ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Városi József**
2022	Hallgató törzskönyvi száma:	**T/008060/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Biomatika és Alkalmazott Mesterséges Intelligencia Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Városi József**
Törzskönyvi száma: T/008060/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

A digitális nyomtatástechnológia IT biztonsági kérdései
IT security issues in digital printing technology

Intézményi konzulens: Vörösné Dr. Bánáti-Baumann Anna
Külső konzulens:

Beadási határidő: 2022. december 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének bizton
IT hálózatbiztonság

SZAKDOLGOZAT
FELADATLAP

A feladat

A munkahelyi környezet folyamatos fejlődésben van. A nyomtatási technológiák és dokumentumkezelési folyamatok a számítástechnikai eszközök evolúcióját követve új formában jelennek meg mindennapjainkban. Új platformokon, applikációkon keresztül készítjük és tároljuk dokumentumainkat. A teljes dokumentum-kezelés folyamatában részt vevők - emberi és számítástechnikai szereplők - egyaránt IT kockázatot jelenthetnek a cégek működésben.
A szakdolgozat célja megvizsgálni a digitális nyomtatástechnológia és a hozzá kapcsolódó dokumentumkezelési folyamatok IT biztonsági kérdéseit, kutatni a gyenge pontokat, majd ezen információkra építve kialakítani egy adott vállalati környezetben megvalósítható legjobb megoldást.
A hallgató feladata megvizsgálni a számítástechnikai hálózaton, dokumentum-management rendszeren keresztüli digitális nyomtatástechnológia folyamatát és az ezekhez kapcsolódó Ügyfél és szervíztevékenységeket.

A dolgozatnak tartalmaznia kell:

- a nyomtatási technológiák ismertetését,
- a dokumentumkezelési folyamatok bemutatását,
- a fenti rendszerelemek sérülékenységeinek vizsgálatát,
- a jelenlegi védelmi mechanizmusok feltérképezését és elemzését,
- ezen új környezetben az emberi tényező kockázatának elemzését,
- a kiértékelést követő vállalatfejlesztési javaslatot.

ÓBUDAI EGYETEM Neumann János Informatikai Kar 1.

Pk.

Dr. Eigner György
intézetigazgató

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

A dolgozatot beadásra alkalmasnak tartom:

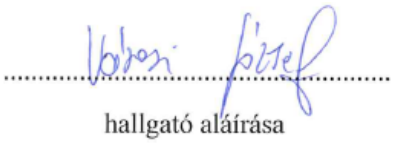
.....
külső konzulens

.....
intézményi konzulens

HALLGATÓI NYILATKOZAT

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

Budapest, 2022. május 04.



hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Városi József

Neptun Kód: [redacted]

Tagozat: Kiberbiztonsági szakmérnök

Telefon: [redacted]

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

Projektmunka címe magyarul:

A digitális nyomtatástechnológia IT biztonsági kérdései

Projektmunka címe angolul:

IT security issues in digital printing technology

Intézményi konzulens: Vörösné Dr. Bánáti-Baumann Anna

Külső konzulens:

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022.02.18.	IRODALOMKUTATÁS	
2.	2022.03.07.	EMBERI TÉNYEZŐ KOCKÁZATA	
3.	2022.04.06.	VÁLALLATFEJLESZTÉSI JAVASLAT	
4.	2022.05.06.	PREZENTÁCIÓ	

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: 5

.....

Intézményi konzulens

Budapest, 2022.05.06.

[1] A megfelelő beksrikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

TARTALOMJEGYZÉK

1 BEVEZETÉS

Egy nyomtató is komoly biztonsági kockázatot jelenthet [1]:

- nem kellően védett hálózati nyomtatók,
- titkosítás/adattörlés nélküli multifunkciós eszközök,
- merevlemezeken tárolt dokumentumok,
- belépési pontként használhatják a hálózatunkhoz való hozzáféréshez vagy más rendszereink megtámadásához is felhasználhatják őket.

A munkahelyi környezet folyamatos fejlődésben van.

A nyomtatási technológiák és dokumentumkezelési folyamatok a számítástechnikai eszközök evolúcióját követve új formában jelennek meg mindennapjainkban. Új platformokon, applikációkon keresztül készítjük és tároljuk dokumentumainkat. A teljes dokumentumkezelés folyamatában részt vevők - emberi és számítástechnikai szereplők - egyaránt IT kockázatot jelenthetnek a cégek működésében.

A digitális nyomtatástechnológia világában az elmúlt 20 évben jelentős változások történtek.

Kiszélesedett a lézernyomtató berendezések portfóliója a multifunkcionális eszközökkel (másolás/nyomtatás/szkennelés/faxolás), amelyek már nagy sebességben, nagy felbontásban is valósághű színes képeket jelenítettek meg, az Ügyfelek papír alapú dokumentumait ugyanezen magas színvonalon digitalizálták és a ”vas”-ra épülő szoftverekkel jelenné vált a korábban futurisztikus jövőkép, amelyben a virtuális térben, felhőalapon tároljuk dokumentumainkat.

Ugyanezen tendencia természetesen a nyomtatáshoz kapcsolódó számítástechnikai rendszerelemek esetén is bekövetkezett, így a vizsgált téma ezen rendszerek komplexitásának fejlődési ívét is figyelembe veszi.

Ma már talán megmosolyogjuk azokat a mondatokat, amelyek a ComputerWorld 2 évtizeddel ezelőtt megjelent tesztelési értékelőjében olvashatóak a Xerox Phaser 790DP nyomtatójáról: ”Ahhoz, hogy a nyomtatót hálózatban is használhassuk, még egy 10/100BaseT Ethernet kártyát is beszereltek a párhuzamos port mellé.” [2].

1.1. ábra: Xerox Phaser 790DP nyomtató [3].

Napjainkban dokumentumaink nyomtatását már vezetékes hálózat nélkül, okos eszközeinkről is megtehetjük, az erre alkalmas eszközök száma két tucat különböző gyártó mintegy 6.000 kompatibilis nyomtató modelljére nőtt. Ezek a printerek beépített módon támogatják az Apple által 2010-ben fejlesztett AirPrint™ technológiát - az okoseszközök az azonos helyi hálózaton található nyomtatókat automatikusan felfedezik.

Papíralapú dokumentumaink elektronikus formában történő tárolása megvalósítható távoli hálózaton lévő szerveren, OCR (optical character recognition – optikai szövegfelismerés) karakterfelismeréssel lehetőségünk van metaadat menedzsment segítségével dokumentum kezelő szoftverbe adatokat automatikusan betölteni, mindezt úgy, hogy a szöveg felismerése a felhőben történik, így nem igényel helyi erőforrást.

A folyamat mindkét irányában (papírból elektronikus adat, elektronikus adatból papír) részt vevő szereplők - emberi és számítástechnikai - egyaránt kockázati tényezőnek számítanak.

És bár azt gondolhatjuk, hogy az asztalunkon lévő irodai nyomtató vagy a cég folyosóin sokszor munkahelyi beszélgetések és pihentető kávézások lehetőségét is magában rejtő multifunkciós printer nem feltétlenül tűnik a legnagyobb biztonsági kockázatnak, tanulmányomban bemutatom, hogy ezen eszköz egész sor pszichológiai manipuláció, rosszindulatú szoftver és zsarolóvírus számára jelenthet olyan kaput, amelynek sokszor a létezéséről sem tudunk [4], [5], [6], [7], [8].

