ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Járki Dániel**
2023	Hallgató törzskönyvi száma:	**T 008041 FI12904 N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Járki Dániel**
Törzskönyvi száma: T/008041/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Biztonsági megoldások tervezése és integrálása kisvállalati környezetben
Designing and integrating security solutions in small business environment

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens: Laskovics Áron

Beadási határidő: 2022. május 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

A mikro-, kis- és középvállalkozások versenyképességében nagy szerepet játszik a digitális fejlettség szintje, az infokommunikációs képességek megléte. A digitális fejlesztések végrehajtása és szolgáltatások nyújtása előnyt jelent a versenytársakkal szemben, azonban a digitalizációval az üzletmenet folytonosságára nézve újabb kockázatok jelennek meg.
A szakdolgozat célja az infokommunikációs képességekkel együtt járó kockázatok számbavétele és a gazdasági szereplők szempontjából elfogadható mértékűre csökkentése. A dolgozat a kkv szektor igényeit figyelembe véve, költséghatékony megoldások nyújtására koncentrál úgy, mint vezetéknélküli megoldások, távoli erőforrás elérés, valamint üzleti adatok védelme. A feladat során a hallgató tanulmányozza a szektorra jellemző igényeket, majd az iparági ajánlásokat és legjobb gyakorlatokat figyelembe véve megtervezi, implementálja és teszteli a kockázatokat csökkentő rendszert. A feladat megoldása során keletkezett tapasztalatok összegzése után a továbbfejlesztési lehetőségek vizsgálatára is sor kerül.

A dolgozatnak tartalmaznia kell:

- a kkv szektorra jellemző igények vizsgálatát és kockázatelemzését,
- a biztonsági architektúra követelményeinek meghatározását,
- az architektúra egyes elemeihez alkalmazható megoldások összehasonlító elemzését,
- az eszközök kiválasztását az összehasonlító elemzés alapján,
- a választott architektúra és eszközök ismertetését,
- a rendszer implementációját,
- a rendszerrel szemben támasztott követelmények teljesülésének igazolását,
- a fejlesztés során szerzett tapasztalatok összefoglalását,
- a továbbfejlesztési lehetőségek vizsgálatát.

Ph.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * 1. Budapest

.....
Dr. habil. Lovas Róbert
intézetigazgató

A szakdolgozat elévülésének határideje: **2024. május 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott Járki Dániel ([redacted]) hallgató kijelentem, hogy a szakdolgozat / diplomamunka saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban / diplomamunkámban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2022. december 14.

Járki Dániel

.....

hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Neptun Kód: [redacted] Tagozat: NSLEKE

Járki Dániel

Telefon: Levelezési cím (pl.: lakcím): [redacted]

[redacted]

Projektmunka címe magyarul:

Biztonsági Megoldások Tervezése és Kivitelezése Kisvállalati Környezetben

Projektmunka címe angolul:

Design and integrating security solutions in small business environment

Intézményi konzulens: Balázsné Dr. Kail Eszter Külső konzulens: Laskovics Áron

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2021.09.26.	**Státusz megbeszélés követelmények átbeszélése**	Kail
2.	2021.11.18.	**Státusz megbeszélés, további teendők átbeszélése**	Kail
3.	2021.11.16.	**Státusz megbeszélés, további teendők átbeszélése**	Kail
4.	2021.12.14.	**Státusz megbeszélés, további teendők átbeszélése**	Kail

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy:

Kail

.....

Intézményi konzulens

---

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1 BEVEZETÉS

A mikró-, kis- és középvállalkozások versenyképességében nagy szerepet játszik a digitális fejlettség szintje, az infokommunikációs képességek megléte. A vállalkozásoknak a pandémia hatására megváltozott igényekkel lépést tartva meg kell felelniük a piaci elvárásoknak. A digitális fejlesztések végrehajtásából adódó többlet szolgáltatások nyújtása előnyt is jelent a versenytársakkal szemben. Viszont a digitalizációval párhuzamosan az üzletmenet folytonosságára nézve újabb kockázatok jelennek meg.

Szakdolgozatom célja felmérni, hogyan lehet egy vállalkozás digitalizációját megvalósítani az informatikai biztonságra törekedve minimális kiadásokkal. A témaválasztás indoka konkrét felkérésen alapszik. Első lépésként bemutatom a kkv szektor helyzetét hazai és nemzetközi viszonylatban a digitalizáció szempontjából, majd megvizsgálom a digitális térben elkövetett bűncselekmények trendjét. Második lépésben a digitalizációval együtt járó legjellemzőbb veszélyforrásokról készítek kockázatelemzést. A harmadik fejezetben meghatározásra kerülnek a megbízó cég igényei. A következő fejezetben a kockázatelemzés és az üzleti igények alapján, az informatikai biztonságot szem előtt tartva megtervezésre kerül a cég informatikai hálózata az ISO27001 szabvány logikai védelmére vonatkozó fejezet alapján. Ezen célok elérésének megvalósítása érdekében intézkedésként a NIST, CISA, NSA, ISMS legjobb gyakorlatait, ajánlásait alkalmazom. Az architektúra egyes elemeihez alkalmazható megoldások feltérképezésére piackutatást és összehasonlító elemzést végzek kategória, funkcionalitás, költséghatékonyság (licence metodika), továbbfejlesztési/bővítési lehetőségek, üzemeltetési konstrukció/gyártói háttértámogatás, energia hatékonyság eszköz életciklus válogatási irányelvek mentén az ötödik fejezetben. A piackutatást tűzfalra, Wi-Fi csatlakozási pontokra, végpontvédelemre végzem el a költséghatékonyságra törekedve. Az eddigi kutató, elemző, szintetizáló és tervező munka során összegyűjtött információk felhasználásával következő lépés az implementálás. A gyakorlati megvalósítást, konfigurálást képernyőképekkel és hozzájuk tartozó magyarázatokkal mutatom be. Szakdolgozatom végén interjú formájában Bánszki Zsoltot, a 4iG Nyrt. kiberbiztonsági üzletágának igazgatóját kérdezem a hazai kkv szektor digitalizációs helyzetéről, IT biztonságról, valamint ismereteiről a témában jelenre, meglátásait a jövőre vonatkozóan. Zárásként a következtetéseket, továbbfejlesztési lehetőségeket a szakdolgozat megírása során szerzett tapasztalatokat összegzem.

1.1 A kkv szektor pozíciója a gazdaságban

A kis-és középvállalkozásokról (továbbiakban kkv-k) elmondható, hogy nem csak Magyarországon, hanem világszerte fontos gazdasági szereplők és a világgazdaság alakulásában is meghatározó szerepet töltenek be. Az amerikai cégek 99,9%-a sorolható a kisvállalkozások körébe és a lakosság 47,5%-át foglalkoztatják [1]. Németországban az

alkalmazottak 38,8%-a dolgozik kkv-kban és az éves bruttó jövedelem 31,9%-át termelte ki 2018-ban [2]. A magyar gazdaságnak is szerves részét képezik a kis- és középvállalkozások. „ A foglalkoztatottak 71%-ának adnak munkát, miközben a vállalatok által előállított hozzáadott érték 54%-át képviselik. [3]”. Ebből kifolyólag kiemelten fontos, hogy napjaink kihívásaival szembenézve és a nemzetközi trendeket követve a digitális eszközök és megoldások segítségével képesek legyenek az üzleti stabilitás és ellenállóképesség fokozásában.

1.2 A kkv-k és a digitalizáció kapcsolata

A digitalizálás emberek és dolgok hálózatba szervezése, valamint valós és virtuális világok konvergenciája, amelyet az információs és kommunikációs technológia tesz lehetővé, mely az elkövetkező évtizedekben az innováció leghatékonyabb mozgatórugójává válik [4]. Másik értelmezésben a digitális technológiák oly módon történő felhasználása, hogy a vállalatnál további bevételnövekedéseket eredményez, skálázhatóságot biztosít, valamint gyors, határokon átívelő növekedést tesz lehetővé. Napjainkban a kkv-k továbbifejlődését a nemzetközi piacon történő jelenlét biztosítaná, azonban sokuk nem képes erre, mivel eredetileg nem ilyen volumenűre tervezték őket, és az üzleti modelljükből hiányoznak a digitális megoldások [5]. A digitalizáció fontosságát támasztja alá a Digiméter – Digitális Versenyképességi Mutató 2020-as kutatási eredménye, miszerint egyenes arányosság van a magyar kkv-k méretének és a digitalizációs fejlettségének szintjében [6]. Tehát minél inkább előrébb jár egy cég a digitalizációs lehetőségek terén, annál fejlődőképesebb és képes a terjeszkedésre.

1.3 A digitalizációval megjelenő kockázatok

A digitalizáció fejlődése és a kibertámadások száma azonban kéz a kézben járnak. A Mcafee egy 2018-as tanulmánya szerint az évi globális GDP 0,8%-át tulajdonítják el kiberbűnözők, ez mintegy 600 milliárd dollár. 2019-ben a kkv-k mintegy 40%-át érte jogsértés kibertámadás következtében [7]. Egy 2017-ben végzett kutatásban, melyet 5 ország (Ausztrália, Franciaország, Németország, Egyesült Királyság, Szingapúr) 254 kkv (1000-nél kevesebb alkalmazott létszámú vállalkozások) szervezeteivel együttműködve végeztek azt olvashatjuk, hogy az 32%-ukat érte zsarolótámadás és 1/5-nél teljes leállás történt ennek hatására [8] [9]. A Cyber Security Breaches Survey 2019-es kutatásából kiderül, hogy míg a nagyvállalkozások többségének van pénzügyi kerete, személyzete, eszköze a kibertámadások megakadályozására, kivédésére, addig a kkv-ról kevésbé mondható el, hogy számolnának ezekkel a veszélyekkel [7]. Európai viszonylatban Magyarország nem áll rosszul a tudatos informatikai biztonság terén. A kkv-k 88%-a használ valamilyen vírusírtót, 81% rendelkezik egyedi jelszóvédelemmel és 32% készít a fájljairól biztonsági másolatot valamilyen fizikai eszközre vagy felhőbe [6]. A pandémia megjelenésével tovább nőtt a digitalizáció fontossága, azonban a cégek a profitot előre sorolva a biztonságtudatosságot csak másodlagosként kezelték. Az Egyesült Királyság

kormánya arról számolt be, hogy a pandémia első hulláma alatt a vállalkozások 46%-a jelentett valamilyen kibertámadást és ezek közül minden 5. vállalkozást ért komolyabb pénz vagy adatvesztés [7]. A koronavírus ideje alatt a bejelentett kibertámadások száma az FBI 300%-kal növekedett, a napi 1000 bejelentésről napi 3.000-4.000 között volt [10]. A lezárások miatt az emberek többsége átállt az internetes vásárlásra és a korlátozások enyhítésének hatására is 40%-uk továbbra is megtartja ezt a szokását, bár kétségeik még mindig vannak a személyes adataik biztonsága felől [11].

2 A DIGITALIZÁCIÓ ÉS KOCKÁZATAINAK ELEMZÉSE

A cyber risk, vagy magyarra fordítva „kiberkockázat” jelentése a Kockázatkezelési intézet (IRM- Institut of Risk Management) megfogalmazásában: minden olyan internetről származó tényező, melynek hatására a szervezetet pénzügyi vagy hírnévbéli veszteség éri, illetve bármilyen módon az informatikai rendszerében meghibásodását okoz [12]. A következőkben megvizsgálom a kkv-k konkrét digitalizációs lehetőségeit és azt, hogy a különböző dimenziókon beül melyek azok a komponensek, melyekre leginkább szüksége van egy cégnek ahhoz, hogy lépést tartson a digitalizációs trendekkel és versenyben maradjon a piacon. Ezzel párhuzamosan felmérem, hogy az egyes komponensekhez milyen mértékű és kockázatú fenyegetettségek járnak.

A cégek digitalizációs lehetőségeinek rendszerbe szervezett kategóriák megalkotására a Digiméter metodikáját veszem alapul kiberbiztonsági szempontból módosítva:

1. Digitális jelenlét, Online kereskedelem
2. Digitális mindennapok
3. Vállalkozásvezetés, Ügyfél kapcsolattartás
4. Digitális pénzügy
5. Informatikai biztonság

A jó stratégia segít a prioritások meghatározásában, egyszerű, a jelenen alapszik és szemelőtt tartja a jövőt. Nem kell túlbonyolítani, csupán a következő kérdésekre kell összpontosítani. Hol vagyunk? Mink van? Hol szeretnénk lenni? Hogy jutunk el oda? A kiberbiztonság egyre inkább a kockázatelemzések fő témakörébe tartozik. De lehet minden egyes fenyegetés ellen védekezni? Sok kereskedő írja a termékéről, hogy teljeskörű védelmet és biztonságot nyújt a szervezet számára. Ha megpróbálunk minden ellen védekezni, az nagyon sokba kerülne, és mégis maradnának biztonsági rések szabadon. A megfelelő kiberbiztonsági stratégia kulcsa a kockázatelemzésen alapul. A kockázat egy adott cselekvés hiányából keletkezett veszteség lehetősége. Bár nincs általánosan elfogadott, előírt formula, amely meghatározná, hogyan kell felmérni a kockázatokat, elengedhetetlen, hogy alaposan ismerjük a kockázatnak kitett környezetet, vagyis saját magunkat. Sun Tzu tanácsát követve: „Ha ismered az ellenséget és ismerd meg önmagad, nem kell félned száz csata eredményétől”. Tehát, hogy megvédjük a vállalkozásunkat a kibertér fenyegetéseitől, meg kell ismernünk az „ellenséget”: nemzetállamok, szervezett bűnözők/hackerek, hacktivisták, belső fenyegetések, nem megfelelő termékek és szolgáltatások [13].

Az ISO szabványok közül a 27005-ös határozza meg a kockázatelemzés folyamatát [14]. A szervezet információbiztonsági kockázatának értékeléséhez kockázatértékelési kritériumokat kell kidolgozni, melynek során figyelembe kell a következőket:

- az üzleti információs folyamat stratégiai értéke,
- az érintett információs eszközök kritikussága,
- jogi és szabályozási követelmények, valamint szerződéses kötelezettségek,
- bizalmasság, sértetlenség és rendelkezésre állás fenntartása,
- a reputációvesztés megelőzése.

A kár mértékének meghatározásához hatáskritériumokat kell meghatározni, aminél figyelembe kell venni a következő szempontokat:

- az érintett információs eszköz besorolási szintje,
- az információbiztonság megsértése (bizalmasság, sértetlenség, rendelkezésreállás),
- a munkafolyamatok megzavarása,
- üzleti vagy anyagi kár,
- a tervek és határidők megzavarása,
- a jó hírnév károsodása,
- jogi, szabályozási vagy szerződéses követelmények megsértése,
- információkkal való visszaélés.

Kockázatelemzéskor fontos kitérni az anyagi károkra, ideértve az ügyvédi kiadásokat, az esetleges üzleti folyamatok leállása miatti pénzügyi kieséseket és az ügyfelek bizalomvesztéséből fakadó üzletkötések elmaradásából fakadó bevételkieséseket [15].

Jelen fejezetben a legjellemzőbb és leginkább előforduló kiberbiztonsági fenyegetésekre helyezem a hangsúlyt, így a természeti katasztrófák, áramkimaradás, földrengés, csőtörés, fizikai betörés, tűzeset stb., valamint a humánjellegű kockázatok elemzésére nem kerül sor. Az kockázatelemzések elkészítéséhez az ISO 27005 szabvány 2011-ben kiadott azon belül is a kvalitatív módszerét veszem alapul. Ennek a módszernek vannak hátrányai, mint például, hogy sok esetben szubjektív lehet, viszont alkalmas a kezdő szűrés elvégzéséhez és rávilágít a későbbiekben részletesebb elemzést igényló területekre, továbbá iránymutatást ad a tervezéshez. Továbbá kvanitatív elemzéshez sok esetben konkrét számszerű adatok meghatározására lenne szükség, amire konkrét, már bekövetkezett eseményeket kellene alapul vennünk, amire nincs minden esetben lehetőségem, vagy pedig téves lenne a meghatározásuk [14].

2.1 Digitális jelenlét (weboldal, webshop)

Digitális jelenlét alatt főleg az online jelenlétet értjük és négy alkomponensét különböztetjük meg: Weboldal/webshop, közösségi média, keresőoptimalizálás és mobil alkalmazás. Az **2.1. ábra** a különböző komponensek fontosságát prezentálja [16]. A kutatás célja mely során a kimutatást készült egy DÉTA modell (a digitális érettség technikai architektúrája) megalkotása volt. A modell célja, hogy a KKV-k fel tudják mérni, hol tartanak a digitalizációban (mennyire fejlett a digitális erőforrásrendszerük, -

szemléletük), illetve hogyan tudnak gyorsabban és hatékonyabban reagálni a környezeti változásokra, milyen digitalizációs hiányosságokkal küzdenek, illetve mely területeket szükséges fejleszteni.

Komponens	Súly
Weboldal/webshop (reszponzív)	0,39790
Közösségi média használata	0,13263
Keresőoptimalizálás	0,25141
Mobilapp	0,21806

***2.1. ábra**: Az online jelenlét súlyszámai [16]*

Az ábráról azt olvashatjuk le, hogy a négy komponens közül 24 megkérdezett szakértőből 10 szakértő a weboldal/webshop meglétét tartotta legfontosabbnak az online jelenlét tekintetében, ami kiemelkedő eredménynek számít. Ez azt jelenti, hogy a cégek online jelenlétének tekintetében a weboldal megléte, ami leginkább irányadó abban, hogy a kkv-k meghatározzák, hol tartanak a digitalizációban, azon belül is, ami az online jelenlétet illeti. A többi komponenst 4-5-5 arányban preferálták első helyen.

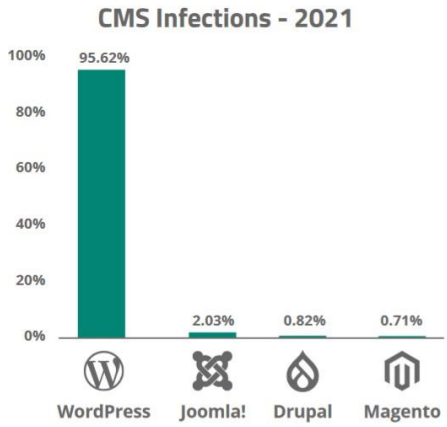
A webshop fogalma összefügg az e-kereskedelemmel. Az ügyfélkapcsolatokról későbbiekben vállalkozásvezetés alatt fog szó esni. Az elektronikus kereskedelem általános megfogalmazásban olyan termékek és folyamatok összessége, amelyek lehetővé teszik meghatározott termékek és szolgáltatások elektronikus úton, biztonságos módon történő forgalmazását - ideértve a hirdetést, vásárlást, beszerzéseket, marketinget és az elektronikus úton zajló fizetést is [17].

2.1.1 A weboldalakat célzó fő támadások trendje

Átlagosan 30.000 weboldalt törnek fel naponta és nagyrészük a kkv szektorhoz tartozó weboldalak, amelyek sokszor alapból malware-ket terjesztenek a különböző hozzáadott pluginok és kiterjesztéseken keresztül, mivel a létrehozásuknál nem vettek figyelembe IT biztonsági alapelveket [18]. 2018-ban az előző évekhez képest nem változott jelentősebben a weboldalakat ért támadások típusai. A támadók leginkább a tartalomkezelőre (CMS) telepített és rosszul konfigurált bővítmények, beépülő modulok, valamint a rosszul konfigurált alkalmazások és szerverek sérülékenységeit használták ki. Nagyrészük harmadik féltől származtak és általában cross-side scripting és SQL injection fertőzöttek voltak. Ezek legtöbbje elkerülhető lett volna, amennyiben a weblap fejlesztők figyelembe vették volna a kiberbiztonságban alkalmazott legjobb gyakorlatokat [12].

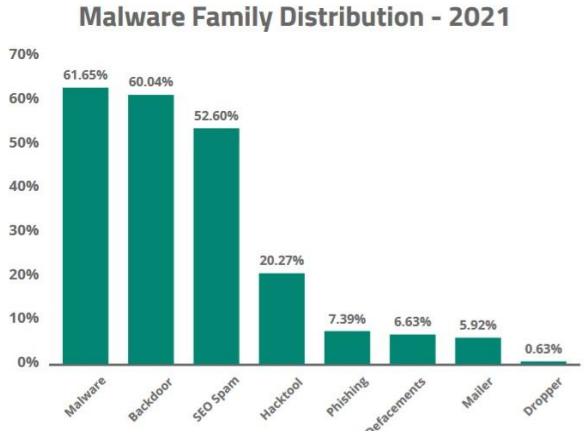
A **2.2. ábra** azt mutatja be, hogy 2021-ben a Sucuri által fejlesztett GoDaddy website security cég webhelytisztító szolgáltatását mely CMS szolgáltatókon vették igénybe és milyen megoszlásban volt rajtuk fertőzés. Ezen támadások többnyire a CMS platform

elavultságából eredő sérülékenységeket használták ki. A legtöbb elavult platformot a wordpress által szolgáltatott weboldalakon találták [19].



