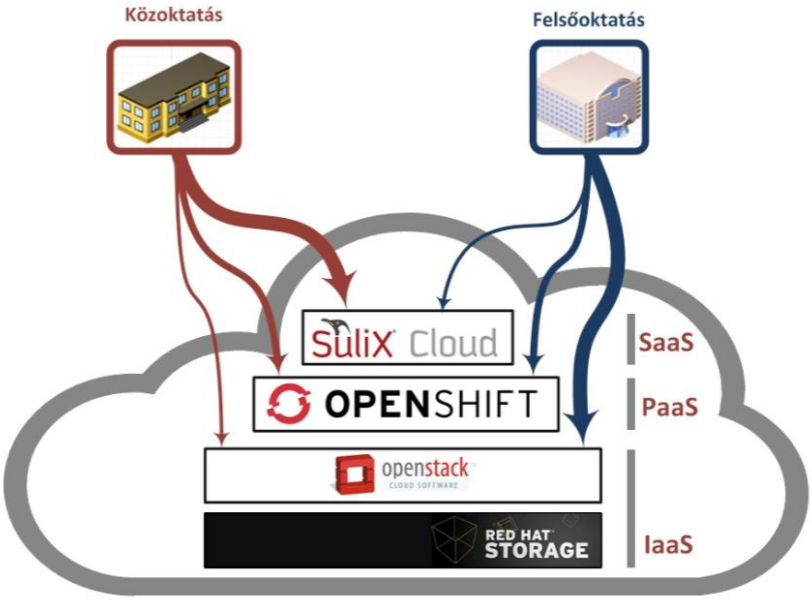
4.3. SuliX és az OpenLab

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

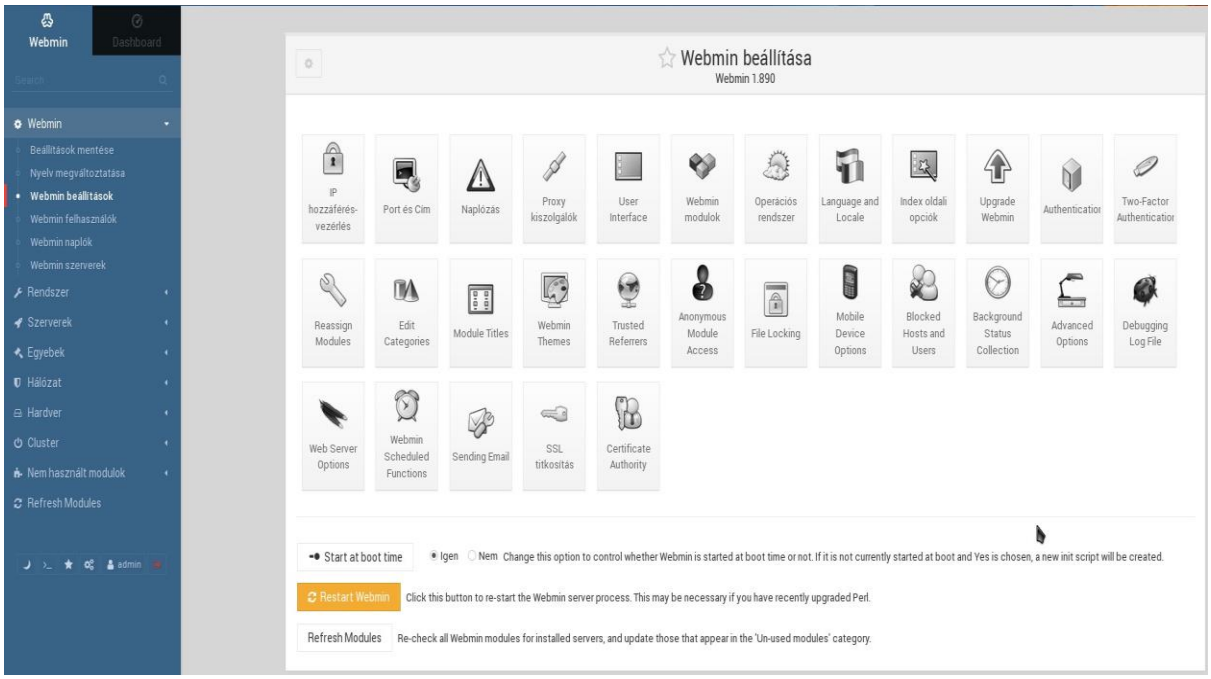
A HuEDU a magyar kormány és a Novell között létrejött megállapodás, amelynek fő célja *„a nyílt forráskódú modellben rejlő lehetőségek kihasználása”*[12]. A HuEDU projekt keretében készült el az openSUSE Linux disztribúció. 2009-től 2012-ig számos felhasználó és oktatási intézmény számára elérhetővé 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.

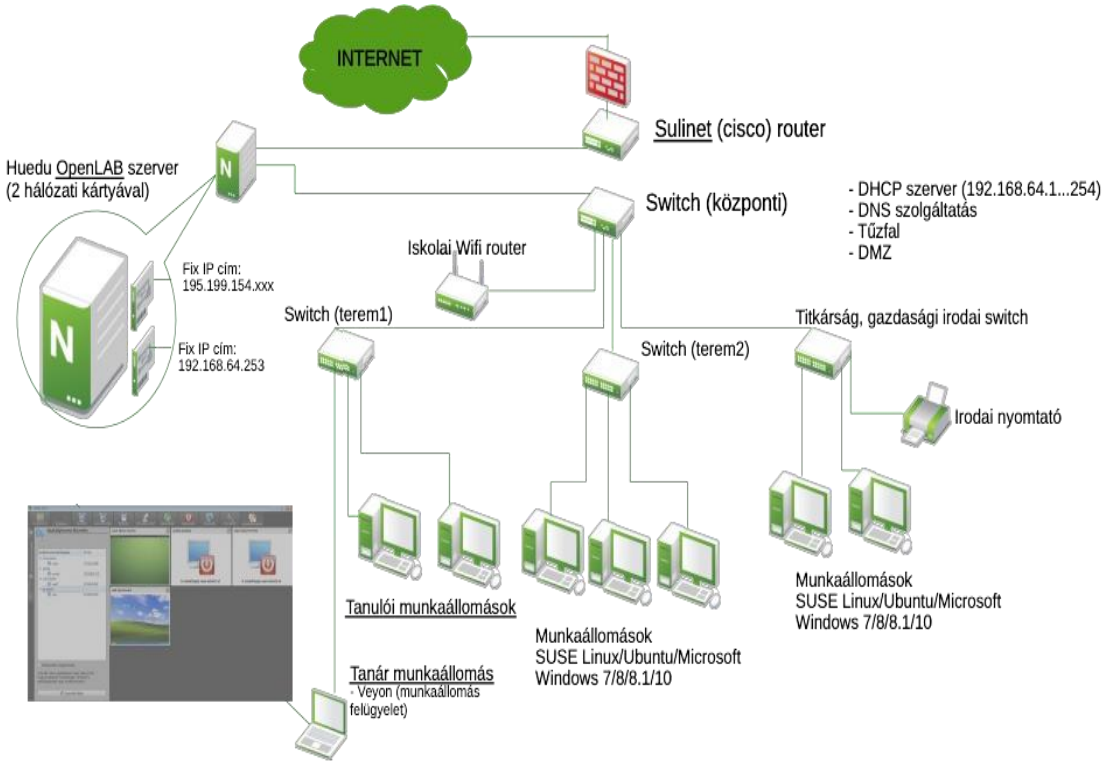


3. ábra - Kiszolgáló adminisztráció az OpenLAB-ban[14]

[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.