ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS

INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Farkasné Utry Gyöngyvér**
2023	Hallgató törzskönyvi száma:	**T/007282/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Farkasné Utry Gyöngyvér Mária**
Törzskönyvi száma: T/007282/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Felhasználói biztonsági rések minimalizálása vállalati környezetben Microsoft Cloud megoldásokkal
Minimizing user security risks at Corporates with Microsoft Cloud solutions

Intézményi konzulens: Balázsné Dr. Kail Eszter
Külső konzulens:

Beadási határidő: 2022. december 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

Az információs technológia fejlődésével egyenes arányban jelennek meg az egyre fejlettebb biztonsági fenyegetések. Erre a szoftverfejlesztő cégek is folyamatosan válaszolnak és a piacon rendkívül széles biztonsági portfólióval találkozhatunk, melyek kikerülése egyre nagyobb kihívást jelent a támadóknak. Éppen ezért könnyebb ellenállásnak tűnhet a felhasználók oldaláról való közelítés.
A szakdolgozat célja bemutatni egy olyan rendszer kiépítését, amely a felhasználó keze alá dolgozik és védi meg külső fenyegetésektől, figyelembe véve a használhatóság és biztonság érzékeny egyensúlyát.
A hallgató feladata a piaci összehasonlításokra alapozva egy biztonsági útmutató kidolgozása, mely egy vállalat biztonságos dokumentumkezelési házirendjének megvalósítását mutatja be. A megoldási javaslat főbb építőkövei a korszerű adatklasszifikáció, intelligens fájlvédelem és jogosultságkezelés, továbbá adatszivárgás megelőzés.

A dolgozatnak tartalmaznia kell:

- a megoldandó feladat bemutatását és elemzését,
- kitekintést a felhasználókat érintő fenyegetettségekről napjainkban,
- a Microsoft biztonsági megoldásainak bemutatását, különös tekintettel a mesterséges intelligencia és gépi tanulással támogatott dokumentum megfelelősség és adatmegőrzési irányelvekre,
- a piacon található megoldások áttekintését, összehasonlítását,
- intelligens, felhasználói védelmi rendszer kialakítását,
- eredmények értelmezését, következtetések megfogalmazását.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * Budapest I. Ph.

.....
Dr. Fleiner Rita
intézetigazgató

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

A dolgozatot beadásra alkalmasnak tartom:

..... külső konzulens

..... intézményi konzulens

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2022 december 10.

.....

hallgató aláírása

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Neptun Kód: Tagozat:

Farkasné Utry Gyöngyvér [redacted] Kiberbiztonsági szakmérnök

Telefon: Levelezési cím (pl.: lakcím):

[redacted]

Projektmunka címe magyarul:

Felhasználói biztonsági rések minimalizálása vállalati környezetben Microsoft Cloud megoldásokkal.....

Projektmunka címe angolul:

Minimizing user security risks at Corporates with Microsoft Cloud Solutios.....

Intézményi konzulens: Külső konzulens:

Balázsné Dr. Kail Eszter ..... nincs .....

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.10.20	Piaci összehasonlítás áttekintése	Kail
2.	2022.10.28	Teljes dolgozat átbeszélése, korrektúrázása	Kail
3.	2022.11.10	Irodalomjegyzék és ábrajegyzék javítása	Kail
4.	2021.11.21	Fedőlapok véglegesítése	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

Budapest, 2022 november 25.

[1] A megfelelő bekarikázandó/aláhúzandó!
[2] A megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1. A BIZTONSÁGI FENYEGETETTSÉGEK ELEMZÉSE, TÁMADÁS TÍPUSOK

1.1. A komplexitást fokozó okok

A negyedik ipari forradalom az információs technológia explicit módon történő fejlődéséről szól. A számítógépek számítási kapacitásának, és az az információ áramlásának gyorsasága lehagyta a humán képességeket. A forradalomhoz tartozik a hálózatok kiépítése, és a digitális transzformáció. A folyamat lassan négy évtizede megfigyelhető, azonban az eddig sem lassú növekedési ütemhez a 2020-as évben kezdődött világjárvány újabb lendületet adott.

1.1.1. Ipar 4.0, azaz az IT forradalom

A 90-es években még számos félelmet tapasztalhattunk azzal kapcsolatban, hogy a számítógépek kiszorítják az emberek munkáját, kiváltják az addigi adatfeldolgozásban történő szerepüket. Ehhez képest éppen az ellenkezője történt. A technológia lehetővé tette a gyors adatáramlást. A postát felváltotta az e-mail, ma már az e-mailt is felváltja a még gyorsabb instant üzenetküldés. A telefon mellé bekerült az információmegosztásban még gazdagabb videóhívás, 1 az 1-hez kapcsolat helyett konferenciahívásokat lehetővé téve. Papír alapú dokumentumok, és az ahhoz kapcsolódó lassabb továbbítási folyamatok, úgymint számlák helyett e-számla, e-ügyintézés, csak néhány gyakorlati példát említve. Ezek az adatok továbbításának és feldolgozásának módját gyorsították fel nem jelentéktelen mértékben, ami több humán feldolgozási kapacitást is igényel. A feladatkörök átalakulását mutatja az 1.1. számú ábra [1].

1.1. ábra A munkakörök változása [1]

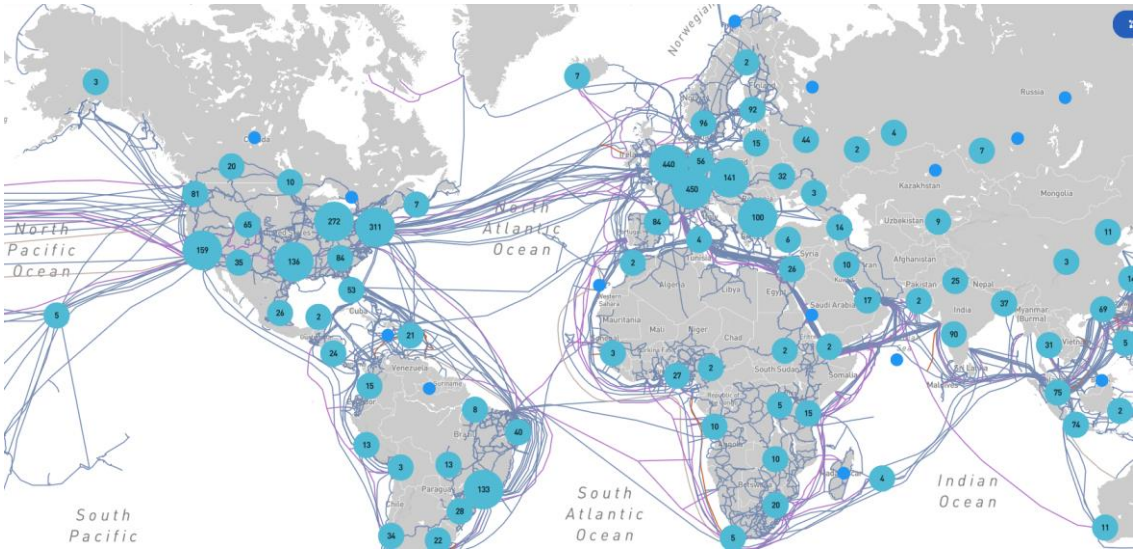
A mai irodai munkavállaló sokkal több feladattal van ellátva, mint korábban. Az informatika korában a munka nemhogy csökkent volna, tovább fokozódott és transzformációt követel a dolgozóktól is. Az eszközök révén a monoton adatfeldolgozási részfolyamatok az informatikai háttérre terhelhetők, míg az érdemi és összetettebb egységekre több emberi fókusz hárul. Ezen összetettebb feladatok nagyobb koncentrációt igényelnek és fáradékonysággal járnak [1].

Projektfeladatom fő feladatának tartom azon megoldások kutatását, amik a felhasználót támogatják a lényegi, értékteremtő munkára az adminisztratív hibákból eredő kiber fenyegetettségek elkerülése mellett. Olyan rendszer kiépítése a cél, ami az emberi figyelmetlenségből, túlterheltségből adódó félrenyúlások kockázatát csökkenti automatizált megoldásokkal, ami egyben kényelmesebb felhasználást is magával hordoz ügyelve a biztonságosság és könnyen használhatóság kényes arányára.

1.1.2. Hálózatok és a digitalizáció fejlődése

Az internet alapjainak fejlesztése az 1960-as években indult. 1969-ben létrejött APRANET-et tekintjük az internet „ősének”. A commercial megjelenéshez azonban egészen a 90-es évekig várni kellett a Word Wide Web megalakulásáig. Ezt követően indult be az internet alapjául szolgáló fizikai hálózat rohamos kiépítése országos és nemzetközi szinten mind az elérés, mind sebesség növelése tekintetében [2].

A hálózatban az optikai kábelek megjelenése volt az áttörés a sebesség valóban élvezhető szintre hozatalában. Ma már az egész világot behálózó, magas sávszélesség áll rendelkezésre az adatok gyors cseréjére, amit az 1.2. ábra mutat. A Gigabites Ethernetek segítségével több 1000 Megabyte per szekundum sebességgel.



1.2. ábra: Globális Internet Infrastruktúra térkép [3]

A kiépült hálózat magával hozza az elérhető szolgáltatások bővülését is a digitális transzformációnak utat engedve. Modernizáció zajlott le a fogyasztói és vállalati kultúrában egyaránt.

A KPMG, vezető tanácsadó cég is hangsúlyozza, hogy a technológiai fejlődés egyet jelent a vállalati kultúra fejlődésének megkövetelésével. „Egyre többet beszélünk a fogyasztói élményről és a digitalizációról, vagyis arról, hogy hogyan lehet digitális eszközökkel mind jobban kiszolgálni a fogyasztót. Mégis, a cégvezetőknek csak a fele állítja, hogy a vállalatának van digitális stratégiája, és csak a negyede látja tisztán, hogy mi lesz a következő lépés ebben. A gond ott van, hogy nem a vállalati stratégia részeként, hanem informatikai fejlesztésként gondolnak legtöbben a digitalizációra.” [4] Olvasható a KPMG blogjában.

Tehát a modernizációt széles körben kell érteni, amikor digitális transzformációról beszélünk és bele kell értenünk a felhasználói kényelmet is, amit az egyre összetettebb rendszerek kihívások elé állítanak és gyakran a biztonsági elvárásokkal ellentétesek.

1.1.3. Felhő technológia

A másik transzformációt jelentősen befolyásoló tényező. A cloud computing újabb komplexitást visz az informatikai rendszerekbe. Jelentése tömören nem más, mint számítási szolgáltatások igénybevétele az interneten keresztül. Ezek a szolgáltatások jelenthetnek szerver erőforrást, adattárolást, adatbázist, hálózat, szoftver és analitikai intelligenciákat. Rugalmasságukban és skálázhatóságukban verhetetlenek a nagy felhőszolgáltatók, amit a gyors fejlődés rendre meg is követel a vállalatoktól. Annak ellenére, hogy a számos cég még mindig a helyileg telepített, ún. on-premise technológiákat preferálja elsősorban, minimum hibrid környezet az általános, hiszen a modern technológiák használata megkerülhetetlenné vált napjainkban [5].

A globális felhőszolgáltatók vezetői az Amazon, Microsoft és Google. Ebből két Bigtech a felhőben született, míg a Microsoft története régebbről, a hagyományos, on-premise operációs rendszerekből indult.

Mindhármuk biztosítja többek között a következőkben felsorolt szolgáltatásokat saját world-wide kiterjedésű adatcenterükből. Publikus Infrastruktúra és Platform, mint szolgáltatás (IaaS, PaaS). Minden méretű szervezetre kínálnak megoldásokat előfizetéses modellben, percalapú fogyasztás alapján. Magas rendelkezésre állást biztosítanak, havi átlagban 99.95%-ot vagy ennél magasabbat. A dolgozat szempontjából legfontosabb, hogy mindegyikük kiemelt Security standardokat követ, az összes rendelkezik a következő tanúsítványokkal: SOC 1, SOC 2 és SOC 3 audit, továbbá SSAE 16, ISO/IEC 27001, ISO/IEC 27017 és ISO/IEC 27018 audit. Rangsoruk az 1.3. ábra alapján látható a Gartner szerint [6].

1.3. ábra: Gartner: A legerősebb IaaS és PaaS szolgáltatók [6]

1.1.4. A technológia felértékelődése 2020-tól

A világméretű járvány terjedésének közismerten legfontosabb lassító tényezője a személyes kapcsolatok minimalizálása. A távoli munkavégzés már eddig is egy jól ismert fogalom volt az IT szakmában, azonban fontossága hamar sokszorosára értékelődött. Azon vállalkozások, akik eddig még halogatták az ilyen típusú munkakörnyezet biztosítását, most rohamléptekkel kényszerültek átállni. A távmunka felállítása szintén újabb biztonsági kihívások elé állítja a résztvevőket.

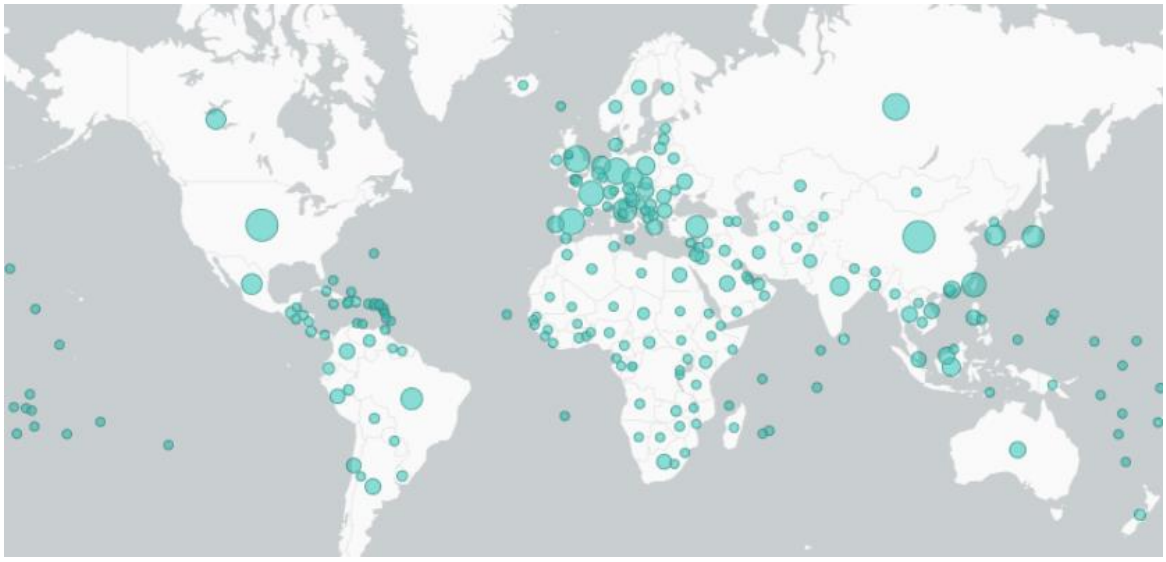
Az információs forradalom megkerülhetetlenségét is bizonyítja, hogy habár Covid-19 a világgazdaságra is nagy csapást mért, a visszaesés az informatikának köszönhetően azonban mérsékletet tanúsított. A hálózat és az eszközök, alkalmazások már kellő kiforrottságot biztosítottak ehhez, a technológia már rendelkezésre állt a remote környezetek kialakításához.

„A Központi Statisztikai Hivatal (KSH) első becslése szerint Magyarország bruttó hazai terméke 2020 negyedik negyedévében a nyers adatok szerint 3,7, a szezonálisan és naptárhatással kiigazított és kiegyensúlyozott adatok szerint 4,3 százalékkal csökkent az előző év azonos időszakához viszonyítva. Az előző negyedévhez képest – a szezonálisan és naptárhatással kiigazított és kiegyensúlyozott adatok szerint – a gazdaság teljesítménye

1,1 százalékkal nőtt. A növekedéshez leginkább az ipar, valamint az információ, kommunikáció nemzetgazdasági ág járult hozzá.” [7] írja a Magyar Nemzet.

Míg a vírus a legtöbb ágazatban visszaesést eredményezett, ez nem volt jellemző a technológiai cégekre, ahogy a KSH is említi, ezen kevesek a gazdaság húzóágazatai közé tartoznak. Világszinten is a Tech vállalatokhoz további tőke és a piacot meghatározó szerep koncentrálódott. 2020 októberére a Big tech cégek főbb szereplői, Apple, Microsoft és Amazon átlépték az 1 billió dolláros piaci kapitalizációt [8].

A Covid-19 ihletet adott a Cyber-bűnözőknek is és számos támadást bújtattak a vírus köntöse alá. Már az első hullám alatt a világ minden táján megjelentek ilyen témájú kártevők. Nem új támadási típusokról beszélünk, hanem kihasználva a felhasználók fogékonyságát a pandémiához kapcsolódó kulcsszavakra, meglévő kártevőkre alkalmazták, kiterjedtségét az 1.4. ábra mutatja az első hullámban. A Microsoft biztonsági monitorozó központja átlagosan napi 60 ezer ilyen jellegű kártékony e-mailt fogott [9].



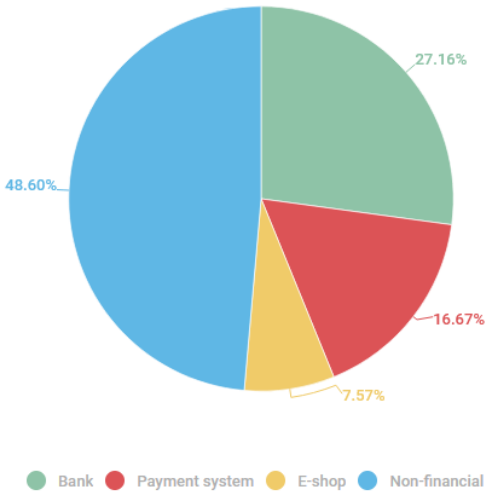
1.4. ábra: Covid-témájú támadások feltűnése 2020 Áprilisban [9]

1.2. Kitekintés a felhasználókat érintő fenyegetettségekről napjainkban

1.2.1. A támadások típusai és méretei globálisan

A Kaspersky 2020 évi statisztikáiból, amit a gobális felhőszolgáltatásuk (Kaspersky Security Network) adataiból származtatnak, kiderül, hogy világszinten az internetet használók 10,18%-át érte valamilyen Malware-osztályú támadás. Csak a Kaspersky rendszere egy év alatt 666 809 967 darab támadást számlált a sikeres elhárításai között. 173 355 902 darab olyan URL-t azonosítottak, ami rosszindulatú helyekre irányítottak. A ransomware típusú támadásoknál 549 301 támadott felhasználót számláltak. Szintén a tavalyi időszak alatt 668 619 banki célú támadást fedeztek fel, ahol az ügyfelek online banki fiókjához kísérelték meg a hozzáférést [10].