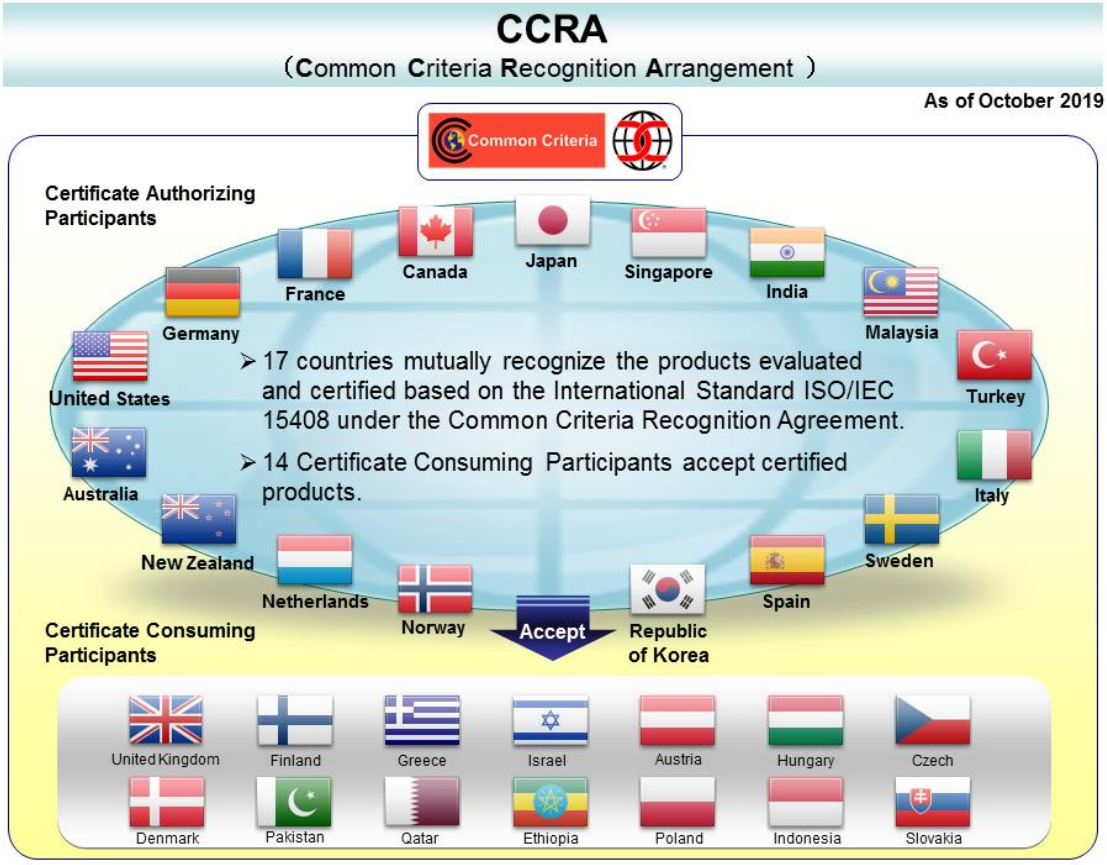
A vállalkozások a technológia fejlődésével új munkahelyi alkalmazásokat vezetnek be, melyekhez flexibilisen és jól skálázhatóan integrálni szeretnék nyomtatási és dokumentumkezelési rendszereiket is. Így válhat a kellő körültekintéssel felépített rendszerben a korábban csak perifériának tekintett nyomtató egyes folyamatokban kimeneti eszköz szerepe mellett új munkafolyamatokat elindító input eszközzé.

Az új üzleti folyamatok, a növekvő produktivitási igény olyan folyamatosan változó irodai környezetet kíván, amelyben napjaink nyomtatója nemcsak nyomtat, másol, faxol és szkennel, de akár fordít is, megoszthat és létre is hozhat elektronikus dokumentumokat, mindezt néhány képernyőkoppintással, felhőalapú csatlakozással is elérhetően.

A digitális nyomtatástechnológiával megjelenő sokszínű irodai felhasználási lehetőség a hozzá kapcsolódó rendszerek komplexitásának növekedésével az IT biztonsági kockázati tényezők számosságát is növelte. Ezen trendre fókuszálva fogom elemezni munkámban a digitális nyomtatástechnológia IT biztonsági elemeit, majd a kapott eredményre alapozva vállalatfejlesztési eljárást mutatok be.

2 TÖRTÉNELMI ÁTTEKINTÉS

A Sharp volt az első multifunkciós nyomtatókat gyártó cég, aki Common Criteria minősítést kapott 2001-ben. [9]



2.1. ábra: Common Criteria Recognition Arrangement (CCRA) [10].

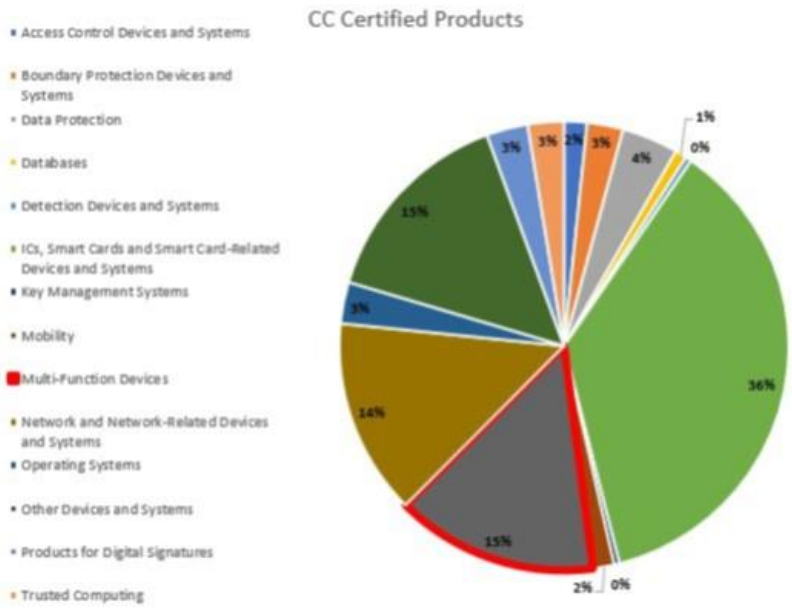
A keretrendszer közös struktúrát és nyelvet határoz meg a termékek/rendszerek IT biztonsági követelményeinek kifejezésére.

Szabványos IT biztonsági követelmény összetevők és csomagok gyűjteményét tartalmazza a fejlesztési folyamatokra, így egy nemzetközileg elfogadott értékelési módszertanná, besorolási rendszerré vált.

A Common Criteria az informatikai berendezések értékelésére használt szabályok gyűjteménye, ahol a vizsgálatok során a specifikációkat független laboratóriumok állítják be és tesztelik.

ISO/IEC 15408 szabványként hagyták jóvá 1999 júniusában, és bár az elmúlt 2 évtizedben több, mint 4.500 termék kapott igazolást, az aktív tanúsítvánnyal rendelkező eszközök száma ennek csak harmadára tehető. Ezen 14 termékcsaládból a multifunkciós eszközök 15 százalékot képviselnek önmagukban, ám ne felejtsük el, hogy a különböző gyártóktól származó összesen 229 eszköz szervesen kapcsolódhat az informatikai rendszerhez, hiszen

minden gyártó már a termék fejlesztésének szakaszában törekszik termékeinek integrálhatóságára.



2.2. ábra: CC tanúsítványok száma a termékcsoportok bontásában 2019-ben.

A 2006-ban az Adobe és a Ricoh által közösen fejlesztett dokumentumkezelő rendszer - amely szkennelési lehetőségekkel, biztonsági funkciókkal és fejlett nyomtatási lehetőségekkel bírt - egy teljesen új utat nyitott a papíralapú folyamatok biztonságos digitális munkafolyamattá alakításához.