2.2. ábra: 2021-ben fertőzött CMS szolgáltatók megoszlása [19]

A **2.3. ábra** a weboldalakat ért leggyakoribb támadások arányát mutatja be. 2018 és 2019-hez képest a sorrend lényegesen változott, a SEO Spam vezető szerepét a malware vette át a 3. helyről, így a veszélyük számottevően nőtt az utóbbi pár évben.



2.3. ábra: Malware családok fertőzési aránya 2021-ben [19]

Spam:

2019-ben a Sucuri hozzávette a spamdexing (SEO spam) malware csoportot is a felmérésbe. Jelenleg ez a leginkább feltörekvő fertőzési család, a vizsgált weboldalak 62%-nál találtak SEO spameket. Ennek a malware családnak az a működési elve, hogy spam-ként bejutva a weboldalra irreleváns vagy tiltott kifejezéseket, linkeket ad hozzá a weboldal indexeihez. Ennek következtében a különböző keresőoldalak (google, bing, yahoo stb.) keresőmotorjai hátrébb sorolhatják vagy letilthatják a weboldalt, ezáltal ellehetetlenítve a szolgáltatást A fenyegetettség jelentőségét tovább növeli, hogy SEO Spam-mel fertőzött weboldalak nagyrészét újra fertőződtek valamilyen backdoor támadással [19].

Backdoor:

A támadás célja, hogy miután a kártékony kód beinjektálódott a weboldalra, előkészítse a feltételeket ahhoz, hogy a támadó a szokványos authentikációt megkerülve privilegizált hozzáféréssel juthasson be a rendszerbe.

Hacktools:

Olyan telepített alkalmazások az eszközön, melyek konkrétan nem befolyásolják a weboldal működését, de a támadó tevékenységét segíti és rejti el. Általában a szerver erőforrásainak elérésére és kihasználására alkalmazzák (blockchain, kriptobányászat). Előfordulhat az is, hogy a weboldal arculatát meghamisítják, spam levelekkel árasztják el az oldalt, botnetet hoznak létre, újjlenyomatot lopnak vagy DDoS támadással ellehetetlenítik a weboldal működését. Másik gyakori formája, hogy az adatbázis szerver authentikációs adatait lopják el és ezáltal a támadás tovább eszkalálódik a webszerver irányába.

Defacements:

Politikai, vallási vagy rongálási indíttatásból elkövetett weblap hamisítás.

Phishing: emailen keresztül személyes adatok kicsalása, főleg pénzügyi szervezetekhez (bank, webshop stb.) történő hozzáféréshez.

Az OWASP Top10:2021 adatai alapján az első három leggyakoribb kockázat webalkalmazások esetén a következők:

- jogosulatlan hozzáférés (összes cwe 19,013db, hatásuk súlyozási átlag 5,93)
- példa: URL lekérdezés
- gyenge titkosítás (összes cwe 32,078db, hatásuk súlyozási átlag 7.15)
- példa: SSL Spoofing (közbeékelődés)
- injekció (összes cwe 3,075db, hatásuk súlyozási átlag 6.81)
- példa: SQL parancs injektálás [20].

Következtetés: A weboldal üzemeltetését esetünkben külső fél fogja végezni, amely rendelkezik megfelelő ISO tanúsítványokkal (ISO 27001, ISO 27002, ISO 27005) ezáltal gondoskodunk a megfelelő biztonságáról, mivel saját személyzet foglakoztatására nincs kapacitás.

2.2 Digitális mindennapok

Gubán Ákos (Budapesti Gazdasági Egyetem) és Sándor Ágnes (Budapesti Gazdasági Egyetem) 2021-ben publikált kutatásának eredménye alapján a szakértők által leglényegesebb komponenseket fogom vizsgálni kiberbiztonsági kockázat szempontjából [16].

A digitális mindennapok során azokat a felhasznált digitális megoldások, hardvereket, szoftvereket értjük, amelyek egy cég mindennapi munkavégzéséhez nélkülözhetetlenek. A veszélyforrások felsorolásánál a munkavégzés során közvetlenül felmerülő veszélyforrásokra összpontosítok.

2.2.1 Internet használat (böngészés) során felmerülő veszélyforrások

Az interneten történő böngészés az információszerzés leghatékonyabb és leggyorsabb módja. A legtöbb munkavégzéshez nélkülözhetetlen, mivel sokszor kerül olyan helyzetbe a munkavállaló, hogy saját magának kell beszereznie bizonyos információkat, ami a feladata elvégzéséhez szükséges.

A CVE Detalis oldalán 2022-ben a termék szerinti csoportosításban a Chrome böngésző a 10. helyet foglalja el a bejegyzett sérülékenységek számát tekintve (2674db). 2022-ben a legtöbb sérülékenység a Chrome böngészőnél a biztonsági szabályok megkerülését tette lehetővé (bypass). Ebből 36db-ot regisztráltak. A legmagasabb besorolásúak 10-es CVSS[1]értékkel rendelkeztek. Az e módon sérülékeny Chrome böngésző használatának kockázatelemzését a CVE Details adataiból kiindulva a **2.4-as ábra** mutatja be.

Jelölések:

- C= Confidentiality (Bizalmasság)
- I= Integrity (Sértetlenség)
- A=Availabilit (Rendelkezésre állás)

Érintettség		Végpont, Céges adatok
Fenyegetés		munkafolyamatok megzavarása, adatok manipulálása, információszivárgás
Kár (D)	C	nagy
	I	nagy
	A	nagy
Hatás		nagy
Valószínűség (P)		nagy
Kockázat (R)		**nagy**

***2.1. táblázat**: Chrome használata – Bypass vuln.*

A második legtöbb sérülékenység a memória túlcsordulásos támadást tett lehetővé. 2022-ben 32 ilyen típusú sérülékenységet fedeztek fel. A legmagasabb besorolású

[1] A Common Vulnerability Scoring System (CVSS) egy ingyenes és nyílt iparági szabvány a számítógépes rendszerek biztonsági rései súlyosságának felmérésére.

sérülékenységek ebben a kategóriában (buffer overflow) 6,8-as értéket kaptak [21]. A kockázat elemzését a CVE Details adataiból dolgozva a **2.5-ös** ábra mutatja be.

Érintettség		Végpont, Céges adatok
Fenyegetés		munkafolyamatok megzavarása, adatok manipulálása
Kár (D)	C	kicsi
	I	kicsi
	A	kicsi
Hatás		kicsi
Valószínűség (P)		kicsi
Kockázat (R)		**kicsi**

***2.2. táblázat**: Chrome használata - Buffer overflow vuln.*

Magának, a Chrome böngészőnek a CVSS Score súlyozott átlaga 1999-2022 között publikált sérülékenyégeivel számolva 6,3, de a Firefox és MS Edge sem áll jobban 7,20-as átlaggal. A Brave ugyenezen szűrési feltételek alapján 5,5-ös értékkel rendelkezik. Általánosságban a nem naprakész böngésző használatának kockázatát a **2.5-ös ábra** mutatja be, a 3 böngésző CCSS számának súlyozott átlagával számolva, ami 6,7 es értéket jelent.

Érintettség		Végpont, Böngésző alkalmazás
Fenyegetés		munkafolyamatok megzavarása, adatok manipulálása, információ szivárgás
Kár (D)	C	nagy
	I	közepes
	A	nagy
Hatás		nagy
Valószínűség (P)		kicsi
Kockázat (R)		**közepes**

***2.3. táblázat**: Kockázat a böngészők sérülékenységi átlaga alapján*

Következtetés: A céges környezetben használt böngésző megválasztására közepes figyelmet kell fordítani, mivel vannak eltérések a megjelenő sérülékenységek számában gyártók között. A böngésző beállításait sem szabad elhanyagolni, a jelszavak, előzmények, cockie-k kezelésére policy-t kell létrehozni és a web biztonságtudatos használatára oktatást kell tartani a felhasználók számára.

2.2.2 Megbízható VPN és Wi-Fi kapcsolat

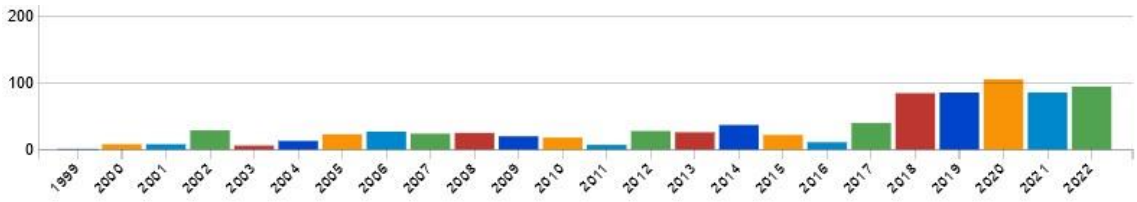
VPN

A VPN (virtuális magánhálózat) lehetővé teszi a vállalatok számára a belső hálózat (intranet) kiterjesztését a nyilvános hálózatok, például az Internet már meglévő infrastruktúrájának felhasználásával. Virtuális magánhálózatokkal felügyelhető a hálózati forgalom, további biztonsági szolgáltatásokat is nyújtva, például a hitelesítést és az adatok bizalmasságát [22].

Fontos megjegyezni, hogy vannak „ingyenes" VPN szolgáltatók, amik nyomon követhetik a böngészést és az előzményeket eladják harmadik félnek vagy reklámokkal tűzdelik tele az alkalmazást, amikre kattintva könnyen veszélyes oldalon találhatjuk magunkat.

Egyre több szervezet létszükséglete a belső hálózat távoli elérése VPN kapcsolaton keresztül. Ebben szerepet játszott a COVID19 megjelenése is. 2020-ig 479 sérülékenység került detektálásra ebből 28db 2020-ban amik a VPN szolgáltatásokat érintették. A legtöbb sérülékenység az eszközök beépített szoftverét érintette, vagyis a nem naprakész firmware-t. A sérülékenységeket kihasználva adatlopás, érzékeny adatszivárgás, belső és külső hálózat elleni támadások érték az áldozatokat. A fenyegetések között szerepel a közbeékelődéses támadás, DNS eltérítés, trójai és féreg (worms), kipróbálásos módszer (brute force) és az olyan alkalmazások nem naprakészsége miatti sérülékenységének kihasználása által, mint például a Putty, amelyet sok szervezet használ, de elhanyagolják a verziófrissítésüket. A VPN-t érintő sérülékenységek száma évről-évre gyarapszik és a legtöbb esetben a firmware elavultsága okozza a sérülékenységet [23]. 2020-ban a közép- és kelet-európai cégek biztonsági prioritásai a következő 6–18 hónapra 65%-ban a biztonságos távmunka és 79%-nál a leggyakrabban használt biztonságos távoli elérés, ami átvette a vezető szerepet a végpontvédelemtől [24].

Jelenleg a CVE Details oldalán 616 regisztrált sérülékenység van, amik valamilyen módon a VPN-t érintik [25]. A NIST statisztikája alapján a **2.7-es ábrán** látható, hogy az utóbbi években jelentősen nőtt a VPN szolgáltatásokat érintő sérülékenységek száma [26].



***2.4. ábra**: VPN-eket érintő sérülékenységek trendje [26]*

A VPN szolgáltatást ért támadások a közbeékelődéses támadás kategóriájába sorolható, így a kockázatelemzésemet ennek fényében készítem a fent leírt információk alapján (**2.8-as ábra**).

Érintettség		Távoli elérés, VPN
Fenyegetés		adatok manipulálsa, adatlopás
Kár (D)	C	nagy
	I	közepes
	A	kicsi
Hatás		nagy
Valószínűség (P)		közepes
Kockázat (R)		**nagy**

***2.4. táblázat**: VPN szolgáltatás kopromittálódásának kockázata*

Wi-Fi

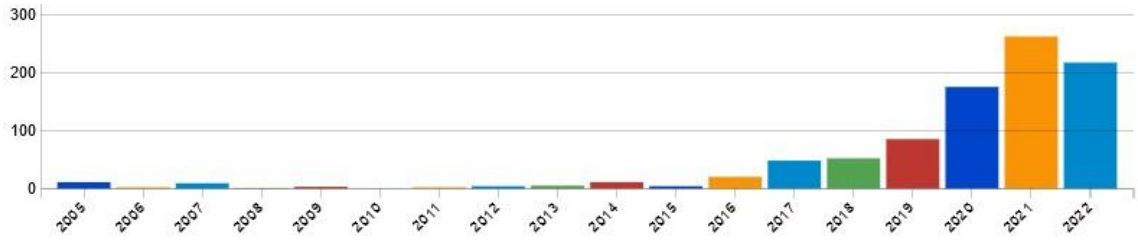
Az egyes végpontok belső hálózathoz történtnő kapcsolódása lényegesen egyszerűbb, mint vezetéken keresztül és az infrastruktúrájának kiépítése is kevesebb munkából áll. Mára szinte mindenhol lehet csatlakozni Wi-Fi (vezeték nélküli belső hálózat)hálózathoz, azonban a biztonságáról alkotott általános közfelfogás méltatlanul alá van becsülve Még az etikus hacker körökben is ritka az olyan megbízás, hogy a Wi-Fi hálózat töréstesztje lenne a feladat, holott míg a vezetékes hálózat feltörése viszonylag bonyolultabb művelet, hiszen fizikailag ott bent kell lenni az adott cég területén, addig a vezetéknélküli hálózat feltörése jóval egyszerűbb, elég a vállalat Wi-Fi sugarának hatókörzetében lenni és a támadók általában nagy hatótávolságú antennákkal is rendelkeznek. A hálózati forgalom lehallgatása, manipulálása lényegesen egyszerűbb ezzel a közbeékelődéses támadással, mintha az áldozat számítógépére kellene eljuttatni egy kártékony objektumot. Általánosságban a bevett gyakorlat, hogy a belső és a publikus Wi-Fi hálózatot, külön VLAN-ba rakják, és ezzel sokszor megoldottnak tartják az üzemeltetők a biztonságra törekvést. A Wi-Fi az IEE szabványt használja, amit a városi, személyi és helyi hálózatokra hoztak létre. Az IEE szabványon belül a 802.11-es vonatkozik a Wi-Fi-re. A 11-es szám használata abból ered, hogy az adatátvitel sebessége 11 MB/s-től akár több százig is terjedhet. A Wi-Fi hálózat illetéktelen használata önmagában is kockázatot jelent, mivel a szervezet erőforrásait veszik igénybe. A vezetéknélküli használat beüzemelésének első lépése a gyári beállítások áttekintése, majd konfigurálása. Az eszköz alapértelmezett felhasználónév-jelszó kombinációja bárki számára elérhető. A megfelelő titkosításról szintén gondoskodni kell, mert a WEP titkosítás könnyedén feltörhető. Ennek továbbfejlesztett változata a WPA, ami a WEP sérülékenységeit javította. A WPA továbbfejlesztése, ami jelenleg biztonságosnak mondható a WPA2-es

titkosítás. További részletek a Wi-Fi szabvány titkosításának módszereiről az implementáció fejezetben, a Wi-Fi AP alfejezet keretein belül történik.

Amikor egy szervezet Wi-Fi hálózatát jogosulatlan használja, két kockázattal kell számolni. Egyik, az erőforrások jogosulatlan használata, másik az adatok bizalmasságának sérülése. A már korábban említett WEP sérülékenysége az ú.n. Frame Spoofing, ami az adatcsomagok eltérítését célozza. A Wi-Fi hálózatkockázatainak felsorolására és kifejtésére a CISA dokumentációját veszem alapul. A CISA 7 ilyen kockázatot sorol fel:

- **piggybacking:** a részben már említett jogosulatlan hozzáférés a Wi-Fi hálózathoz, aminek az erőforrásait használják és veszélybe kerül a rendelkezésre állás. illegális tevékenységet is végezhetnek rajta illetve lehallgathatják, eltéríthetik a forgalmat, ami által sérül az adatok bizalmassága, sértetlensége,
- **evil twin:** a támadó lemásolja a hálózat hozzáférési pontját, pl. hálózat neve, azonosítója stb., és erősebb jel sugárzásával maga felé irányítja a rá csatlakozni kívánó felhasználókat. Innentől bizalmas adatokhoz férhet hozzá,
- **sniffing:** a gyenge titkosítást, (WEP) kihasználva a támadó hozzáfér az adatforgalomhoz, érzékeny adatokhoz férhet hozzá lehallgatásával,
- **jogosulatlan hozzáférés eszközön tárolt adatokhoz:** a támadó a Wi-Fi jel feltörésén keresztül hozzáfér a hálózatba kapcsolt eszközök megosztott adataihoz,
- **vállszörf:** a támadó ellesi a monitorról vagy billentyűzetről az érzékeny adatokat, jelszavakat,
- **mobileszköz ellopása:** a támadó eltulajdonítja az áldozat mobiltelefonját, aminek feltörésével bizalmas adatokhoz fér hozzá [27].

A Wi-Fi szolgáltatást érintő sérülékenységek számának statisztikáját mutatja be a NIST adatainak felhasználásával a **2.9-es ábra** [28].



***2.5. ábra**: Wi-Fi sérülékenységek számának statisztikája [28]*

A fenti adatok alapján a Wi-Fi sérülékenység kihasználásának kockázatelemzését a **2.10-es ábra** mutatja be.

Érintettség		Wi-Fi AP, Belső hálózat, Végpont,
Fenyegetés		adatszivárgás és manipulálás, munkafolyamatokban fennakadás
Kár (D)	C	nagy
	I	nagy
	A	közepes
Hatás		nagy
Valószínűség (P)		közepes
Kockázat (R)		nagy

***2.5. táblázat**: Wi-Fi hálózat sérülékenységének kockázata*

Következtetés:

VPN: rendszerek távoli elérésére mindenképpen VPN alagút kiépítése szükséges, azonban az eszköz rendszeres frissítése minden esetben fontos. A VPN szolgáltatás kiválasztásakor figyelembe kell venni, hogy ennek kivitelezése minél gördülékenyebben valósulhasson meg.

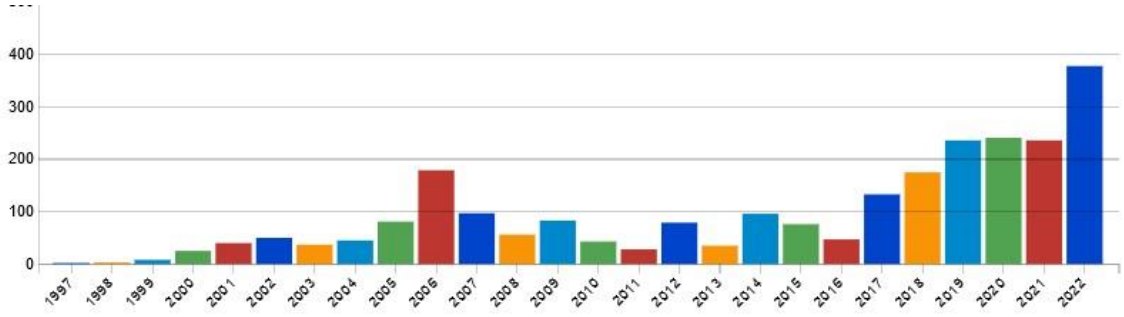
Wi-Fi: a vezeték nélküli hálózat implementációja során a biztonságos konfigurációra különös hangsúlyt kell fektetni. WPA2-es titkosítás, külön VLAN létrehozása és az adatforgalom tűzfalon történő szűrése indokolt.

Email használat

Két email szolgáltatást különböztetünk meg: web alapút és kliens alapút. A legnagyobb különbség köztük az, hogy a web alapúnál a levelek csak egy másik eszközön (szerveren) tárolódnak és internetkapcsolatra van szükség az elérésükhöz, míg a kliens alapúnál a levelek egy szerveren vannak eltárolva és a megnyitásuknál a levél letöltődik, a levél átmásolódik / áthelyeződik a kliens eszközre, így azt utána internetkapcsolat nélkül is olvasni tudjuk. Az elküldött/fogadott email-ek száma évente folyamatosan stabilan növekszik (felhasználó szinten évente 6%-kal, vállalati szintem pedig 3%-kal). Fontos kiemelni, hogy a növekedést nem az elküldött levelek száma okozza, hanem a fogadottaké, ami a spameknek tudható be [29].