A tavalyi évben a pénzügyi tranzakciókat célzó támadások, phishing eljárások száma is nőtt. Itt főként az online banking és e-shop alatti csalások jelennek meg ügyfél oldalról, és a pénzügyi intézetek sérülékenység kutatása, eloszlásuk az 1.5-ös ábrán. Az APT (Advanced Persistent Threats) tartós támadási típusok csoportjában már folyamatosan támadják ezen pénzügyi területeket is. Az EMOTET-et a tavalyi év egyik legveszélyesebb malware-jeként tartotta számon az Interpol, a botnet megtöréséhez world-wide szintű összefogásra volt szükség. A Kaspersky kimutatása szerint minőségi transzformáción esnek át a kibertámadások, sokszor kevesebb, ám annál célzottabb fajtával találkozunk. Egyre inkább üzlet-orientált célpontok detektálhatók. A pénzügyi támadásokon belül is elmozdulást látható az elmúlt évek alapján az egyéni felhasználóktól vállalati szektor irányába. Ezen az is ronthatott, hogy sok távmunkára kényszerült cég erre infrastrukturálisan még nem volt felkészülve. A PC-k mellett a mobiltelefonok is egyre dominánsabb támadási felületet nyújtanak, számos pusztító trójai banki vírus debütált Android rendszereken, mint például a Ghimob, Gorgona vagy Knobot [11].



1.5. ábra Phising támadások eloszlása [11]

A 2021-es predikciók csak további növekedését látják a támadások számának. A digitális szolgáltatások köre és felhasználó száma továbbra is növekszik, a távoli munka felerősödésével és a vásárlói szokások megváltozásával egyre nagyobb adat- és pénzforgalom terelődik az internet felé, az online szociális élettérről nem is beszélve. A Privacy, a személyes adatok védelmére minden eddiginél nagyobb szükség van és jól látható, hogy erre még a kormányzatok és a vállalatok sem készültek fel teljeskörűen, csak folyamatban van jó esetben az irányelvek és védelmi rendszerek kialakítása [12].

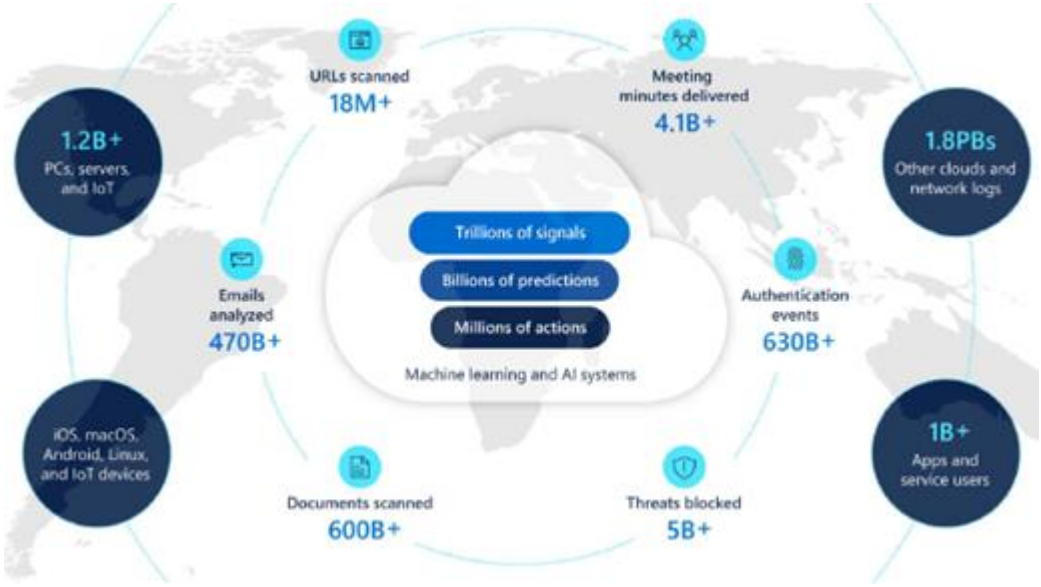
A szolgáltatási körök szélesedésével egyre többrétű privát adatunk kerül rögzítésre. Már a biometrikai adatainkat is felhőben tároljuk a minket körülvevő, például sporteszközök szenzorainak révén, emellett aktivitásunk és helyzetünk is ismertté válhat. A közösségi

médiaszolgáltatók reklámozási célokból szintén előszeretettel gyűjtenek, és profilozzák látogatóikat. Egyre fejlettebb viselkedéselemző technológiák jelennek meg, amik a Big Data mérete ellenére is hatékony analizálást valósít meg. Válaszként erősebb privacy megoldásokra van szükség és tudatosabb magatartása is, hiszen gyakori az önkéntes szenzitívadatmegosztás azon otthoni, internetes látogatóktól, akik részben dolgozói is valamely vállalatnak, intézménynek és hozzáférési pontot jelenthetnek a belső hálózathoz [12].

Ezek a világszintű trendek kis méretünk ellenére Magyarországot is jelentősen érintik. Az év első negyedéves adatai szerint hazánkban történt Franciaország és Izrael után a legtöbb phishing jellegű támadás. Industry specifikusan a leginkább célzott ágazatok sorrendben az Online boltok (15,77%), Globális internetes portálok (15,5%), Bankok (10,04%), Tranzakciós rendszerek (7,63%), Social networkök és blogok (6,1%), IMS, Telekommunikáció, IT cégek, Pénzügyi szolgáltatások, Szállítók és 33% egyéb [13].

1.2.2. Kiberbűnözési trendek alakulása, avagy a lopás digitalizációja

A Microsoft 2005 óta minden évben elkészíti összefoglaló riportját a napjainkat érintő leggyakoribb támadásokból. Az adatokat saját SOC rendszerükből származtatják, a csaknem napi 8 billiónyi biztonsági jelenségből, ahogy az 1.6-os ábra mutatja. Adatcentereikből több milliárdnyi felhasználót szolgálnak ki világszinten vállalati, kormányzati és otthoni felhasználókból egyaránt. Az adatok származása a felhőből, végpontokból és perifériákból áll össze. A nagy mennyiségű, diverz adattömeg lehetővé teszi a Microsoft számára az aggregált biztonsági adatok tanulmányozását, támadási típusok és trendek megállapítását. Több ezer, a vállalat alkalmazásában álló biztonsági szakértő, mint például elemzők, kutatók, mérnökök, adatspecialisták dolgozzák fel az eredményeket, amiben a Machine Learning és Mesterséges intelligencia is segíti munkájukat. A riport az ezen alapuló meglátásokat, adatokat publikálja [14].



1.6. ábra Microsoft SOC-ból származó havi biztonsági adatmennyiség [14]

A technológiai fejlődéssel együtt a kiberbűnözésben is jelentős fejlődést tapasztalhatunk. Az adathalászatban (phising) és üzleti emailek kompromittálása mutat egyre nagyobb dominanciát. A korábbi rosszindulatú, malware támadásokról a fókusz áthelyeződik a zsarolóvírusokra és adathalászatra, irányulva a felhasználói azonosítók megszerzésére, főként banki szolgáltatásoknál, egyre több financiális háttérmotivációt mutatva. Másik jelentős változás, hogy a Covid-19 járvány hatására a távoli munkavégzés lett az elsődleges metódus. Az addig, jellemzően zárt, vállalati hálózaton belüli kommunikáció teljesen át kellett költöznie a publikus hálózatokra, amely számtalan előnye mellett megannyi kitettséget is magával hordoz. A változásokat nem csak az infrastruktúrának kell lekövetnie, hanem a személyzetnek is [14].

1.2.3. Kiberbűnözés legnépszerűbb típusai

A Microsoft riportja alapján a leggyakoribb támadási formák a 2020-as évben az adathalászat (phishing), üzleti emailek kompromittálása (BEC), zsarolóvírusok (ransomware) és kártékony programok (malware) [14].

1. **Hitelesítő adatok halászata.** Gyakori, hogy az adathalászok egy közismert szolgáltatóra hivatkoznak levelükben, megtévesztés technikáját alkalmazva. A gyanútlan egyént a levélben található hivatkozások a támadó saját áloldalára irányítják, ahol a belépési adatok megadására kérik. Amennyiben vállalati azonosítók megadásáról van szó, így már nem csak az egyén, hanem az egész szervezet veszélybe kerül.
   A Microsoft telemetriai adatok alapján az öt leggyakoribb brand, akire hivatkozni szoktak world-wide szinten a Microsoft, UPS, Amazon, Apple és Zoom. A

phising emailek száma a covid hatására igen jentősen megnövekedett, 667%-kal az első hullám betörésekor [15].

2. **Üzleti email kompromittálás** egy olyan adathalászati típus, mely elsősorban a cégvezetőket, CXO-kat célozza meg a vállalat minél nagyobb elérése érdekében, belevonva az üzleti partnereket is, hogy a B2B tranzakciókat is manipulálni tudják. Ennek lehet akár pénzügyi motivációja is, például ál-fizetési kérelmek indításával. A kibertámadók a haszon érdekében hajlandók egyre több időt tölteni az ehhez szükséges háttérmunkák feltárásával, például, hogy az adott vállalat milyen szolgáltatókkal, üzleti partnerekkel vagy kiemelt ügyfelekkel áll kapcsolatban, így elérve a még meggyőzőbb megtévesztést. Kiadhatják magukat meglévő üzleti partnernek, és a nevükben írhatnak leveleket. Szintén a Microsoft telemetria adatai alapján a 10 leggyakrabban támadott iparág a pénzügyi konzultációs cégek, nagykereskedések, IT szolgáltatók, ingatlan irodák, oktatási intézmények, egészségügy, gyógyszergyártók, High-tech, Jogi tanácsadók és Outsourcingot végző szervezetek [14].
3. A támadók akár **kombinálhatják** is a fentebb említett két technikát. Egy előzetesen elhalászott felhasználói fiókból történő üzenetek vagy egyéb tranzakciók indítása tökéletes álcát jelentenek, illetve további illetéktelen adatgyűjtésnek adnak teret. Ezek is gyakran irányulnak pénzügyi műveletek felé, számlakifizetések vagy bankszámla információk gyűjtésére [14].
4. A **zsarolóvírusok** az elmúlt évek legnagyobb növekedését mutató fenyegetése, amely iparágtól függetlenül minden szervezet számára veszélyt jelent. Gyakori tévhit, hogy ez is csak egy rosszindulatú program, azonban sokszor emberi támadó irányítása végett tud célzott pusztítást végezni. Ekkor a támadás két lépésben zajlik, ahol a titkosítást a hitelesítő adatok megszerzése előzi meg, lehetővé téve a zárt hálózaton belüli célzott támadást. Egy felkészületlen szervezet nem tud jól kijönni egy ilyen támadásból, az adatok visszaállítása éppúgy jelentős költséget jelent, mint a váltságdíj megfizetése. Utóbbi gyorsabbnak tűnhet, ám ezzel újabb hozzáférést nyújtunk a támadónak további hátsó ajtókat elrejteni. Az eddigi felmérések alapján egy támadó akár 45 percen belül találhat behatoláshoz rést a hálózaton [14].

   Felmérések szerint 2013. október. és 2019. július között csaknem 144,25 millió dollár került kifizetésre bitcoinban cyber-zsarolók részére. Az esetek 70-80%-ban a Windows Remote Desktop Protocol (RDP)-on keresztül szereztek hozzáférést a hálózatokoz [16].
5. **Kártékony programok**. Ezen belül az elmúlt évtizedben kiemelkedő teljesítményt nyújtott az ún. banki trójai vírus. Nevéből eredően szintén pénzügyi bűntény áll a háttérben. Online banki és pénzügyi fiókok megszerzése irányul. Emellett a fertőzött vállalat IP címeit és DNS tartományait feltérképezve a vírus képet kapott a hálózatról és további kémprogramokat juttathat be [14].

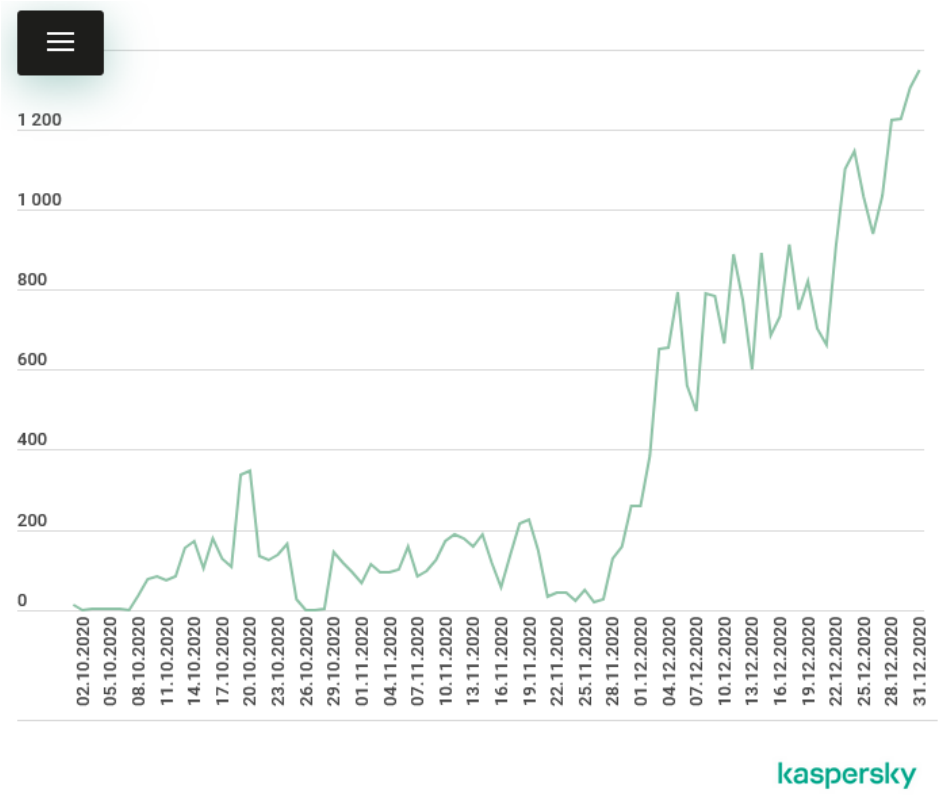
1.2.4. Távoli munkavégzés

A XXI. század egyébként is kiemelkedő digitális transzformációs eleme a távoli munkavégzés térnyerése. A felgyorsult üzleti világnak megnőtt az igénye a bármikor és bárhonnan történő munkavégzésre, a mobil eszközöket is beleértve. A 2020-as év gyakorlatilag kikövetelte ezt az igényt, és azokat a vállalkozásokat is lépésre kényszerítette, ahol korábban nem volt támogatott a home office. Amennyiben a dolgozók részére biztosított a felügyelt távkapcsolat és a háttérrendszer, az irodai munka hatékonysága nem sérül. A vállalatnak szükséges kiépítenie a kellő infrastruktúrát, beleértve a VPN hálózatot és virtualizációt, továbbá az eszközmenedzsmentet, ami kiterjed a BYOD (munkavállalók sajátjai) eszközökre is. Ám ez önmagában mit sem ér, ha a kollégák oktatására nem kerül sor, nekik mire kell jobban figyelni a mobilis környezetben [14].

Infrastruktúra mobil munkavégzésre Zero Trust biztonsági modellben, amit a Microsoft saját magára nézve is alkalmaz. “Never trust, always verify.” Lényege, hogy attól még, hogy valami a corporate tűzfal mögül érkezik, még nem tekinthető biztonságos kérésnek. A hozzáféréseket mindig authentikáció és authorizáció előzi meg, titkosítással ötvözve, így még egy bejutó támadó is számos akadállyal szembesül. Ezzel szemben a korábbi, tradícionális model a perifériák védelmére fókuszál, így itt egy óvatlan felhasználótól megszerzett belépési azonosítóval a további károkozásnak felfedezéséig nincs korlátja [14].

Másik probléma a hagyományos infrastruktúrával, hogy ugyan a VPN-ek használata már korábban is széles körben elterjedt volt, a terhelése az nem a mai napok forgalmára lett felkészítve. VPN infrastruktúra jellemzően a központ és telephelyeinek összeköttetésére volt alkalmazva, a csatorna leggyakrabban csak email és dokumentum transzferrel volt terhelve, azonban ma már a kollaborációs alkalmazások a meghatározók a maguk nagyobb sávszélesség igényével például audió- és videókonferenciákra [14].

A vállalati forgalom a távmunka révén áttolódott a publikus internet és a felhő irányába, amik segítik az elérés és a fokozott terheléssel való megbirkózást, de nagyobb kitettséget is hordoznak magukban. Az egyik ilyen veszély a DDOS támadás, amely volumene szintén növekedő tendenciát mutatott az elmúlt időszakban, az 1.7. ábra szerint a Kaspersky kimutatása alapján. Az elosztott, terheléses támadás ellehetetleníti az internetre kihelyezett kiszolgáló szervereket, így a felhasználók napi feladatvégzése lebénul. Nem kisebb probléma, hogy egy ilyen támadás elhárítása a teljes IT személyzetet is kimeríti, olyannyira, hogy ilyenkor a további, „hátsó ajtós” betörésérek kezeléséről is elvonhatja a figyelmet, amit a támadó ismét kihasználhat a károk fokozására [17].



1.7. ábra DDOS attack növekedése 2020 utolsó negyedévében [17]

Számosságban 2020 utolsó negyedévében átlag napi 200 eseményt mértek. A támadások legnagyobb részt az Egyesült Államokat érintik, azonban Magyarország is bekerült a Top 10 országok közé a maga 3,42%-val [17].

Érdekesség, hogy az ún. dark weben akár DDOS szolgáltatásokat is vásárolhatnak a cyber-bűnözők $48.63/óra átlagáron, amelynek ára csaknem háromszorosára növekedett 2020-ban az előző évhez képest [18].