Az új rendszer segítségével egy nyomtatott lap szkennelt verziója kereshetővé, könnyen archiválhatóvá, biztonságos és kisméretű Adobe PDF fájlként tárolhatóvá vált. A felhasználókhoz engedélyezési irányelvek rendelhetők, ezért a rendszer üzemeltetői által kialakított szabályok segítségével mindenki csak a saját, hitelességi bizonyítvánnyal ellátott, digitálisan aláírt, megfelelő titkosítású dokumentumához férhet hozzá. Ezen dokumentumkezelő rendszerrel a munkafolyamatok digitalizálásának biztonsági kérdései is felkerültek az IT kockázatértékelések listájára. Az eltelt 15 évben több gyártó is dokumentummenedzsment szoftvert fejlesztett, így a kockázatértékelések során már komplex rendszert kell vizsgálni az auditornak.

2017-ben szintén elsőként felelt meg a Sharp eszköze a Protection Profile for Hardcopy Devices v1.0 (HCD-PP v1.0) védelmi profilnak - ez a minősítés a kormányzati és katonai hivatalok legújabb biztonsági szabványait tartalmazza -, melyet a japán IT biztonsági értékelési és minősítési rendszer (JISEC) alapján végzett vizsgálatok után érdemelt ki.

A HCD-PP (Hardcopy Device Protection Profile) az amerikai és japán kormány által - biztonsági követelmények alapján - meghatározott új követelmény-rendszer digitális multifunkciós berendezésekre. A NIAP (National Information Assurance Partnership) és az

IPA (International-Technology Promotion Agency) közösen fejlesztette ki egy ipari együttműködés keretében. Célként fogalmazták meg, hogy az MFP-k által feldolgozott információkat megóvják a biztonsági fenyegetésektől, ezenkívül tartalmaz még tűzfalakra és titkosításra vonatkozó specifikációt is.

A következő fejezetekben a nyomtatási technológiákat, dokumentumkezelési folyamatokat mutatom be, majd a rendszerelemek gyenge pontjait vizsgálom.

3 NYOMTATÁSI TECHNOLÓGIÁK ISMERTETÉSE

A különböző típusú nyomathordozókra közvetlenül rányomtatott, digitális módon létrehozott képinformáció megjelenítését nevezzük digitális nyomtatástechnológiának.

Ekkor vagy közvetlenül a kreatív (grafikusi/szerkesztői) munka után, vagy más digitális forrásból - száraz vagy folyékony toner technológiával, illetve tintasugaras technológiával - kis példányszámú munka készíthető el.

Éppen a kis példányszám miatt élvez előnyt a gyorsaság és a kisebb számú előkészítési művelet (az egy ívre osztott költség ugyanakkor nagyobb, mint az offset technológia esetén). Ez a technológia a rövid átfutási idejű, konkrét igényre való nyomtatás lehetőségét teremtette meg, ahol változó információk jelennek meg egymásutáni íveken.

Elsőként a formanyomtatványok és a kereskedelmi nyomtatványok területén jelent meg alternatívaként, majd a termékbemutató szórólapok dinamikus üzleti piacára tört be.

A színmenedzsment fejlődésével a csomagolóanyagok gyártása is fókuszba került: termékcímkézésre használt öntapadó címkék, flexibilis csomagolóanyagok, kartondobozok készítésére használják.

A változó információk nyomtatásával új korszakot nyitott: testreszabott ajánlatok és reklámok juttathatók így el a címzettekhez.

Három fő nyomtatási technológia létezik:

- a tintanyomtatókban a fúvókákon keresztül ionizált tintacseppeket permeteznek papírra a kialakítandó betű vagy kép helyén,
- a mátrix nyomtatókban kerek tűk csoportja üti meg a papírlapot a festékszalagon keresztül,
- lézernyomtatás.

A lézernyomtató elve a következő lépéssorozatban érthető meg.

A dobot először a koronaáram pozitív töltésűvé teszi, majd forgása közben a lézeregység sugarakkal létrehozza a látens képet (ott negatív töltésűvé válik). Ezután pozitív töltésű festék kerül a dobra, amely a látens kép helyén odatapad. A papír negatív töltése odavonzza a látens kép festékszemcséit.

Ekkor a leválasztó korona kisüti a dobot - törli a látens képet-, felkészítve azt a következő íven megjelenítendő adatokra, végül a nyomóhenger és a fűtőhenger között átfutó papírív rostjaiba magas hőfokon beég a festékpor.

A legjobb nyomtatási minőséget a lézernyomtatók biztosítják, őket követik a tintasugaras, majd a mátrix nyomtatók. A lézernyomtatók ára folyamatosan csökkent, így számos felhasználó számára elérhetővé váltak. Napjainkban a speciális területeken kívül lézer vagy tintasugaras nyomtatók láthatóak irodai és otthoni környezetben egyaránt.

”Minden az egyben”

Irodai színes és fekete-fehér nyomtatók jellemzői, egységeik [11].

Nyomtatás, másolás és szkennelés a fő profil és bár már egyre több helyen elektronikusan történik, de vannak még hagyományos analóg vonallal rendelkező, faxolni képes eszközök is használatban.

Szkennerek

- lap szkenner: egyszerre csak 1 dokumentumot lehet beletenni és csak manuálisan lehet a lapokat cserélni, forgatni,
- ADF-es: automatikusan behúzza a lapokat,
- DADF-es: automatikusan behúzza a lapokat és tud kétoldalasan szkennelni,
- Dual Scan ADF-es: behúzza a papírt, egy menetben beszkennelve mind a két oldalt.

Duplex nyomtatás esetén a lapok automatikusan forgatásával időt takaríthatunk meg. Az LCD kijelző/érintőképernyő használata nemcsak trendi, de az is jól látható, hogy mit csinál a nyomtató, emellett gazdaságos az áramfogyasztása is.

Nyomtatók kapcsolódási típusai:

- a nyomtatás USB kábel segítségével történik, közvetlenül a számítógéphez csatlakozva,
- vezetékes LAN kábellel csatlakozik a hálózatra, így nem kell megosztani az USB-s nyomtatót egy számítógépen keresztül, amennyiben más kíván nyomtatni,
- a WIFI nyomtató vezetéknélküli hálózati kapcsolaton keresztül kapcsolódik a routerhez,
- a WIFI Direct nyomtató külön router segítsége nélkül, önmaga tud vezeték nélküli hálózatot létrehozni, amely driver és egyéb telepítő program telepítése nélküli nyomtatást tesz lehetővé.

A beépített fax modemmel rendelkező készülék küldésre és fogadásra is alkalmas telefonvonalakon keresztül. Az NFC (Near field Communication) rövid hatótávú rádiós kommunikációs lehetőség; egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel, maximum pár centiméterről működik.

4 DOKUMENTUMKEZELÉSI FOLYAMATOK BEMUTATÁSA

A dokumentumkezelés olyan tevékenységsorozat, mely során létrehozzuk, kezeljük, digitalizáljuk, tároljuk és keressük a dokumentumokat.

A mindennapi munka során létrehozott, felhasznált, tárolt és végül megsemmisített több ezer dokumentum eredményes kezelésére minden vállalatnak jól működő dokumentumkezelési folyamattal kell rendelkeznie a hatékony és szervezett munka fenntartása érdekében [12].

Egy jelentős része az adatlopással és kiszivárogtatással összefüggő eseményeknek emberi hibára vezethető vissza. Ezen emberi hibákból fakadó valószínűséget egy irattári terv integrálásával a vállalatok jelentősen csökkenthetik, nyomon követhetővé válnak a dokumentumok, azok nyilvántartása és különböző file-ok cégen belüli útja és tárolási helye.

A jól működő irattári tervnek hat fő eleme van:

- leltár készítése a vállalat összes dokumentumáról,
- felelős meghatározása, aki az egész folyamatot irányítja,
- cégen belüli dokumentummegőrzési politikát kell kialakítani,
- az iratok tárolásának és kezelésének legjobb módját meg kell határozni,
- a mindennapi munka során alkalmazott dokumentumkezelési folyamatokat kell kialakítani,
- a fölösleges és használaton kívüli iratok és file-ok megsemmisítésének lépéseit meg kell határozni.