Az e-mail mindennapi üzletünk kritikus részévé vált. Az email használatával kapcsolatos üzleti előnyök messze meghaladják a negatívumokat. A vállalkozásnak azonban muszáj hangsúlyt fektetnie az email használatával kapcsolatos biztonsági alapelvekre, hogy biztosítsa az adatvédelmet, az ügyfelek és az üzleti információk védelmét. Jól dokumentált, hogy a spam, az adathalász kísérletek és az egyéb kéretlen e-mailek gyakran magánszemélyek vagy vállalkozások által kapott összes e-mail több mint 60 százalékát teszi ki. Az e-mail az elsődleges módszer vírusok és rosszindulatú programok terjesztésére, de tudatossággal a védekezés is egyszerű ellenük [30].

Egy vállalat számára saját email cím (domain) név mára szinte elvárás. Megbízhatóságot és hitelességet kölcsönöz. Ennek igénybevételére egy email szerverre van szükség, amely lehet helyi, saját szerver, illetve külső szolgáltatás. Az email szerver plusz biztonsági megoldásokkal szolgál, ilyen például a spam szűrés, antivírus, illetve a domain név szűrés. A saját email szerver üzemeltetése folyamatos karbantartást, menedzselést igényel, mivel sérülékenység kihasználásából adódó kár nagyon nagy hatással lehet a szervezet munkafolyamataira. Ahogy NIST sérülékenységi adatbázisának statisztikája is mutatja (**2.8-as ábra**), az email szolgáltatással kapcsolatos sérülékenységek száma az elmúlt évben jelentősen megugrott [31].



***2.6. ábra**: NIST sérülékenységi adatbázisának statisztikája email szolgáltatás vonatkozásában [31]*

2021-ben a TOP 15 rutin szerűén kihasznált sérülékenységekből 7 sérülékenység a MS Exchange szervert érintette, ebből 5 távoli kódfuttatást tett lehetővé [32]. A CVE Details adatai alapján az MS Exchange levelezőszerverre 2022-ben összesen 18 sérülékenyéget jegyeztek be. Ebből 8 távoli kódfuttatásra adott lehetőséget a támadók számára. A legmagasabb értékű sérülékenység 8,3-as. 1999-óta bejegyzett az MS Exchange-re kiadott összes sérülékenység CVSS átlaga 3,2. Ezek többsége (32%) távoli kódfuttatást tett lehetővé. Ezek mindegyike könnyű vagy közepesen komplexitással bír [21]. Egy távoli kódfúttatás lehetőségével rendelkező sérülékenység kockázatát a szervezet saját MS Exchange szerverén a **2.6-os ábra** mutatja be.

Érintettség		Levelező szerver, Levelezés
Fenyegetés		munkafolyamatok megzavarása, adatok manipulálása, információ szivárgás
Kár (D)	C	nagy
	I	nagy
	A	nagy
Hatás		nagy
Valószínűség (P)		kicsi
Kockázat (R)		**közepes**

***2.6. táblázat**: MS Exchange szerver RCE sérülékenységgel*

Az FBI Internet Crime Complaint Center (IC3) statisztikája kimutatta, hogy csak a hozzájuk bejelentésre került és saját rendelkezésre álló 19db ország hivatalos adatainak alapján 323,972 ember vált adathalász (phishing), 51,829 személyes adat ellopása, 19,954 átutalásokhoz kapcsolódó csalások (BEC), 16,750 hitelkártyaadatok kicsalása és 3,729 zsaroló támadás (ransomware) áldozatául. Az esetek száma évről-évre jelentősen növekedett. A legjelentősebb anyagi kár a BEC támadásokból keletkezett, csak 2021-ben 2,395,953,296 USD és a számok itt is évről évre minden szegmensben növekednek [33]. 2022 első félévében 10db új ransomware családot fedeztek fel. Az email formájában történő behatolás továbbra is a legnépszerűbb egyszerűségéből adódóan. A támadók legtöbbször a Google Drive-on keresztül kézbesítettek például a BazarLoader-t, valamint számos sérülékenység érintette az MS Exchange szervert is. Ezek a fenyegetettségek többnyire email formájában jelentkeznek az áldozatoknál [34]. Ahhoz, hogy ezek az email-ek kézbesítésre kerüljenek, rendelkezniük kell a támadóknak az email címmel, amire elküldik a veszélyt jelentő email-t, valamint el kell érniük, hogy azt meg is nyissák. Ezt az OSINT[2] módszerével érik el, ami súrolja a bizalmasság sérülésének határát. 2020-ban 70%-ban adathalász email-ekkel próbálták megszerezi a felhasználók hitelesítési adatait. 2019-ben 13milliárd rosszindulatú email-t blokkoltak a Microsoft eszközei [24]. Ennek okán szükséges felmérnünk a **2.12-es ábrán**, hogy egy email-ben kapott phishing, spam vagy ransomware vírus milyen kockázatot jelent egy vállalkozás számára.

Érintettség		Levelezés			
Fenyegetés		SPAM	BEC	Phising	Malware (ransomware)
Kár (D)	C	kicsi	nagy	nagy	nagy
	I	kicsi	kicsi	kicsi	nagy
	A	kicsi	kicsi	kicsi	nagy
Hatás		kicsi	közepes	közepes	nagy
Valószínűség (P)		nagy	nagy	nagy	nagy
Kockázat (R)		**közepes**	**nagy**	**nagy**	**nagy**

***2.7. táblázat**: levelezés kockázatai*

Következtetés: A email használata során szembesülhetünk a legtöbb fenyegetettséggel. A fenyegetettségek kézbesítésének nagyrésze (malware, phishing, átirányítás veszélyes weboldalra, adatlopás stb.) email-en keresztül történik. Saját email szerver üzemeltetése esetén kiemelten fontos annak karbantartása, precíz konfigurálása. Ennek hiányában nagyobb fenyegetést jelent, mint hasznot. A megfelelő email védelmi szolgáltatások használatának fontos szempontnak kell lennie a tervezés és implementálás során.

[2] Open Source Intelligence, magyarul nyílt forráskódú hírszerzés

Továbbá a munkavállalók felkészítése a káros emailek beazonosításának képességére szintén kiemelten fontos faktor.

2.2.3 Hálózati végpontok (munkaállomások, IoT eszközök, hálózati csomópontok)

Végpont minden olyan eszköz, ami csatlakozni tud a belső hálózathoz. A végpontok közkedvelt célpontjai a kiberbűnözőknek. A legfrissebb adatok szerint a támadások közel harmada a végpontokat célzó malware-ekkel (rosszindulatú szofver) valósul meg [35]. Végpontok közé soroljuk a különböző IoT eszközöket is, melyek alkalmazása egyre inkább kritikus a digitális átalakulás folyamatait követve. A Microsoft által vizsgált hálózati végpontok firmware-e (eszközök beépített szoftvere) 27%-ánál nem használtak megfelelő titkosítást a jelszavak tárolására (MD5/DES). A Microsoft Security Services for Incident Response Team által vizsgált incidensek 52%-a megelőzhető lett volna megfelelő végpontvédelemmel [36]. Ebből kifolyólag megfelelően konfigurált és menedzselt végpontvédelemmel a behatolások egyharmada detektálható, megakadályozható. Ahogy a távmunka egyre gyakoribbá válik, a végpontok biztonsága minden eddiginél fontosabb. A BYOD (használd a saját eszközöd) terjedésével megnő az esély arra, hogy a munkavállalók eszközeit a peremvédelem (tűzfal) nem képes megfelelő védelemmel ellátni, így sebezhetőbbek lesznek az adathalász támadásokkal, rosszindulatú programokkal és egyéb fenyegetésekkel szemben. A végpontvédelem, független a tűzfaltól. A távoli dolgozók számítógépére telepített biztonsági megoldások képesek azonosítani és reagálni a fenyegetésekre, amikor az eszközök a vállalati-, és a nyilvános hálózatok között mozognak. A végpontot fenyegető veszélyforrások a zsarolóvírus, adathalászat, vírusok belépési adatok ellopása. Végeredményben a legtöbb támadási forma célpontjai között szerepel valamilyen végpont, ez az egyik legkritikusabb szegmens. A Ponemon 2019-es felméréséből kiderül, hogy a megkérdezett IT biztonsági szakemberek (691 fő) 49% a bekövetkezett incidensek okaként a végpontvédelem nem megfelelőségét határozta meg. 68%-uk számolt be arról, hogy az előző évben végpontot ért támadást tapasztalt és szintén 68%-ék tapasztalta az előző évhez képest ezen támadások növekedését [37].

A zsaroló támadások (ransomware) leggyakoribb célja a céges adatok letitkosítása. A ransomware taktikák és technikák folyamatosan fejlődnek évről-évre. A hálózatokhoz történő hozzáférést általában a felhasználó hitelesítési adatainak ellopásán keresztül távoli asztali kapcsolattal valósul meg. A zsarolóvírus végpontokon keresztüli telepítése a hálózatba a leggyakoribb támadási módszerek közé tartozik napjainkban és a kísérletek száma valószínűleg egyre gyakoribbá fog válni a jövőben. Miután egy zsarolóprogramot fenyegető szereplő kódot szerzett [38].

A fenyegetés valószínűségét számos példa tanúsítja, többek között a hazai 4iG SOC által Magyarországon elsőként detektált „.Play” ransomware 2022.08.09.-én és ami napjainkban (2022.12.12.) épp Belgiumban, Antwerpenben aktív. Egy 31 országot

magába foglaló felmérés szerint 2021-ben az előző évhez képest 37%-kal nőtt a ransomware incidensek száma, és 65%-ban volt sikeres a támadás. Magyarországon a támadások 78%-a bizonyult sikeresnek [39].

A fenti adatok alapján ransomware sérülékenységre **2.14-es ábra** mutatja be, ami reprezentálja a végpontot érő támadások kockázatát.

Érintettség		Végpont, Céges adatok
Fenyegetés		fennakadás a munkafolyamatokban, adatok manipulálása, információszivárgás
Kár (D)	C	nagy
	I	nagy
	A	nagy
Hatás		nagy
Valószínűség (P)		nagy
Kockázat (R)		**nagy**

***2.8. táblázat**: kockázatelemzés végpontra vetítve (ransomware)*

Következtetés: A végpont a legtöbb támadás egyik célpontja, majdnem a végső. Mivel ha egy végpontra sikeres behatolás történik, az azt jelenti, hogy a kiber támadási lánc (Cyber Kill Chain) 5. pontján van a támadó és már csak egy lépés választja el a sikertől. Az utolsó védelmi bástya, ezentúl csak különböző XDR (kiterjesztett detektálás és reagálás) vagy SIEM (biztonsági információk és események kezelésére alkalmas megoldás) detektálható a támadás. Következtetésképp a végpontok védelmére kiemelt hangsúlyt kell fektetni és a megfelelő megoldás kiválasztásához további szűrést kell végezni a tervezés során.

2.2.4 Felhőalapú szolgáltatások

A felhő kiszolgálók olyan globális hálózatát jelenti, amelyben mindegyik kiszolgálónak egyedi feladata van. A felhő nem fizikai entitás, hanem világszerte elhelyezkedő távoli kiszolgálók hálózata, melyek össze vannak kapcsolva, így egyetlen egységes rendszerként működnek [40]. A felhőalapú szolgáltatások előnyeit és hátrányait az **1. számú táblázat** sorolja fel.

Előnyei:	Hátrányai:
Rendelkezésre állás, hozzáférhetőség, Információ megosztás, együttműködés lehetősége, Rendszerek rugalmassága, Alacsony infrastrukturális költségek, Megbízhatóság, Beruházási kockázatok csökkentése, Skálázhatóság, méretezhetőség	Késleltetett elérés, hálózati problémák, Adatvédelmi, adatbiztonsági kérdések, Platform, illetve nyelvi függőség, Használat, alkalmazás védelme, Felhő szolgáltatók, szolgáltatások elérhetősége

2.9. táblázat: *a felhőszolgáltatás előnyei és hátrányai*

Platform alapján 4 felhőtípust különböztethetünk meg:

- nyilvános (nyilvánosan elérhető erőforrások, szolgáltatások),
- magán (belső magánhálózaton keresztül elérhető erőforrások, szolgáltatások),
- közösségi (egy bizonyos közösség számára elérhető erőforrások, szolgáltatások),
- hibrid (a nyilvános és magán felhő tulajdonságaival bír kívánalomtól függően).

Szolgáltatás alapján 3 különböző felhőtípust különböztetünk meg:

- IaaS (Infrastruktúra mint Szolgáltatás): Infrastruktúra mint szolgáltatás elem. Virtuális gép, szerver, tároló adhat pl. Microsoft Azure,
- PaaS (Platform mint Szolgáltatás): környezetet biztosítása. Adatbázis, fejlesztőkörnyezet /futtatókörnyezet (Pl. az Amazon),
- SaaS (Szoftver mint Szolgáltatás): meghatározott szolgáltatás. (Pl.: Google Drive, vagy a Microsoft Office 365).

A felelősségi körök és kockázatok megoszlanak a szolgáltatás típusának alapján. Felelősségben vannak átfedések a szolgáltató és a felhasználók között (leginkább a PaaS esetében) és előfordulhatnak speciális esetek, de általában a **2. számú táblázat** alapján történik a biztonsági felelősségek felosztása a CISCO értelmezésében [41].

SaaS		PaaS		IaaS	
Felhasználó felelőssége	**Szolgáltató felelőssége**	**Felhasználó felelőssége**	**Szolgáltató felelőssége**	**Felhasználó felelőssége**	**Szolgáltató felelőssége**
Emberi tényezők Adatok	Alkalmazások Futásidő Köztes szoftver Operációs rendszer Virtuális hálózat Hypervisor Szerverek Tárhely Fizikai hálózat	Emberek tényezők Adatok Alkalmazások	Futásidő Köztes szoftver Operációs rendszer Virtuális hálózat Hypervisor Szerverek Tárhely Fizikai hálózat	Futásidő Köztes szoftver Operációs rendszer Virtuális hálózat	Hypervisor Szerverek Tárhely Fizikai hálózat

***2.10. táblázat**: Biztonsági felelősségek megoszlása különböző felhőszolgás típusok alatt Cisco vállalat értelmezésében [41]*

Mivel a felhőszolgáltatások sokszínűsége és személyre szabottsága egyre több vállalatnak könnyíti meg az üzleti folyamatait, ezért egyre többen veszik igénybe ezeket a szolgáltatásokat. Ebből kifolyólag a kiberbűnözők közkedvelt célpontjává vált. Előnyeinek és hátrányainak, kockázatainak számbavétele fontos kérdés lehet egy vállalat döntéshozatalában.

Következtetés: Esetünkben a felhőszolgáltatást SaaS formában fogjuk igénybe venni Google Cloud és Office 365 szolgáltatások részeként, így a kockázatok lehető legtöbb része áthárul a szolgáltatóra a **2.10-es ábra** alapján.

2.3 Vállalkozásvezetés

A vállalati tevékenységeket üzlet célkitűzések határozzák meg. A célkitűzésekhez folyamatokat és elvégzendő tevékenységek. Az üzleti folyamatokat időről-időre felül kell vizsgálni, ahhoz, hogy a cég a gyorsan változó környezeti kihívásoknak megfeleljen (BPR = Business Process Reengineering, BPM = Business Process Management, illetve BE = Business Engineering.) [42]. A sikeresen végrehajtott BE biztosítja, hogy az üzleti folyamatok kulcsfontosságú lépései az adott körülmények között hatékonyak, rugalmasak és szolgáltatás orientáltak legyenek. Ehhez integrálnia kell valamennyi kritikus üzleti folyamatot, egyszerűsíteni kell, vagy teljesen kiiktatni az üzleti tevékenységek bonyolult láncolatait.

Ebben segítenek az integrált vállalatirányítási rendszerek (ERP - Enterprise Resource Planning) és az ügyfélkapcsolati menedzsment (CRM - Customer Relationship Management) eszközök.

ERP: olyan alapvető folyamatokat értünk, amelyek egy a vállalat futtatásához (pénzügy), HR, gyártás, ellátási lánc, szolgáltatások, beszerzés szükségesek. Az ERP rendszerek megkönnyítik a valós idejű információáramlást az egyes részlegek között, így a vállalkozások képesek adatközpontú döntéseket hozni és jobb teljesítményt nyújtani [42].

CRM: olyan stratégia, mely a folyamatokat az ügyféligények kiszolgálása érdekében integrálja, informatikai megoldások segítségével ügyfél adattárházat hoz létre, melyet feldolgoz és a folyamatokat automatizálja [43].

Az ERP üzleti folyamatok szempontjából, a CRM pedig az ügyfelek adatairól tartalmaz nagyon érzékeny adatokat így a kiberbűnözők kedvelt célpontjává vált, ezért is igen nagy kockázati tényező.

A sebezhetőséget tovább növeli, hogy ezek a rendszerek nagyon sok beállítási lehetőséggel rendelkeznek, éppen ezért a hozzáértő szakember megléte kiemelten fontos lenne [44].

Következtetés: A megbízó cég nem tervezi vállalatirányitási rendszer használatát, azonban amennyiben erre sor kerülne, a munkavállalóknak oktatáson kell résztvenniük.

2.4 Digitális pénzügy (Elektronikus bank, Fintech)

Ide tartozik a vállalatok elektronikus számlázása, könyvelése és a bankügyeinek intézése. A számlázást és a könyvelést az előző fejezetben (vállalkozásvezetés) tárgyalt ERP rendszer nagyrészt lefedi, így most főleg az internetbankra és kártyás fizetésre, átutalásokra térnek ki.

2.4.1 Az elektronikus banki szolgáltatások

Az elektronikus banki szolgáltatások utóbbi években kijelenthetjük, hogy kiforrottak.

Elektronikus banki szolgáltatások:

- home (saját eszközről történő kapcsolódás a pénzintézettel) és Office (a vállalat eszközéről lép kapcsolatba a pénzintézettel) banki ügyintézést,
- kártyákkal végezhető elektronikus szolgáltatások,
- telebank és Call Center szolgáltatás,
- internet bank,
- mobilbank.

2.4.2 Financial technology (fintech)

A financial technology (fintech) egy innovatív vállalkozások által digitális környezetben létrehozott, digitális eszközökön működtetett termék vagy szolgáltatás, mely a pénzügyi szektorban versenyre lép a hagyományos pénzügyi módszerekkel és intézményekkel. Más értelmezésben a fintech egy új iparág, amely innovatív technológiát alkalmaz a pénzügyi tevékenységek fejlesztésére [45].

A fintech elterjedésének fő mozgatórugója a technológia fejlődése. A fintech szolgáltatások igénybevétele az elmúlt 5 évben évente 30-40%-kal nőtt nemzetközi szinten. A magyar tulajdonú FinTech cégek között méret tekintetében a mikró vállalatok dominálnak. A magyar tulajdonú vállalatok több mint 85%-a mikró és kisvállalati szegmensbe tartozik, ami duplája a nemzetközi átlagnak [46] Az innovatív pénzügyi technológiákkal párhuzamosan a kiberbiztonsági veszélyek is megjelennek, amelyek elhárítása érdekében elengedhetetlenné válik az egyes szereplők közötti, földrajzi piacokon átívelő együttműködés kialakítása [47].

Következtetés: Célszerű a már kiforrott módszer alkalmazása, vagyis a hagyományos digitális szolgáltatások használata. Az ezzel kapcsolatos kockázatokat a fent leírt fejezetek magukba foglaljak.

2.5 Informatikai biztonság

Fontos különbséget tenni az információbiztonság és az informatikai biztonság között. Az információbiztonság minden kommunikációs csatorna védelmére (beszéd, rajz, írás, elektronikus rendszerek stb.) hivatott, míg az informatikai biztonság informatikai rendszerekben kezelt adatok, és az azt kezelő rendszer védelmét jelenti.

Informatikai biztonság: „A rendszerben kezelt adatok bizalmasságának, sértetlenségénekés rendelkezésre állásának, valamint a rendszerelemei sértetlenségének és rendelkezésre állásának védelme” [48].

A Microsoft „Jelentés: Kiberbiztonsági trendek Közép- és Kelet-Európában” 2013.05.13-án kiadott felméréséből kiderül, hogy régiónkban a cégek 58%-ának nincs átfogó biztonsági stratégiája és ezt tetézi, hogy Ennek ellenére a többségük (86%) általában véve elégedett saját IT-rendszereinek biztonságával. A hamis biztonságérzet tovább fokozza a cégek fenyegetettségét. A cégek, amikor a biztonságstratégia fejlesztéséről van szó, általában úgy technológiák bevezetésére asszociálnak a már meglévő rendszer felmérése, tesztelése és auditálása és a munkavállalók képzése helyett. A távmunka hatására a virtualizációs megoldások nagymértékben fejlődtek, ennek okán a biztonságos távoli elérés és a belső veszélyforrások kérdésének prioritása megnőtt és ugyan olyan fontossá vált [49]. A közép- és kelet-európai cégek biztonsági prioritásai:

- rosszindulatú szoftveres támadások (67%)
- biztonságos távmunka (65%)
- a kiberbiztonság valós idejű monitorozása (57%)
- a munkatársak hozzáférésének kezelése (47%)
- belső veszélyforrások észlelése (46%) [49].