1.2.5. Felhasználói szokások, támadási felületek

Napjaink leggyakoribb támadási formáiban szinte mindben közös, hogy felhasználói oldalról tudnak a legegyszerűbben érvényesülni. Valamilyen felhasználói interakció kiváltása az első lépés a támadások megindításához. Hiába építjük ki a legmagasabb szintű védelmet, ha a felhasználók önként adnak hozzáférést szenzitív adatokhoz. Persze a kettő nem független egymástól, olyan rendszer kiépítésére kell törekedni, ami kevesebb lehetőséget ad a „mellé kattintásoknak”. A felhasználói oldalról az oktatás, tudatosítás a legfontosabb. A Cisco tíz hasznos tippet gyűjtött össze, amire minden felhasználónak kellene figyelnie, egyben ezek a leggyakoribb hibák, amiket elkövetnek és támadási felületet adnak [19]:

1. Bárkiből lehet célpont, ne gondoljuk, hogy ez csak másokkal történhet meg.

2. Jelszavak, az egyik leggyakoribb hiba, hogy a nem megfelelő komplexitásút választunk, ráadásul akár több platformon is ugyanazt használjuk fel.
3. Az eszközeink, legyen laptop, mobiltelefon, mindig zárolva tartsuk, amíg nem használjuk őket, mégha csak rövid időre is készülünk távozni.
4. Mindig legyünk óvatosak és gyanakvóak, amikor egy email csatolmányt vagy hivatkozást kívánunk megnyitni, figyeljünk bármilyen apró eltérésre a feladó címében vagy hivatkozásaiban.
5. Szenzitív böngészéskor, például pénzügyi műveletek végzésénél (netbank, webshop vásárlás) kiváltképp megbízható, hozzánk tartozó eszközről indítsuk a tranzakciót, kerüljük a publikus gépeket és hálózatokat.
6. Mentsük adatainkat rendszeresen és a vírusvédő szoftverek frissítéseit ne halogassuk.
7. Ismeretlen eredetű külső drivert ne csatlakoztassunk eszközeinkhez, sokszor ezek is bekészített csapdák.
8. Alaposan fontoljuk meg, milyen információkat és milyen körökben osztunk meg magunkról a közösségi hálókon, a felhasználók gyakran önként szolgáltatják ki személyes adataikat, ami csak megkönnyítik a támadók munkáját.
9. Amikor egy reprezentatívnak látszó személy emailben vagy telefonon keresztül szeretné elkérni bejelentkezési adatainkat, tekintsük természetesnek a nemleges választ és mindig ellenőrizzük le a másik felet, mielőtt megosztanánk vele bármilyen információt is.
10. Soha ne ignoráljuk, ha valami gyanús vagy szokatlan jelenséget tapasztalunk a fiókjainkkal, jelezzük proaktívan az IT osztálynak. Fontos, hogy ne érezzük úgy, valami rosszat csináltunk, hiszen mi az elszenvedői vagyunk a támadásnak, nem az okozói [19].

2. A PIACON TALÁLHATÓ MEGOLDÁSOK ÁTTEKINTÉSE ÉS FEJLŐDÉSI TÖRTÉNETE

2.1.1. Biztonsági igények

Véleményem szerint a vállalatoknak olyan megoldásokra van szüksége, ami átfogó megoldást nyújt a gyakori támadási típusok ellen (phishing, ransomware, egyéb malware-k) a munkavállalók által elkövetett adatszivárgások megakadályozására, és azok fiókjainak emelt szintű védelmére egyaránt. Mivel a felhasználók valamilyen végponti interfészen keresztül lépnek kapcsolatba a rendszerrel, így minimum a professzionális Endpoint megoldások használata elengedhetetlen a vállalatok számára. Emellett az Email security és az Access management is kiemelt komponens a kiberbűnözés gátlásában.

Az **Endpoint security** védi az asztali számítógépeket, laptopokat, mobileszközöket vagy akár IoT eszközöket is. A végponti eszközök gyakori támadási vektornak számítanak, célja nem csupán az adott eszköz feltörése, hanem az azon keresztüli bejutás a védett corporate hálózatba. A végpont védő rendszerek fő feladata, hogy minél gyorsabban detektálja, analizálja és blokkolja a támadásokat. Ehhez a rendszerek összehangolt működésére van szükség, az adminisztrátorok számára a folyamatos monitorozást biztosítani kell, hogy elvégezhessék a helyreállítás lépéseit a fejlett támadások ellen is [20].

Az endpoint egyik fő eleme az anti-malware védelem, melyek a különféle rosszindulatú programok bejutását akadályozza, fellép a ransomware és phising módszerekkel szemben, amit egy végfél válthat ki, amikor rákattint egy veszélyes linkre a weben vagy emailben. Az anti-malware megoldás jó esetben gátat szab, hogy a bejutott program tovább terjeszkedjen a hálózaton és megállítsa a kliens fertőzését is. Egy egyszerű anti-vírus program ma már kevés, mivel a vírusok is egyre fejlettebbek, így a mai megoldások is számos új funkcionalitással kerültek felvértezésre. Ilyenek például a machine-learning és mesterséges intelligencia alapú blokkoló algoritmusok, threat intelligence, a milliónyi ismert fenyegetettségi minták gyors felismeréséhez naprakészen és a Sandbox megoldások, a biztonságos detonáláshoz és detektáláshoz [21].

Email védelem. Mivel az üzleti emailek kompromittálása is kiemelt támadási felületnek számít napjainkban, így erre is külön megoldások léteznek. A leggyakrabban a szövegtörzs, csatolmány, link vagy a küldő kiléte kerül manipulálásra. Nemcsak a végfelhasználók tudatosítása segíthet, hanem az is, ha egy intelligens email szűrő alkalmazás előre megvizsgálja helyettünk karantén környezetben a levéllel érkező csatolmányokat és linkeket és csak azokat engedi tovább a célpostaládába, amelyeket biztonságosnak talált, ez akár a zero-day attack felderítésére is alkalmas. Továbbá a multi-faktor authentikáció és az accountok MI-val támogadott védelme a baj bekövetkezése után még mindig megfoghatja idejében a támadót [22].

Authentikáció, hozzáférés menedzsment. A fiókok, különösen, ha vállalati, nagy értéket jelentenek, és belépést nem csak egy adott személyhez, hanem egy teljes vállalathoz adnak. Identitás és hozzáférés kezelő megoldásokkal jobban védhetőek a céges erőforrások, adatok, emellett biztosítani kell a munkavégzéshez szükséges jogosultságokat minél gördülékenyebben. Cybersecurity támadások hatékony védelmi megoldása a multi-faktor authentikáció, a single sing-on vagy a conditional access, azaz feltételes hozzáférés. Nem utolsó sorban a korábbi hozzáállás a jelszavakhoz is átalakulóban van az access management szolgáltatások révén, hiszen ezek a megoldások segítenek a korszerű jelszótárolásban és kezelésben egyaránt [23].

2.2. Piaci szereplők végpont védelemre

Endpoint megoldások közül rengeteg névvel találkozhatunk a piacon, a választék terjedelmes. Mivel a végponti megoldások a védelem rendszerébe illeszkedik be és kiegészülhet más szoftverekkel, így a funkcionalitás mellett a kompatibilitás is fontos választási szempont. A Gartner peer-insight oldala szerint a vásárlói értékelések alapján az alábbi Top 10 Endpoint megodás [24]:

1. Kaspersky Endpoint Security for Business
2. SentinelOne Endpoint Protection Platform
3. Falcon
4. Microsoft Defender Antivirus
5. McAfee Endpoint Security
6. Sophos Intercept X
7. ESET Endpoint Security
8. Malwarebytes Endpoint Protection
9. Symantec Endpoint Protection
10. VMware Carbon Black Cloud [24]

Ugyanez az összesítés a Gartner Magic Quadrant szerinti bontásban:

2.1. ábra Gartner Endpoint megoldások [25]

A 2.1-es ábra szerint a Microsoft számít vezető Endpoint megoldás szállítónak, emellett a Microsoft további négy Security kategóriában is élen jár, úgymint az Access Management, Unified Endpoint Management tools, Cloud Access Security Brokers és Enterprise Information Archiving kategóriák a Gartner, független elemző kutatásai alapján [26].

Kevés olyan univerzális tech cég van, aki olyannyira széleskörű portfólióval rendelkezik, mint a Microsoft. Komponensekre bontva szinte mindenhol találkozhatunk más vendorokkal is, de ezek összetétele heterogeneitást mutat.

2.3. Összehasonlítás irodai megoldásokra és védelmére

Dolgozatom célja a felhasználói oldalról való megközelítése a mindennapi biztonságnak, hatékonyságnövelésnek. Ideértve a költséghatékonyságot is, különben a vállalatok nem engedhetik meg maguknak ezeket az eszközöket. A széles Microsoft portfólion belül a Microsoft 365 család vállalatoknak szánt cloud-szolgáltatáscsomagját fogom részletesen vizsgálni. Ez a termékcsoport az MS Office-ból nőtte ki magát, de ma már túlnyomó részt felhőszolgáltatásokból épül fel, illetve integrálta magába a teljes kliensportfóliót.

A Microsoft 365 csomagok három fő komponensből állnak össze: Windows Pro, Office alkalmazások (Word, Excel stb.) és szolgáltatások (Exchange Online, SharePoint, Teams, stb.), végül a Security és Eszközmenedzsment (Defender, Intune, MDM). A szolgáltatások komponensekben is előfizethető. Jelen összehasonlítás a teljes csomagokra vonatkozik, melynek három szintje van, növekvő szolgáltatási szintekkel. Már az első

csomag, a Vállalati Prémium is tartalmazza a legtöbb általam ismertetett biztonsági funkciót, melyet 300 fős létszámig ajánlanak, a Nagyvállalati E3 és E5 jellemzően olyan többlet funkciókat tartalmaznak, amire inkább e feletti méret esetén érdekes. Jellemzően nagyobb analitikával, több automatizációval ellátottak, amit a nagyobb létszám indokolttá tehet. Havi díja 18,6 Euro felhasználónként (vagy 20 $), amit az információmunkás réteg számára szolgálja a mindennapi irodai eszközkészletet [27].

A piacon nehéz egy az egyben ezt helyettesitő megoldást találni más gyártóktól. Az irodai részhez legközelebb a Google Workspace vállalati szolgáltatásai állnak. A felhőben született vállalkozásokhoz talán utóbbi áll közelebb felhasználói oldalról, míg előbbihez a Windows-os környezet, beleértve az on-premise Server infrastruktúrát illeszkedhet jobban. Közel 50-50%-ban uralják a globális piacot.

Tapasztalatom szerint a felhasználás célja, a munkakörnyezet adottságai révén választanak a cégek. Akik jobban kibékülnek a webapplikációkkal, és kedvelik a Gmail, Drive stb. alkalmazásait, felhasználóbarátabbnak tartják azt, fogyasztói piacon kétségtelenül népszerűbb szolgáltatásokról beszélünk, azoknak a Workspace illeszkedhet jobban. Ahol viszont nélkülözhetetlenek az asztali megoldások, a komplex szöveg, táblázat vagy adatbázis feladatok vannak, továbbá a környezet is tartalmaz on-premise lábakat, arra a Microsoft tud egy vendorként megoldást nyújtani. Kompatibilitási problémákkal is kell számolni a Google rovására, hiszen az Online Google Appok vagy Online MS Office bárki számára elérhető ingyenesen, de a makrókat, függvényeket tartalmazó Office fájlokat csak asztali alkalmazással lehet érdemben használni. Árban nem jelentős a különbség, 18 $/hó felhasználó a Google Business Plus csomagja, ami kollaborációs megoldásokban lényegében ugyanazt tartalmazza, mint az M365 társa, de a Google védelme nem terjeszthető ki a teljes infrastrukturára. Erre a Microsoft 365 Defender képes, amit a Vállalati Prémium alapszinten már tartalmaz. Azon KKV-k számára, akik inkább a középvállalatok felé húznak komplexitásban, mintsem lefele SOHO irányba, a Microsoft megoldásai tudnak teljes lefedettséget adni az igényekre véleményem szerint [28].

A részletes funkcióösszehasonlítást a 2.2. számú táblázat mutatja:

	Google Worskspace Business Plus 18$	**Microsoft 365 Business Premium 20$**
Dokumentumkezelő alkalmazások		
szövegszerkesztő, táblázatkezelő, prezentáció, jegyzetek, űrlapok	Docs, Sheets, Slides, Keep, Forms Web-alapú	Word, Excel, PowerPoint, OneNote, Forms Web-alapú és Asztali
adatbáziskezelő	-	Access
Kollaborációs eszközök		
levelezés, tárhely, meeting, megosztás	Gmail, Drive, Meet, Chat, Jamboard, Sites	Outlook, OneDrive, Teams, SharePoint
Biztonság		
levélszemét, kártevők és ismert veszélyforrások elleni védelme	igen	igen
MFA, Csoportházirendek	igen	igen
Megőrzési házirendek	megőrzés	megőrzés és törlés
Feltételes hozzáférés	-	Nincs. Add-on
Végpont vírusvédelem		Defender Vállalati
DLP, adatszivárgás	Nincs. Add-on	igen (Online O365 szolgáltatásokhoz)
Címkézés, megosztás korlátozása	-	igen (Purview adatosztályozás, jogkör meghatározás, másolás, mentés stb. korlátozása)
Címtárkezelés	LDAP	Azure AD
Komplex veszélyforrások		Defender for O365
csatolmány, link védelem	igen	igen
adathalászat, hozzáférés	igen	igen
zero-hour malware	-	igen
karantén	igen	igen
Eszközkezelés		
MDM	igen	igen

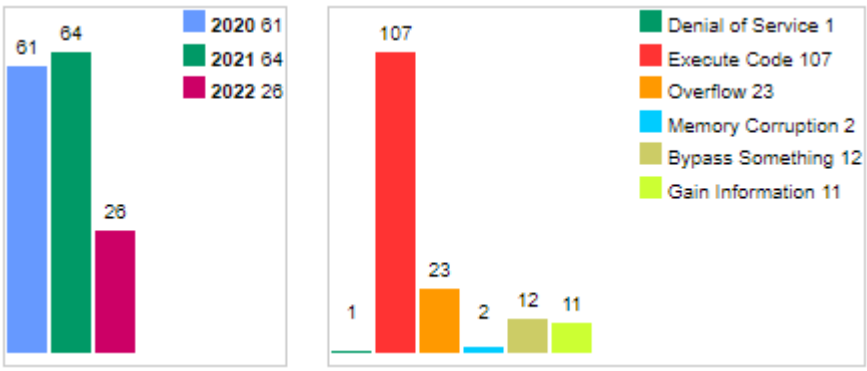
2.2. ábra Google és Microsoft összehasonlítás [28] [27]

2.3.1. Sebezhetőség

Ahogy a 2. fejezet elején is látszik, mint Security megoldás szállító, számos gyártót találhatunk a piacon, főleg, hogy ebben sokáig lemaradásban volt a Microsoft. A Microsoft Defender elérhető mind kliensek védelmére, mind pedig az online kommunikáció védelmére, mint Microsoft Defender for O365 (az Exchange Online Protection-t kiegészitve). Mivel a felhasználók elsősorban a külső kommunikáció során a legkitettebbek rosszindulatú szoftvereknek, adathalász kísérleteknek, igy ezt fogom sebezhetőség szempontjából vizsgálni és összevetni piaci konkurensekkel, az Email biztonságot mutatom be.

Az Egyesült Királyság felmérése alapján a támadások csaknem 83%-a email adathalász kísérletekből jön [29].

Először nézzük, hogy milyen támadás típusok érintik a Microsoft 365 Appokat. A 2.3. számú ábrán látható, hogy az elmúlt három évben a legutóbbiban jelentős visszaesés tapasztalható. A támadási típusokból pedig kiugróan vezet pirossal az “Remote Code Execution Vulnerability”. Ez hozzáférést ad a támadónak a fertőzött géphez, aki igy szinte bármilyen adatot olvashat, módosíthat, vagy törölhet. A támadás a Microsoft szerint két úton érkezhet: phising email csatolmányaként, vagy csaló weboldalra történő irányitással. Ezért is fontos a megfelelő jogosultságkezelés és a rétegzett hozzáférés házon belül [30].



2.3. ábra Támadástípusok M365-re [31]

Ezek ellen kíván védelmet nyújtani a Microsoft Defender for O365 és számos piacon található társa, amik add-onként nyújtanak magas szintű védelmet a levelezési szolgáltatás felé.

A piacon található email security megoldások funkcionalitásban igen hasonlóak, mindegyik az aktuális malware-ek ellen próbál védelmet nyújtani. Kutatást végezve a legtöbb összehasonlító oldal érdemben említi a Microsoft biztonsági megoldásait. A Gartner Email Security vélemények és értékelésekben folyamatosan törekszenek felfele

a Defender számai. Alábbi 2.4. számú tábla mutatja, mik ma a piacon gyakran értékelt megoldások. A legtöbb email security add-on ára 3$ és 7$ között mozog. A Defender for O365 a Vállalati Prémium része, de ha add-onként vásároljuk egy kisebb csomaghoz például, akkor 2$ a havidíja.

	Gyártó	Értékelés 5-ből	Értékelések száma
1	Proofpoint Email Protection Suite	4,5	458
2	Avavan	4,7	433
3	Mimecast Secure Email Gateway	4,5	352
4	Barracuda Email Security Gateway	4,4	240
5	Cisco Secure Email	4,4	206
6	Trend Micro Cloud App Security	4,8	165
7	FortiMail	4,5	150
8	Symantec Email Security.cloud	4,5	112
9	Symantec Messaging Gateway (SMG)	4,40	110
10	Abnormal Security	4,8	109
11	Darktrace/Email	4,8	108
12	Tessian Cloud Email Security Platform	4,6	106
13	Microsoft Defender for Office 365	4,5	96
14	Microsoft Exchange Online Protection (EOP)	4,4	91

2.4. ábra Gartner rangsor: email security szállítók [32]

Konkrét teszteken azonban ennél jóval eredményesebben szerepel. Az SE Labs, Egyesült Királyság beli kutatócég, aki az IT szolgáltatókat teszteli biztonságosság szempontjából, legutóbbi riportjában négy email security megoldást vizsgált. Ezek a Microsoft, Google, mint email platform és a Percepcion-Point, Fortinet FortiMail Cloud Email Security mint add-on szállítók voltak. A Microsoft a 3. helyen végzett, de még így is megkapta a legkiválóbb AAA minősítést. A helyezést elsősorban a fals-pozitívak száma miatt kapta. A Percepcion-point végzett az első helyen 100%-os pontossággal, majd a Fortinet. A Google jelentősen lemaradt, negatív értékelést kapott, 27%-on végzett. A teszt az elmúlt évek támadásaiból készít mintát, így igen valóságos szimulációt ad. A metrika nem csak a támadásokat vizsgálja, hanem a legitimitási-rátát is. Hiszen fontos, hogy a veszélyt nem jelentő, ám sokszor fontos üzenetet ne kerüljenek blokkolásra, feleslegesen Spam-mappába. Ez komoly szempont hatékonyság és felhasználói kényelem szempontjából is [33].