Egy jól működő dokumentumkezelési terv elengedhetetlen a dokumentumok biztonságának biztosítása érdekében, emellett a megsemmisítés ugyancsak kritikus szerepet játszik biztonsági szempontból: a régi és eldobott dokumentumok komoly kockázatot jelentenek a még aktív, használatban lévő iratokon és file-okon túl [13].

A megsemmisítési folyamat integrálása biztosítja az érzékeny dokumentumok vagy a tulajdonosi információk teljes körű védelmét.

A DMS (Document Management System) szoftverek a szervezet dokumentumkezelését és a dokumentum alapú munkafolyamatokat optimalizálják: számlajóváhagyás, szerződésvéleményezés.

A vállalatok az ERP rendszereket DMS rendszerekkel egészítik ki a hatékonyságnövelés érdekében üzleti dokumentumaik strukturált nyilvántartásával.

Ezzel a munkafolyamatok felgyorsulnak, a vállalati működés átláthatóbbá válik, iktathatók, rendszerezhetők és egységesen kezelhetők lesznek az e-mailek és egyéb forrásból érkező dokumentumok, a számla- és szerződésnyilvántartás.

Precíz és naprakész kimutatások készíthetők el, hatékonyan támogatva a vezetői döntéshozatalt.

A jó rendszer magas fokon integrálható: két irányú adatkapcsolatot tesz lehetővé, illeszkedik egy már meglévő ERP vagy kialakított workflow megoldáshoz is, így bevezetése ennek köszönhetően gördülékenyen és gyorsan végezhető el.

Azokban az esetekben, amikor egy cég nem rendelkezik külön workflow szoftverrel, megoldást jelentenek az olyan DMS szoftverek, amelyek beépített workflow modult tartalmaznak, támogatva a hatékony ügyintézést több telephely, szervezeti egység esetén is.

Ezen rendszerek megoldást kínálnak az adminisztrációs problémákkal küzdők számára, működési területtől és mérettől függetlenül. Implementálásuk előtt felmérés történik, melynek során azonosítják az adott szervezet dokumentumkezelési gyakorlatát és workflow szintjét. A felmérés eredménye alapján a szervezet számára legjobban testreszabott megoldás ajánlható. Így a bevezetett szoftver valóban a várt megtérülést hozza, ténylegesen támogatva a workflow-t, az információk adásvételét is hatékonyabbá téve.

Dokumentumaink kezelését fontos elektronikus mederbe terelni.

A munkafolyamatok dokumentumkezelés szempontjából kétfelé csoportba sorolhatóak.

Egyes workflow folyamatok nem igényelnek dokumentum megjelenítést a task végrehajtása alatt (pl.: szabadságigénylés).

Más folyamatokban a process lefutásának előfeltétele, hogy a dolgozó hozzáférjen a dokumentumhoz (pl.: egy szerződésjóváhagyás esetén). Amennyiben a workflow végrehajtásához szükséges dokumentumok csak papír alapon léteznek, akkor azokat először digitalizálni kell, majd a már elektronikus, beszkennelt dokumentum verziót alkalmazhatjuk a későbbi folyamat során.

Az így bekerült dokumentumok egy egyedi azonosítószámot kapnak, ezzel is segítve a későbbi visszakeresést. A dokumentumtárban elérhetjük mindazon dokumentumokat, amelyekhez jogosultságot szereztünk, láthatjuk az egyes verziók alakulását, letölthetjük/módosíthatjuk a keresett dokumentumot.

Sokféle metaadat szerint lehet keresni a dokumentumtárban: ki és mikor készítette az adott dokumentumot, módosítása milyen időpontban és mely felhasználóhoz köthetően történt, emellett rákereshetünk konkrét fájlnevekre is. Mindezeken túlmenően az adott munkafolyamatból és magából a dokumentumtárból is elérhetővé válnak így a dokumentumaink.

Lehetőségünk nyílik a dokumentumkezelés funkció segítségével:

- elektronikus tárolásra,
- különböző szempontok szerinti keresésre,
- verzió nyomon követésére,

- megjegyzések, kommentek megőrzésére (pl. szerződés véleményezésével kapcsolatban), kapcsolatok rögzítésére adott dokumentumhoz szorosan kapcsolódó más dokumentumok (számla, szállítólevél stb.) között,
- felhasználókkal vagy felhasználói csoportokkal való dokumentummegosztásra,
- a jogosultságnak megfelelő dokumentumhoz való hozzáférésre.

5 RENDSZERELEMEK GYENGE PONTJAINAK VIZSGÁLATA

2017-ben az IDC MARKET SPOTLIGHT kiadásában megjelent tanulmányban a szerző arról számolt be, hogy jelentősen megnövekedett a tárgyak internete (IoT) biztonságára fordított figyelem a közelmúltban [14].

Nagy horderejű, elosztott szolgáltatásmegtagadási (DDoS), illetve népszerű webhelyek leállásához vezető támadásokat valósítottak meg hackerek, forgalom veszélyeztetett megfigyelő kamerák, digitális videó-felvevők és egyéb hálózatra csatlakoztatott IoT elektronikai eszközökön keresztül.

Melyik eszközt célozzák meg legközelebb?

Miközben környezetünkben más IoT -eszközöket keresünk - amelyek megegyeznek a használt eszközök néhány jellemzőjével a legújabb támadások során - figyelmünket elkerülheti a nyomtatók szerepe.

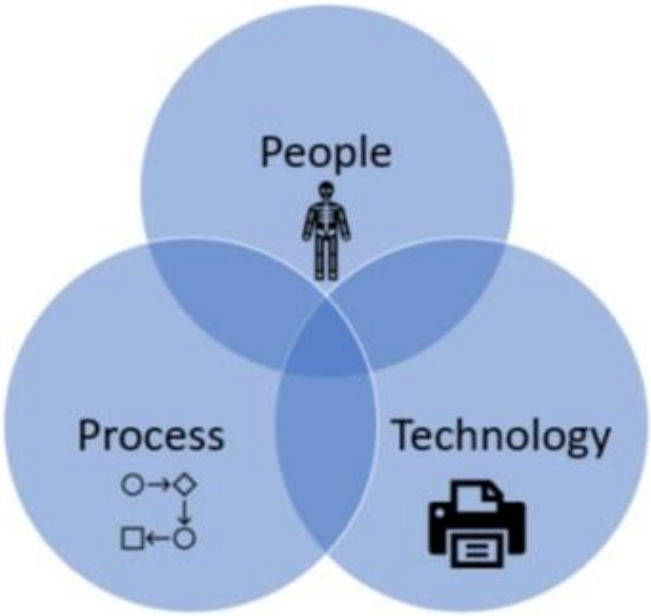
Az otthoni, kisvállalkozói vagy vállalati környezetben alkalmazott szoftverfrissítések és a hozzáférésszabályozás, amelyek a hagyományos informatikai termékek prioritásai, gyakran figyelmen kívül hagyják a nyomtatókat. A nyomtatók eszközei lehetnek a következő nagy IoT-támadásnak, de az üzleti műveletekre új veszélyeket jelentő célpontként is megjelenhetnek:

- DDoS lehetőség a hálózat belső részén,
- vállalati hálózaton belül található adatlopás.

A 2005-ben megjelenő ISO 27001 szabvány és a 2018-ban érkező GDPR szabályozás által magasabb szintre került az adatok, illetve a személyes adatok megsértésének következménye, ugyanakkor a hálózatban a nyomtató egy olyan elfelejtett végpont, amely sürgős figyelmet igényel.

A nyomtató - mint periféria -, vagy nagyobb léptékkel vizsgálva, a digitális nyomtatástechnológia egy-egy eleme vagy funkciója szervesen kapcsolódik a vállalati környezethez, így vizsgálandó a szerepe a GDPR és az ISO 27001 szabályozásban egyaránt.