Minden technológiai rétegben figyelembe kell venni a kiberbiztonságot, mert napjainkban utólagos külső védőréteggel ellátni az infrastruktúrát, az alkalmazást vagy a szolgáltatás egyes elemeit nem elég. Ezen szemlélet alapján a kialakítás első pillanatától központi szempontként kell tekinteni a biztonságos működésre [50].

2.6 A kockázatelemzésekből nyert következtetések összegzése

A támadók gyakran az e-mail (phishing), és a web kombinált/összehangolt és kártékony szoftverek használatával érik el a sikeres támadásokat. A támadások célpontjai legtöbb esetben a végpontok és azon valamilyen kiterjesztés, parancs futtatása. Mivel a támadók hatékonyan kombinálják ezt a három vektort, a webes, e-mail-es és végpont védelmet integrált megoldással kellene megközelíteni. Ez leegyszerűsítheti mindhárom üzleti szempontból kritikus információs rendszer védelmét.

3 A BIZTONSÁGI ARCHITEKTÚRA KÖVETELMÉNYEINEK MEGHATÁROZÁSA

Az előzőekben meghatározásra kerültek azok a veszélyforrások, melyeknek egy céget fenyegethetnek a digitális világban. Jelen fejezetben összegzésre kerülnek a konkrét üzleti igények. Ezek a megrendelő által megosztott információk alapján a következők.

3.1 Az üzleti igények meghatározása

A biztonsági architektúra követelményeit öt szempont alapján fogjuk vizsgálni:

1. Üzleti adatok
2. Eszközök
3. IOT eszközök
4. Üzleti igények
5. Egyéb követelmények
6. Üzleti Adatok

3.1.1 Üzleti adatok

Érzékeny adatok:

Az érzékeny adatok olyan bizalmas információk, amelyeket biztonságban, és minden kívülállótól elzárva kell tartani, hacsak nincs engedélyük a hozzáférésre. Jelen esetben:

- az ügyfelekkel és partnerekkel kötött szerződések,
- a mindennapi munka során használt Office alkalmazások,
- az ügyfelek adatai,
- rendszertervek.

Nem érzékeny adatok:

- különböző audiovizuális tartalmak,
- az ügyfelek és partnerek részére készített marketinganyagok,
- egyéb állományok.

Telemetriai és termelésadatok (érzékeny/nem érzékeny):

- a cég székhelyéül szolgáló épület megfigyelésére alkalmazott felügyeleti rendszerek, azokról készített videófelvételek,
- napelem és hőszivattyú adatok,
- időjárási adatok,
- a különböző épületben használt energiafogyasztók és -termelők adatai.

3.1.2 Eszközök

Minden olyan eszköz, amely használatra kerül bármilyen munkafolyamat és/vagy a munkafolyamatok fenntartása céljából.

Munkaeszközök:

- munkaállomások: (laptopok, pc-k, nyomtatók, tabletek stb.) 5-12db,
- 2-4db TV és multimédiacenter a tárgyalóban a különböző prezentációk megtartására,
- NAS belső tároló.

IOT Eszközök:

- minden olyan nem szabványos számítástechnikai eszköz, amelyek vezeték nélkül csatlakoznak a hálózathoz és képesek adatátvitelre,
- napelemes inverterek, ezek termelési adatai, a szoftver verziója és a hozzájuk tartozó szoftverfrissítéseket tartalmazzák. A távoli elérést, karbantartást és konfigurációt biztosítani kell. Figyelembe kell venni, hogy csatlakozik az internethez a gyártó felhőjéhez, valamint asztali alkalmazás is van hozzá, csatlakozik a belső hálózatra,
- kamera rendszer,
- dedikált DVR-el és tárhellyel rendelkezik. Szempont, hogy belső hálózatról is elérhető legyen és TV-vel/munkaállomással csatlakozni lehessen hozzá,
- egyéb IOT eszközök (például épület automatizálási eszközök, időjárás szenzorok stb.),
- minden IOT eszközt távolról is biztonságosan el lehessen érni.

3.1.3 Üzleti Igények

Olyan alkalmazások és szolgáltatások, melyek az üzletmenet fenntartását és továbbfejlesztését hivatottak biztosítani:

- Office alkalmazások,
- email szolgáltatás,
- file megosztás,
- prezentációk,
- konferencia hívás,
- weblap,
- távoli erőforrás elérések,
- távoli felügyelet,
- távoli munkavégzési lehetőségek.

3.1.4 Egyéb Igények

A megbízó további igényei a következők:

- Wi-Fi és NAS elérés szeparált vendég funkcióval a különböző marketing anyagok eléréséhez,
- a Wi-Fi roaming a szintek közötti átjárás során felmerülő kapcsolatmegszakadás érdekében,
- minden adatot távolról is el lehessen érni biztonságosan (érzékeny üzleti, marketin és multimédiás adatokat egyaránt),
- biztonsági mentés minden fontos adatról, akár marketing, akár érzékeny adat akár felhőben amennyiben az adatszivárgás esélye minimális.

4 AZ ARCHITEKTÚRA MEGTERVEZÉSE

Az alábbi fejezet tartalmának részben a megvalósítás során kell megvalósulnia a saját hatáskörömben, részben pedig a megbízó felé ajánlás, iránymutatás.

4.1 A hálózat biztonsági architektúrájának és logikai védelemének megtervezése

A hálózat megtervezésekor az **ISO27001** követelményeit veszem alapul. A megfeleléshez a **NIST** (National Institute of Stardards and Technology), **CISA** (Certified Information System Auditor) és **ISMS** (Information Security Managament System) valamint **NSA** (National Security Agency/Central Security Service) ajánlásokat fogom alkalmazni.

A legtöbb biztosági problémát támadók okozzák. Ezek az emberek magas informatikai tudással rendelkeznek, és nem okoz problémát az alapvető biztonsági beállítások és eszközök védelmén átjutni. Azonban a rendőrségi feljegyzések alapján legtöbbször elégedetlen munkavállalók követik el károkat. A biztonságos hálózat megtervezésénél alapvető követelmény, hogy minden felhasználónak annyi, és csakis annyi jogosultsága és hozzáférése legyen, amennyi feltétlenül szükséges a munkája végzéséhez. Ebből kifolyólag a hálózatot úgy kell megtervezni, hogy a benne működő eszközök beállításai magán a teljes belső és külső hálózatról érkező fenyegetések ellen is a lehető legnagyobb védelmet tudják nyújtani, vagyis a **Zero Trust** modell alapján. A hálózat védelmét segítő útmutatások folyamatosan fejlődnek, azonban vannak alapvető logikai szempontok, amik általános iránymutatásként szolgálnak a tervezés folyamán. Ezen a tervezési alapelvek és konfigurációs beállítások és folyamatos felülvizsgálatuk hiányában az adatok és információk nagyobb valószínűséggel kompromittálódhatnak [51] [52] [53].

Az implementálás során fő feladatom az architektúra hálózat biztonságának megvalósítása: Ez a jogosulatlan hozzáférés észlelése és megakadályozása a hálózati eszközök, ill. hozzájuk csatlakozó rendszerekhez és végberendezésekhez, kapcsolókhoz, portokhoz hálózaton belülről vagy kívülről. Ajánlásként az ISO 27001 egyéb követelményeire is kitérek, valamint a megvalósításukhoz egyaránt ajánlást adok.

4.2 Hálózati architektúra tervezése

A több védelmi réteg kialakítása kritikus fontosságú a hálózaton belüli elemek védelméhez. A tervezés során figyelembe kell venni a legjobb gyakorlat és a Zero Trust elvét mind a hálózat peremén, mint pedig azon belül. Ezen követelmények megfeleléséhez a legmegfelelőbb eszköz a tűzfal, illetve a hálózat peremén az ISP eléréséhez jól konfigurált router [53].

4.2.1 Fizikai és környezeti biztonság

Cél: Meg kell előzni a jogosulatlan hozzáférést, károkozást és zavarást a szervezet információi és információfeldolgozó eszközeire vonatkozóan [54].

Intézkedések:

- fizikai biztonsági határokat kell létrehozni - az érzékeny és kritikus információkat vagy információfeldolgozó eszközöket az ügyfelek számára kijelölt szabad mozgásterületén kívül kell elhelyezni - a szerverterem zárható lesz, az épületbe érkező vendégek szabad mozgásterületén kívül kerülnek elhelyezésre,
- a szerverterembe történő belépést naplózásra kerül,
- az érzékeny információkat tartalmazó dokumentumok (céges adatok, szerződések, számlák stb.) külön, zárható helységben kerülnek elhelyezésre az épületbe érkező vendégek szabad mozgásterületén kívül
- az iroda, ahol a szerződéseket, érzékeny adatokat kezelik el lesz különítve és zárható lesz,
- az ügyfelekkel történő üzleti tárgyalásokra és a szerződések megkötésére használt helység el lesz különítve a többitől
- az olyan belépési pontokat, mint szállítási/rakodási területek, valamint az épület közvetlen környezetét megfigyelés alatt kell tartani Ehhez kamerarendszert fogok alkalmazni melyet távolról is lehet irányítani,
- az illetéktelen behatolásra riasztást kell alkalmazni. Ehhez a helységeket riasztóval, mozgásérzékelőkkel fogom ellátni, valamint azokat a helységeket, ahol érzékeny adatok kerülnek tárolásra ajtó/ablak nyílásérzékelőkkel.

További intézkedés az eszközök hozzáférhetőségének korlátozása, amely érdekében a következő intézkedések megtételére lesz szüksége a megbízónak:

- hozzáférések dokumentálása,
- hitelesített hozzáférés,
- érzékeny adatok védelme,
- erős jelszavak használata,
- bejelentkezési próbálkozások korlátozása,
- jelszavak biztonságos tárolása.

4.2.2 Naplózás és megfigyelés

Cél: Nyilvántartani az eseményeket és létrehozni bizonyítékokat [54].

Intézkedések:

- hálózat adatforgalmát monitorozni kell a támadások észlelésének és kivédésének érdekében,
- az eseményeket naplózni kell a későbbi elemzés, threat hunting és ”POC” érdekében [53].
- a végpontok eseményeiről és a hálózat forgalmáról a végpontvédelem és a tűzfal gyűjt információkat, log-okat.

4.2.3 A hálózat biztonsága

Cél: Biztosítani a hálózatokban lévő információk és az azokat támogató információfeldolgozó eszközök védelmét [54].

A hálózat peremének védelme

A hálózatokat gondozni és felügyelni kell, hogy a rendszerekben és az alkalmazásokban meg lehessen védeni az információkat [54].

Intézkedések:

Szükség van több réteg felépítése, ami a külső támadások ellen véd, illetve monitorozza a kijövő és bemenő forgalmat [53]. Ennek megvalósítására a tűzfalak, ezek közül is a”next generation” tűzfalak a legmegfelelőbb eszközök. A tűzfal lehet szoftveres, illetve hardveres. Célja, a hálózat kimenő és bejövő forgalmának ellenőrzése, szabályozása konfigurált szabályrendszer alapján. Esetünkben hardveres eszköz kerül majd alkalmazásra. A megfelelő biztonság érdekében a következő intézkedéseket teszem meg:

- a hálózat peremére az ISP szolgáltató elérését biztosító eszköz (router) biztonsági konfigurálása,
- következő generációs tűzfal alkalmazása mellyel biztosítani lehet a:
  - a hálózat kimenő és bejövő, valamint a belső hálózat különböző szegmensei közötti forgalom ellenőrzését, ami magába foglalja a DPI tűzfalat, IDS/IPS technológiát, antivírus szűrést, proxy és VPN kiszolgálót, valamint az SSL/SSH kapcsolatok szűrését,
  - az alkalmazások kommunikációjának ellenőrzését,
  - a web és webes alkalmazások használatának korlátozását,
  - a házirend érvényesítését az arra alkalmas eszközön/felhasználón az adott házirendet figyelembe véve,
  - a különböző szignatúrák/profilok alapján a gyanús csomagokat, illegális/gyanús, a megszokottól eltérő tevékenységeket és a küszöbértéket meghaladó forgalmának érzékelését,
  - az IDS rendszerek által detektálást, az IPS rendszerek által beavatkozást [53].

Esetünkben azonban DMZ-re nem lesz szükség, mivel mind a weboldal üzemeltetésétét/karbantartását, mind pedig az email szervert külső szolgáltató fogja biztosítani.

A belső hálózat védelme

Az információs szolgáltatások, a felhasználók és az információs rendszerek különböző csoportjait el kell különíteni a hálózatokban [54].

Intézkedések:

A belső hálózat védelme érdekében szükséges:

- a hálózati eszközökön az adminisztratív felhasználót megfelelően komplex jelszóvédelmével kell ellátni,
- a hálózat szegmentálása,
- a hálózat szegmentálásakor mind a két módszert figyelembe vesszük és felhasználjuk: felhasználói csoportok, valamint a kritikus, legsebezhetőbb szolgáltatások szerinti elkülönítést. Ezáltal megakadályozhatjuk a támadó oldalirányú mozgását, ha már a hálózaton belül tartózkodik,
- a munkaállomásokat, szervereket, nyomtatókat, távközlési rendszereket, egyéb hálózati perifériákat, ipari vezérlőrendszereket stb. el kell különíteni egymástól,
- általában a Native VLAN a Default VLAN (VLAN1)- hez van társítva - default VLAN nem, de a Native VLAN tiltható, így az ajánlásnak megfelelően tiltásra kell kerülnie, mert a címkézetlen, egyik VLAN-hoz sem tartozó csomagokat továbbítja, tehát minden olyan forgalmat, amely nem köthető egy adott VLAN-hoz sem továbbításra kerülne,
- a felhasználókat csak olyan hálózatokhoz és hálózati szolgáltatásokhoz való hozzáféréssel szabad ellátni, amelyek használatára kifejezetten fel lettek jogosítva
- a felhasználók csoportjait és információs rendszereket a hálózaton belül el kell különíteni egymástól VLAN-ok használatával, ezért külön VLAN-okat hozok létre:
  - VLAN20 vendég (internet elérés),
  - VLAN30 produktív, kritikus szerverek (internet elérés),
  - VLAN40 IOT eszközök (internet elérés),
  - VLAN50 beléptető/kamera rendszer,
  - VLAN60 managament (internet elérés),
  - VLAN70 teszt (internet elérés),
  - VLAN80 belső kliens (internet elérés),
  - VLAN90 admin (internet elérés),
  - VLAN100 VPN (a tűzfalon kell csak konfigurálni, a switch-en nem szükséges) [55] [53].

A VLAN-okat a switch fogja elszeparálni egymástól. Ahhoz azonban, hogy bizonyos VLAN-ok elérjék egymást, a tűzfalon kell a szabályrendszert beállítani. A szabályok IP subnet-ek alapján lesznek beállítva.

A VLAN-ok közötti átjárhatóságot a tűzfal fogja biztosítani.

Átjárhatóságot a következő VLAN-ok között fogok engedélyezni a tűzfal szabályok megalkotása során:

- VLAN90 > összes VLAN,
- VLAN80 > teszt, produktív,
- VLAN70 > csak az internet,
- VLAN60 > minden VLAN és internet,
- VLAN40 > produktív,
- VLAN30 > kamera rendszer, IOT eszközök, kliens, admin,
- VLAN20 > csak internet.

A belső alhálózatot el kell szeparálni egymástól, valamint a külső hálózattól, ehhez tűzfalat fogok alkalmazni.

A tűzfalon az alapbeállításként minden tiltásra kerül, és ezután adom hozzá szabályokat, amik lehetővé teszik majd a VLAN-ok közötti megfelelő kommunikációt és az internetelérést. A távoli elérés biztonságát, távolról történő konfigurációt biztosítani kell, ehhez IPsec VPN-t fogok használni, amit szintén a tűzfal fog biztosítani. A VPN-en keresztül az Adminisztrátornak és Klienseknek dedikált alhálózatot fogok beállítani annak érdekében, hogy távolról is elérjék a szükséges hálózatokat. Ezt a tűzfalon fogom bekonfigurálni és a bejelentkezési folyamatot lokális felhasználókkal oldom meg.

4.2.4 Adathordozók kezelése

Cél: Adathordozón tárolt információk jogosulatlanul történő nyilvánosságra hozása, módosítása, eltüntetésének megsemmisítésének megelőzése.

Intézkedések:

Kizárólag cég által biztosított, jelszóvédelemmel és titkosítással ellátott adathordozó (pendrive, külső merevlemez stb.) használata engedélyezett. Szállítás során védeni kell jogosulatlan hozzáféréstől, megrongálástól.

4.2.5 Hozzáférés felügyelet

Cél: Biztosítani a hozzáférést az arra jogosult felhasználók számára, megelőzni a jogosulatlan hozzáférést mind a fájlrendszerek, mind a hálózati beállítások, módosításokat illetően.

Intézkedések:

- mind a fájlrendszer, mind a hálózati hozzáféréseket illetően a minimális, a feladatkörhöz nélkülözhetetlen jogköröket kell megalkotni és kiosztani,
- minden eszközhöz, amin arra lehetőség van, csak nevesített felhasználóval és jelszóval lehessen hozzáférni,
- interaktív jelszókezelőrendszert kell alkalmazni, melyekkel kellően komplex és hosszúságú (min. 12 karakter, különleges karakterek, kis- és nagybetűk alkalmazása) jelszavakat lehet tárolni, illetve szükség esetén megosztani (keepass2/passbolt),
- a jelszavak titkosított hash-sel történnek tárolásra a jelszókezelő menedzser segítségével (AES),
- a jelszavak élettartamát maximum 90 napra korlátozni,
- a hálózathoz illetéktelen hozzáférést meg kell akadályozni. Ezt dedikált MAC címekkel lesz megvalósítva (port security),
- a vendég hálózat elérése jelszóval lesz védve, ami negyedévente kerül megváltoztatásra [53].

4.2.6 Védelem kártékony szoftverek ellen

Cél: Az információk és információ feldolgozó eszközök védelme rosszindulatú szoftverek ellen

Intézkedések:

- a munkaállomásokat végpontvédelemmel kell ellátni. Ezt végpontokra telepített vírusvédelmi szoftverrel fogom megoldani, ami websecurity megoldást is nyújt,
- a tűzfalon SSL bontást fogok alkalmazni mely további védelmi réteget biztosít a titkosított (https) forgalom tekintetében,
- a káros adatállományú, URL tartalmú és zsaroló levelek ellen email védelmi rendszert kell használni. Ehhez a Google Business Starter SaaS megoldását fogom igénybe venni, mivel a biztonság mellett saját domain nevet is biztosít a cégnek, így a karbantartási és üzemeltetési feladatok áthárulnak,
- a munkaállomásokra csatlakoztatott adathordozók a végpontvédelem által ellenőrizésre kerülnek.

4.2.7 Wi-Fi

Wi-Fi hálózat VLAN-on keresztül támogatni fogja a vendég hozzáférést, valamint a munkavállalói csatlakozást is.

Cél: A vendég VLAN-t a fő vállalati hálózatoktól történő elkülönítése, hogy sehol se legyen átjárható a vállalat belső rendszereire [56].

Intézkedések:

- vendégek és a munkavállalók számára külön SSID lesz biztosítva, melyek VLAN20 és VLAN80-ba fognak tartozni,
- A VLAN-ok adatforgalma a tűzfalon keresztül valósul meg, így biztosítva a vezetékes hálózattal azonos biztonsági szintet.

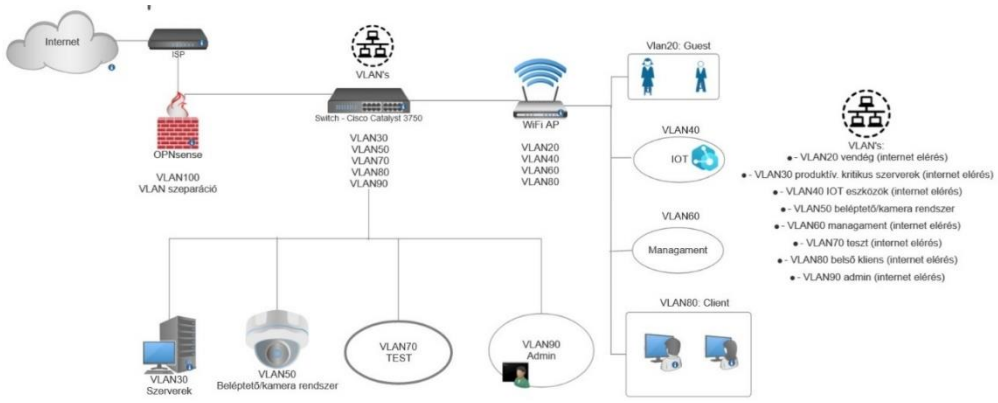
4.2.8 Mentés

Cél: Az üzleti információk elvesztésének kockázatát csökkentve biztonsági mentések létrehozása fontos fájlokról, ügyfél adatokról, pénzügyi nyilvántartásokról a természeti katasztrófák, lopások, hacker támadások elkerülése érdekében [56].