A támadásicsoport szimulációk az alábbiak voltak:

- Sandworm/Voodo Bear: Windows sebeszhetőség Office csatolmányokon keresztül. Egy zero-day sebezhetőség volt, eredetije áramszünetet okozott Ukrajnában.
- ATP28: Microsoft Office Makrók, a csatolmány megnyitása után indul el további ajtókat nyitva.
- FIN4: Man-in-the-middle adathalászat, pénzügyi cégeknél.
- FIN7: adathalászat sriptekkel, kereskedelmi szektort célozta ügyfél kapcsolatfelvételnek tűnő levelekkel és csatolmányaival.
- Dragonfly & Dragonfly 2.0: energiaszektort célzó hozzáférés-megszerzés phishinggel [33]

A Microsoft Defender a támadások 98%-át sikeresen kiszűrte. A Business email kompromitálásában volt tévesztése, ahol átengedett támadásnak szánt leveleket is. Phising-ben, Social Engeenering-ben és Malware-ban 100%-osan teljesített. Üzenetek legitimitás-vizsgálatában, fals-pozitívak tekintetében 86%-os volt a hatékonysága [33].

2.4. Microsoft, mint Security megoldásszállító

A következő fejezetekben a megoldandó feladat bemutatása és kiértékelése következik. A konzekvenciák közt elsősorban azt célzom levonni, miként lehet kialakítani egy olyan felhasználói környezetet, ami egyszerre véd a napjainkat érintő számtalan kibertámadási lehetőségtől, ugyanakkor a bonyolult rendszerek nem keserítik meg a munkavállalók mindennapjait feladataik ellátása során.

Választásom több szempontból is a Microsoft Security portfóliójára esett. Egyrészt, mint Microsoft alkalmazott, engem is ezen megoldások vesznek körbe és licensz szerződési specialistaként szinte kizárólag érzékeny, bizalmas dokumentumokat kezelek. Továbbá globális szinten is elterjedt gyártóról beszélünk, amit minden vállalati környezet jól ismer és ahogy az előző fejezet mutatja, az összehasonlításokban és teszteken is jó eredményeket ér el. Még ha elsősorban az operációs rendszer és Office alkalmazás a legismertebb szoftverük, a teljes paletta ezen messze túlmutat és vendor függetlenül biztosít integrációt az alap operációs rendszerrel.

Be fogom mutatni a vállalatoknak szánt, security specifikus megoldásokat a szoftver mogultól. Különösképp az automatizációs funkciókat vizsgálva, hogy azok miként tudnak a felhasználók kényelmére lenni, azok hogyan tudnak asszisztálni a fenyegetettségek elkerülésében akkor is, ha erre a végfél maga nem figyel fel. Ilyenek lehetnek az intelligens fájlvédelem, adatszivárgásmegelőzés és jogosultságkezelés.

Ezen biztonsági modulokból KKV vállalatok számára szánt dokumentummenedzsment módszertant alakítok ki Microsoft 365 megoldásokkal. A felhő alapú, vállalati tenant egyre elterjedtebb a piacon. Legnagyobb előnyének azt tartom, hogy kis felhasználói

létszám mellett is elérhető, Enterprise szintű biztonsági megoldásokat lehet felhasználni. A felhő modell abban is előnyös, hogy a hagyományos on-premise infrastruktúráknál a komplexebb védelmi rendszerek kiépítése általában véve csak nagy volumenben gazdaságosak, pedig a védelmi szintet nem a cég méretében, hanem az adat szenzitivitásában célszerű meghatározni.

3. PIACI KIHÍVÁSOK ÉS BIZTONSÁGI MEGOLDÁSAI

Jelen fejezetben a megoldandó feladat bemutatása következik. A dolgozatomban vállalati biztonsági megoldásokra építkezem. A hazai gazdaság mozgatórugóját számosságában és foglalkoztatottságában a KKV szektor teszi ki. A kiberbiztonság megteremtése itt is kihívásokat jelent, hanem nagyobbat, mint egy nagyvállalatnál, ahol méretükből adódóan megéri professzionális rendszereknek akár házon belüli fejlesztése is, és minden egyedi kívánalom teljesülhet. Kisvállalatoknál ennek hatékonysága és minősége már kérdéses, ezért a dolgozatomban olyan megoldásokra támaszkodom, amik kereskedelmi forgalomban könnyen elérhetőek, megfizethető áron, beleértve ezek testre szabásának és üzemeltetésének költségeit is.

Ahány cég, annyi szokás, de a nevezetes információ- és dokumentumkezelési munkafolyamatok valamennyi helyen hasonlóképpen zajlanak, tehát célszerűnek tartom olyan termékek használatát, amik alapvetően standard munkafolyamatokat támogatnak, de testre szabási lehetőségekkel, hogy az egyéni preferenciákat is figyelembe lehessen venni.

A biztonsági kívánalmak egyaránt érintenek minden gazdasági szervezetet, hiszen mint az előző fejezetben utalva rá, a mai kibertámadások gyakorta pénzügyi motivációt rejtegetnek, így nem csak indirekt hatnak rosszul a vállalat értékére, mint például a rossz hírnév adatszivárgás miatt, hanem konkrét megkárosítás rizikó faktora is magas.

Azonban az szintén hordozhat magában anyagi hátrányt, amennyiben a vállalat által alkalmazott biztonsági házirendek bonyolultak a munkavállalók számára. Ha ezen eszközök használata túl összetett és időigényes, az hatékonyságromlást fog eredményezni. Nem ritka esetben a dolgozók éppen ezért terhelhetik át a céges információ irányát olyan 3rd party SaaS termékekre, amik nem állnak belső kontroll alatt, de egyszerűbb a használata. Ezért minden vezetőnek jól felfogott érdeke, hogy egyszerre biztosítson használható és biztonságos munkaplatformot.

A következő fejezetben olyan megoldást keresek, amik a fenti kívánalmakat teljesítik és széles körben használhatók különböző szokásokat követő vállalatoknál. Dolgozatomban a legnagyobb számban előforduló szolgálatói szektor, kereskedelmi tevékenységet folytató KKV-k számára fogok egy Biztonsági Útmutatót készíteni adat- és dokumentumkezelési folyamatokra. Ehhez a Microsoft Security portfoliójára fogok támaszkodni.

Korábbi munkahelyeimen magam is megtapasztaltam a KKV-k főbb kihívásait, emellett számtalan ilyen kategóriájú ügyfél működésébe is nyílt betekintésem dokumentumkezelő rendszerek felmérése során, a Biztonsági Útmutatómban ezen tapasztalatokra is fogok építkezni.

3.1. A KKV-k jellemzői Magyarországon

Tapasztalataim a KKV-k felső felére, a középvállalatokkal való kapcsolattartásból származnak, így a néhány fős cégekre ebben a dolgozatban nem térek ki. Automatizált munkafolyamatot bevezetni 50-100 fős cég felett érdemes, ahol tere van a standardizálásnak, nem úgy, mint amikor még kis létszámmal a rugalmasság a fő előny.

A KSH adatai szerint a hazai vállalatok 99%-a KKV, és a foglalkoztatottak száma 65%, az összárbevételnek ugyanakkor 41%-át teszi ki a nagyvállalatokhoz képest. A magas darabszám a mikrovállalkozásoknak köszönhető, csaknem 577 ezer a 850 ezerből, a középvállalati szegmens ennél jóval szűkösebb, 5000-es darabszámra tehető, ám a nagyvállalatok után itt a második legmagasabb érték az egy főre jutó árbevétel. Az összárbevétel (KKV és KKV-n kívüli szervezetek) 14%-át a középvállalatok adják, 26%-ot pedig a mikro- és kisvállalatok, a „maradék” 60% pedig a nagyoktól olvasható ki a 3.1. ábrából [34].

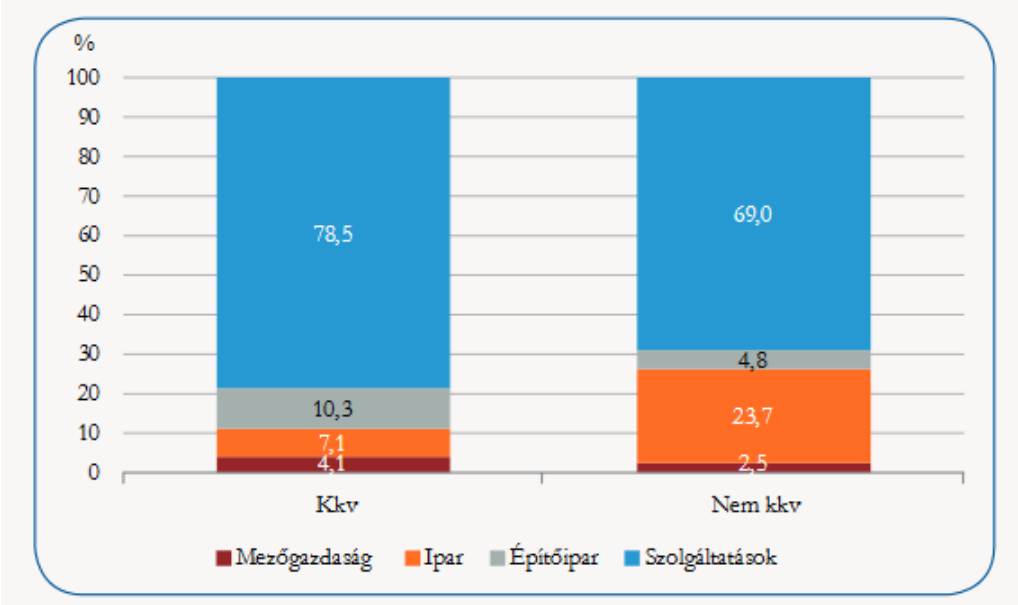
Kis- és középvállalkozási kategória	Vállalkozások száma, darab	Foglalkoztatottak létszáma, fő	Egy foglalkoztatottra jutó árbevétel, ezer forint/fő	Foglalkoztatottak létszámának megoszlása, %	Értékesítés nettó árbevétele, millió forint
2020					
0 fős mikrovállalkozások	31 689	–	–	–	31 118
1 fős mikrovállalkozások	577 753	577 753	8 252	18,1	4 767 839
2–9 fős mikrovállalkozások	194 754	644 240	16 291	20,1	10 495 276
Kisvállalkozások	33 376	532 145	30 746	16,6	16 361 568
Középvállalkozások	5 135	351 331	47 690	11,0	16 754 948
Nem KKV körbe tartozó szervezetek	8 040	1 093 425	63 297	34,2	69 210 371
Összesen	**850 747**	**3 198 894**	**36 769**	**100,0**	**117 621 120**

3.1. ábra A vállalkozások teljesítménymutatói kis- és középvállalkozási kategória szerint [34]

A KKV-k fontosságáról maga az EU is rendelkezik. Az 1980-as évektől kezdve célul tűzték ki, hogy a versenyhátrány leküzdésében segítséget érdemelnek a nagyvállalatokkal szemben, mert úgy látják, a nagyobb árbevételen kívül minden másban ez a szektor ad többet a közjónak: magasabb foglalkoztatottságot biztosítanak, rugalmasabbak giga társaiknál, piaci változásokra sokkal gyorsabban reagálnak és képesek megújulni, továbbá személyesebb szolgáltatásokat tesznek lehetővé ügyfeleiknek. Dolgozatom is a hatékonyság növelést tartja fontosnak e szegmens számára [35].

Ami a tevékenységi körüket illeti, a KKV-k főleg a szolgáltatóiparban erősek, mintegy 68,5 százalékot kitevő részben, ahogy a 3.2. ábra mutatja. Szolgáltatáson belül is a kereskedelem és gépjárműjavítás áll az első helyen. Ennek okai, hogy ebben a szegmensben nagyobb a kis tőkeigényű tevékenységek száma, míg a nagyvállalatokra

jellemző nagytőkeigényes ágak kevésbé vannak jelen. A kisebb tőke- és munkaerőforrás erre ad nagyobb lehetőséget. Nagy beruházások erőforráshiányban szenvednek, így informatikai rendszerek beszerzésében nekik is a szolgáltatás/előfizetéses alapú konstrukciók a hozzáillők [36].



3.2. ábra A működő vállalkozások számának megoszlása összevont gazdasági ágak szerint, 2018 [36]

A KSH 2021-es adatai szerint az össz társasvállalkozásból az első helyen a Kereskedelem, gépjárműjavítás kategória áll több mint 116 ezer vállalkozással, ezt követi a Szakmai, tudományos, műszaki tevékenység, Építőipar majd az Ipar. Az egyre növekvő Információ, kommunikáció a 8. helyen áll 30 ezer vállalkozással [37].

3.1.1. Kereskedelmi tevékenység jellemzői

A továbbiakban a KKV-k ezen körére fókuszálok és bemutatom az erre a tevékenységre jellemző adminisztratív munkafolyamatokat. Az ügyfelekkel való minőségi kapcsolattartás túlzás nélkül létfontosságú az eredményes vállalkozások számára, amelynek a kiberbiztonság alatt értett hitelesség is építőeleme. A kommunikáció ma már nem a telefonra és a postai levelezésre, hanem a nyílt hálózaton való csatornákra koncentrálódik. A kommunikáció tárgyát az adat- és dokumentumok képzik. Mindennapos az árajánlatok, szerződések, árlisták, számlák interneten keresztüli megosztása, amelyek egytől egyik szenzitív ügyféladatokat tartalmaznak. Továbbá éles a határ a belsős és külsős dokumentumok között, egy beszerzési árakat tartalmazó árlista nem kerülhet külsős felekhez. Ezek olyan házirendek, melyeket nem lehet megszegni, sokszor ennek még sincs semmilyen fizikai akadálya. Az igény a szofisztikált jogosultságkezelésre erős.

4. MEGOLDÁS ÉPÍTŐELEMEINEK BEMUTATÁSA

A Microsoft Security portfolio teljes IT rendszerre kiterjedő megoldásokat rejt magában kliens, szerver és felhő irányban. Az utóbbit fogom kiemelten vizsgálni, azon belül is az irodai munka kapcsán felmerülő területeket. Erre elsősorban A Microsoft 365 megoldásai szolgálnak.

A fejezetben taglalt modulokat a szakdolgozat megoldásának megfelelően válogattam össze, ez a biztonsági házirend eszközkészlete.

4.1. Microsoft 365 Compliance (Purview)

Információvédelem és irányítása

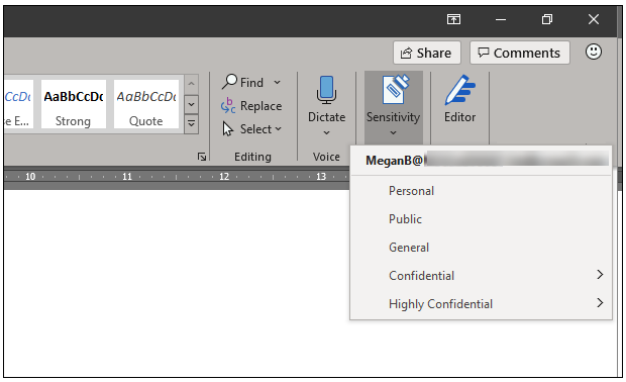
Az információ, mely leggyakrabban dokumentumok, email üzenetek formájában jelenik meg, különböző mértékben képviselnek értéket. A navigáció komoly figyelmet igényel, melyet humán képességeinkkel kell túlnyomórészt lekövetni. Ez komoly erőfeszítést követelhet nagy mennyiség esetén és a figyelmetlenség is jelentős rizikófaktor. Az információvédelmi modul abban segít, hogy feltérképezze a vállalati adatvagyon összetételét és azonosítsuk a szenzitív elemeket (Know your data). Megvédje titkosítással, hozzáférés-korlátozással és megjelöléssel (Protect your data). Megakadályozza az adatszivárgást és egyaránt detektálja a gyanús viselkedést és a véletlen megosztásokat (Prevent data loss). Végül segítse az adatkezelést, automatikus tárolási és eltávolítási házirendekkel (Govern your data) [38].

A Microsoft adatosztályozási metódusa segít kategorizálni és indexelni az információk szenzitivitását. A kategóriákhoz és címkékhez megannyi házirendet hozzárendelhetünk, hogy ezt követően mik történjenek a fájljainkkal. Ezeket a felhasználók maguk rendelhetik hozzá a dokumentumokhoz vagy e-mail üzenetekhez (Office appokon), de automatikusan is besorolhatók, illetve a rendszer machine learning techológiákkal is tanítható. Az automatika előre definiált mintázatok, maszkok alapján (pl. IBAN szám formátum, azonosítók stb.) tudja megcímkézni a tartalmakat. Az öntanuló rendszerek pedig egy betáplált, nagyméretű adatmintából dolgoznak. Az adatvagyon feltérképezés az Azure Information Protection szolgáltatás segítségével az on-premise rendszerekre is kiterjeszthető, a Microsoft Defender for Cloud Apps pedig egyéb 3rd party SaaS-okra is, így minden lokalizáció lefedhető [38].

A feltérképezés után a fájl-védelemre és annak szintjére a Microsoft Information Protection titkosítást, hozzáférés-korlátozást és vízjelölést biztosít. Emellett az adatszivárgás megelőzést gyanús viselkedés-elemzéssel támogatja. Védelmi megoldások mellett a dokumentum-életciklus menedzsment szolgáltatások is találhatók, így a fájlkezelés a jogi szabályozásokkal is összhangba hozhatók [38].

Hogyan működik a gyakorlatban? Kategorizálás, szenzitív információ típusok

A szenzitív információk azonosítása és besorolása az első lépés az információvédelmi irányelvek felállításában, melyre három mód használható a Microsoft megoldásában: manuális, humán kategorizálás – a 4.1-es ábra, mintázatok vagy sablonok szerinti automatikus mód vagy Machine Learning alapú. Ezekről a meghatalmazott admin csoport dönt és készíti el. A végfelhasználói oldalon megjelenik az adatklasszifikációs lehetőség az emaileken és dokumentumokon. Ezt követően pedig meghatározzuk, hogy kik és milyen jogkörrel rendelkezhetnek az adott kategóriában [39].