A rendszerelemek gyenge pontjainak vizsgálatakor az aktuális információbiztonsági szabványrendszert, mint értelmezési keretrendszert veszem alapul.



5.1. ábra: People_Process_Technology.jpg.

Az ISO 27001 szabvány egy évek óta bevált keretrendszerbe foglalja a jól ismert, biztonsággal kapcsolatos „people – process – technology” hármast, s ebben a rendszerben az IT erőforrások, mint vagyontárgyak a következő csoportosításban jelennek meg:

- data (adat),
- human resources (humán erőforrás),
- technology (technológia, HW és SW),
- facility (üzemeltetési környezet),
- application (üzleti folyamatok).

Ezen IT erőforrásoknak, mint rendszerelemeknek a viszonylatában a szakdolgozatomban tárgyalt digitális nyomtatástechnológiát akár sorolhatnánk a „technology” halmazba, mint ahogy korábban is tették a rendszergazdák: „a nyomtató csak egy periféria a sok közül”.

Érdemes ezt a perifériát úgy kiválasztani és a rendszerünkbe illeszteni, hogy meggyőződünk a megfelelőségéről.

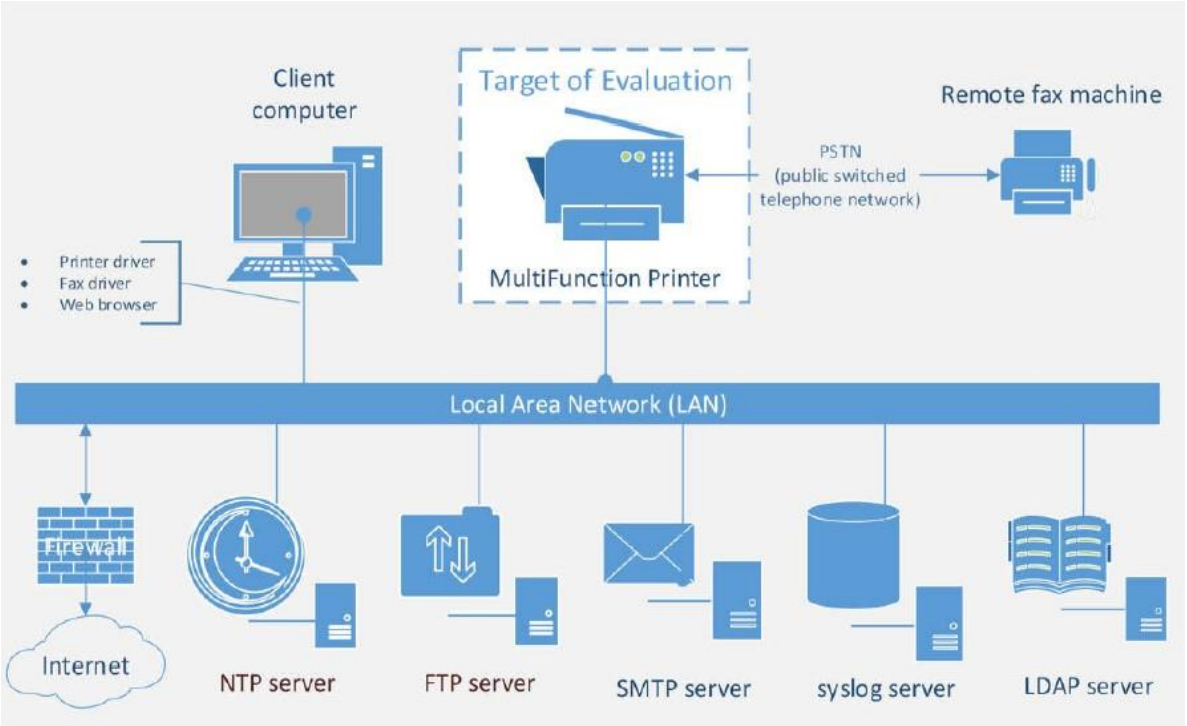
Megfelelőség alatt egyészt a szabványoknak való megfelelőséget értem, másrészt a meglévő rendszerelemekkel és az azokhoz tartozó szabályozásokkal való kompatibilitást.

Ellenőrizhetjük a „Történelmi áttekintés” fejezetben már említett Common Criteria minősítés meglétét, melyet a tanúsító szervezetek és a gyártó oldalán is megtalálhatunk.

5.2. ábra: CC tanúsítvány Ricoh MFP berendezésekre [15].

Ezen tanúsítás kiadását egy olyan vizsgálat előzi meg, amelyben a tanúsító szervezet a multifunkciós eszközt (Target of Evaluation-t) egy vizsgálati környezetben értékeli annak működése során, különböző feltételrendszereknek való megfelelőségében.

Amint az ábrán látható, az MFP helyi hálózaton (LAN) keresztül kapcsolódik működési környezetéhez, valamint nyilvános kapcsolt telefonhálózaton (PSTN - Public Switched Telephone Network) egy távoli fax-hoz. A felhasználók a printert a kezelőpaneljéről vagy LAN kommunikáción keresztül működtethetik.

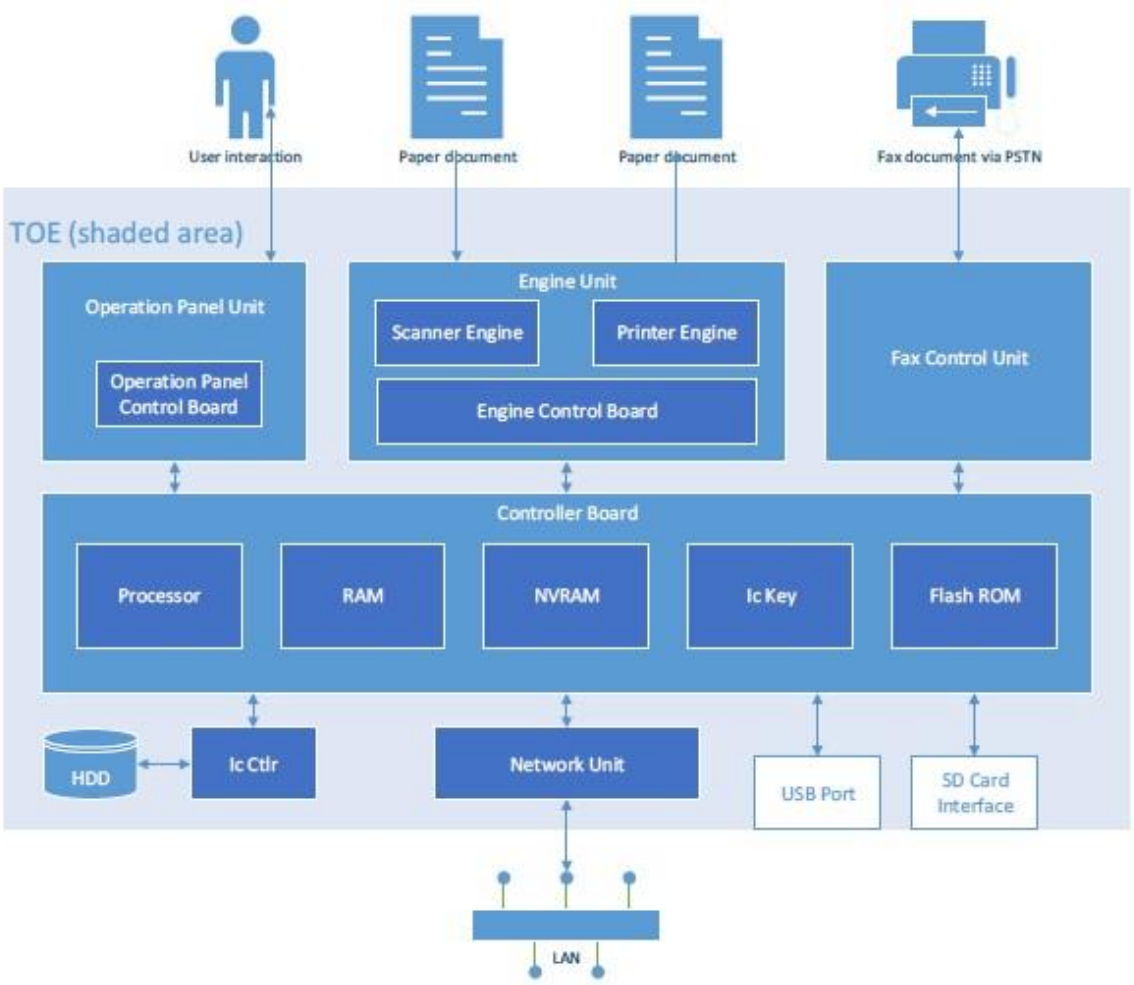


5.3. ábra: MFP berendezés vizsgálati architektúrája [16].