Intézkedések:

- a céges dokumentumokról rendszeresen biztonsági másolatokat kell készíteni, melyet a hálózattól logikailag elkülönített helyen kell tárolni ,
- a munkaegységeken használt szoftverekről, beállításokról biztonsági mentést kell készteni (felhő/helyi tároló eszköz),
- a dokumentumok tömörítve és jelszóval védve (titkosítva) kerülnek mentésre a GDPR követelményének eleget téve a OneDrive felhőben továbbá annak EU-n belüli mentés funkció lehetőségét kihasználva,
- lokálisan a VLAN30-ban elhelyezésre kerülő backup szervert fogom használni biztonsági mentésre.

A hálózat topológiáját a **4.1-es ábra** prezentálja.



***4.1. ábra**: a megtervezett hálótat topológiája*

5 PIACKUTATÁS – AZ ARCHITEKTÚRA EGYES ELEMEIHEZ ALKALMAZHATÓ MEGOLDÁSOK

A következő alfejezetben olyan eszközöket, alkalmazásokat gyűjtök és hasonlítok össze, amelyekkel az üzleti és biztonsági igényeket ki lehet elégíteni, valamint meg lehet valósítani azokat kisvállalati környezetben. Mivel a szervezet még nem rendelkezik a teljes infrastruktúrával (pl.: backup szerver, kamerarendszer, munkaállomások, IoT eszközök), így a piackutatás főként azon eszközökre történik, amely eszközök a hálózat gerincét képezik és a beüzemelésére lehetőségem van. Ilyen a tűzfal, Wi-Fi csatlakozási pont és a switch. A végpontvédelem pedig a közeljövőben kerül implementálásra, amint a végpontokkal a megbízó rendelkezni fog. Továbbá a saját switch használatához a megbízó ragaszkodik a kiadások csökkentése végett és a közeljövőben nem tervez vásárolni, így arra piackutatást még nem végzek el. A fejezet végén ismertetem az ügyféllel történő egyeztetés után az általa választott megoldásokat.

Alkalmazott válogatási irányelvek:

- kategória,
- funkcionalitás,
- költséghatékonyság (licence metodika),
- továbbfejlesztési/bővítési lehetőségek,
- üzemeltetési konstrukció/gyártói háttértámogatás,
- energia hatékonyság,
- eszköz életciklus (régi/új frissítések).

Az eszközökkel szemben támasztott követelmények az előző fejezetben részletezett elvárások figyelembevételével kerülnek meghatározásra.

5.1 Tűzfalak

Az eszközzel szemben támasztott követelmények:

Kategória	Kisvállalati (branch office) esetleg nagyobb otthoni környezetre
Funkcionalitás	Next generation firewall (VPN; IDS/IPS, statefull)
Licence metodika	Egyszerű és áttekinthető legyen; ár/érték arányban a lehető legtöbbet lehessen kihozni az eszközből
Továbbfejlesztési/bővítési lehetőségek	Igények jövőbeli növekedésével a kiadások és a hálózat átalakítása minimális legyen | naprakész verzió legyen, hogy a jövőben a gyártói frissítéseket kiadják az adott típusra is
Üzemeltetési konstrukció/gyártói háttér támogatás	Rendelkezzen lehetőleg magyarországi képviselettel és 7/24 helpdesk-kel | az üzembehelyezése és üzemben tartása egyszerű legyen | ne feltételezzen specifikus szaktudást | a vírusadatbázis naprakészen tartása automatizált legyen
Energia hatékonyság	Biztonsági és gazdasági okokból is az üzemeltetése nem igényeljen pluszköltségeket Fogyasztás, hűtés, az elektromos hálózat feszültség/áramerősség ingadozása ne okozzon kárt az eszközben
Eszköz életciklus	5-10 év /gyártó támogatás vége

***5.1. táblázat**: A tűzfal kritériumai*

A követelményeknek megfelelő ajánlott termékek:

5.1.1 FortiGate® FortiWi-Fi 61F Series

Előnyök:

- a típus 128GB SSD-vel van felszerelve, így a loggyűjtés megoldott, más eszköz kapacitását nem terheli,
- IPS funkcióval rendelkezik (real-time védelem), a vírus adatbázis frissítését a gyártó felhőjéből ütemezni lehet,
- IPSec/SSL VPN biztonságos távoli elérést biztosít,

- nincs lekorlátozva a VPN kapcsolatok száma,
- bővíthető, 5x GE RJ45 Internal Port-tal rendelkezik, amihez ha switchet csatlakoztatunk, megsokszorozódik a kapacitása,
- USB csatlakozóval is rendelkezik, IPhone eszközzel összekötve FortiGate applikáción keresztük menedzselhető.

Hátrányok:

- IPS, NGFW, Threat Protection Throughput funkciók lényegesen csökkentik a teljesítményét ahogy a mellékelt,
- VPN funkció szintén igencsak korlátozza a teljesítményt,
- kiadást jelent,
- fogasztás átlag/maximum: 17.2 W / 18.7 W.

Összefoglalva:

A licence metodika alapján kiemelkedő a többi termék között, mivel az összes eszközön alapból elérhető az összes funkció és a későbbi igényeknek megfelelően aktiválhatja/deaktiválhatja azokat bármikor, nincs szükség új licence megvásárlására. A korlátok az eszköz teljesítményében vannak. Így, ha több funkciót is ki szeretnénk használni egyszerre, az lényegesen csökkenti az eszköz teljesítményét ezért kellő előre tervezéssel kell megválasztani az eszközt, hogy esetleges továbbfejlesztési igények esetén ne legyen szükség egy eszköz megvásárlására.

Ár: kb. 250 000 HUF

5.1.2 Pfsense

A Pfsense egy opensource tűzfal. Gyártói támogatás is vásárolható hozzá, azonban ami miatt igazán megérheti, az pont az ingyenes mivolta annak előnyeivel és hátrányaival együtt.

Előnyök:

- szabadon méretezhető teljesítmény a hozzá rendelt erőforrással így mindig az aktuális igényekhez továbbfejleszthető,
- web grafikus felhasználói felülettel rendelkezik, így a konfigurálása nem igényel termékspecifikus szaktudást és távolról is elérhető,
- tűzfal, VPN, IDS/IPS egyben,
- open source,
- a legtöbb harmadik féltől származó szolgáltatással integrálható,
- load-balance (Multi-WAN és Load Balance),,
- inter-vlan routing kompatibilis
- automatikus biztonsági mentés lehetőség saját felhőbe,

- sok kiegészítő szolgáltatás elérhető hozzá így továbbfejleszthető és személyre szabható.

Hátrányok:

- a webes grafikus felhasználói felület (GUI) korlátozott beállítási lehetőségekkel rendelkezik,
- nincs magyarországi gyártói képviselet és a technikai támogatás már nem ingyenes, valamint kevésbé biztosított,
- kevés dokumentáció érhető el hozzá az interneten,
- a beállított konfigurációkhoz mivel webes felületen történik, így fennáll a veszélye, hogy mások is hozzáférhetnek.

Összefoglalás:

Mivel ingyenes, így a leginkább költséghatékony megoldás. Hardware korlátozottsága nincs, mivel bármikor lehet allokálni hozzá plusz erőforrást, ezáltal könnyedén továbbfejleszthető, ha új funkciókat, kiegészítőket szeretnénk hozzárendelni. Mivel nyílt forráskódú, így a legtöbb harmadik féltől származó szolgáltatással, alkalmazással összekapcsolható, konfigurálható. A webes grafikus konfigurációs felületet ha illetéktelen eléri, akkor ez veszélyt jelent az egész hálózatra. Gyártói háttértámogatás ingyenes verziónál nem biztosított így, ha valamilyen hiba keletkezik a működésében, azt a felhasználónak kell elhárítania. Azonban vásárolható hozzá licence amiért cserébe gyártói támogatás is igénybe vehető.

Ár: ingyenes

Support: 399 / 799 USD per year

Netgate fizikai eszközzel: 189 USD

Cloud: 0,01/hr

5.1.3 OPNsense

Elődje a fent említett Pfsense, így igen hasonló tulajdonságokkal bír, tehát opensource, ingyenes, de vásárolható hozzá gyártói támogatás. Amiben azonban több a pfsense-nél, hogy dobozos termékként is megvásárolható business változatban, valamint a többféle support szolgáltatásból választhatunk Lehetőségünk van kiegészítésként további szolgáltatásokat és alkalmazásokat hozzárendelni, melyek kifejezetten hozzá lettek tervezve, mint például a Zenarmor (Sensei), vagy a Proofpoint ET Pro Ruleset mely egy network alapú IDS.

Licence metodikát tekintve igencsak körültekintőnek kell lennünk, mivel van egy alapdíj, ami kizárólag a Branded verziót tartalmazza és évi 2 frissítést. Továbbá van Business

verzió, amihez tartozik dokumentáció és néhány plusz hasznos szolgáltatás. Support szolgáltatást külön kell vásárolni minden esetben, de csak support szolgáltatás egymagában nem vásárolható. A fenti szolgáltatások valamelyikét (Brand vagy Business edition) mindenképpen megkellene vásárolni.

Összefoglalás:

A Pfsense-hez képest nagyobb szabadságunk van a számunkra megfelelő verziót megvásárolni, amennyiben a licenc verziót szeretnénk igénybe venni. Több lehetőség közül választhatunk és a támogatást paletta is színesebb. Egy újabb, modernebb „megbrandelt" mégis opensource termékről van szó. Ez természetesen a licenc metodika és az árak is tükrözik.

Ár: ingyenes

Branded version: 2198 EUR végleges változat vagy 800 EUR/year

Business version: 150 EUR/year

Support: 300-1680 EUR

5.2 Wi-Fi csatlakozási pontok (AP-k)

Az eszközzel szemben támasztott követelmények:

Kategória	Kisvállalati (branch office) esetleg nagyobb otthoni környezetre
Funkcionalitás	Bővíthető legyen további AP-okkal/Mesh | VLAN támogatás | minimum 4 Wi-Fi SSID
Licence metodika	-
Továbbfejlesztési/bővítési lehetőségek	Igények jövőbeli növekedésével a kiadások és a hálózat átalakítása minimális legyen | Naprakész verzió legyen, hogy a jövőben a gyártói OS frissítéseket kiadják az adott típusra is | több Wi-Fi SSID-t is lehessen létrehozni
Üzemeltetési konstrukció/gyártói háttér támogatás	Elérhető legyen megfelelő és részletes dokumentáció a konfigurálásához
Energia hatékonyság	Biztonsági és gazdasági okokból is az üzemeltetése nem igényeljen pluszköltségeket | Fogyasztás, hűtés, az elektromos hálózat feszültség/áramerősség ingadozása ne okozzon kárt az eszközben
Eszköz életciklus	5-10 év /gyártó támogatás vége

*5.2. **táblázat**: A Wi-Fi csatlakozási pont kritériumai*

A követelményeknek megfelelő ajánlott termékek:

5.2.1 MikroTik hAP ac

Előnyök:

- jó ár/érték arány (40-50.000Ft),
- hasonló árkategóriájú termékeknél jóval több funkcióval rendelkezik,
- 2.4Ghz és 5.0Ghz es frekvencián is képes jelet sugározni,
- számos további access point csatlakoztatható hozzá,
- számos dokumentáció fellelhető hozzá,
- PoE kimenetek (2db),
- MU-MIMO funkció,
- számos VLAN létrehozható rajta a LAN-on,

- távoli elérés mobile app-al,
- rendkívül sokoldalú és személyre szabható szkriptekkel.

Hátrányok:

- a konfigurálása gyártóspecifikus szaktudást igényel,
- nincs rajta vendég Wi-Fi funkció.

Energia felhasználás:

- Number of DC inputs: 2 (DC jack, PoE-IN),
- DC jack input Voltage: 11-57 V,
- Max power consumption: 17 W (függ a felhasználástól),
- Cooling type: Passive,
- PoE in: Passive PoE,
- PoE in input Voltage: 11-57 V.

Összefoglalás:

a MikroTik hAP ac egy nagyon sokoldalú és kiválóan konfigurálható eszköz. Ebben az árkategóriában messze felülmúlja a versenytársait, ami a konfigurációs lehetőségeket illeti. Kiváló kisebb munkahelyi hálózatok üzemeltetéséhez. Bármennyi virtuális Wi-Fi AP létrehozható VLAN-ok számára, valamint tanúsítvány és MAC cím alapú RADIUS authentikácó is megvalósítható. A PoE kimenetek és a hozzá gyártott AP-k tökéletesen kielégítik az igényeinket és továbbfejlesztési lehetőséget is biztosítanak. Gyártói támogatás, dokumentáció bőven található hozzá. Az energiafelhasználás tekintetében nagyban függ a felhasználástól (max 17W). A frissített OS rendelkezik mobile app hozzáféréssel, ami távoli elérést és konfigurációt is biztosít. A gyártó intenzív fejlesztéseinek köszönhetően mára felhőn keresztül számos fejlesztés és funkció érhető el hozzá [57].

5.2.2 Linksys EA6350

Előnyök:

- rendelkezik vendég Wi-Fi-vel,
- kedvező ár (20-30.000 HUF),
- MU-MIMO funkció,
- Linksys app support,
- Linksys Smart Wi-Fi Tools (távoli elérés).

Hátrányok:

- nincs POE csatlakozó,

- korlátozott VLAN konfigurációs lehetőségek,
- IPQ401x. kompatibilitásbeli problémákat okozhat

Energia felhasználás:

- Reported Power (Watts): 5.47
- 12V, 2A.

Összefoglalás:

A Linksys EA6350 széria az kiemelkedően jó árazású eszköz a szolgáltatásaiért cserébe. Előny, hogy rendelkezik vendég Wi-Fi funkcióval, ami kissé ellensúlyozza a létrehozható VLAN-ok számának korlátját. Konfigurációs nehézségeket és inkompatibilitást eredményezhet IPQ401x standard használata a VLAN-ok használata során vagy további szolgáltatás igénybevételét igényelheti (OpenWrt) [58].

5.2.3 Cisco Meraki Go GR10

Előnyök:

- egyszerű konfigurálhatóság és menedzselés GUI-n keresztül mobil app-al is (VPN, weboldal blokkolás, adatforgalom limit stb…),
- A VPN konfigurálás GUI-n keresztül nagyon egyszerű,
- 50db kliens kiszolgálására képes 500 négyzetméteren belül,
- rendelkezik izolált vendég Wi-Fi-vel és hozzá tartozó beléptető oldallal,
- frissítés és support tartozik hozzá,
- priotizált Wi-Fi sávszélesség,
- MU/SU-MIMO,
- Cisco OS,
- PoE csatlakozó (1db).

Hátrányok:

- maximum 4db SSID létrehozására ad lehetőséget,
- magyarországi forgalmazónál nem kapható,
- korlátozott konfigurálhatóság (CLI hiánya),
- $230.85.

Energia felhasználás:

- power over Ethernet: 37 - 57 V (802.3af compatible),
- alternative 12 V DC input,
- power consumption: 11W max (802.3af).
- power over Ethernet injector sold separately.

Összefoglalás:

Modern, egyszerűen konfigurálható eszköz. Az átlagnál jóval több, funkcióval rendelkezik. Kényelem szempontjából nagy előny, hogy mobil appal felhős GUI-n keresztül is konfigurálható sok funkció, viszont biztonsági szempontból ez kockázat. Az ügyféltámogatás magas színvonala szintén előny. A Cisco OS a konfigurálás szempontjából további pozitívumot jelent. A 4db SSID viszont számunkra éppen elég, így ez korlátot jelent a továbbfejlesztési lehetőségek tekintetében. Továbbá az ára viszonylag magas és inkább a kényelmi funkciókra koncentráltak a fejlesztésénél. A szolgáltatások tekintetében az átlagnál kicsit jobb, azonban ár-érték arányban (mivel a kínált kényelmi funkciók számunkra kevésbé priorizáltak) drágának számít [59].

5.3 Végpontvédelem

Kezdetben külön szolgáltatásként csak végpontvédelmet veszünk igénybe az alábbi táblázatban feltüntetett követelményeknek megfelelően. Napi szintű sérülékenység menedzsmentre, threat/malware analízisre, XDR illetve SIEM monitoring-ra a cégnek nincs kapacitása. Ezeket a lehetőségeket továbbfejlesztési lehetőségként fenntartjuk szakemberek számára, külön szolgáltatásként megvásárolva. Ez történhet egyszer rendszeres automatizált sérülékenység vizsgálattal és/vagy SOC szolgáltatásként a logokat - win-event logs, syslogs, végpontvédelem logjai – SIEM rendszerbe továbbítva. Ezekről a lehetőségekről szintén készül piackutatás.

Az eszközzel szemben támasztott követelmények:

Kategória	Kisvállalati (branch office) esetleg nagyobb otthoni környezetre
Funkcionalitás	Végpontok megfelelő védelme | események logolása | ütemezett scan | heti report készítés | ne terhelje túl a rendszererőforrásokat
Licence metodika	Áttekinthető licence metodika | Legalább 10 eszközre 1 éves licence-el számolva |
Továbbfejlesztési/bővítési lehetőségek	központi menedzselhetőség/SIEM rendszerekkel kompatibilitás |
Üzemeltetési konstrukció/gyártói háttér támogatás	Elérhető legyen megfelelő és részletes dokumentáció a konfigurálásához | magyarországi képviselet
Energia hatékonyság	-
Eszköz életciklus	gyártó támogatás vége (legalább 5 év)

***5.3. táblázat**: Végpontvédelem kritériumai*

5.3.1 Trend Micro Apex One

Gartner Overall Rating: 4.6/5

Előnyök:

- naprakész vírus adatbázis,
- bővíthető adatbázis (URL és IP-cím feketelista hozzáadás),
- live monitoring funkció,
- központi managament felületen (Apex Central) keresztül könnyen kezelhetőek a végpontok,
- letisztult, személyre szabható dashboard(ok),
- önálló működés,
- policy-k létrehozása,
- reportálási lehetőség,
- továbbfejlesztési lehetőségek (email védelem, XDR sandbox, szerver védelem),
- on-premis és cloud szolgáltatásként is igénybevehető,
- SIEM APP-ok rendelkezésre állnak.

Hátrányok:

- a bejelentésekre megtett intézkedések reakcióideje kissé lassú,
- relatív nagy rendszererőforrás igény,
- a policy managament kevésbé felhasználó barát,
- relatív magas ár,
- a központi managament távoli elérést nem tesz lehetővé,
- a teljeskörű védelem több terméket igényel.

Ár: relatív magas

Továbbfejlesztési lehetőségek:

- TM Deep Discovery Director (email védelem),
- TM Vision One (IDR, XDR, Machine Learning),
- szerver védelem,
- Deep Security (minden komponens központilag kezelhető, összehangolható) [60].

Összefoglalás:

A naprakész vírus adatbázis hatékony védelmet biztosít a végpontok tekintetében. Észrevétlen működés, a felhasználót csak indokolt esetben zavarja meg a munkában. Detektál, beavatkozik és fejleszthető (host alapú behatolásgátló rendszert (HIPS) használ az ismert és ismeretlen sebezhetőségek kivédésére, mielőtt a javítás elérhető vagy

telepíthető lenne.) A machine learning által feltérképezi a felhasználók szokásait és a nem megszokott tevékenységeket rögzíti. Továbbfejlesztési lehetőségei által egy vállalat teljeskörű IT biztonsági védelmét a gyártó által le lehet fedni. SIEM rendszerekhez APP-ot biztosít. A rendszerigényei azonban viszonylag nagyok – nagy memória igény és a teljes vizsgálat terheli a processor. Összességében az egyik legjobb termék a piacon, ez azonban az árán is megmutatkozik. Ár/érték arány magas, inkább nagyobb vállalati környezetben éri meg alkalmazása.

5.3.2 Symantec Endpoint Protection

Gartner Overall Rating: 4.4/5

Előnyök:

- ”all-in-one”, széleskörű védelem egy termékben,
- letisztult licence methodika,
- alacsony rendszererőforrás igény,
- hatékony, nagy, naprakész vírusadatbázis,
- böngésző védelem,
- ransomware védelem,
- hatékony tűzfal beépített IPS (egyénre szabható konfigurációs lehetőséggel),
- Symantec’s Insight Intelligence (speciális védelem a C&C kommunikációk, CryptoLocker és drive-by downloads ellen),
- reportálási lehetőség,
- policy létrehozási lehetőség,
- központi managment (felhőben, távoli elérés),
- machine learning alap szolgáltatásként (Behavior monitoring-”SONAR”),
- system lockdown (automatikusan blockolja a gyanús tevékenységeket és felajánlja az engedélyezést),
- egyértelmű fenyegetésnél automatikus végpont szeparálás.