4.1. ábra Egy Word fájl manuális osztályozása [38]

A szenzitív információtípus (SIT) meghatározása mintázat alapján működik, azonosítókat, megnevezéseket keresve. A rendszer számos beépített sablonnal rendelkezik nevezetes azonosítók felismerésére nemzetközi és hazai tartalomtípusokra vonatkozóan. A beépített SIT-ek nem módosíthatók, de a sablonok másolhatók, testreszabhatók. Az adatábisnak része az ún. nevesített SIT-ek, amik személynevekre, lakcímekre, orvosi rekordokra alkalmazhatók. Utóbbi nem, míg az első kettő magyar nevekre is működik. Meglévőn kívül új, egyéni SIT-eket is létrehozhatunk. A mintázat meghatározásakor egy elsődleges (primary) és az azt támogató kifejezések (supporting element) is segítenek abban, mi alapján keressük a kívánt tartalmat a dokumentumokban, levelekben. Az elsődleges elem lehet egy tipikus kifejezése a tartalomnak, illetve kulcsszavas lista, kulcsszavas szótár vagy funkció. A támogató elem az elsődleges kifejezés pontosítását, magabiztosságát segíti elő. Például egy adott kártyaszám megtalálásánál a „kártyaazonosító” kifejezés várhatóan a szám környezetében lesz. Itt is használható kulcsszó lista vagy szótár. A magabiztosságon (confidence level) is szabályozhatunk, hogy a támogató elemek száma magas, alacsony vagy közepes legyen. Magasnál pontos találatok várhatóak alacsony fals pozitív mellett, ám sok fals negatívot is hagyhat, míg alacsonynál fordítva. A közelségen (proximity) is szabályozhatunk, hogy az adott támogató elemeket milyen szélességben keressük az elsődleges elemhez képest [39].

Címkék és jogköreik

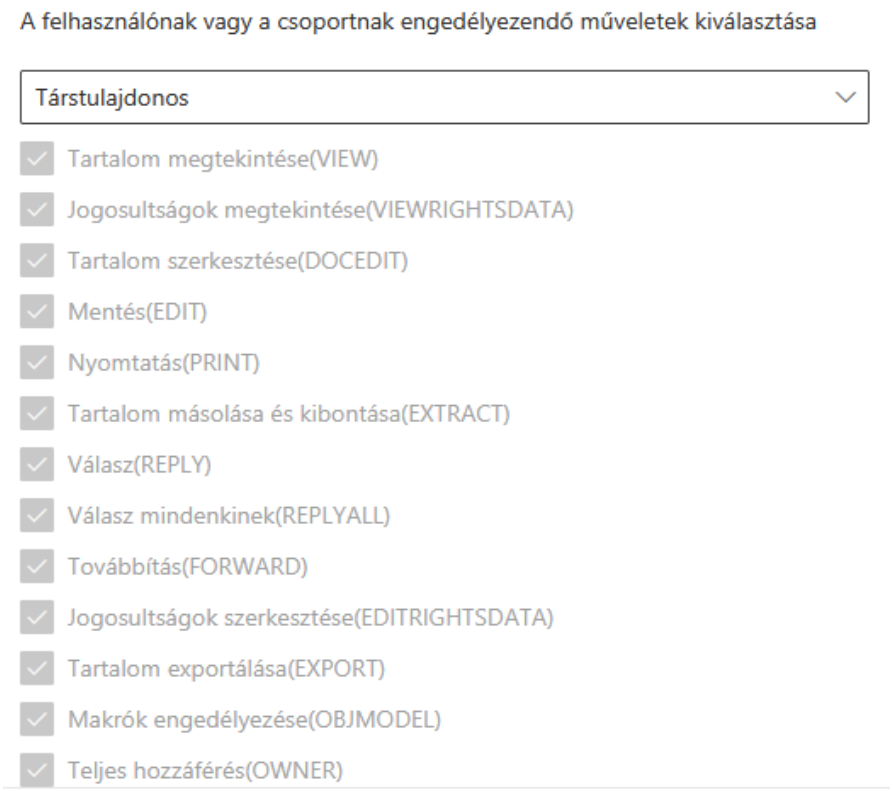
A Microsoft 365 öt alapértelmezett címkét kínál fel, melyek jó kiindulási alapot biztosítanak a kategorizáláshoz, ezek az alábbiak. További egyedi címkék is létrehozhatók és az alapértelmezettek is átkonfigurálhatók. A vizsgálathoz aktiváltam egy M365 demo környezetet, ahol a fejezetben beszélt megoldásokat kipróbáltam, azokból illusztrációkat merítettem. Az itt talált alapértelmezett címkék:

- **Személyes**, csak a létrehozó számára elérhető
- **Nyilvános**, kifejezetten külső ügyfél/partner kommunikációra
- **Általános**, belsős, de nem kritikus adatokat tartalmaz
- **Bizalmas**, megosztása maximum együttműködő partnerekkel
- **Szigorúan titkos**, csak belső felhasználásra

A címkéknél megadhatjuk a hatókört (3), ezek fájlok és emailek, MS Teams csoportok és SharePoint webhelyek, vagy sémaalapú nagyméretű adatbázisok (SQL, Azure SQL, AWS RDS stb.) lehetnek. A védelemnél titkosíthatunk, és ezzel egyben adott körre szűkíthetünk hozzáférést vagy megjelölhetjük egyéni fejlécekkel, vízjelekkel dokumentumainkat. Titkosításnál levelezés esetén engedélyezhetjük a felhasználóknak, hogy „Nem továbbítandó" titkosítást állítsanak be, sem küldeni, nyomtatni vagy másolni nem fogják tudni a címzettek a levelet és annak csatolmányait. Emellett kiválasztható Outlookban a „Csak titkosítás" mód is, ahol a megcímzettek szabadon használhatják az email tartalmát, de ez csak is kizárólag rájuk vonatkozik, tovább nem oszthatják. Office fájlok esetén kötelezővé tehető, hogy a vállalati dokumentumhoz mindenképpen fel kelljen címkézni, segítve az adatvagyon higéniáját [40].

A címke jogosultsági körét rábízhatjuk a felhasználókra, vagy előre definiálhatjuk a csoportokat, szinteket. A csoportokon belül megkülönböztethetünk belsős és külsős felhasználókat, külsős domaineket is (pl. partnercég, külső auditor, tanácsadó), melyektől az authentikáció kikövetelhető, így garantálva, hogy csak az illetékesek nyertek hozzáférést, a 4.2.-es ábra pedig az általuk használható jogosultságokat mutatja. Emellett a hozzáférés időtartalma és az offline-elérés is korlátozható [40].

Offline elérés alatt értjük azt, amikor egy fájl máshova mentve, azonosítás nélkül is megtekinthető. Ezt szigorúan bizalmas információknál feltétlen ki kell zárni, ám így a jogosult felhasználót is éri kényelmetlenség, hogy nem dolgozhat akárhol az adott anyaggal. Az offline access-t tiltva a megtekintés mindig aktív internetkapcsolatot követel. Nagy előnye viszont, hogy az így kiosztott jogosultságok azonnali hatállyal vissza is vonhatók, tehát egy téves megosztás vagy idő közben megszüntetett jogviszony azonnal érvényre léptethető. A felhasználhatóság kedvére téve megadható x nap, ameddig ezt az offline hozzáférést megadhatjuk. Alapértelmezetten legfeljebb 30 napig érhető el egy fájl bejelentkezés nélkül [41].



4.2. ábra Felhasználói jogkörök lehetőségei

Fontos döntés, hogy a címkézést a felhasználókra bízzuk, vagy esetleg valamilyen gép által elvégzett besorolást alkalmazzunk-e. Itt egy logikai függvény állítható be, milyen kulcsszavakra lépjen életbe az automatizmus. A tartalomban szerepel az „XY" kifejezés, számlaszám, azonosító stb. Manuális és előre definiált azonosítókat (nemzetközi lista igazolvány vagy számlaszám formátumokról beépítetten) is használhatunk, de betaníthatunk saját vállalatunkra jellemző dokumentum-sablonokat (céges szerződés, számlakép, szállítóleveleink, árlistáink stb.). Amennyiben a feltétel igaz, az automatikus címke érvénybe lépése helyett csak javaslatot is tehetünk a felhasználónak [42].

Miután a címkék konfigurálásra kerültek és alkalmazzuk őket dokumentumokra, minden kívánt védelmi beállításunk végrehajtódik. Titkosítási beállítást követően csak a megadott személyek, csoportok nyerhetnek betekintést. Ezen belül is megadhatjuk, hogy ki milyen jogkörrel rendelkezik. Például egy „Bizalmas" címkével ellátott dokumentumra házon belül minden felhasználó olvasó módot kap, de szerkesztési joggal csak a létrehozó csoport bír. A titkosítás Azure Rights Management service-t használ. Ez a megoldás egyaránt titkosít, azonosít és authoritást menedzsel fájl szintig. A beállításokkal egyensúlyozhatunk a biztonság és kényelem között. Egy titkosított Office file-nak ugyanis limitációkkal kell szembenéznie. Főbb hátrányai, hogy nem kereshető a teljes szöveg, DLP házirendek csak a metaadatokra működik, webes nézet nem elérhető, és nem, vagy csak limitáltan lehet egy időben, közösen szerkeszteni [42].

Külsős megosztások, nem MS-account hitelesítések eseténél is számos védelmi metódust állíthatunk be. Például automatizálható, hogy minden titkosítással ellátott dokumentumnál külső domainre való küldésnél a „Nem továbbítható” szabályt léptesse életbe, így azt a címzett ugyan megtekintheti, de nem másolhatja, nyomtathatja, vagy küldheti tovább. Az is beállítható, hogy egy adott domainre szabott címkét hozunk létre, itt a jogosultság beállításakor a felhasználóknál megadható adott felhasználó vagy domain. A nevét begépelve, pl. fabrikam.com, máris az egész tartományra érvényes szabályt adhatunk meg. Így állítható be az is, hogy egy partnercégünk csak olvashatja a nekik szánt árlistáinkat, de azt nem szerkesztheti, használhatja fel másra. Végül az is egy praktikus példa, ahol előre definiált felhasználói csoport nélkül titkosítunk fájlokat például olyan kampányanyagokat, amelyek széles körben publikálhatóak, de idővel érvényüket vesztik. Az így megosztott fájlok nem maradnak őrizetlenek, a továbbiakban is módosítható lesz a jogkörürük, lejárati idejük és offline hozzáférésük [43].

Adatszivárgás-megelőzés (DLP)

Adatszivárgás-megelőzés alatt az illetéktelenekkel való szándékos- vagy véletlenmegosztás megakadályozását értjük a Microsoft DLP házirendek segítségével, a Microsoft Purview/Információvédelmi megoldás részeként. Ezzel a modullal azonosítható, monitorozható és automatikusan védhető a tartalom nem csak Microsoft környezetben, hanem MacOS-en egyéb cloud app területeken is. A DLP képes mély tartalomelemzése, analizálja és validálja az elsődleges egyezéseket és ellenőrzi a közelséget a másodlagos adattalálatokkal, mindez Machine Learning algoritmusokkal kiegészítve. A DLP képes folyamatosan monitorozni a fájlokon végzett user aktivizást és a válaszlépések szigora bármilyen lehet. Amikor egy felhasználó szenzitív szöveget kíván például kimásolni, a válaszreakció az egyszerű figyelmeztető üzenettől kezdve a fájl zárolásáig terjedhet. Az aktivitások bekerülnek az Audit logba is, és beállíthatunk értesítéseket is a nem kívánt felhasználói műveletekről. Az aktivitások dashboardján emellett összesített nézetek, riportok segítik az adminisztrátorok munkáját a felderítésben. A felhasználói élmény érdekében a pop-up üzenetek egyszerre segíthetik a felhasználók figyelmét vezetni, hogyan bánjanak az érzékeny dokumentumokkal és az adminisztrátoroknak nagyobb betekintést adni azokról a személyekről, aki ezek ellenére gondatlanul kezelik a céges adatvagyont. Házirendek az előző alfejezetben részletezett címkézett fájlokra is beállíthatók. A szenzitivitási címke szerint is érvénybe léptethetünk védelmi válaszreakciókat a rendszerben [44].

Megőrzési házirendek (Retention labels)

Az adathalom tisztaságáért, ami segít megőrizni, ami fontos és elvetni, ami nem. Amikor a dokumentumok életciklusát szeretnénk szabályozni, akkor célszerű rájuk megőrzési, törlési házirendet alkalmazni. Meghatározható, mennyi ideig tárolható egy adott dokumentum, mennyi ideig legyen legalább, vagy legfeljebb eltárolva, vagy mikortól legyen véglegesen törölve. Segít megfelelni a törvényi szabályozásoknak is, a

megoldással pontosan addig őrizhetünk meg például egy e-számlát, bizonylatot, ameddig feltétlen szükség van rá. A rég érvényét vesztett dokumentumok takarításáról, amiket a felhasználók sokszor még gondatlanabbul kezelnek, nem kell manuálisan törölnünk, nem hagyva ezzel sem adatszivárgási felületet. Szintén hasznos felhasználási terület az időszakos kampányanyagok, promociós árlisták, ajánlatok ezen megjelölése, amire jellemzően adott határidőig van szükség, majd utána törölhetőek, archiválhatóak [45].

A megőrzési házirendek hatóköre a szenzitivitási címkékkel ellentétben az M365 környezetre korlátozódik, azon belül alkalmazhatjuk teljes SharePoint dokumentumtárakra, Teams vagy Yammer csatornákra, illetve Exchange postafiókokra. Tárolók mellett címkézhetünk egy-egy fájlt vagy emailt is, de értelmezhető felhasználóra is. Adott fájlra és adott verzióra is alkalmaz. Amennyiben egy megőrzési címkével ellátott fájlt vagy emailt módosítanak, úgy az eredeti verzió is megőrzésre kerül egy külön erre a célra szakosodott tárolóban. A policy-k kombinálhatók. Amennyiben egy egész SharePoint mappára alkalmaztunk egy házirendet, az azon belüli fájlokra is tehetünk külön címkéket, ha azok további szabályozásra kényszerülnek. A mappákra, postafiókokra alkalmazott házirendek áthelyezés esetén nem utaznak az elemmel (de az eredeti helyen is megmaradnak), míg a megőrzési címkék az M365 környezeten belül igen [45].

Megőrzési címkék alkalmazása történhet manuálisan, vagy automatikusan a szenzitivitási címkék metódusával megegyező módon. A címkézést egy adott event is kiválthatja, mint például egy dolgozó távozásánál az ő OneDrive-jára, postafiókjára életbe léphet egy megőrzési házirend. Alapértelmezett házirendeket is létrehozhatunk, amit szélesen alkalmazhatunk M365 környezetünkre, mintegy alapvédelemmel ellátva minden könyvtárat, csatornát vagy postafiókot. A címke egy DPL házirend feltételeként is használható, így kiterjeszthető, hogy a megőrzés alá bevont állományok például nem megoszthatók házon kívül [46].

4.2. Felhasználók azonosítása és identitás kezelés

A Microsoft 365 a felhasználók kezelésére és védelmére Azure Active Directory (AAD) szolgáltatást használ. A felhőalapú szolgáltatás biztosítja a hozzáférést mind a belsős tartalmakhoz, mind pedig egyéb külsős forrásokhoz, SaaS alkalmazásokhoz. A klasszikus Windows Server AD-n felül számtalan további kibővített cloud funkciót tartalmaz és integrálható egyéb 3rd party appokba, támogatva a Single Sign On-t (SSO) is. Az AAD az Identity Protection moduljával machine learning alapokon detektálja a gyanús jeleket, amihez a tanulási mintát a Microsoft saját platformjairól érkező napi 6,5 billiónyi jelből veszi. Ennek köszönhetően automatikusan deríthetők fel a különféle támadások és a válasz-védekezési mechanizmusok. A beérkezett jelek alapján felállíthatók feltételes-hozzáférések, amik gyanús események alapján blokkolják a bejelentkezéseket és adatbázisául szolgálnak SIEM rendszereknek is a további kivizsgálások végett. Az

automatizálás védelmet biztosíthat többek között brute force attack és társai, anonim IP-k, bejelentkezés távoli helyről, malware stb [47].

Másik hasznos funkció a feltételes hozzáférés (Conditional Access) konfigurálása. Itt lehetőség nyílik a szervezetre jellemző házirendek beállítására és az oda nem illő bejelentkezési kísérletek kizárására személy, eszköz és hely vonatkozásában. Kockázatos bejelentkezésnek tekinthető, ha egy felhasználó a tőle nem megszokott helyről, eszközről jelentkezik be. Lokalizáció tekintetében az adminisztrátor megadhat és/vagy kizárhat adott IP range-eket, például biztonságosnak állíthatja be a vállalat telephelyeiről érkező kéréseket. A szokatlan bejelentkezéseket a rendszer tilthatja, vagy további authentikációra kötelezheti multifaktor authentikáció (MFA) segítségével. MFA-t tartalom szerint is hangolhatunk, szenzitív adatokhoz való hozzáférésnél is addícionálisan kikényszeríthető [48].

Nem csak a vállalat felhasználóinak hozzáférésére állíthatunk fel szabályokat, az Azure AD B2B és B2C üzleti partnereink és ügyfeleink hozzáférését is finomhangolhatjuk a hatékony és biztonságos együttműködés érdekében. Így megszabható, hogy egy partner milyen tartalmakat láthat és milyen további azonosítást követelünk ki a biztonság érdekében. A B2C-vel pedig publikus ügyfeleink számára szabályozhatjuk, hogyan férhetnek hozzá hosztolt alkalmazásainkhoz [47].

Jelszókezelés

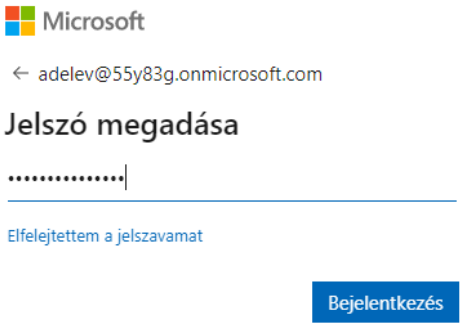
A felhasználói kényelem sarkalatos pontja a bejelentkezés módja, amit termesztésen a túlzottba vitt óvatosság megnehezíthet. Az AAD-ben az authenikációnak is számos módja van, ami segít optimalizálni ezt a területet.