A nyomtató tárolja a dokumentumokat, illetve dokumentumokat küld és fogad a LAN-hoz csatlakoztatott informatikai eszközökre és azokról. Az ilyen dokumentumok titkosságának és integritásának biztosítása érdekében a következő biztonsági jellemzőkkel kell rendelkezzen:

- azonosítás és hitelesítés,
- funkcióhasználati engedélyezés,
- hozzáférés-szabályozás,
- tárolt adatok titkosítása,
- megbízható kommunikáció,
- adminisztratív szerepkörök,
- auditálás,
- megbízható működés,
- PSTN fax-hálózat elkülönítése.

Ezen biztonsági jellemzők teljesítése az eszköz hardver konfigurációjának be- illetve kilépési pontjainak nem megfelelő védelme esetén sérülhet alapvetően.



5.4. ábra: MFP berendezés hardver konfigurációja [17].

A felhasználó elsődleges fizikai interakciója a berendezéssel annak LCD kezelőfelületén keresztül valósul meg azonosítás és hitelesítés után, egyúttal megtörténik a funkcióhasználati engedélyezés és a jogosultság alapján a hozzáférés-szabályozás is.

Az ezen belépési ponton elérhető, jogosulatlanul megszerzett (talált vagy eltulajdonított smart kártya, belépési account/jelszó páros) vagy nem megfelelően kialakított (NTFS, share jogosultságok) hozzáféréséből adódóan a felhasználó így számára nem engedélyezett dokumentumokat nyomtathat, és egy nem helyesen definiált funkcióhasználat esetén akár törölhet is az eredeti tárhelyről.

Ugyancsak problémát okozhat, ha az adatbeviteli lehetőségeket nem körültekintően tervezzük meg.

Jogosulatlan adattovábbítás fordulhat elő, ha a felhasználó jogosultsági körétől eltérő lehetőségeit nem szabályozzuk megfelelően: így fordulhat elő, hogy email-es szkenneléskor megadható lesz számára olyan külső címzett e-mail címe vagy mappa elérhetősége (FTP szervere vagy egyéb drive-ja), amely nem tartozik a szabályozott kapcsolati körébe.

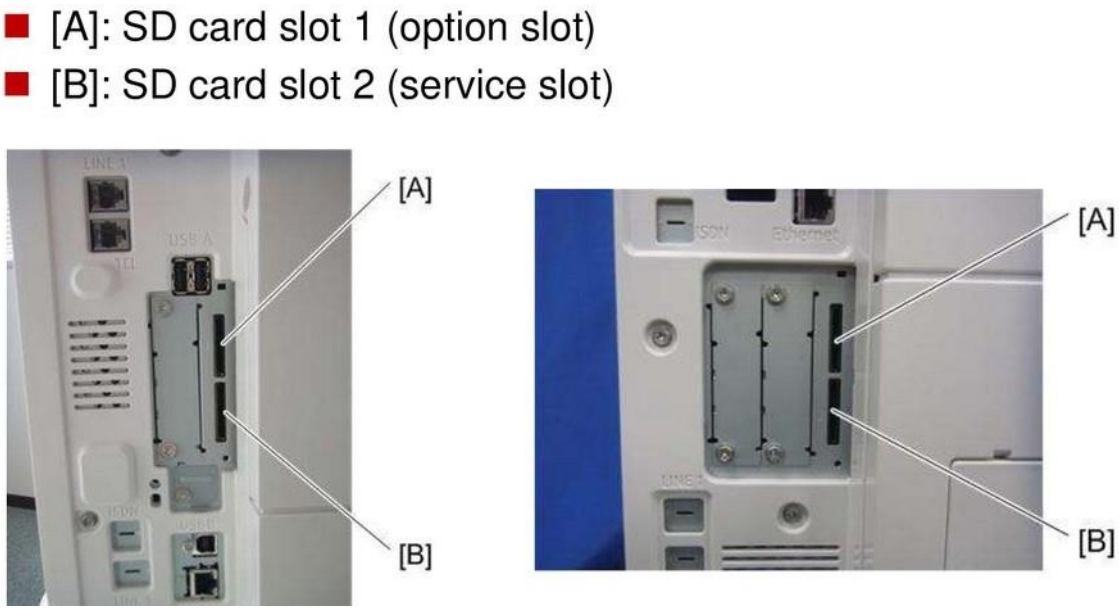
Ha a szkennelt dokumentum a cég LAN hálózatán vagy a bérelt felhőben kialakított mapparendszerében nem megfelelő helyre kerül egy rosszul tervezett jogosultság miatt, az ügyviteli problémákat generálhat az üzleti folyamatban. Az informatikai biztonságtudatosság a workflow folyamatok tervezésénél is szempont kell legyen, hogy egy, a szkennelt dokumentumban lévő QR-kód vagy metaadat csak a megfelelő munkafolyamatot indíthassa el.

Az új generációs multifunkciós eszközökben a hardver konfigurációban két újabb input/output lehetőség jelent meg, melyek kockázatot jelenthetnek, ha nem a valós tevékenységhez illesztve engedélyezzük/korlátozzuk szerepüket.

USB portok találhatóak az eszköz LAN hálózathoz való kapcsolódási pontja mellett közvetlenül a felhasználó PC-jéről vagy külső adattárolóról való nyomtatási lehetőséghez. Ezen USB porton keresztül a lánc további elemei - printer/PC/belső hálózat - támadhatóvá válhatnak egy fertőzött adathordozó csatlakoztatásával. USB porton keresztül jutott be a megtámadott hálózatba a felfedett APT (Advanced Persistent Threat - Fejlett tartós fenyegetés) támadások közül a Stuxnet is 2010-ben.

Két SD-kártyahely áll rendelkezésre a printerben: egy a telepítés során használható a műszaki személyzetnek, egy pedig a felhasználók számára engedélyezett az SD-kártyán lévő dokumentumok nyomtatására.

Ezen SD card slot-okat kihasználva szintén kártékony programok juttathatóak be a printeren keresztül a hálózatba.



5.5. ábra: Service SD card slot [18].

Amennyiben a printeren a felhasználók számára is elérhető, korábban felsorolt USB portokat/SD card slot-okat megfelelően konfigurálva védtük, ne feledkezzünk meg arról, hogy a legújabb multifunkciós eszközök kezelőfelülete tulajdonképpen egy olyan okos LCD

kijelzős beviteli lehetőség, amely USB portot és SD card slot-ot is tartalmaz, így ezeken keresztül szintén támadható válhat a printer és a hálózat többi eleme is.

5.6. ábra: SOP- Smart Operational Panel [19].

Míg a felhasználók számára korlátozott ezeknek a port-oknak és slot-oknak a hozzáférése, azokat elérhetővé kell tenni a berendezés szervizelése során teszteléskor/konfiguráláskor vagy javításakor.