Hátrányok:

- exploit adatbáízis kissé késve reagál az új fenyegetettségekre,
- konfigurálása, (különösen a tűzfal és IPS) kevésbé felhasználóbarát,
- kevés dokumentáció érhető el hozzá,
- akár speciális tudást is igényelhet a hatékony üzemeltetése (kevésbé automatizált),
- a teljes scan hosszú idő vesz igénybe,
- support kevésbé elérhető.

Ár: jó ár/érték arány

Továbbfejlesztési lehetőségek:

Endpoint Security Complete- teljeskörű védelem [60] [61].

Összefoglalás:

Erőssége, hogy alapvetően a teljeskörű védelemre összpontosít. Már az alap megoldás (Endpoint Security Enterprise) is. a ES. Complete pedig lefedi az egész vállalat védelmét minden végpontvédelmi szegmensből. További erőssége a már alap verzióban is elérhető magas színvonalú tűzfal és beépített IDS-el, azonban a konfigurálása komplikált (amit a megosztott vélemények is tükröznek, sokan kikapcsolják és inkább a windows defender tűzfalát használják). Ransomware védelemmel. Alapjában véve az egyéni konfigurációja kevésbé felhasználóbarát, így az erősségei egyben gyengeségek is, inkább zavaróak lehetnek átlag felhasználó számára. Hatékony használata szaktudást igényelhet. Dokumentáció kevés, a support szolgáltatás gyenge minőségű. Összességében, ha van kapacitás a konfigurálására, korszerű, hatékony és átfogó védelmet biztosít. Jó ár/érték arányban és a licence metodikája is átlátható. Kis- és középvállalatoknak ideális megoldás lehet.

5.3.3 Windows Defender for Endpoint (MDE) plan 1

Gartner Overall Rating: 4.3/5

Előnyök:

- felhasználó barát,
- egyszerű policy létrehozás,
- egyszerű tűzfal konfiguráció,
- központi managament (Microsoft 365 Defender portal),
- web protection és filtering,
- nagyon jó ár/érték arány,
- átfogó védelem,
- alapfelszereltsége a Windows OS-nek,
- sokoldalú továbbfejlesztési lehetőségek,
- felhasználóként 5 eszköz,
- viselkedés alapú észlelés és élő reagálás,
- kis- és középméretű vállalatokra optimalizálva,
- modern, az egyik legújabb fejlesztés a piacon,
- könnyen implementálható,
- reportálási lehetőség,
- a saját operációsrendszeréhez specializálva,
- email védelem (online Exchange védelem).

Hátrányok:

- viszonylag új a piacon, kevés tapasztalattal,
- hatékonyságát tekintve vannak jobb termékek is a piacon hasonló áron,
- a zero-day sérülékenységekre a patch-ek sokszor hibásan kerülnek ki,
- a felhasználói felület hétköznapi felhasználónak komplex lehet,
- kevésbé alakítható a felhasználó speciális igényeire, illetve speciális tudást (query-k létrehozása) vagy plusz költséget igényelhet,
- a támogatás és a dokumentáció kevésbé összpontosít a felhasználók egyéni igényeinek kiszolgálására,
- a reportálás nem elég részletes.

Ár: Microsoft Office 365-höz kiegészítésként igényelhető

Továbbfejlesztési lehetőségek:

- plan 2,
- Microsoft Defender Vállalati Verzió,
- további bővített kiegészítő szolgáltatások/termékek elérhetőek, így a továbbfejlesztési lehetőségek biztosítottak.

Ár: egyéni ajánlatkérés (az MS Office 365 alapkövetelmény, az MDE-kiegészítésként vásárolható hozzá) [62] [63].

Összefoglalás:

Mivel az Office 365 elengedhetetlen egy vállalat működéséhez, ideális megoldást biztosít az MDE választása kiegészítésként. A legkorszerűbb és sokoldalú megoldásokat alkalmaznak. Felhasználóbarát felület, letisztult reportálás, alapszintű, de átfogó védelem. A saját operációs rendszerének a sérülékenységeit könnyen ismerheti a gyártó, mégis, a professzionális végpontvédelem területén még tapasztalatlannak számít. Azonban intenzív munkát fektetnek a fejlődésbe, ami mindenképpen pozitívum. A közeljövőben akár felzárkózhat a csúcs kategóriás végpontvédelemre specializálódott versenytársai mellé. Ezek tekintetében érthető, hogy jelenleg csak kis- és középvállalatokra specializálódnak, számukra viszont a termékkapcsolás (Office 365) által kézenfekvő és költséghatékony opció. A negatívumok ellenére funkciók tekintetében megfelelnek az alap követelményeknek és elvárásoknak egy kis esetleg középméretű vállalkozás esetén. Kevésbé koncentrál a felhasználók speciális igényeinek kiszolgálására, inkább több termék létrehozásával, a vállalat méretére koncentrálva próbálja bővíteni, optimalizálni a szolgáltatás/termék palettát. Ez valószínűleg üzletpolitikai megfontolásokra vezethető vissza. A célzott vásárlóközönség számára valószínűleg optimálisabb is lehet egy ilyen szolgáltatás, mert nincs kapacitásuk IT biztonsági szakemberek alkalmazására. A funkciók teljeskörű kihasználása által és egy

kis utánajárással azonban lehetőséget adhat egy IT biztonsági szempontból felelősen gondolkodó cég számára a hatékony védelemre.

5.4 A piackutatás eredménye

Miután az ügyfél számára bemutatásra kerültek a közeljövőben üzembe helyezhető, a hálózat gerincét képező eszközökre elvégzett általam javasolt megoldások, a következő eredmények születtek.

5.4.1 Tűzfal

A továbbfejlesztési lehetőségei, a későbbiekben megvásárolható szolgáltatások és kompatibilitás más gyártokkal kedvezőbb a pfSense-el szemben, valamint a FortiGate-nél olcsóbb (ingyenes), így az **OPNsens**-re esett a választás.

Az ügyfél rendelkezésére áll két régebbi, már gyártói támogatást nélkülöző tűzfal hardware, így azt a megoldást választottuk, hogy az OPNsense-t feltelepítjük az egyikre. Mivel a költséghatékonyságra törekvés az egyik fő szempont, így ez semmilyen plusz költséggel nem járt az SSD vásárlást kivéve.

Az OPNsense egy következő generációs (next generation), ingyenesen elérhető, csomagszűréssel bíró (stateful), IDS/IPS-el, VPN-el és Syslog-ng logolással rendelkező nyílt forráskódú tűzfal A támasztott követelmények mindegyikének megfelel. Az interneten rengeteg dokumentáció elérhető hozzá, így a beüzemelése sem okoz gondot, a vírusadatbázis frissítését pedig ütemezni lehet.

5.4.2 Wi-Fi Csatlakozási Pont (Wi-Fi AP)

Abban az árkategóriában, amelyet a megbízó megjelölt, a **MikroTik hAP ac** funkcióinak és szolgáltatásainak számában is egyaránt felülmúlja a piaci versenytársait. Sávszélességtől függően bármennyi SSID létrehozható rajta, ami esetünkben a VLAN-ok tekintetében igen lényeges. Dokumentáció szintén elérhető hozzá, nagyobb mennyiségben is mint a többi termékhez. Képes RADIUS authentikációra, VPN szolgáltatás, valamint további eszközökkel trunk módban összekapcsolva a bővítési, továbbfejlesztési lehetőségek bőven adottak.

5.4.3 Végpontvédelem

Mivel Office 365-re az üzleti igények miatt mindenképpen szükség van, így hozzá kiegészítő szolgáltatásként a **Windows Defender for Endpoint (MDE) plan 1** a legköltséghatékonyabb választás. Üzemeltetése nem igényel szaktudást, kkv-k számára tervezett, rendelkezik webszűréssel és reportálási lehetőséggel, IDS szolgáltatással így a támasztott követelményeknek megfelel. A licence metodikája segíti a továbbfejlesztést, bővítést. Microsoft termék lévén beleillik a szervezet ökoszisztémájába.

A másik két megoldással szemben egyszerűbb a beüzemelése, üzemeltetése, ”felhasználóbarátabb”, és lényegesen olcsóbb is. A legtöbb céges környezetre szánt végpontvédelmi eszköz, miként a Trend Micro is inkább a nagyobb vállalati környezeteket célozta meg a szolgáltatásával/áraival, míg a választott termék kifejezetten kkv-kra specializálódott. A Symantec pedig legalább olyan hatékony, mint a Windows Defender for Endpoint (MDE), talán még széleskörűbb is a védelme, azonban lényegesen drágább és szolgáltatásainak teljeskörű kihasználása, hatékony üzemeltetése szaktudást igényelhet, amelyre a cégnek nincs kapacitása.

Továbbfejlesztési lehetőségei adottak, ha a vállalkozás a gyarapodást követően később saját email szerver üzemeltetése mellett dönt, vagy szüksége lenne további végpontvédelmi szolgáltatásokra, esetleg SIEM rendszerre, esetleg speciálisabb, precízebb védelemre, monitorozásra, csomagváltással könnyedén kivitelezhető a továbbfejlesztés, nincs szükség termékváltásra.

6 IMPLEMENTÁLÁS

A következő fejezetben dokumentálom a megbízó által választott és rendelkezésre álló eszközöket, valamint ellenőrzöm helyes működésüket.

6.1 Switch implementálása

Cél, hogy a hálózathoz csatlakoztatott eszközök megfelelő IP tartományból kapjanak IP címet és megfelelő jogosultságokkal rendelkezzenek. Ehhez a DHCP és VLAN szolgáltatásait konfigurálom és veszem igénybe.

Az átláthatóság érdekében létrehozott DHCP pool-ok a későbbiekben hozzájuk rendelt VLAN-okról kapták az elnevezésüket. Az IP alhálózati tartományok a VLAN számának megfelelő konvenció alapján kerültek kiosztásra, ahogy az 1. mellékleten látszik.

Minden pool-ból az első 10 kiosztható címet kizártam a felhasználhatóságból, amennyiben a későbbiekben szükség lenne a manuális kiosztásukra (2. számú melléklet). A virtuális belső hálózat létrehozásához a switch portjait access módba kellet állítani és a szükséges VLAN-t hozzájuk rendelni az alábbi ábra metodikájának alapján.

- 1-2. port: management VLAN60
- 2-4. port: vendég VLAN20
- 5-6. port: produktív VLAN30
- 7-8. port: IOT VLAN40
- 9-10. port: kamera VLAN50
- 11-12. port: teszt VLAN70
- 13-14. port: belső VLAN80
- 15-16. port: admin VLAN90

Az így létrehozott VLAN-okhoz a már létrehozott DHCP pool-ok szerinti IP alhálózatot rendeltem a 3. számú melléklet alapján. Ahhoz, hogy a VLAN-ok mindegyike továbbításra kerüljön mind a tűzfal, mind a Wi-Fi AP-k irányába, két portot a switchen Trunk módba állítottam valamint, a default nativ VLAN megszűntetése érdekében a VLAN 60-at állítottam be Natívnak (4. számú melléklet). Végül teszteltem a konfiguráció működésének helyességét. Ehhez egy laptopot csatlakoztattam a switch adott portjához és ellenőriztem, hogy a csatlakoztatott porthoz tartozó VLAN címtartományából kerül-e az IP kiosztásra. A switch 4-es portjára csatlakozva megfelelő tartományból kaptam IP címet, vagyis a 20-as (vendég)VLAN-ból. A konfiguráció helyes működéséről az 5. számú melléklet tanúskodik.

6.1.1 Biztonság megerősítése

Miután meggyőződtem a switch megfelelő működéséről, kiadtam biztonságot megerősítő parancsokat. Beállítottam a jelszó minimális hosszkövetelményét 12 karakterre, a

konfigurációs módba történő belépéshez jelszót adtam meg ami alapján titkosítja a konfigurációs beállításokat. Bannert állítottam be figyelmeztetésként illetéktelen csatlakozási kísérlet esetére. A jelszavak megjelenítését a konfigurációs fájlban titkosítottam. A konzol portra történő csatlakozást jelszóhoz kötöttem és 5 perc inaktivitás esetén automatikus kijelentkeztetést állítottam be. A próbálkozásos támadás kivédésére limitáltam a bejelentkezések számának lehetőségét 2 percen belül 3 sikertelen bejelentkezés esetén 30 percre. Továbbá a trunk portokra kiadtam a nonegotiate parancsot. A switch nem használt portjait access módba raktam és hozzáadtam a vlan999-hez, valamint lekapcsoltam.

6.2 Wi-Fi Access Point implementálása

Cél, hogy a hálózathoz vezeték nélkül csatlakozó eszközök is a megfelelő VLAN-ba csatlakozzanak be. Ehhez elengedhetetlen, hogy a switch-en konfigurált DHCP szerver, valamint a létrehozott VLAN-ok konfigurációi érvényesüljenek a Wi-Fi csatlakozási ponton. A tervezésnek megfelelően a 20-as, 40-es, 60-as és a 80-as VLAN-oknak kell vezetéknélküli kapcsolaton keresztül elérhetőnek lenniük. Ezt úgy érem el, hogy a switch trunkportján továbbított VLAN-okhoz virtuális Wi-Fi interfészeket rendelek wlan3, wlan4, wlan5 és wlan6 néven. Beazonosításukhoz a VLAN nevét használom SSID-ként.

A létrehozott virtuális Wi-Fi interfészeket híd módba kell állítani, használniuk kell a tag-eket és mester interfésznek az alapbeállításként már működő, Wi-Fi interfészek valamelyikéhez kell rendelni (esetemben a 2,4GHz-es wlan1-hez, mivel ez a frekvencia ”erősebb”, hatékonyabban áthatol a falakon ezáltal nagyobb távolságban fogható).

Az eszközön alapállapotban híd létre van hozva és hozzá van rendelve az Ethernet portokhoz így új híd létrehozására nincs szükség, csak a VLAN szűrést kell beállítani rajta. Ahhoz viszont, hogy a VLAN szűrése megvalósulhasson, a hídon be kell állítani a VLAN-okat, pontosabban meg kell határozni, hogy melyik fizikai ethernet porton jön be az adott VLAN tag-ej, mi az és, hogy azt melyik virtuális Wi-Fi interfészen továbbítsa. A 20-as VLAN beállítása: vendég VLAN tag-je a 20-as, az ethernet2-es porton jön a switch irányából és a wlan6 „vendeg_Wi-Fi SSID-val ellátott interfészen kerül továbbításra. (Az 1-es port dedikáltan az internetelérést szolgálja, így a switch trunk módra konfigurált portja (GigabitEthernet1/0/23) és a Wi-Fi AP Ethernet 2-es portján került csatlakoztatásra.)

Az egyes virtuális Wi-Fi interfészek biztonsági profilján beállításra került a WPA és a WPA2-es titkosítás megfelelően komplex jelszóval a NIST ajánlása vezeték nélküli kapcsolatok IEE 802.11i alkalmazása esetén. A Federal Information Processing Standards (FIPS) által jóváhagyott titkosítás átesett a Wi-Fi tanúsítványt használó eszközök tesztelésén, így biztosítva van a megfelelően védett kommunikáció és az együttműködés ezen tanúsítvánnyal rendelkező eszközök számára. 2006 március 1-től minden Wi-Fi tanúsítvánnyal rendelkező eszköznek kötelező a WPA2 kompatibilitás,

valamint a WPA szabvány is engedélyezve maradt. Csak azok a Wi-Fi szolgáltatást biztosító létesítmények tüntethetik fel a Wi-Fi Zone logót, ahol biztosítva van a megfelelően biztonságos csatlakozási lehetőség az internetre. A megfelelően biztonságos vezeték nélküli kommunikáció esetén két féle módszert kell alkalmazni. A vezeték nélküli eszközöknek FIPS 140-2 tanúsítvánnyal és FIPS üzemmódban kell működniük, továbbá a hálózatok közötti vezeték nélküli kapcsolat során a VPN titkosítást végző moduljának egyaránt FIPS-140-2 tanúsítvánnyal kell rendelkeznie. 2003-ban a Wi-Fi Alliance a korábbi WEP-ben (Wired Equivalent Privacy) talált súlyos sebezhetőségek miatt kifejlesztette a WEP továbbfejlesztéseként a WPA-t. A WEP-et 1997-ben hozták létre és 2003-ig az IEE802.11 protokol része volt. Legfőbb sérülékenyége a titkosítás könnyű feltörhetősége, mivel az adatcsomag keretében a forrás és a cél nincs titkosítva, a támadó ezeket meghamisítva eltérítheti az adatcsomagokat (frame spoofing). A továbbfejlesztés tartalmazza többek között az EAP protokollt (Extensible Authentication Protocol), amely a hitelesítést szolgálja egy hitelesítő szerver által, amely legtöbb esetben RADIUS alapú [64]. Továbbá kiküszöbölték a visszajátszhatóságot, lehallgathatóságot. Míg a WPA-t a WEP sérülékenyégeinek kiküszöbölésére tervezték. A WEP továbbfejlesztése, a WPA2 a WPA azon továbbfejlesztése, amely teljes egészében megfelel az IEE 802.11i specifikáció összes követelményének [65]. A telephely helyszínén felmérem, hogy a környező Wi-Fi eszközök milyen frekvencián sugároznak, és beállítom a kevésbé használt csatornára.

Tesztelésként ellenőrzöm, hogy a Wi-Fi SSID-k láthatóak-e és hogy a rájuk csatlakozott eszköznek az IP, a megfelelő VLAN-hoz rendelt IP alhálózatból kerül-e kiosztásra. A konfiguráció helyes működését a 6. mellékleten mutatom be.

6.3 Tűzfal implementálása

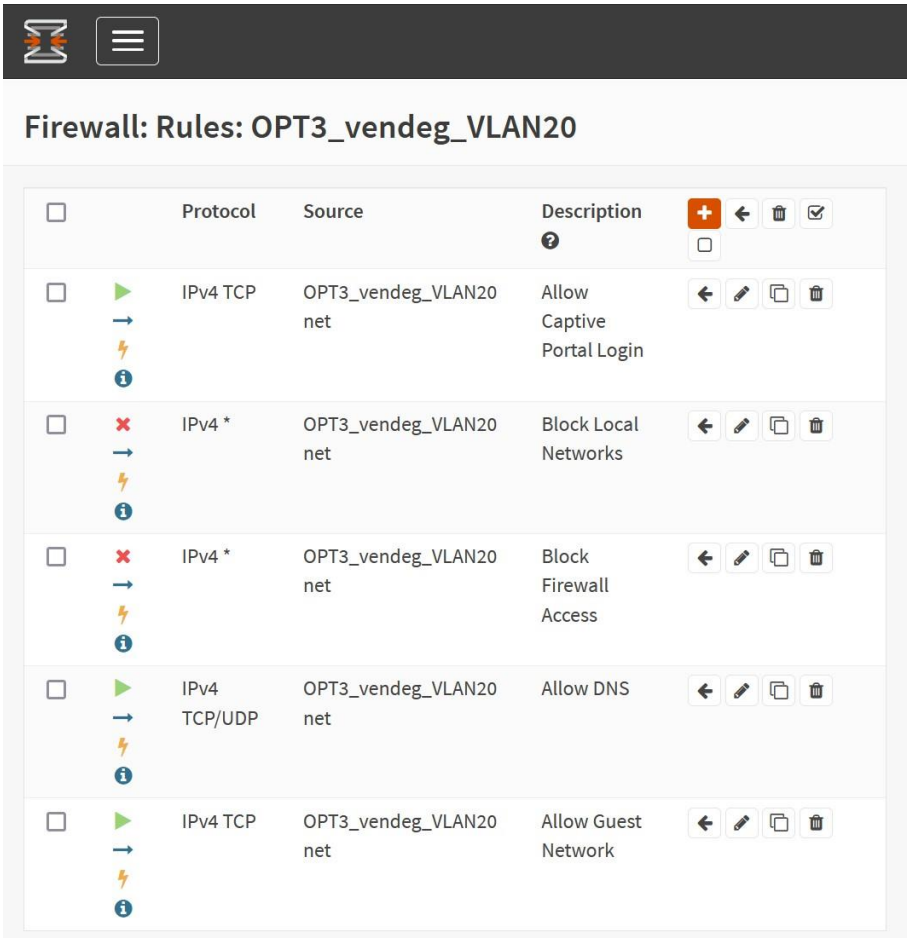
Cél, hogy az átjárhatóság megvalósuljon bizonyos VLAN-ok között, egyes VLAN-ok rendelkezzenek internetelérással a **4.2.3**-as fejezetben leírtak szerint, továbbá kiemelten fontos a tűzfal IDS és IPS szolgáltatásai által a hálózat peremvédelmének biztosítása.