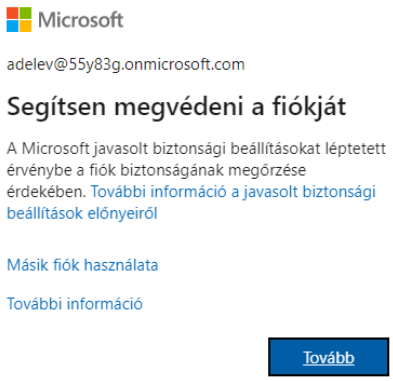
Ma már minden valamire való szolgáltató (bankok, közösségi oldalak, levelező szolgáltatások) multifaktor authentikációt biztosít a felhasználók részére, hogy jobban védhessék fiókjaikat. A Microsoft megoldásával már a kisebb vállalkozások is profi MFA-t építhetnek be saját IT-jukba. A multifaktor elemei itt is a leggyakoribb jelszó és egy eszköz (mobil, usb kulcs) vagy biometrikus jellemző (ujjlenyomat, arc) kombinációból adódnak [49].

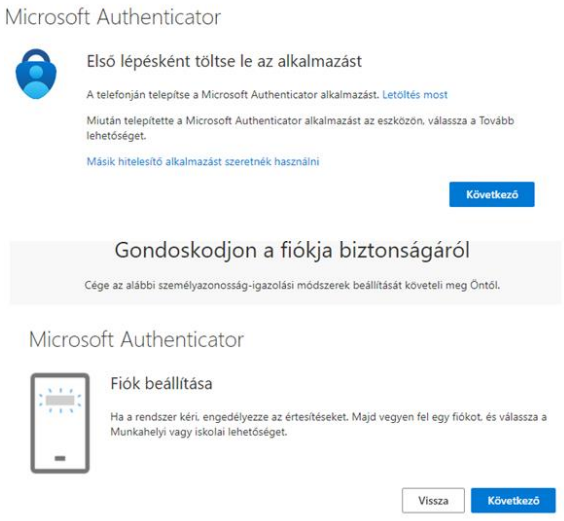
Az MFA beállítása az adminisztrátorok számára is kényelmes, hiszen a felhasználók önkiszolgáló módon állíthatják be maguknak, ugyanúgy, ahogy a password-resetet is. Az eljárás mindössze néhány lépés az alábbiak szerint:

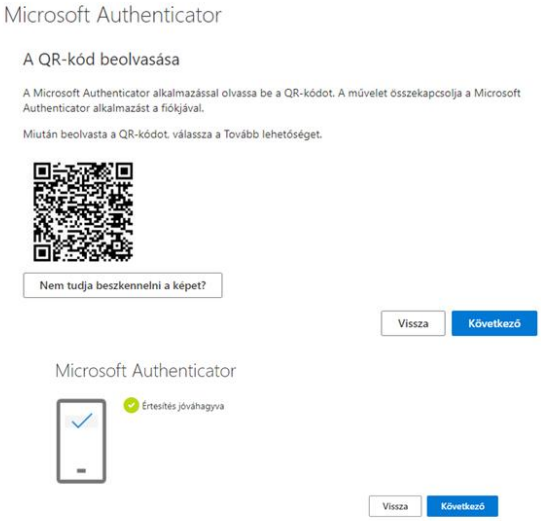
1. A felhasználó belép a portal.office.com oldalon, megadja felhasználói email címét, majd jelszavát.
2. Az oldal tájékoztat, hogy biztonsági beállítások szükségesek
3. A Microsoft Authenticator app letöltéség kéri iOS vagy Android telefonra, ami ingyenesen letölthető arra a telefonra, ami ezentúl a felhasználó másodlagos azonosítójaként fog szolgálni.

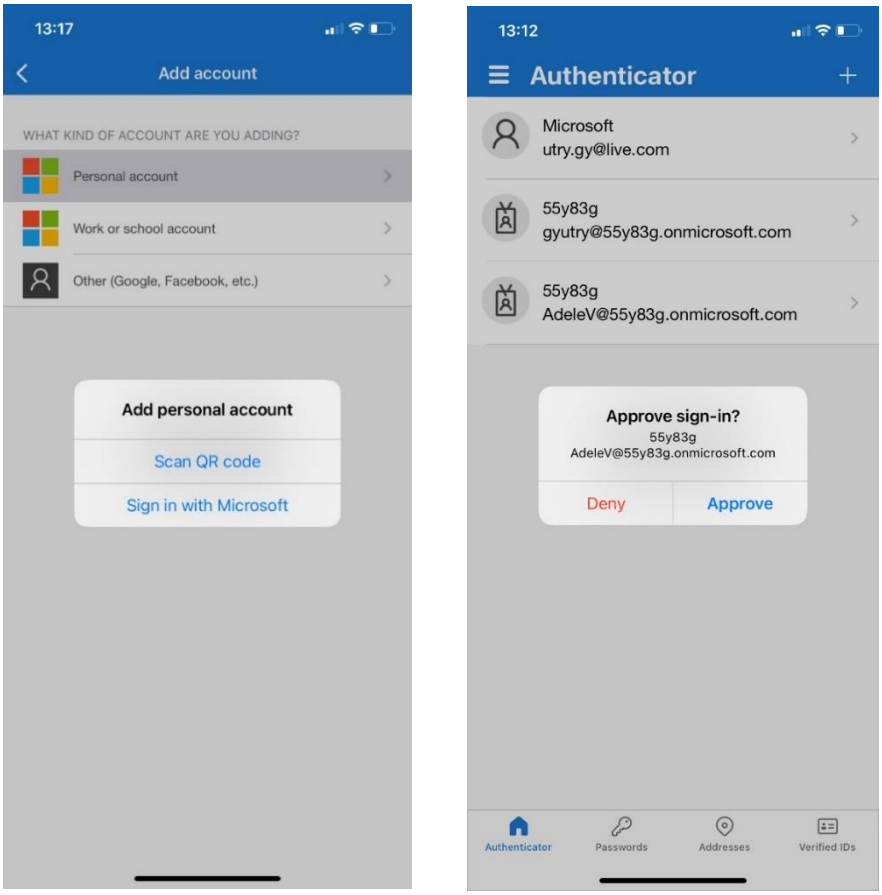
4. Tájékoztatja a felhasználót a telefonon elvégzendő néhány lépésről.
5. QR kód segítségével a telefon és PC összekapcsolódik.
6. Eközben a mobilos oldalon megjelenik a QR-kód beolvasás és a bejelentkezés jóváhagyás.











4.3. ábra Multifaktoros azonosítás beállítása

MFA-ra legkényelmesebbnek számomra az Applikációs megoldás, de elérhető az SMS vagy telefonos azonosítás is. Másik, telefont nem igénylő mód a Windows Hello for Business, ahol PIN kód vagy ujjlenyomat/arcfelismerés alkalmazható. Mind a két megoldás egyúttal a passwordless megközelítést is támogatja. Mivel a többlépcsős azonosítás hosszadalmasabb is, és a jelszavak egyébként sem jelentenek erős védelmet, így lényegében kihagyva az első lépést, jelszó nélkül is használhatjuk az Appot vagy a Windows Hellot. Mivel a rendszer a háttérben minden sessionhoz egy egyedi, időkorlátos azonosítót generál, ami egyszer használható, így a biztonságosság sem sérül [50].

Az egyszeri bejelentkezés (SSO) a Microsoft applikációin belül egyszerűen értelmezhető, a felhasználó miután belépett a Windows alapú számítógépére, ugyanazon azonosítókkal tovább léphet az M365 alkalmazásokba. Az Azure AD ezen felül 3rd party integrációs szolgáltatást is nyújt. Ez egyszerre emeli meg a biztonsági és a kényelmi szintet. On-premise megoldásnál az első belépésnél meg kell adni a 3rd party szoftver felhasználónevét és jelszavát, ezt követően az AAD tárolja és összeköti a felhasználó fiókjával azt és ezentúl az biztosítja a belépési adatokat minden alkalommal a felhasználó helyett. Cloud applikációk esetén federációs protokollal érhető el ugyanez, itt a OpenID

Connect, OAuth, és SAML konnektorokkal kompatibilis applikációkkal megoldható [51].

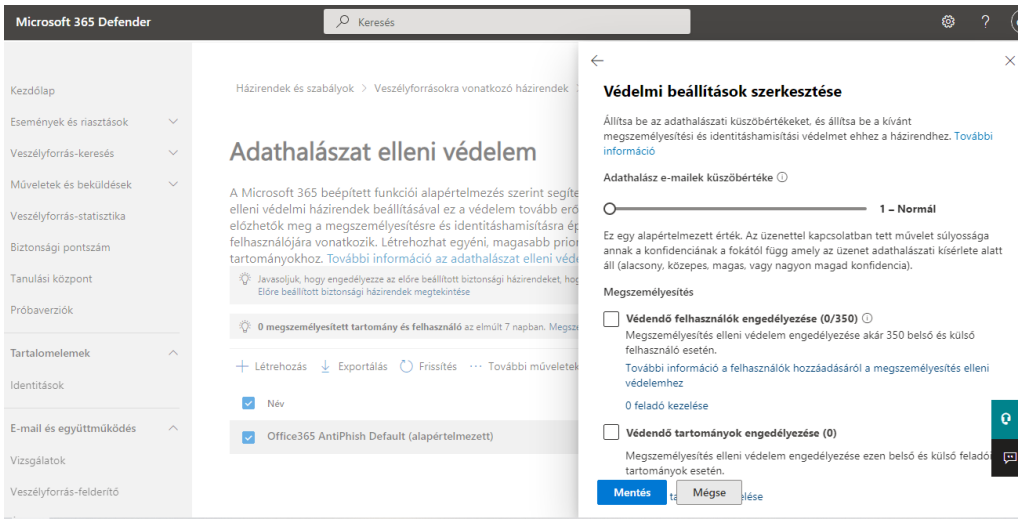
4.3. Levelezés biztonság

Másik fontos témakör az üzleti levelezések védelme. Az első fejezetre visszautalva az egyik legnagyobb veszélyforrást teszik ki a kártékony levelek, a kéretlenek pedig a hatékonyságot is rontják. Mind a kettőt időigényes a felhasználóknak maguk kiszűrni, így itt is jól jön az automatizált besegítés. Itt két megoldás kombinációja segít a teljeskörű veszélyelhárításban.

Első része az Exchange Online Protection (EOP) szolgáltatás, ami anti-spam, malware és egyéb kártékony levél elleni védekezésben vesz részt. Működésének lényege, hogy a beérkező levelek szisztematikusan, szűrőkön haladnak át, mielőtt a postafiókban landolnának. Az internet és a szervezet tenantja közé a Microsoft EOP adatközpont szervere ékelődik a maga „bölcsességével" (wordwide jelelemzés), mint szeparációs réteg, ami elvégzi ezeket a lépéseket. Az első a spamszűrő, ahol a feketelistás feladók pattannak vissza a levelezőszerverről. Ezt követi a levél- és csatolmányellenőrzés, ahol ismert malware esetén a levél karanténba kerül, és alapértelmezetten csak az adminisztrátor interaktálhat vele. Utána policy filtering következik, ahol egyéni utakat és értesítéseket adhatunk hozzá a cég igényei szerint. Végül a szövegtörzs vizsgálata is megtörténik káros tartalmak után kutatva (spam, spoofing, phishing). Ha minden vizsgálaton átment az email, csak akkor jelenik meg a felhasználónál [52].

Az adminisztrátori felületen tudjuk ezeket a szolgáltatásokat aktiválni és testreszabni, a beállítása egyszerűen zajlik, az alábbiakban az anti-phishing védelmet fogom beállítani [53].

1. Védelmi beállítások szerkesztése alapállapotban.
2. Szabályozható a magabiztossági szint, milyen határozottsággal utasítson vissza egy levelet, megszemélyesítés elleni védelem, kiemelt felhasználók hozzáadása, pl. vezetőség és kiemelt tartományok hozzáadása.
3. Megbízható személyek és tartományok hozzáadása, akik a szabályok alól kivételt élveznek. Célszerű a saját vállalaton belül érkező leveleket annak tekinteni.
4. Mesterséges intelligencia engedélyezése, mintázatok alapján gépi szűrések elvégzése megszemélyesítés és spoof elleni védelemre.
5. Találat esetén kiválasztható, milyen műveletet végezzen a gyanús elemmel. Javasolt beállítás a karanténba helyezés, ahol az arra illetékes személy felülvizsgálatot tarthat, de lehetséges opció még a levélszemét mappába irányítás. [53]



Védelmi beállítások szerkesztése

2 – Agresszív

Azok az üzenetek, amelyek adathalászati magas konfidenciaszinttel rendelkeznek, úgy vannak kezelve, mintha nagyon magas konfidenciaszinttel lennének azonosítva.

Megszemélyesítés

Védendő felhasználók engedélyezése (4/350)
Megszemélyesítés elleni védelem engedélyezése akár 350 belső és külső felhasználó esetén.
További információ a felhasználók hozzáadásáról a megszemélyesítés elleni védelemhez

4 feladó kezelése

Védendő tartományok engedélyezése (1)

Megszemélyesítés elleni védelem engedélyezése ezen belső és külső feladói tartományok esetén.

A tulajdonomban lévő tartományok belefoglalása
Saját tartományok megtekintése

Egyéni tartományok belefoglalása

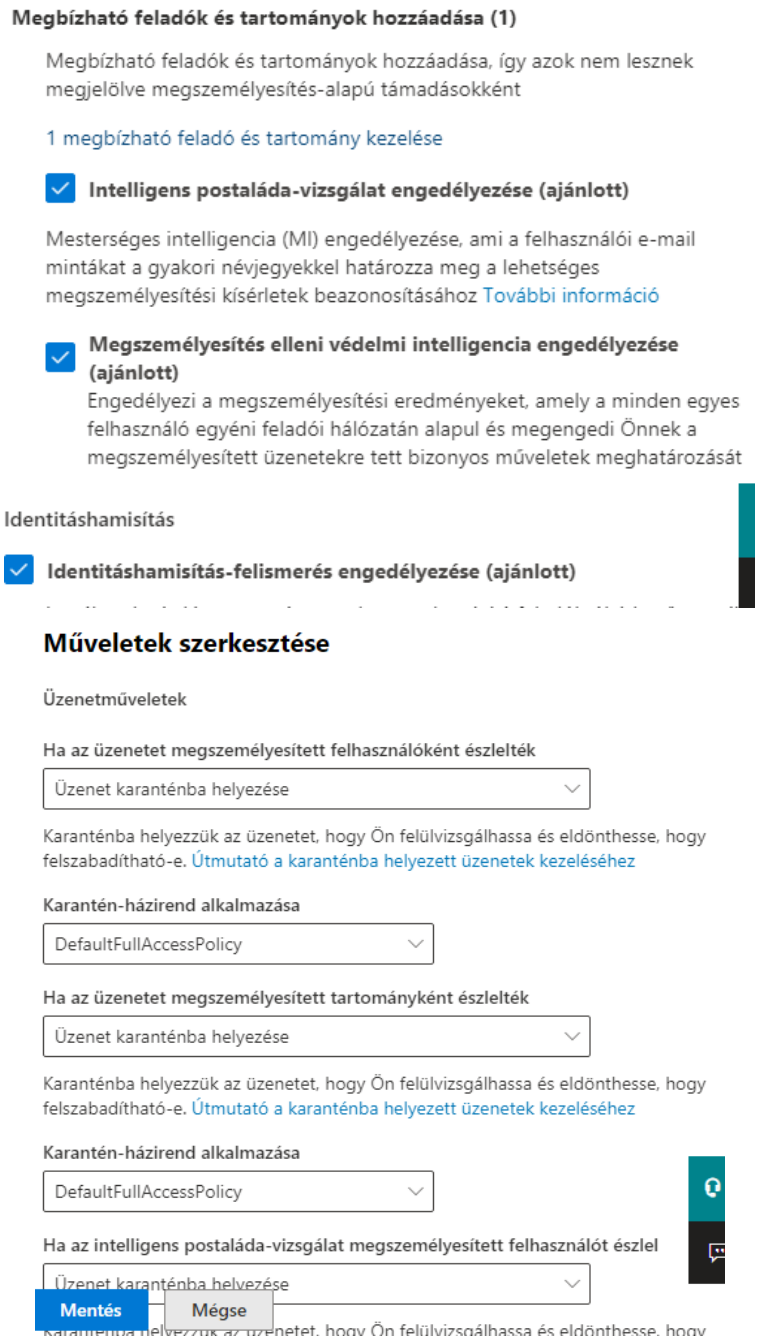
Műveletek szerkesztése

Üzenetműveletek

Ha az üzenetet megszemélyesített felhasználóként észlelték

Ne végezzen semmilyen műveletet

Üzenet átirányítása más e-mail-címekre
Üzenet áthelyezése a címzettek Levélszemét mappájába
Üzenet karanténba helyezése
Az üzenet kézbesítése és további e-mail-címek felvétele a Titko...
Az üzenet törlése a kézbesítése előtt
Ne végezzen semmilyen műveletet



4.4. ábra Adathalászat elleni védelem beállítása a demo környezetben

Másik megoldás az Exchange Online Protection mellett a Microsoft Defender for M365. Míg előbbi a már jól ismert, fekete listás támadásokat és spamokat szűri, a Defenderrel további védelmet szerezhet a vállalat a még nem ismert vagy komplexszebb támadásokkal szemben. Fő területe az új, zero-day támadások, adathalászat és üzleti

email kompromittációk. A szolgáltatás hasonlóan az EOP-hoz, szintén egy külön szeparációs réteget jelent az ügyféltenant és a nyílt internet között, ahol egy sandbox környezetben vizsgálaton esnek át az üzenetek, machine learning algoritmusokon esnek át, így még a korábban nem ismert gyanús elemek is fennakadnak. Segítségével az emailben érkező linkek, csatolmányok biztonsági ellenőrzése megtörténik, a linkeket szövegtörzsből és Office dokumentumból egyaránt kinyeri. A támadásokat a Defender segítségével az adminisztrátorok valós időben monitorozhatják és felülvizsgálhatják. Alapértelmezetten mindig az elmúlt egy hét támadásairól lehet betekintést nyerni [54].