A felhasználói üzemmód mellett a rendszergazdai, valamint a szerviz üzemmódba való jogosulatlan belépés is kockázatot jelent.

Rendszergazdaként a printer kezelőfelületén vagy a Web Image Monitoron keresztül további biztonsági beállítási lehetőségekhez férhet hozzá a támadó.

A Web Image Monitor segítségével távoli eszközöket lehet elérni a hálózaton keresztül.

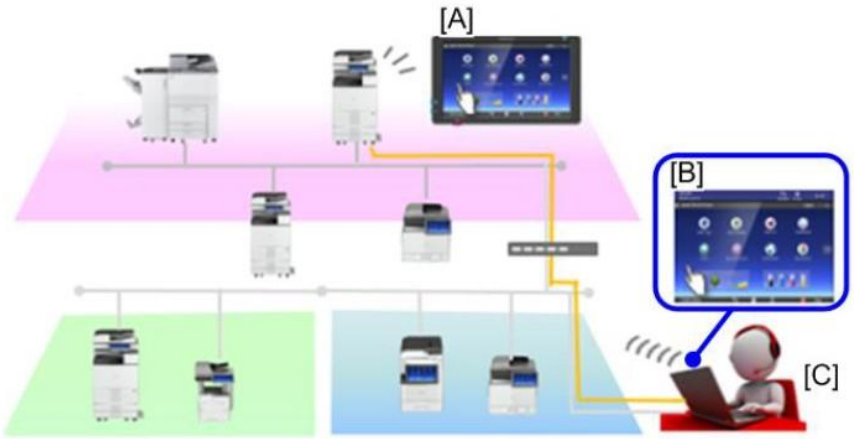
Az eszköz állapotának figyelése és a konfiguráció beállítása/módosítása szabványos webböngészőn keresztül érhető el.

A Web Image Monitor a következőkre használható:

- megjeleníteni az eszköz beállításait/állapotát,
- a munka állapotát és előzményeit ellenőrizni,
- lehetőség van a dokumentumszerveren és a fax funkcióval fogadott és tárolt fájlok ellenőrizésére, módosítására, nyomtatására, továbbítására és törlésére,
- kezelhető a címjegyzék,
- módosítani lehet az eszköz hálózati és biztonsági beállításait.

Egy technikustól ellesett jelszóval a szerviz üzemmódba való belépéssel lehetőség nyílik a hálózati beállítások megváltoztatása, tiltások feloldása.

Az új kezelőfelület oldalán egy kis műanyag burkolattal elfedett, 3 apró gombot tartalmazó tasztatúrán keresztül belépve a panel szerviz módjába hozzáférést engedélyezhetünk a berendezésen egy olyan távoli szerviz lehetőséghez, amellyel hálózaton belüli (RPO - Remote Panel Operation) vagy hálózaton kívüli (RCS - Remote Connect Support) segítséget kaphat a felhasználó.



[A]: Smart Operation Panel G2.5

[B]: Web browser

[C]: IT manager/ administrator

- Eliminating a trip to device
- Reducing end-user's wait time

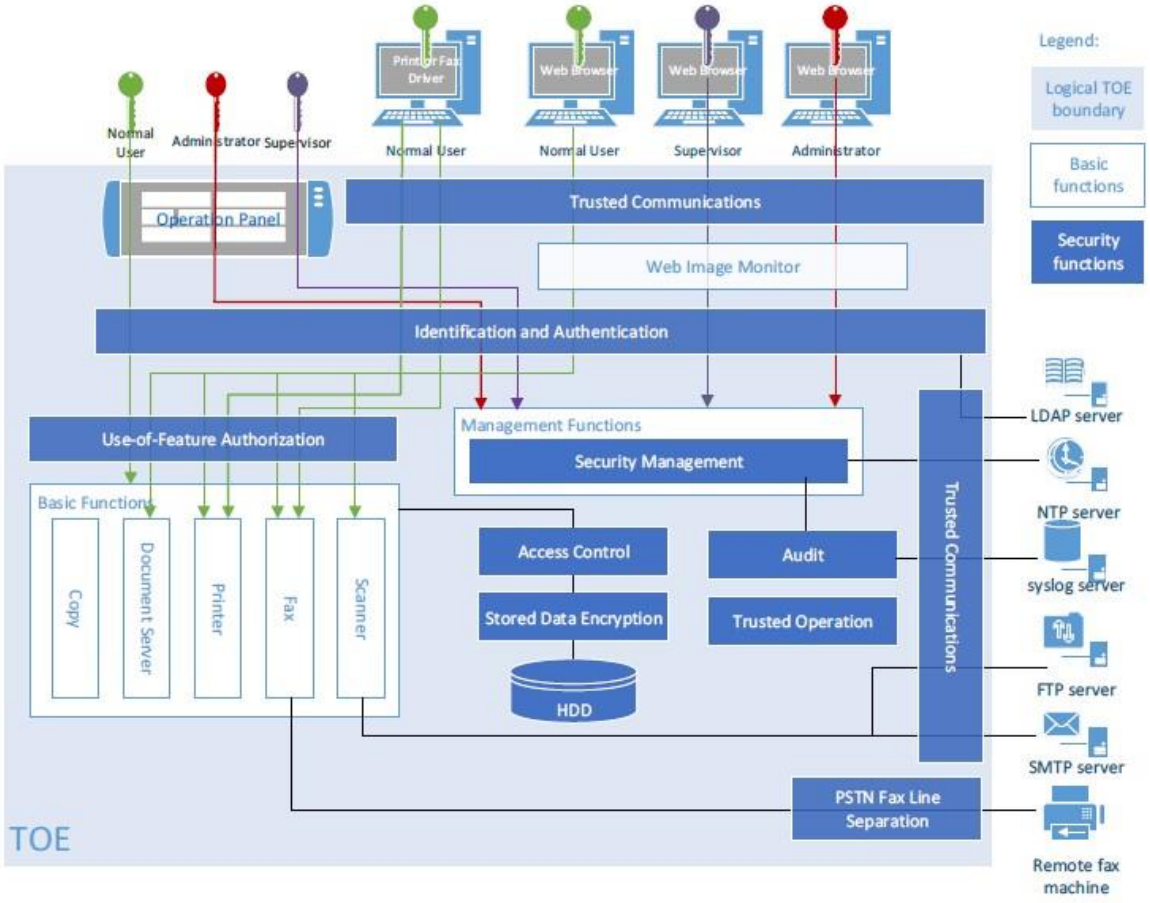
5.7. ábra: Remote Panel Operation [20].

5.8. ábra: Remote Connect Support [21].

Ezen berendezések beépített lehetőségként már tartalmaznak egy webes help funkciót is, így egy jól felépített támadással a printer segítségével a következő módon válhatunk áldozattá:

- a támadó első lépésben ezen funkciókhoz való hozzáférést kell megszerezze (akár az épületbe behatolva, akár a berendezés külső szervizelése során),
- második lépésben a social engineering-et alkalmazó támadó kiadhatja magát belsős IT kollégának vagy külső szerviz szakértőjének és segítségnyújtása során elnavigálhatja egy teljesen valid-nak tűnő másik weboldalra a web help oldalról és néhány kattintásra kérve a felhasználót rosszindulatú kódot indíthat el.