6.3.1 Telepítés

Az implementálás során kezdeti nehézséget okozott az OPNsense telepítése a fizikai tűzfal eszköre, mivel csak USB 2.0 szabványú adathordozóról lehetett telepíteni a szoftvert, valamint a serial kapcsolaton keresztül az átviteli sebességet módosítani kellett 112500-ra 9600-ról.

A sikeres telepítést követően a konfigurálás során létrehoztam a megfelelő VLAN-okat a switchen konfiguráltakkal megfelelően. A VLAN-ok master interfésze a 2-es tűzfal fizikai em02-es portjára lett beállítva, ami a switch trunk módra konfigurált 24-es portjával került csatlakoztatásra. Ezt követően a tűzfalszabályok által biztosítottam a

meghatározott VLAN-ok közötti átjárhatóságot be. Kiemelném a kritikus fontosságú vendég Wi-Fi VLAN20 tűzfalszabályait melyet az alábbi, **6.1-es ábra** mutat be.



***6.1. táblázat**: Vendég VLAN tűzfalszabályai*

A tűzfalszabályok megalkotása által törekedtem arra, hogy csak a valóban munkamenet folytonosságát biztosító portok legyenek nyitva az internet irányába. Ilyen a DNS feloldást biztosító port alapértelmezés szerint az 53-a. Mivel a DNS feloldás többször időtúllépés miatt nem történt meg, így hozzáadtam a beállításoknál a Cloudflare és a Google címeit is. Az összes többi port lezárásra került. Az internetelérést úgy definiáltam a tűzfalszabályoknál, hogy IPv4-TCP Protokollal a 443 HTTPS porton valamint a DNS kommunikációs portján engedélyeztem az adatforgalmaz. Ezáltal az összes többi porton a komminukáció blockolva lett, így szűkítettem a sérülékenységre esélyt adó portok számát.

A tesztelés során a managament VLAN60 DNS feloldását blockolta a tűzfal, így nem volt internet hozzáférés. A hibát egy korábbi, switchen kiadott beállítás okozta. Mivel a default natív VLAN1-et úgy szüntettem meg, hogy a VLAN60-ra állítottam be, így ez egy prefox-et adott az IP címéhez és ez okozta a problémát. A natív VLAN-ra a switchen

létrehoztam egy új VLAN-t és disable-be állítottam, vagyis kikapcsoltam ezáltal szüntetve meg a switch ezen irányú sérülékenységét.

6.3.2 Konfigurálás, biztonsági beállítások

A tűzfal és a hálózat minden szegmense ezek után megfelelően működött. Következett az OPNsense biztonsági megoldásainak aktiválása. Először aktiváltam a Domain Name System Security Extensions (DNSSEC) szolgáltatást, ami ellenőrzi a tartomány név és titkosítás validitását, valamint, hogy a feloldott IP-cím valóban a hozzá rendelt tartománynévhez tartozik-e. Engedélyeztem a "bogon" szűrést, ami által a tűzfal megakadályozza a regisztrálatlan, vagy hamis IP címekkel történő kommunikációt valamint tiltottam a WAN portra érkező belső IP-cím tartományok kéréseit. Letöltöttem és frissítettem az IDS szabályokat és beállítottam az szignatúra adatbázis ütemezett frissítését minden éjszaka 01:10-re. Ezt követően beállítottam a rendszeridőzónát, ami a logok visszakövethetősége és értelmezhetősége szempontjából is nélkülözhetetlen. Végül engedélyeztem az IDS és IPS szolgáltatást a tűzfalon.

A tűzfal rendelkezik syslog-ng szolgáltatással. A logok rotálását 7 napra állítottam.

Az OPNsense Firmware frissítése előtt futtattam a biztonsági auditot, ami 8 sérülékenyéget adott fel. A firmware frissítésével ezek a sérülékenységek javításra kerültek.

Mivel a vállalkozásnál nem lesz külön személy a hálózat monitoring feladatainak betöltésére, így a Monit szolgáltatást nem aktiváltam, azonban a későbbiekben itt lehetőségünk lehet különböző riasztások és hozzájuk tartozó akciók automatikus kiküldésére és végrehajtására (pl.: VPN kapcsolat megszakadása esetén újraindítja a VPN szolgáltatást, vagy a backup szerver működésének figyelése és riasztás generálása és email kiküldése, szkript végrehajtása hiba esetén, kamerarendszer működésének fennakadásai stb.) . A logok gyűjtése és lementése külső adattárolóra a későbbiekben audit formájában reportálás készítésére is lehetőséget ad.

6.3.3 Az IDS/IPS tesztelése

Az IDS/IPS funkció működésének tesztelésére egy eicar.txt file-t töltöttem le, amit első próbálkozásra le is töltött és a végpontvédelem jelzett csak rá. Ezután beállítottam, hogy az IDS nem csak a WAN, hanem a LAN portot is figyelje. Ezután a tesztfile még mindig eljutott a végpontig, így telepítettem az antivirus (ClamAV, c-icap)beépülő modulokat valamint letöltöttem a Suricata szignatúra adatbázisát. A szolgáltatások között engedélyeztem és beállítottam a web proxy használatát. Fontos lépés volt, hogy az olyan weboldalaknál, amelyeknél személyes adatokat adok meg, a proxy szerver ne lásson bele a forgalomba, ott ne a tűzfal tanúsítványát használja (No SSL Bump). Létrehoztam a tűzfal SSL tanúsítványát, majd a tanúsítványt importáltam a böngészőbe. Ekkorra a tűzfal riasztott az eicar tesztfájl letöltésére.

6.3.4 VPN telepítése a tűzfalon

A távoli elérés biztosításának érdekében a tűzfalon VPN kapcsolatot hozok létre. Ehhez az OpenVPN alkalmazást fogom igénybe venni.

Először létrehozom a tanúsítványt. Utána beállítom a VPN szervert. A titkosításhoz AES-256 algoritmust alkalmazok, amiről kijelenthető, hogy megfelelően biztonságos. AVPN-hez csatlakozható kliensek számát 10-re korlátoztam. A varázsló létrehozta a tűzfalszabályokat a VPN-hez mind a WAN porthoz, mind pedig egy külön VPN VLAN-ban. A szabály szerint a VPN-en csatlakozott felhasználó eléri a teljes hálózatot. Jelenleg erre van szükségünk, mint admin felhasználónak. Létrehoztam egy VPN felhasználót, akihez hozzárendeltem a korábban elkészített tanúsítványt. A későbbiekben más felhasználók létrehozásánál (pl. munkavállaló) külön profilt fogok létrehozni korlátozott engedélyekkel és a hozzá tartozó VLAN IP tartomány beállításával, hogy a csatlakozás során hozzá tartozó tűzfalszabályok legyenek érvényesek. Végül letöltöttem a tanúsítványt és importáltam a végpontra telepített OpenVPN klienshez a felhasználó profiljának tanúsítványát.

6.4 Továbbfejlesztési, bővítési lehetőségek, ajánlások

Az implementált hálózatnak vannak gyenge láncszemei, amik hatással lehetnek az üzletmenet folytonosságára. A hálózat tervezéséből adódóan alkalmas a bővítésre, amire szükség is van, hogy az üzletmenet folytonossága teljes a lehető legbiztosabb módon biztosítva legyen. Ilyen gyenge láncszem a tűzfal és a switch. Amennyiben ezek valamelyike meghibásodik, annyiban a hálózat nem képes megfelelően betölteni a szerepét. Ezt a jelenséget nevezik “Single Point of Failure”-nek. Ajánlott további tűzfal és switch beszerzése és ezen eszközök ugyan ilyen módon történő felkonfigurálása és a switchek esetében a trunk portok összekapcsolása, a tűzfal esetében pedig az egyik készenléti módba kapcsolása. Továbbá a végpontok hálózatba kapcsolása esetén további teendő a tűzfal szabályrendszerét VLAN-ok megadása helyett IP címekre pontosítani.

7. INTERJÚ BÁNSZKI ZSOLTTAL, A 4IG NYRT. KIBERBIZTONSÁGI ÜZLETÁGÁNAK IGAZGATÓJÁVAL

Milyen a KKV-k helyzete digitalizáció szempontjából magyarországi és külföldi viszonylatban?

Úgy látom, hogy Magyarországon sokkal jobban állunk, mint mondjuk 2-3 évvel ezelőtt köszönhetően sajnos a Covid-nak. Előtte a cégek mindent az addigi megszokott módon oldottak meg: úgy, ahogy sikerült, évtizedekkel ezelőtt bevált módszerekkel. Azonban a pandémia hatására ki kellett lépniük ebből a komfortzónából. Ez az egyik oka annak, hogy mára a digitalizáció az eddigiekhez képest jobban áll Magyarországon kis- és középvállalati viszonylatban is. A másik ok pedig az állami gépezet és apparátus digitalizációt megkövetelő hatása. Olyanokra gondolok itt, mint például az ügyfélkapu, online NAV stb… Ugyanis, miután a NAV digitálisan, elektronikus úton kéri be az adatokat, innentől kezdve nem úgy van, mint régen, hogy a könyvelő dossziékkal a hóna alatt sétál be a kormányablakhoz. Ki van kényszerítve a cégektől a digitalizáció. Továbbá az online ügyintézési lehetőségek, melyek nagyban leegyszerűsítik, megkönnyítik és felgyorsítják az ügyeink intézését, szintén katalizálja ezt a folyamatot. Ezeknek is köszönhetően **a digitalizáció mára már egy nagyon alapvető szükséglet lett, olyan, mint a víz, megkerülhetetlen és nélkülözhetetlen.**

Meglátásod szerint milyen a hazai KKV-k helyzete IT biztonság szempontjából?

Na, ez már egy nagyon érdekes kérdés! Nemzetközi szinten annyival járnak előttünk, hogy egy picit tudatosabban használják ezeket a lehetőségeket, vagyis a digitalizációt. Hazai KKV szinten digitalizációt tekintve sajnos azt kell mondanunk, hogy kevésbé áldoznak a cégek szakmai munkára. Általában az a szempont, hogy szükség van valamire, például egy számítógépre és keresnek egy ismerőst vagy ismerős ismerősét, aki valamennyire ért a számítógépekhez és képes azt megcsinálni számunkra annyira, amennyire minimálisan szükségük van (pl. internet elérés, online pénztárgép, email-ek olvasása és küldése, Office alkalmazások, esetleg valamilyen vállalatirányítási rendszer). És itt véget is ér a történet. Egészen addig, amíg valamilyen váratlan esemény be nem következik. Abba már kevesebben gondolnak bele, hogy mi történik, ha például meghibásodik az egyetlen router, ami az internet eléréshez szükséges. Hogy akkor ennek következtében mi áll még meg? Gyakorlatilag minden. Vagy például leáll az egyetlen számítógép akár műszaki okból, vagy egy email-ben kapott/adathordozóról megnyitott káros adatállomány következtében, ami által megfertőződik az egész belső hálózat. Tehát az már nagyon jónak mondható, ha egy vállalat elgondolkozik azon, hogy mi történik például egy fent említett esetben. Kvázi a működésük lehetetlenülhet el egy időre. Olyan, mintha elmenne az áram, amire sokszor úgymond fel is készülnek azáltal, hogy az épület biztosításának a díjába beletartozik az az összeg is, ami egy ilyen esetet (áram kiesés) kárát enyhíti. Az IT biztonság szempontjából is érdemes lenne hasonlóan gondolkozni, hogy nekem most van egy kevés plusz kiadásom, ami majd megtérül akkor,

amikor egy nemvárt esemény hatására bevételkiesés következne be, de nem fog azáltal, hogy erre fel voltam készülve. Ezt a szakmában dolgozók számára természetesen nem kell magyarázni, de a KKV-k esetében sajnos még nem igazán tartunk ott, hogy ez evidencia lenne. Az egyik konferencián, amin előadhattam végre lehetőségem volt megválaszolni egy kérdést, amit már régen szerettem volna, ez pedig a következő: -„én egy vidéki kisvárosban vagyok karosszéria lakatos. Ugyan mégis miért válnék célpontjává bármilyen ország vagy szervezet hacker csoportjának?". Erre a válasz pedig az, hogy ha célpont nem is, de eszközzé bármikor válhat. Egy zombie hálózat tagjaként a szó szoros értelmében ő maga nem célpont, de egy nagyobb célpont támadásához eszközzé válhat. Ezek a nagyobb cégek, vállalatok pedig előbb-utóbb vissza fognak ütni, vagy a támadók veszik át az irányítást az eszközei felett, holott alapból semmi köze nem volt az adott konfliktushoz. És a kedves vállalkozó mindebből csak azt fogja érzékelni, hogy valamiért mindig meghibásodik a tűzfala/számítógépe/routere stb. aminek hatására nem tud dolgozni. A másik veszélyforrás, aminek szintén teljes létjogosultsága van, az a ransomware. Ezekkel bármilyen kisvállalkozás is szembesülhet és tapasztalatból tudjuk, hogy ennek a veszélye és előfordulási gyakorisága jelentősen megnőtt az utóbbi időszakban. Ezek mind megalapozott és komoly veszélyek. **Tehát a kérdésre válaszolva sajnos azt kell mondanom, hogy a hazai KKV-k még nem jutottak el arra a szintre, hogy az IT biztonságukra tudatosan gondoljanak és költsenek. Sokan csak a kiadást látják benne, a megtérülést nem.**

Szükség van-e egy KKV-nak IT biztonsági szolgáltatásra?

Ez egy nagyon érdekes kérdés, hogy egy KKV hogyan gondolkozik. Valamilyen kiberbiztonságra mindenképpen szüksége van. Az, hogy milyen szintű kiberbiztonságra van szüksége, az nagyon nagyban függ attól, hogy milyen méretű és kitettségű az az IT infrastruktúra, amivel rendelkezik. Kitettség alatt azt értem, hogy milyen függősége van az IT infrastruktúrától. Ha például egy tészta gyárat nézünk, ahol a tésztakészítő gép, ha van áram, akkor megy, és ha kikapcsolunk minden számítógépet, akkor sem történik leállás, akkor ebben az esetben nyilvánvalóan kisebb mértékben van szüksége rá. Azonban, ha ugyanez egy CNC üzemben történik, ahol a munka példányok számítógépeken keresztül érkeznek és egy gép biztonsági okokból leáll, akkor ott a termelés is leállhat. Ez már egy sokkal komolyabb kérdéskör. Amit ezzel a példával szemléltetni és mondani szeretnék az nem más, mint hogy kockázat arányosan kell az IT biztonsági szolgáltatásokat igénybe vennie egy KKV-nak. Ez pedig költséghatékonyan csak úgy történhet, ha ezt egy központi szolgáltatástól veszi igénybe, nem pedig saját maga próbálja kivitelezni. Ennek kapcsán eszembe jutott az előző évi UNIX autós incidens. Pontosan nem tudom, hogy ez mennyibe került az UNIX számára, de azt igen, hogy rengeteg autószerelő és karosszéria lakatos stb. kapott UNIX fémjelzésű phishing email-t. Ez pedig a cég reputációját, valamint az ügyfeleinek munkáját is veszélyezteti. **Összegezve tehát egy KKV-nak szüksége van IT biztonsági intézkedésekre,**

mégpedig kockázat arányosan van szüksége erre és egyértelműen szolgáltatásként igénybe véve történik a legköltséghatékonyabban.

Említetted, hogy úgy látod, napjainkban kezd el egyre inkább tudatosulni az IT biztonság a KKV-k körében.

Igen. Úgy látom és tapasztalatom, hogy a kis- és középvállalkozások kezdenek egyre nagyobb mértékben igénybe venni ilyen szolgáltatásokat, tehát látni a fényt az alagút végén. És **vannak cégek, akik kifejezetten az ő igényeik kiszolgálására építenek.** Itthon például, hogy egyet említsek ilyen az Invitech adatközponti szolgáltatása mellé kapcsolt IT biztonsági szolgáltatás, ami kifejezetten erre van pozícionálva. Tehát nem nagyobb enterprise vállalatokra vannak specializálódva, hanem kifejezetten a kis- és középvállalkozásokra, így számukra is megfizethető árakkal dolgoznak.

IT biztonsági szakemberek számát tekintve mik a kilátások?

Finoman fogalmazva eléggé rosszul állunk hazai szinten, ami az IT biztonsági szakemberek létszámát illeti. A KKV-k esetében nem mondanám bizonyos méret alatt, hogy megtérülne egy saját IT staff fölállítása, mivel kevés a szakember és ennek okán elég drágák is. Továbbá egy kis-, vagy egy középvállalkozásnál nem is lennének eléggé kihasználva. Az IT biztonsággal, mint szolgáltatással foglalkozó cégek esetében is elmondható, hogy sok helyen hiányokkal küzdenek. Tehát azt kell, hogy mondjam: **kevés az igazán jó szakember.** Az igény a szolgáltatók oldalán mindenképpen megvan rájuk, illetve a nagyobb középvállalkozások is miután eljutnak arra a szintre, hogy azt mondják: „igen én már tudnék foglalkoztatni egy egész embert, aki az IT biztonságunkkal foglalkozik" és körülnéz a munkaerő piacon, szembesülve az árakkal általában arra a következtetésre jut, hogy ő ezt nem tudja kifizetni. Ilyenkor sokszor fel is hagynak az igényükkel sajnos.

Merre tart a digitalizáció? Várható tendenciák, előre tekintés?

Ha egyetlen dolgot kéne megemlítenem, akkor azt mondanám, hogy a digitalizáció a jövőre tekintve egyértelműen a felhő irányába megy. Hogy ez egy nemzetközi szolgáltató által üzemeltetett felhő, mint például az AWS vagy a Cloudflare, vagy egy „magyar égre magyar ufót", mint például az Invitech vagy a DTSM, azt még nem lehet egyelőre látni. El kell gondolkoznunk azon, hogy mennyire biztonságos, ha az adataink egy harmadik országban vannak. Gyakorlati példa erre a napjainkban zajló orosz ukrán válság. Ukrán szempontból például előnyösnek bizonyult egy harmadik országban tartani az adataikat, mert ha valamelyik adatközpontjukat egy találat érte volna, akkor ezek az adatok megsemmisülnek. Azonban, ha a másik oldalt nézzük, ha az orosz vállalkozások és állami intézmények nagyobb mértékben építettek volna felhő alapú szolgáltatásokra, (amik köztudottan többségében amerikai kézben összpontosulnak), akkor ez az ő szempontjukból kevésbé lett volna szerencsés, mert az adataikhoz a hozzáférést nagyon rövid időn belül megtagadhatták volna. **Tehát, ha a digitalizáció fejlődési lehetőségeit**

nézzük, a legszámottevőbb mindenképpen a felhő. Viszont itt megint képbe jön az IT biztonság kérdése, hogy ezt milyen formában érdemes megvalósítani. Az nem kérdés, hogy kell-e, mert csak jön, mint a lavina, és aki nem veszi figyelembe, azt maga alá temeti. Azonban stratégiai szempontból mindenképpen szükséges ezt is a biztonság oldaláról egyaránt megvizsgálni.

8- ÖSSZEGZÉS

A megbízó igényeinek megfelelően felmértem a kkv szektor digitalizációs helyzetét és kockázatait. Az elkészített kockázatelemzések kimutatták, hogy legkritikusabb aspektusai a digitalizációnak kiberbiztonsági szempontból a levelezésbiztonság, a belső hálózat biztonsága, valamint a végpontvédelem. A megbízó speciális üzleti igényeit is kiszolgálva sikerült költséghatékony módon megterveznem és implementálnom ezen fenyegetések mitigálását biztosító hálózatot, többek között az ISO 27001, NIST, CISA és NSA ajánlásainak megfelelően. A megbízónak továbbfejlesztési ajánlásokat tettem az üzletmenet folytonosságának fenntartása érdekében.

Az alkalmazott megoldások használata nem igényli külön IT biztonsági szakember/ek alkalmazását, viszont menedzselést igen. Ennek érdekében szükséges a rendszeres felülvizsgálatuk, auditálásuk. Amikor a cég mérete eléri azt a kritikus pontot, hogy a belső munkatársak már nem képesek hatékonyan ellátni a biztonsággal kapcsolatos eseményeket, meg kell fontolni a SOC szolgáltatások igénybevételét.

Minél kisebb egy vállalkozás, annál egyszerűbb és olcsóbb a kiberbiztonság kialakítása oly módon, hogy az bővítési lehetőségekre is lehetőséget adjon, így biztosítva a növekedés lehetőségét. Az elvégzett kutatás bemutatja, hogy amennyiben egy cég nem invesztál a kiberbiztonság megteremtésébe, súlyos kockázatoknak van kitéve és a trendek alapján idő kérdése, hogy mikor kell egy összegben kifizetnie a tévesen megspóroltnak vélt kiadásokat.