4.4. Infrastruktúra biztonság

Végezetül a kliensek védelme, az infrastruktúra teljeskörű felügyelete szükséges ahhoz, hogy a vállalati biztonság általánosan is kielégítő legyen. A Defendernek a levelezés-védelem csak egy része, a megoldás ezen felül lefedi a végpontok, felhasználók és az alkalmazások közötti veszély detektálást, megelőzést, kivizsgálást és válaszadást. Azonosítható vele, hogyan jutott be a támadás a szervezetbe, mely rendszerek érintettek, mi a kiterjedtség jelen állapota, és mely rendszerek nem működnek megfelelően miatta. A védelmi válaszlépések pedig automatikusan elindulnak [55].

A Microsoft 365 Defender szolgáltatásai az alábbiak:

- Végpont védelem preventív és utókezelés jelleggel egyaránt.
- Email és kollaborációs eszközök (Teams, SharePoint) védelme.
- Azure AD identitások kezelése.
- App security, SaaS alkalmazások felügyelete [55].

Emellett a kényelmes eszközkezeléshez korszerű eszközkezelő megoldások is szükségesek a teljeskörű végpont védelem érdekében. A Microsoft 365 Intune Mobile Device Management moduljával a mobilis eszközök, mint laptop, telefon is felügyelet alá helyezhetők. A modul kikényszeríti a céges házirendet ezen eszközökön is, kötelezi a felhasználót, hogy léptesse be az eszközt, mielőtt azt vállalati célokra használná. Itt az IT el is döntheti, hogy engedi-e a dolgozó saját eszközeit így beléptetni, vagy csak a cég tulajdonában állókra végezhető el a beállítás. Miután a biztonsági házirendek érvényre léptetésre kerültek (ilyenek lehetnek a kötelező telefont lezáró kódok, authentikáció megkövetelése), a vállalati adatok távolról is eltávolíthatók lesznek ezekről az eszközökről az eszköz elvesztése/ellopása ügyén [56].

5. BIZTONSÁGI HÁZIREND VÁLLALATI DOKUMENTUMOKRA ÉS KOMMUNIKÁCIÓRA

A 4. fejezetben célom annak az eszköztárnak a bemutatása volt, amellyel korszerűen kezelhető a vállalati dokumentumvagyon, amivel csökkenthetővé válik a manuális adathigénia fenntartása. Áttekinthettük a céges dokumentumok kategorizálását és életútját az M365 környezeten belül és hogy ezt milyen felügyeleti réteg veheti körbe a Microsoft Defender megoldásaival. Ennek nyomán, az M365 részeként központi fájl tárolásra a SharePoint Online-t, illetve munkahelyi személyes dokumentumokra a OneDrive-ot javaslom, levelezés lebonyolítására az Exchange Online-t. A csoportmunka, kollaborációra pedig a Teams-et. A megoldások összekapcsolódnak és azonos biztonsági szintet képviselnek.

Az eszközkészlet ebből adódik, azonban minden vállalatnak különböző az adatvagyona, mindenkinek a sajátja fontos. Meg kell alkotni, mi mentén sorolják be a tartalmakat, mi alapján kategorizálják őket és azt követően mik történjenek velük. E fejezetben erre alkottam meg egy dokumentumkezelési és biztonsági házirendet.

Az előző fejezetben is belülről, az adatból kiindulva haladtam az azt körül vevő infrastruktúráig, itt is így haladok a hagymahéjakon.

5.1. Besorolás szenzitivitás szerint

A dokumentum besorolására az alábbi pontok szerint, ezt követően egy folyamatábrát is eszközölök a könnyebb besorolás érdekében.

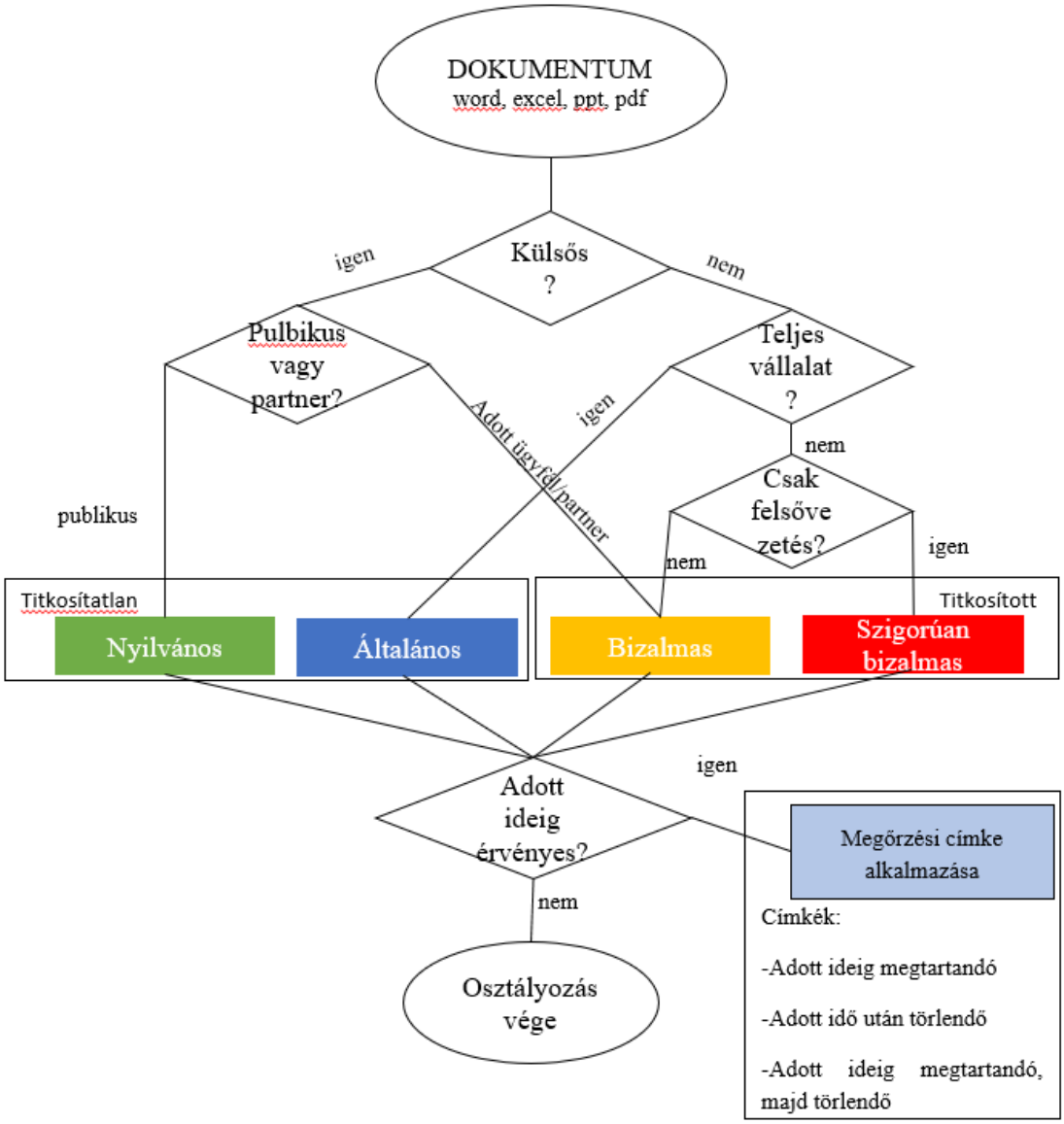
1. Dokumentum típusa:
- Általános (üzleti titkokat nem tartalmazó, tájékoztató jellegű anyag)
- Ügyleti (szerződés, számla, szállító levél, árajánlat ügyféllel, partnerrel)
- Üzleti (árlisták, beszállítói szerződések, műszaki dokumentációk)
- Marketing (brosúra, termék leírások, prezentációs anyagok)
2. Információ jellege, bizalmassági szintje:
- Nyilvános (bárki számára hozzáférhető, közérdekű vagy reklámértékű információ a vállalatról pl. weboldal adatok)
- Általános (üzleti titkokat nem tartalmazó belső felhasználású anyag pl. útmutatók, leírások, házirend)
- Személyes (adott dolgozó munkafájljai)
- Bizalmas (csak házon belüli, szenzitív adatok, szervezeti információk)
- Szigorúan bizalmas (Vezetői szinten közzétett, kiemelten szenzitív információk, munkaügyi adatok)
3. Dokumentum hatóköre:
- Publikus (bárki számára nyilvános lehet)
- Ügyfél (csak adott ügyfél, vagy ügyfélkör, kapcsolattartók)

- Partner (csak adott partner, vagy beszállítói kör, kapcsolattartók)
- Belső (teljes, cég, top mng, csoportvezetők, mely részleg,)

4. Érvényességi idő:

- Korlátlan
- Adott ideig megtartandó
- Adott idő után törlendő
- Megtartandó, majd törlendő

5.1.1. Folyamatábra



5.1. ábra Adatosztályozási folyamatábra

Személyes címke: Alapértelmezetten személyesnek tekinthető minden olyan állomány, ami a munkavállalói OneDrive-on került tárolásra. Adatszivárgás-megelőzés érdekében azonban célszerű a „Személyes” címke alkalmazása, nehogy véletlenül olyan fájlt csatoljunk egy emailhez, ami még közzétételre nem áll készen.

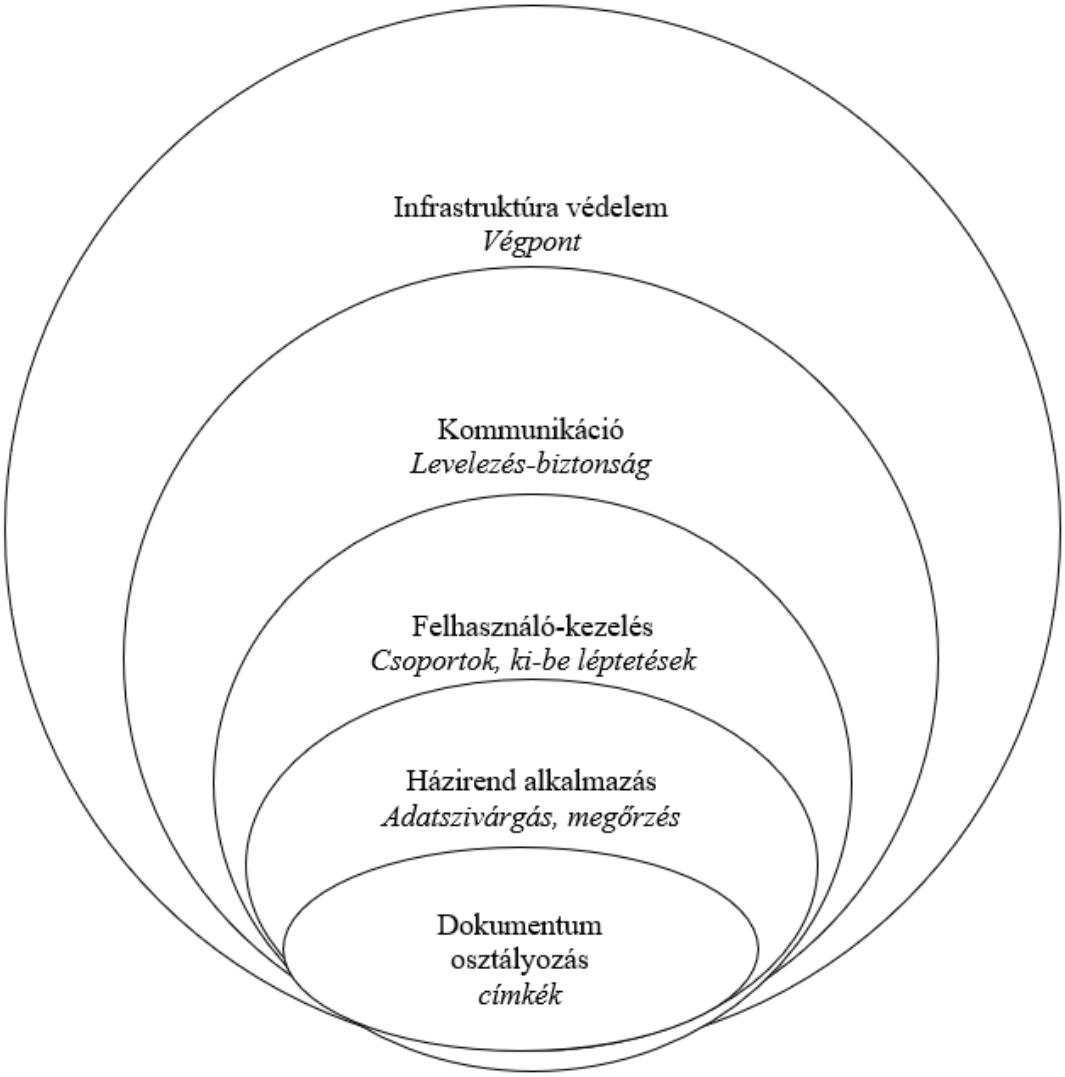
Az öt címkét alkalmazva adatszivárgási házirendeket hozhatunk létre, illetve már önmagukban is tartalmaznak olyan beállításokat a titkosítással ellátott címkék, amelyekkel szándékosan vagy óvatlanul sem lehet illetéktelenekkel megosztani, vagy emailhez hozzácsatolni. Címkét magára az email üzenetre is tehetünk, így a szövegtörzs tartalma is biztosított. Emailnél további plusz funkcióként jelenik meg a „nem továbbítható” opció is. A címkézésnek kiemelt jelentősége van akkor is, ha egy támadó valahogy behatol a vállalati rendszerbe. Ekkor az adatvagyon mégsem cukorkabolt szerűen tárul elé, hiszen a bizalmas, titkosított dokumentumokhoz további hozzáférésre lenne szüksége.

5.2. A védelem kialakítása lépésenként

1. **Dokumentum osztályozás:** Első lépésként határozzuk meg a vállalati adatvagyont, miként szeretnénk őket osztályozni, besorolni.
2. **Házirend alkalmazás:** Automatizáció segítségével tegyünk az illetlen adatszivárgás ellen, akadályozzuk meg a külsős megosztásokat a szigorúan szenzitív, belsős anyagok számára. Továbbá a bizalmas beszállítói és ügyféldokumentumoknál is biztosítsuk, hogy máshoz ne kerülhessenek a harmadik fél által sem. Határozzuk meg a védelem és tárolás idejét is, ez kényelmet is jelent, ha az egyre növekvő adathalomból automatikusan kiszórásra/archiválásra kerül az, ami már aktualitását vesztette.
3. **Felhasználó-kezelés**: Ha már tudjuk az osztályozások és házirendek felépítését, ráilleszthetjük a felhasználói csoportokat is a tömeges kezelés végett. Nagyon fontos, hogy a címtár mindig az aktuális dolgozókat és csapatokat mutassa. A távozó kollégáknál ne maradhassanak kint bizalmas fájlok. Ha a jogosultság megszűnik, a hozzáférés is eltávolítható még az offline példányokról is.
4. **Kommunikáció**: Dokumentum megosztás szerves eszköze a levelezés. A címkézés segítségével leveleinket és csatolmányainkat is védhetjük, egyszerűen kizárható az adatszivárgás, hiszen könnyen bele keveredhet egy külsős email cím a benti levelezésbe. Ekkor a hibás címzett hiába próbálja megnyitni a levelet. A vírusvédelemnek köszönhetően pedig a beérkező, kártékony levelek ellen emelhetünk pajzsot, nem teret engedve az adathalász-kísérleteknek sem.
5. **Infrastruktúra-védelem**: Természetesen a kliensek védelme sem maradhat el, az eszközpark, ami kiszolgálja a felhasználókat (laptop, Pc, mobiltelefonok). A kártékony kódok, és a jogosulatlan behatolások ellen egyaránt védekezhetünk és az eszközkezelés sem maradhat el. MDM megoldások segítségével a távozó kollégák, vagy elhagyott eszközök esetén a céges tartalom távolról is

visszavonható. A szerverek védelme tisztán felhős környezet esetén tárgytalan, de a Microsoft portfóliója alapvetően on-premise környezetből indult, így természetesen arról is tudunk gondoskodni.

5.2.1. Halmazábra



5.2. ábra Védelmi vonalak felépülése

Költségvonzat

A teljes M365 csomag havi 18,6 Eurós ára egy 100 fős KKV-ra levetítve mai árfolyamokkal borsos kiadásokat (744 ezer forint) eredményezhet, ám még ez is elenyészik, ha csak üzemeltetési feladatok miatt veszünk fel hiányszakmából származó IT szakembert. Ugyanakkor át kell gondolni a felhasználói profilokat, ki az, aki készíti és ki az, aki csak fogyasztja a dokumentumokat. Utóbbinak nem feltétlenül kell asztali

Office, és egy csak online szolgáltatásokat tartalmazó csomag havi 5,1 Euro. Továbbá nem válnak feleslegessé a már korábban megvásárolt licenszek sem. Az on-premise Office 2016-tól felfelé kompatibilis a Microsoft 365 szolgáltatásokkal. [57]

A költségekért cserébe magas rendelkezésre állást kapunk, mindegyike 99% feletti, továbbá megspóroljuk a nagy teljesítményű szerverek árát is, és a biztonságos távoli kapcsolat kiépítését is. Emellett nincs gondunk a folyamatos rendszerfrissítésekre sem, ami azért is fontos, mert az elmulasztott frissítések az egyik leggyakoribb rizikófaktor támadás esetén. Az értékes IT osztály humán erőforrása így nem aprózódik el, nem is válik feleslegessé, hiszen a konfigurálásokat, testreszabási beállításokat el kell végezzék. Egy kisebb cég jellemzően nem tud mindent saját erőből üzemeltetni és számos tevékenységet outsourcingolnak. A Microsoft, mint cloud üzemeltető, ezekből a költségekből is tud lefaragni. Amire implementáláskor számítani kell, az a felhasználói oktatás, hogyan alkalmazzák a házirendeket, ami összevonható belépő oktatásokkal, biztonsági tudatosságot növelő előadásokkal.

6. ÖSSZEGZÉS, A KÖVETKEZTETÉSEK LEVONÁSA

Az első fejezetben felkutattam napjaink biztonsági fenyegetettségeit, rámutatva, hogy szinte mind felhasználói interakciót követel az aktiváláshoz. Nagy népszerűségnek örvendenek az adathalász kísérletek, amik az azonosítókat megszerezve célzott anyagi károkat tudnak okozni. Ezt követően bemutattam, mik a komplexitást fokozó okok, úgy, mint a felhőtechnológia széleskörű használata, és a távmunka felértékelődése az elmúlt években. A 2. fejezetben összehasonlítottam a piaci megoldásokat vírusvédelemre végpont és levelezésre az általam választott Microsoft megoldással, illetve azt is felmértem, milyen támadások érik ezt a vendort.

Ezt követően vizsgáltam az általam választott vállalati szegmenst, milyen jellemzőkkel és kihívásokkal bír. A KKV-knak költséghatékony, de magasszintű védelemre van szüksége. A 4. fejezetben összeválogattam és bemutattam azokat a Microsoft megoldásokat, amiket a probléma megoldására alkalmasnak találok. Végül összeállítottam egy vállalati adat- és dokumentummenedzsment útmutatót, amik segítik szisztematikusan beépíteni a javasolt IT megoldásokat és megalkotni az áttekinthető és biztonságos információkezelést a felhasználhatósági és kényelmi szempontokat is figyelembe véve.

Dolgozatomban célom volt a biztonság olyan oldalról való kialakítása, ami nem az infrastruktúra irányából közelít, hanem az üzleti érdekeket helyezi középpontba. Sokan a meglévő környezetből építkeznek, ami kompromisszumos megoldásokat eredményezhet. Középpontba helyeztem a vállalati adatvagyont, mert annak integritása és sérthetetlensége nem lehet alárendelve más szempontoknak. Az általam készített útmutató segítségére lehet a KKV vállalatoknak megtalálni az optimális megoldást a biztonság és a felhasználhatóság között. A maximális kényelem csak egy vírusmentes világban lenne kivitelezhető, így a vállalatoknak adaptálnia kell a többszörös authentikáció és a fájlszintű védelem eszközeit.

A Microsoft dokumentumosztályozási megoldásai igen unikálisak, a portfólió viszonylag új elemei, amik megoldást szolgálnak a folyamatos kézi kontroll helyett. Ez felhasználói szempontból kiemelten fontos. Megszűnteti a rendszertelenséget, megszűnteti a felesleges biztonsági kockázatokat. Az eszköztár többi elemei is mind-mind korszerű megoldást nyújtanak, beleértve a bárhonnani munkavégzést. A védelem pedig két irányú. A vírusvédelmi vonalak megakadályozzák a külső irányból érkező támadásokat, szűrik a kéretlen leveleket, hogy azok ne is rontsák a munkavégzést. Az adatkategorizálással és házirendekkel pedig megakadályozható a kifelé való szivárgás. Emellett az adatvagyon rendezetté és áttekinthetővé válik, növelve a felhasználói élményt.

A Microsoft szoftverei elég széleskörben elterjedtek, gondoljunk csak a Windowsra, így a felhős megoldásokra való nyitásban folytathatjuk egy már jól ismert beszállítóval. A hibrid infrastruktúra és mixelt előfizetői csomagok is adottak.

Dolgozatom nem tér ki, hogy a Microsoft ERP és CRM rendszereket is szállít Dyamics néven, on-premise és cloud verzióban egyaránt, tehát az integritási lehetőségek az itt taglalt eseteknél nem állnak meg.

Végezetül a biztonság. Az jól látszik, hogy nem a Microsoft az egyetlen aktív résztvevő, de megállja a helyét a piacon, emiatt sem szükséges egy vállalatnak külön end-point megoldásokkal növelnie a kiadásait. Továbbá a Microsoft Defender messze nem az egyetlen biztonsági vonala a gyártónak. Az Azure szolgáltatásokon belül is találhatunk szép számmal, ha a vállalat igényli. Kiemelném például az Azure Sentinelt, ami a SIEM megoldást fedi, ha fejlett analitikával kívánjuk megfigyelni rendszerünk eseményeit.

7. SUMMARY

In the first chapter, I explored today's security threats, pointing out that almost all of them require user interaction to activate. Phishing attempts, which can cause targeted financial damage by obtaining identifiers, are very popular. After that, I presented the reasons that increase complexity, such as the widespread use of cloud technology and the rise in value of remote work in recent years. In Chapter 2, I compared the market solutions for endpoint virus protection and correspondence with the Microsoft solution I chose, and I also assessed what kind of attacks this vendor faces.

After that, I examined the company segment I chose, what characteristics and challenges it has. SMEs need cost-effective but high-level protection. In Chapter 4, I selected and presented the Microsoft solutions that I find suitable for solving the problem. Finally, I compiled a corporate data and document management guide that helps you systematically incorporate the proposed IT solutions and create clear and secure information management, taking usability and comfort aspects into account.

My goal in my dissertation was to develop security from a perspective that does not approach from the direction of infrastructure, but focuses on business interests. Many build from the existing environment, which can result in compromise solutions. I focused on corporate data assets, because their integrity and inviolability cannot be subordinated to other aspects. With the help of the guide I created, SMEs can find the optimal solution between security and usability. Maximum convenience would only be feasible in a virus-free world, so companies must adapt tools for multiple authentication and file-level protection.

Microsoft's document classification solutions are very unique, relatively new elements of the portfolio that serve as a solution instead of continuous manual control. This is extremely important from the user's point of view. Eliminates irregularity, eliminates unnecessary security risks. The other elements of the toolbox also all provide a modern solution, including working from anywhere. The protection is two-way. Virus protection lines prevent attacks from the outside and filter unsolicited e-mails so that they do not impair work performance. Leakage to the outside can be prevented with data categorization and policies. In addition, the data wealth becomes organized and transparent, increasing the user experience.

Microsoft's software is quite widespread, just think of Windows, so we can continue opening up to cloud solutions with an already well-known supplier. Hybrid infrastructure and mixed subscriber packages are also available.

My thesis does not cover the fact that Microsoft also supplies ERP and CRM systems under the name Dyamics, both on-premise and cloud versions, so the integrity options do not stop at the cases discussed here.

Finally, safety. It is clear that Microsoft is not the only active participant, but it has a strong position in the market, so there is no need for a company to increase its expenses with separate end-point solutions. Furthermore, Microsoft Defender is far from the manufacturer's only security line. We can also find quite a few within Azure services, if the company requires it. For example, I would highlight Azure Sentinel, which covers the SIEM solution, if we want to monitor the events of our system with advanced analytics.

8. HIVATKOZÁSOK

[1] Á. Turzó, „A ma ismert világot totálisan elsöpri a negyedik ipari forradalom,” 20 09 2016. [Online]. Available: https://www.portfolio.hu/uzlet/20160920/a-ma-ismert-vilagot-totalisan-elsopri-a-negyedik-ipari-forradalom-237125. [Hozzáférés dátuma: 07 03 2021].

[2] B.Klára, „Network.hu,” 2013. [Online]. Available: http://informatikatortenet.network.hu/blog/informatika_tortenet_klub_hirei/az-internet-tortenete. [Hozzáférés dátuma: 16 03 2021].

[3] Infrapedia, „The World largest network,” 2021. [Online]. Available: https://www.infrapedia.com/app. [Hozzáférés dátuma: 3 10 2021].

[4] H. KPMG, „A digitális transzformáció nem technológiai kérdés,” KPMG, 2018. [Online]. Available: https://blog.kpmg.hu/2018/10/a-digitalis-transzformacio-nem-technologiai-kerdes/. [Hozzáférés dátuma: 17 03 2021].

[5] D. Microsoft, „What is cloud computing?,” 2020. [Online]. Available: https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/what-is-cloud-computing. [Hozzáférés dátuma: 17 03 2021].

[6] Gartner, „Magic Quadrant for Cloud Infrastructure and Platform Services,” 2020. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-1ZDZDMTF&ct=200703&st=sb. [Hozzáférés dátuma: 17 03 2021].

[7] N. Magyar, „A vártnál sokkal kisebb a tavalyi gazdasági visszaesés,” 16 2 2021. [Online]. Available: https://magyarnemzet.hu/gazdasag/a-vartnal-sokkal-kisebb-a-tavalyi-gazdasagi-visszaeses-9382754/. [Hozzáférés dátuma: 7 3 2021].

[8] F. Rodrigo, "COVID-19 pandemic accelerates the monopoly position of Big Tech companies," 17 12 2020. [Online]. Available: https://www.somo.nl/covid-19-pandemic-accelerates-the-monopoly-position-of-big-tech-companies/. [Accessed 7 3 2021].

[9] R. Lefferts, "Microsoft shares new threat intelligence, security guidance during global crisis - Microsoft Security," 8 4 2020. [Online]. Available:

https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/. [Accessed 7 3 2021].

[10] Kaspersky, "Kaspersky Security Bulletin 2020. Statistics," 15 12 2020. [Online]. Available: https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/. [Accessed 11 5 2021].

[11] Kaspersky, „Financial Cyberthreats in 2020," 31 3 2021. [Online]. Available: https://securelist.com/financial-cyberthreats-in-2020/101638/. [Hozzáférés dátuma: 11 5 2021].

[12] A. Larkina, "Privacy predictions for 2021," 28 1 2021. [Online]. Available: https://securelist.com/privacy-predictions-for-2021/100311/. [Accessed 11 5 2021].

[13] T. Kulikova, „Spam and phishing in Q1 2021," 3 5 2021. [Online]. Available: https://securelist.com/spam-and-phishing-in-q1-2021/102018/. [Hozzáférés dátuma: 11 5 2021].

[14] Microsoft, „Microsoft Digital Defense Report," 2020. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-intelligence-report. [Hozzáférés dátuma: 20 03 2021].

[15] P. Muncaster, "COVID19 Drives Phishing Emails Up 667% in Under a Month," 26 3 2020. [Online]. Available: https://www.infosecurity-magazine.com/news/covid19-drive-phishing-emails-667/. [Accessed 7 3 2021].

[16] A. Lawrence, "FBI Says $140+ Million Paid to Ransomware," 27 2 2020. [Online]. Available: https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/. [Accessed 8 3 2021].

[17] Sharat, "DDoS attacks in Q4 2020," 16 2 2021. [Online]. Available: https://securelist.com/ddos-attacks-in-q4-2020/100650/. [Accessed 8 3 2021].

[18] M. Wilczek, „Marc Wilczek," 3 11 2020. [Online]. Available: https://www.darkreading.com/vulnerabilities---threats/cybercrime-nation-states-go-prime-time/a/d-id/1339188. [Hozzáférés dátuma: 8 3 2021].

[19] L. Bellon, „Cisco Umbrella’s Top 10 Cybersecurity Tips,” 1 7 2020. [Online]. Available: https://umbrella.cisco.com/blog/cisco-umbrella-top-10-cybersecurity-tips?utm_medium=web-referral&utm_source=cisco&utm_campaign=cs-fy2020-q2-cisco-100-day-sprint&utm_term=pgm. [Hozzáférés dátuma: 13 4 2021].

[20] Cisco, „Endpoint Security,” 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html. [Hozzáférés dátuma: 13 4 2021].

[21] Cisco, „What Is an Endpoint Protection Platform,” 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-endpoint-protection-platform.html. [Hozzáférés dátuma: 13 4 2021].

[22] Cisco, „What Is Email Security,” 2021. [Online]. Available: https://www.cisco.com/c/en/us/products/security/what-is-email-security.html#~best-practices. [Hozzáférés dátuma: 13 4 2021].

[23] Microsoft, „Secure access for a connected world,” 2021. [Online]. Available: https://www.microsoft.com/en-us/security/business/identity-access-management. [Hozzáférés dátuma: 13 4 2021].

[24] Gartner, „Endpoint Protection Platforms (EPP) Reviews and Ratings,” 2021. [Online]. Available: https://www.gartner.com/reviews/market/endpoint-protection-platforms. [Hozzáférés dátuma: 14 4 2021].

[25] S. Microsoft, „Gartner names Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant,” 23 8 2019. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2019/08/23/gartner-names-microsoft-a-leader-in-2019-endpoint-protection-platforms-magic-quadrant/. [Hozzáférés dátuma: 23 9 2021].

[26] Microsoft, „Microsoft Security is a Leader in five Magic Quadrants,” 2021. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-leaders-gartner-magic-quadrant#coreui-contentrichblock-z6vg0fz. [Hozzáférés dátuma: 14 4 2021].

[27] Microsoft, „Microsoft 365 Vállalati verzió | Kisvállalat | Microsoft 365,” 2022. [Online]. Available: https://www.microsoft.com/hu-hu/microsoft-365/business#coreui-heading-hiatrep. [Hozzáférés dátuma: 14 10 2022].

[28] Google, „Compare Flexible Pricing | Google Workspace (formerly G Suite),” 2022. [Online]. Available: https://workspace.google.com/pricing.html. [Hozzáférés dátuma: 14 10 2022].

[29] Gov.uk, „Cyber Security Breaches Survey 2022,” 11 07 2022. [Online]. Available: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022. [Hozzáférés dátuma: 24 10 2022].

[30] Cyware, „Remote Code Execution Vulnerability: What is it and how to stay protected from it? | Cyware Alerts - Hacker News,” 10 02 2019. [Online]. Available: https://cyware.com/news/remote-code-execution-vulnerability-what-is-it-and-how-to-stay-protected-from-it-12a1b250. [Hozzáférés dátuma: 18 10 2022].

[31] D. CVE, „Microsoft » 365 Apps : Vulnerability Statistics,” 2022. [Online]. Available: https://www.cvedetails.com/product/80308/Microsoft-365-Apps.html?vendor_id=26. [Hozzáférés dátuma: 1 9 2022].

[32] Gartner, „Email Security Reviews and Ratings,” 2022. [Online]. Available: https://www.gartner.com/reviews/market/email-security. [Hozzáférés dátuma: 5 10 2022].

[33] L. SE, „Reports published in 2022,” 30 6 2022. [Online]. Available: https://selabs.uk/wp-content/uploads/2022/06/email-security-services-ess-enterprise-small-business-2022-06.pdf. [Hozzáférés dátuma: 24 10 2022].

[34] S. KSH, „9.1.1.17. A vállalkozások teljesítménymutatói kis- és középvállalkozási kategória szerint,” 2021. [Online]. Available: https://www.ksh.hu/stadat_files/gsz/hu/gsz0018.html. [Hozzáférés dátuma: 24 01 2021].

[35] H. E. –. K. Á. –. T. Jeneiné Gerő, A hazai kkv-k területi jellegzetességei, Statisztikai Szemle: KSH, 2021.

[36] KSH, „A kis- és középvállalkozások,” 01 01 2018. [Online]. Available: https://www.ksh.hu/docs/hun/xftp/idoszaki/pdf/kkv18.pdf. [Hozzáférés dátuma: 27 01 2022].

[37] KSH, „A regisztrált vállalkozások száma nemzetgazdasági ág szerint,” 2021. [Online]. Available: https://www.ksh.hu/stadat_files/gsz/hu/gsz0003.html. [Hozzáférés dátuma: 27 1 2022].

[38] L. Microsoft, „Manage information protection and governance,” 2022. [Online]. Available: https://docs.microsoft.com/en-us/learn/paths/m365-compliance-information/. [Hozzáférés dátuma: 30 8 2022].

[39] D. Microsoft, „Learn about sensitive information types,” 10 5 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about?view=o365-worldwide. [Hozzáférés dátuma: 12 6 2022].

[40] S. Microsoft, „Apply sensitivity labels to your files and email in Office,” 01 05 2022. [Online]. Available: https://support.microsoft.com/en-us/office/apply-sensitivity-labels-to-your-files-and-email-in-office-2f96e7cd-d5a4-403b-8bd7-4cc636bae0f9. [Hozzáférés dátuma: 20 05 2022].

[41] D. Microsoft, „Encryption Sensitivity labels,” 20 05 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide. [Hozzáférés dátuma: 31 05 2022].

[42] D. Microsoft, „Sensitivy labels,” 05 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide. [Hozzáférés dátuma: 31 05 2022].

[43] D. Microsoft, „Restrict access to content by using sensitivity labels to apply encryption,” 20 5 2022. [Online]. Available: https://docs.microsoft.com/hu-hu/microsoft-365/compliance/encryption-sensitivity-labels?view=o365-worldwide#considerations-for-encrypted-content. [Hozzáférés dátuma: 29 5 2022].

[44] D. Microsoft, „Learn about data loss prevention,” 22 5 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide. [Hozzáférés dátuma: 9 06 2022].

[45] D. Microsoft, „Learn about retention policies and retention labels,” 13 8 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide#retention-labels. [Hozzáférés dátuma: 15 8 2022].

[46] D. Microsoft, „Get started with data lifecycle management,” 08 07 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-data-lifecycle-management?view=o365-worldwide. [Hozzáférés dátuma: 20 07 2022].

[47] D. Microsoft, „What is Azure Active Directory?,” 15 7 2022. [Online]. Available: What is Azure Active Directory? - Microsoft Entra | Microsoft Docs. [Hozzáférés dátuma: 01 08 2022].

[48] D. Microsoft, „Conditional Access: Conditions,” 1 8 2022. [Online]. Available: Conditions in Conditional Access policy - Azure Active Directory - Microsoft Entra | Microsoft Docs. [Hozzáférés dátuma: 1 8 2022].

[49] D. Microsoft, „How it works: Azure AD Multi-Factor Authentication,” 25 08 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks. [Hozzáférés dátuma: 27 08 2022].

[50] D. Microsoft, „Passwordless authentication options for Azure Active Directory,” 25 8 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless. [Hozzáférés dátuma: 27 8 2022].

[51] D. Microsoft, „What is single sign-on in Azure Active Directory?,” 2 6 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on. [Hozzáférés dátuma: 27 8 2022].

[52] D. Microsoft, „Exchange Online Protection overview,” 19 8 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview?view=o365-worldwide. [Hozzáférés dátuma: 28 8 2022].

[53] D. Microsoft, „Protect against threats,” 13 7 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-

security/protect-against-threats?view=o365-worldwide. [Hozzáférés dátuma: 28 08 2022].

[54] D. Microsoft, „Microsoft Defender for Office 365 service description,” 30 9 2021. [Online]. Available: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description. [Hozzáférés dátuma: 29 8 2022].

[55] D. Microsoft, „What is Microsoft 365 Defender?,” 5 7 2022. [Online]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?view=o365-worldwide. [Hozzáférés dátuma: 29 8 2022].

[56] D. Microsoft, „Device management overview,” 1 9 2022. [Online]. Available: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management. [Hozzáférés dátuma: 15 9 2022].

[57] Microsoft, „A hatékonyság újragondolása a Microsoft 365-tel és a Microsoft Teamszel,” 2022. [Online]. Available: https://www.microsoft.com/hu-hu/microsoft-365/business/compare-all-microsoft-365-business-products?tab=2. [Hozzáférés dátuma: 31 10 2022].

[58] [Online]. Available: What is cloud computing? - Learn | Microsoft Docs. [Hozzáférés dátuma: 17 03 2021].

9. ÁBRAJEGYZÉK