9 SUMMARY

In the framework of my thesis in accordance with my client's needs, I intended to assess the digital transformation and the cyber security risks of the sector of the Small and medium-sized enterprises (SME). The performed risk analyses shows that the most critical aspects of digitalization from a cybersecurity point of view are email security, network security, and the endpoint protection. Thus serving the client's special business needs, I managed to cost-effectively design and implement a network to mitigate the above-mentioned threats, in accordance with ISO 27001, NIST, CISA and NSA recommendations. I made further recommendations to my client in order to increase cyber security.

The applied solutions does not require IT security specialists, but Administrators are needed for handling daily bases task such as management, maintenance, and repair. For this purpose, it is necessary to regularly review, audit and manage the infrastructure. If the size of the company reached the critical point when internal staff are no longer able to effectively respond security related events, the use of SOC services should be considered.

The smaller a business is, the simpler and less expensive to design cyber security. Even it allows expansion options, thus ensuring the possibility to scale up. The results of my research show that if a company does not invest in cyber security, it is exposed to serious risks and, based on the trends, it is only a matter of time before it has to pay the expenses that were mistakenly believed to have been saved.

10 ÁBRAJEGYZÉK

11 TÁBLAJEGYZÉK

12 IRODALOMJEGYZÉK

[1] SBA Office of Advocacy (https://irp-cdn.multiscreensite.com/7d9a86a6/files/uploaded/2018-Small-Business-Profiles-All.pdf), [Utoljára megtekintve: 2021.05.04.].

[2] N. Huaman,. B. von Skarczinski, Y. Acar, C.Stransky, D. Wermke, A. Dreißigacke, S. Fahl: A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. (https://www.usenix.org/system/files/sec21fall-huaman.pdf), utoljára megtekintve: 2021.05.04.

[3] Innovációs és Technológiai Minisztérium: A magyar kkv-k megerősítésének stratégiája, (https://www.edutus.hu/wp-content/uploads/2020/10/KKV-Stratagia-2019-2030.pdf), utoljára megtekintve: 2022.12.14.

[4] H. Kagermann: Change Through Digitization - Value Creation in the Age of Industry 4.0, Springer Fachmedien Wiesbaden, 2014 (https://www.scribd.com/document/365621401/Change-Through-Digitization-Value-Creation-in-the-Age-of-Industry-4-0), utoljára megtekintve: 2022.12.14.

[5] M. Westerlund: Digitalization, Internationalization and Scalingof Online SMEs," *Technology Innovation Management Review,* pp. 48-57., 2020. április.

[6] Digimeter: Hazai digitalizáció:nagy lendület, kis hatásfok, (https://digimeter.hu/wp-content/uploads/2020/11/Digimeter_2020.1_osszefoglalo.pdf), utoljára megtekintve: 2022.12.14.

[7] Department for Digital, Culture, Media & Sport: Cyber Security Breaches Survey 2019, (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950063/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised_V2.pdf), utoljára megtekintve: 2022.12.14.

[8] Second Annual State of RansomwareReport: Survey Resultsfor Australia, (https://go.malwarebytes.com/rs/805-USG-300/images/Second%20Annual%20State%20of%20Ransomware%20Report%20-%20Australia.pdf), utoljára megtekintve: 2021.05.04.].

[9] McAfee Economic Impact of Cybercrime - No Slowing Down, (https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf), utoljára megtekintve: 2022.12.14.

[10] M. Miller: FBI sees spike in cyber crime reports during coronavirus pandemic, The Hill, 2020

(https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic), utoljára megtekintve: 2022.12.14.

[11] Deloitte: Accelerated digitalisation leave businesses susceptible to cyberattacks, (https://www2.deloitte.com/uk/en/pages/consumer-business/articles/accelerated-digitalisation-leave-businesses-susceptible-to-cyberattacks.html), utoljára megtekintve: 2022.12.14.

[12] Institut of Risk Management: Cyber risk, (https://www.theirm.org/what-we-say/thought-leadership/cyber-risk/), utoljára megtekintve: 2022.12.14.

[13] G. J. Touhill, in *Cybersecurity for executives : a practical guide*, Wiley-AIChE, 2014, pp. 95-97. 37.

[14] ISO/IEC, *Information technology - Security techniques - Information security risk management,* BSI, 2011.

[15] I. Sotnikov: How to Perform IT Risk Assessment (https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/), utoljára megtekintve: 2022.12.14.

[16] Sándor, Á., Gubán, Á.: A KKV-K DIGITÁLIS ÉRETTSÉG MÉRÉSÉNEK LEHETŐSÉGEI," *VEZETÉSTUDOMÁNY, Vol.*3, p. 14, 2021.03.02..

[17] S. Róbert, *Elektronikus kereskedelem,* Debrecen: Debreceni Egyetem Agrártudományi Centrum, Agrárgazdasági és Vidékfejlesztési Kar, Gazdasági- és Agrárinformatikai Tanszék, 2004., p. 4..

[18] I. Sotnikov: How to Perform IT Risk Assessment (https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/), utoljára megtekintve: 2022.12.14.

[19] Sucuri Inc.: Sucuri Website Threat Research Report, (https://sucuri.net/wp-content/uploads/2022/04/22-sucuri-2021-hacked-report.pdf), utoljára megtekintve: 2022.12.14.

[20] OWASP: OWASP TOP Ten, (https://owasp.org/www-project-top-ten/), utoljára megtekintve: 2022.12.14.

[21] CVE Details (https://www.cvedetails.com), utoljára megtekintve: 2022.12.14.

[22] IBM: Virtuális magánhálózatok, (https://www.ibm.com/docs/hu/i/7.3?topic=security-virtual-private-networking), utoljára megtekintve: 2022.12.14.

[23] A. G. Rama Bansode: IOPScience - Common Vulnerabilities Exposed in VPN – A Survey," 2021,

(https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045), utoljára megtekintve: 2022.12.14.

[24] Microsoft: Jelentés: Kiberbiztonsági trendek Közép- és Kelet-Európában, 2020.. (https://info.microsoft.com/CE-SCRTY-CNTNT-FY21-04Apr-27-JelentesKiberbiztonsagitrendekKozepesKeletEuropaban-SRGCM4609_01Registration-ForminBody.html), utoljára megtekintve: 2022.12.14.

[25] CVE Detalis, (https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vpn), utoljára megtekintve: 2022.12.14.

[26] National Institute Of Security Agency and Technology, NIST, (https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=vpn&queryType=phrase&search_type=all&isCpeNameSearch=false), utoljára megtekintve: 2022.12.14.

[27] Cybersecurity & Infrastructure Security Agency, CISA, (https://www.cisa.gov/uscert/ncas/tips/ST05-003), utoljára megtekintve: 2022.12.14.

[28] National Institute Of Security Agency and Technology, NIST, (https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=Wi-Fi&search_type=all&isCpeNameSearch=false), utoljára megtekintve: 2022.12.14.

[29] THE RADICATI GROUP,INC.: Email-Statistics-Report-2015-2019-Executive-Summary, (https://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf), utoljára megtekintve: 2022.12.14.

[30] Federal Communication Commission: Cyber Security Planning Guide, (https://www.cisa.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide.pdf), utoljára megtekintve: 2022.12.14.

[31] National Institute Of Security Agency and Technology, NIST, (https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&query=email&queryType=phrase&search_type=all&isCpeNameSearch=false), utoljára megtekintve: 2022.12.14.

[32] Cybersecurity & Infrastructure Security Agency, CISA, (https://www.cisa.gov/uscert/ncas/alerts/aa22-117a), utoljára megtekintve: 2022.12.14.

[33] Federal Bureau of Investigation: FBI Internet Crime Complaint Center - Internet Crime Report 2021, (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf), utoljára megtekintve: 2022.12.14.

[34] Trend Micro: Defending the Expanding Attack Surface - Trend Micro 2022 Midyear Cybersecurity Report (https://documents.trendmicro.com/assets/rpt/rpt-defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report.pdf), utoljára megtekintve: 2022.12.14.

[35] IBM: How much would a data breach cost your business?, (https://www.ibm.com/security/data-breach), utoljára megtekintve: 2022.12.14.

[36] Microsoft: Microsoft Digital Defense Report 2022, (https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022), utoljára megtekintve: 2022.12.14.

[37] Ponemon Institute LLC: The Third Annual Study on the State of Endpoint Security Risk, (https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf), utoljára megtekintve: 2022.12.14.

[38] Cybersecurity & Infrastructure Security Agency, CISA: 2021 Trends Show Increased Globalized Threat of Ransomware, (https://www.cisa.gov/uscert/ncas/alerts/aa22-040a), utoljára megtekintve: 2022.12.14.

[39] SOPHOS: The State of Ransomware 2022, (https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf), utoljára megtekintve: 2022.12.14.

[40] Microsoft: Mi a felhő? (https://azure.microsoft.com/hu-hu/overview/what-is-the-cloud/), utoljára megtekintve: 2022.12.14.

[41] O. Santos, Cisco CyberOps Associate CBROPS 200-201, Hoboken, NJ: Cisco Press, 2021., p. 86., ISBN-13: 978-0-13-680783-4

[42] P, Dr.. Holyinka: Vállalati információs rendszerek, 2001-2014., (https://docplayer.hu/1960802-Vallalati-informacios-rendszerek.html), utoljára megtekintve: 2022.12.14.

[43] Mester, Cs.: Hogyan válik a CRM a vállalatok versenyképességének meghatározó elemévé?, Vezetéstudomány XXXVII. évf. 2006/különszám pp. 87-97

[44] G. T. Ivan Stankov, „Vulnerability and Protection of Business Management Systems: Threats and Challenges,” *PROBLEMS OF ENGINEERING CYBERNETICS AND ROBOTICS*, pp. 29-40., 2020.

[45] Hillbrown Consulting Kft., Digitális jólét nonprofit kft.:Magyarország Fintech Stratégiája, 2019,

(https://digitalisjoletprogram.hu/files/67/01/67018780db39d25c02d4b736abe8d1a1.pdf), utoljára megtekintve: 2022.12.13.

[46] Magyar Nemzeti Bank: FINTECH ES DIGITALIZÁCIÓS JELENTÉS, 2020.. (https://www.mnb.hu/letoltes/fintech-es-digitalizacios-jelente-s-final.pdf), utoljára megtekintve: 2022.12.14.

[47] H. Nuyens: How disruptive are FinTech and digital for banks and regulators?,"J*ournal of Risk Management in Financial Institutions,* Vol. 12, Issue 3.

[48] Muha, L.: Informatikai biztonság, (https://docplayer.hu/25373281-Muha-lajos-informatikai-biztonsag.html), utoljára megtekintve: 2022.12.14.

[49] Microsft: State of global customer service report, (https://info.microsoft.com/rs/157-GQE-382/images/EN-US-CNTNT-ebook-2018-State-of-Global-Customer-Service.pdf), utoljára megtekintve: 2022.12.14.

[50] Bánszi, Zs.,:www.4ig.hu, Kiberbiztonság, (https://www.4ig.hu/megoldasok/kiberbiztonsag), utoljára megtekintve: 2022.12.14.

[51] A., S., Tanenbaum, D., J., Wetherall: „Számítógép Hálózatok," Panem, Vol. 5., 2013, pp. 791-794., ISBN: 978-963-545-529-4

[52] National Institute Of Security Agency and Technology, NIST: NSA Details Network Infrastructure Best Practices, (https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2949885/nsa-details-network-infrastructure-best-practices/), utoljára megtekinve: 2022.12.14.

[53] National Institute Of Security Agency and Technology, NIST: Network Infrastructure Security Guidance, 2022. June., U/OO/118623-22, PP-22-0293, Version 1.1, (https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF), utoljára megtekintve: 2022.12.14.

[54] (IEC), Nemzeti Szabányügyi szervezet, (ISO) Nemzetközi Eletrotechnikai Bizottság: MSZ ISO/IEC 27001:2014,

[55] National Security Agency, Cybersecurity Information: Layering Network Security Through Segmentation, (https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf), utoljára megtekintve: 2022.12.14.

[56] Federal Communication Commission: Cyber Security Planning Guide, (https://www.cisa.gov/sites/default/files/publications/FCC%20Cybersecurity%20Planning%20Guide.pdf), utoljára megtekintve: 2022.12.14.

[57] SIA Mikrotīkls, Aizkraukles iela 23, Riga, LV-1006 LATVIA, (https://mikrotik.com/product/hap_ac2), utoljára megtekintve: 2022.12.14.

[58] Linksys, „www.linksys.com, (https://www.linksys.com/linksys-ea6350-ac1200-dual-band-Wi-Fi-router/EA6350.html), utoljára megtekintve: 2022.12.14.

[59] Meraki, meraki-go, https://www.meraki-go.com/, (https://www.meraki-go.com/product/indoor-Wi-Fi-access-point/), utoljára megtekintve: 2022.12.14.

[60] Gartner, www.gartner.com, (https://www.gartner.com/reviews/market/endpoint-protection-platforms/compare/product/microsoft-defender-for-endpoint-mde-vs-symantec-endpoint-protection-vs-trend-micro-apex-one), utoljára megtekintve: 2022.12.14.

[61] Symantec, www.broadcom.com, (www.broadcom.com), utoljára megtekintve: 2022.12.14.

[62] Microsoft, learn.microsoft.com, (https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/microsoft-defender-for-office-365-product-overview?view=o365-worldwide), [Hozzáférés dátuma: 2022.11.23.].

[63] Microsoft, learn.microsoft.com, (https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/microsoft-defender-for-office-365-product-overview?view=o365-worldwide), utoljára megtekintve: 2022.12.14.

[64] Sztrik J., K., K., C., Soong., Orosz., P.:Központosított EAP alapú hitelesítés vezeték nélküli hálózatokban, 2005. augusztus 24-26 szerk., Debrecen., (https://irh.inf.unideb.hu/~jsztrik/publications/papers/OroszSztrikC14.pdf), utoljára megtekintve: 2022.12.13.

[65] S., Frankel, B,. Eydt, L., Owens, L., Scarfone: National Institute of Standards and Technology (NIST), Special Publication 800-97, 2007. (https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50897), utoljára megtekintve: 2022.12.14.

13 MELLÉKLETEK

```
ip dhcp pool vlan20_vendeg
   network 192.168.20.0 255.255.255.0
   dns-server 192.168.20.254
   default-router 192.168.20.254
!
ip dhcp pool vlan30_produktiv
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.254
   dns-server 192.168.30.254
!
ip dhcp pool vlan40_IOT
   network 192.168.40.0 255.255.255.0
   dns-server 192.168.40.254
   default-router 192.168.40.254
!
ip dhcp pool vlan50_kamera
   network 192.168.50.0 255.255.255.0
   default-router 192.168.50.254
   dns-server 192.168.50.254
!
ip dhcp pool vlan60_managament
   network 192.168.60.0 255.255.255.0
   dns-server 192.168.60.254
   default-router 192.168.60.254
!
ip dhcp pool vlan70_teszt
   network 192.168.70.0 255.255.255.0
   default-router 192.168.70.254
   dns-server 192.168.70.254
!
ip dhcp pool vlan80_belso
   network 192.168.80.0 255.255.255.0
   dns-server 192.168.80.254
   default-router 192.168.80.254
!
ip dhcp pool vlan90_admin
   network 192.168.90.0 255.255.255.0
   dns-server 192.168.90.254
   default-router 192.168.90.254
```

1. melléklet: DHCP pool-ok létrehozása

```
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
ip dhcp excluded-address 192.168.50.1 192.168.50.10
ip dhcp excluded-address 192.168.60.1 192.168.60.10
ip dhcp excluded-address 192.168.70.1 192.168.70.10
ip dhcp excluded-address 192.168.80.1 192.168.80.10
ip dhcp excluded-address 192.168.90.1 192.168.90.10
```

2. melléklet: DHCP kioszthatóságból kizárt IP címek

```
interface Vlan20
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 ip address 192.168.30.1 255.255.255.0
!
interface Vlan40
 ip address 192.168.40.1 255.255.255.0
!
interface Vlan50
 ip address 192.168.50.1 255.255.255.0
!
interface Vlan60
 ip address 192.168.60.1 255.255.255.0
!
interface Vlan70
 ip address 192.168.70.1 255.255.255.0
!
interface Vlan80
 ip address 192.168.80.1 255.255.255.0
!
interface Vlan90
 ip address 192.168.90.1 255.255.255.0
!
```

3. melléklet: VLAN-okhoz rendelt alhálózati IP cím tartományok

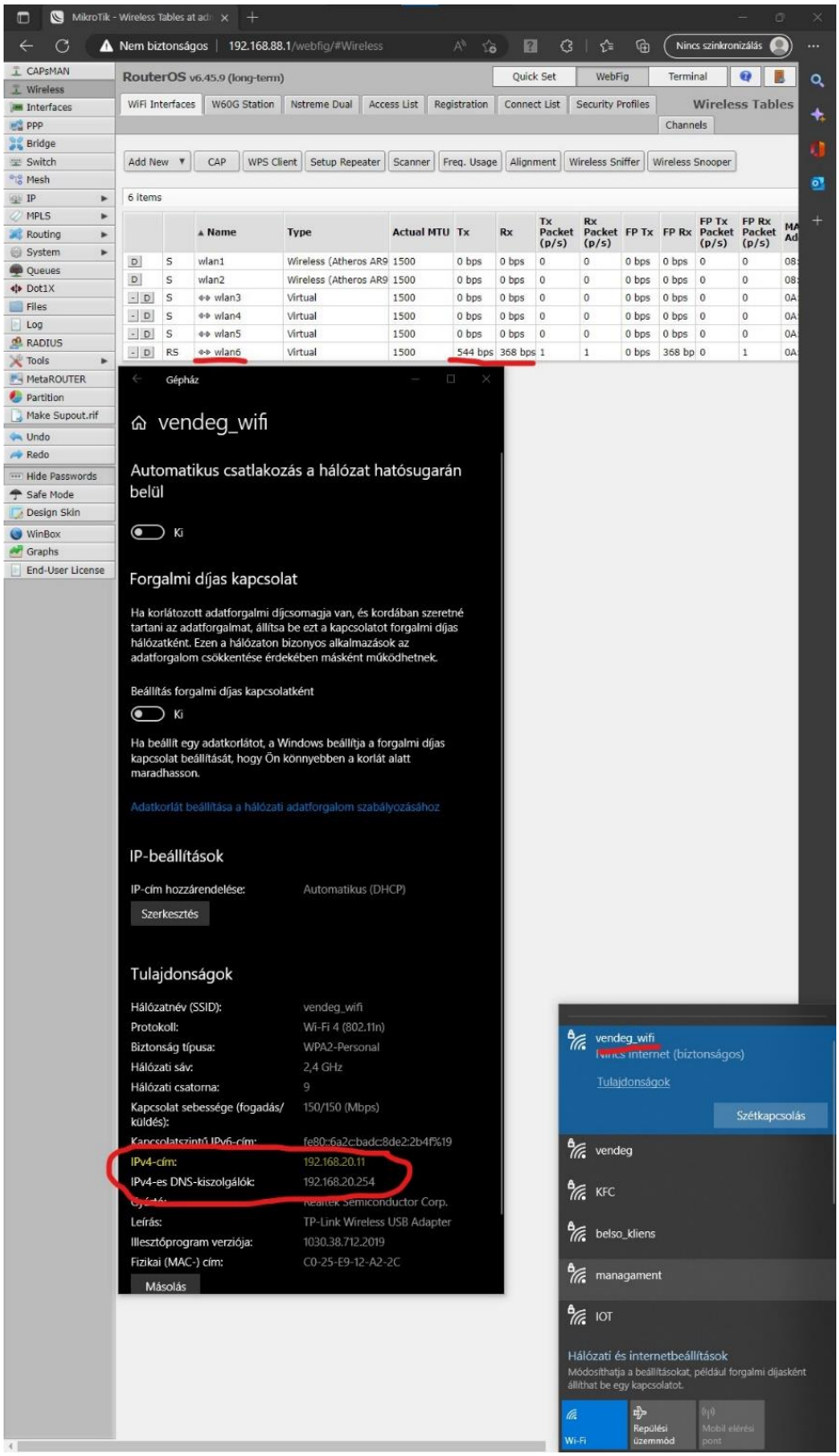
```
interface GigabitEthernet1/0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/24
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 60
 switchport mode trunk
!
```

4. melléklet: Trunk portok létrehozása

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::fed1:e1d2:d9f3:1ecc%13
   IPv4 Address. . . . . . . . . . . : 192.168.20.12
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.20.254
```

5. melléklet: A konfiguráció működésének ellenőrzése (DHCP, VLAN)



6. melléklet: A Wi-Fi konfigurációjának ellenőrzése