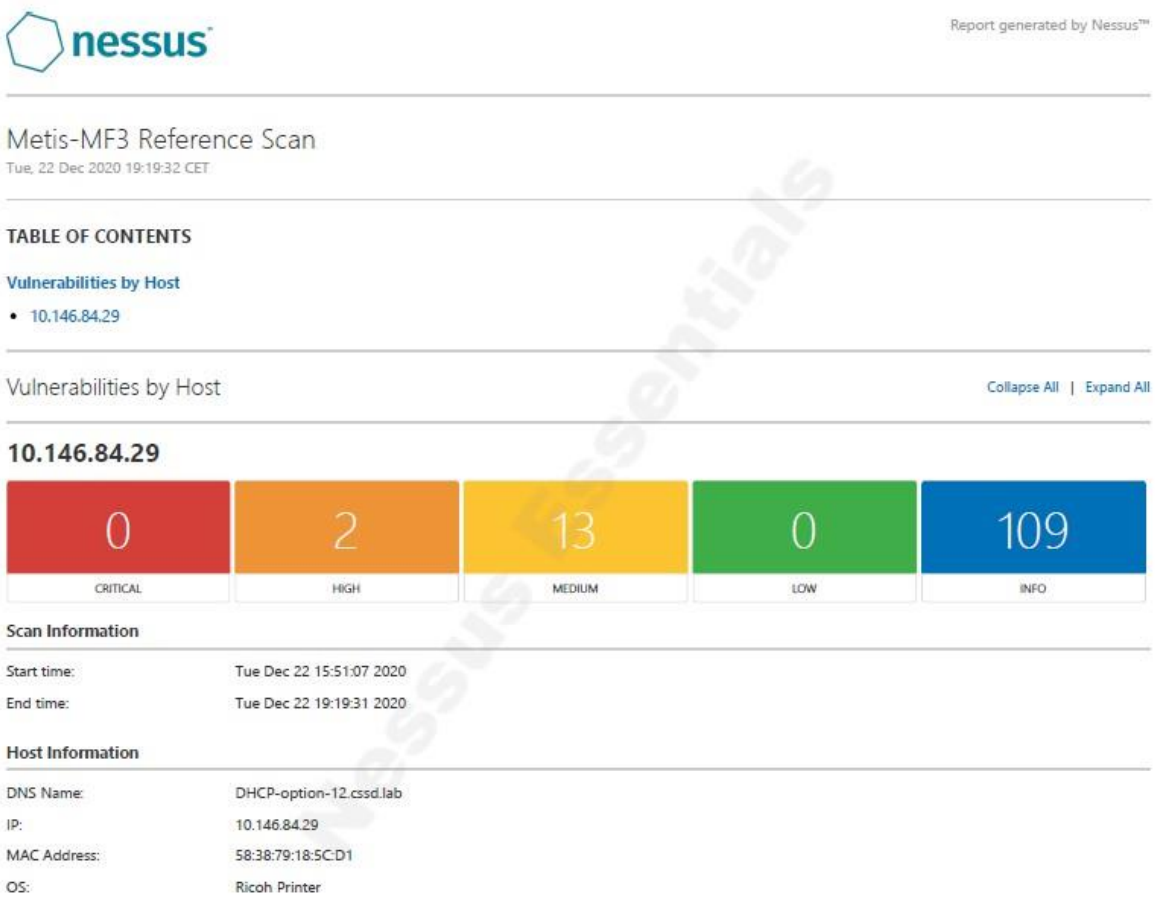
Az alapvető és biztonsági funkciók a lenti ábrán feltüntetett módon kapcsolódnak a printerhez és környezetéhez. A korábban említett biztonsági funkciókon felül (Azonosítás és hitelesítés, Funkcióhasználati engedélyezés, Hozzáférés-szabályozás, Tárolt adatok titkosítása, Megbízható kommunikáció, Adminisztratív szerepkörök, Auditálás, Megbízható működés, PSTN fax-hálózat elkülönítése) meg kell említeni a Kép felülírást is, mely funkció aktívan felülírja a merevlemezen tárolt maradék kép-adatokat, miután egy dokumentum feldolgozási feladat befejeződött.



5.9. ábra: Alapvető és biztonsági funkciók logikai ábrája [22].

Ingyenes vagy fizetős változattal több olyan szoftver is elérhető a piacon, amely hálózatbiztonsági szkennerként alkalmas szerverek/munkaállomások állapotának ellenőrzésére. Egy ilyen szoftverrel végzett vizsgálat során feltárhatjuk a rendszerünkbe már

beillesztett nyomtató sérülékenységeit, illetve ajánlásokat is kapunk ezen sérülékenységek kockázatának csökkentésére.



5.10. ábra: Metis-MF3 Reference Scan.pdf

Érdemes a fent említett vizsgálatot elvégezni, hiszen így olyan sérülékenységek kerülhetnek napvilágra, amelyeket a gyártó akár már be is foltozhatott, de emellett felhasználói oldalon még akadhat tennivaló.

Ilyen például két olyan biztonsági rés is a közelmúltból, amelyet 150 különféle típusú HP printernél detektáltak az F-Secure biztonsági kutatói (a hibák az egység kommunikációs kártyájában és a betűtípus-elemzőben voltak):

- a CVE-2021-39237 azonosítójú, mely a fizikai portok útján képes hozzáférést biztosítani a támadóknak, hogy azok adatokat nyerjenek ki (akkor tudják végrehajtani, ha fizikai kontaktusba kerülnek a hibás eszközzel),
- a CVE-2021-39238 azonosítójú távolról is kihasználható és tetszőleges kódfuttatásra is lehetőséget ad, emellett féregszerű vírusterjesztőként működik, így egy egész hálózatra veszélyt jelenthet.

Ezen sérülékenységet kihasználva a leghatékonyabb támadási módszer az lenne, ha egy megcélzott szervezetből származó felhasználót rávennének egy rosszindulatú webhely

meglátogatására, így a szervezet sebezhető MFP-jét az úgynevezett több telephelyen történő nyomtatási támadásnak tennék ki. A webhely automatikusan távolról kinyomtat egy rosszindulatú betűtípust tartalmazó dokumentumot a sérülékeny MFP-n, így a támadó kód végrehajtási jogokat biztosítana az eszközön.

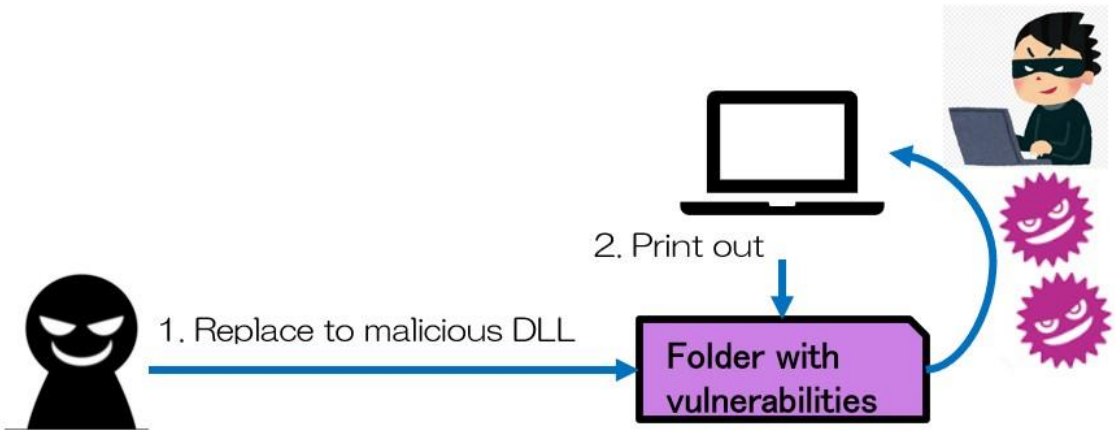
Így az ezekkel a kódvégrehajtási jogokkal rendelkező támadók csendben ellophatnák az MFP-n keresztül futott (vagy gyorsítótárban tárolt) információkat. Ez nem csak a nyomtatott, szkennelt vagy faxolt dokumentumokat foglalja magában, hanem az olyan információkat is, mint a jelszavak és a bejelentkezési adatok, amelyek az eszközt a hálózat többi részéhez kapcsolják.

A támadók a kompromittált MFP-ket akként is használhatják, hogy más célok érdekében (például más adatok ellopása vagy megváltoztatása, zsarolóvírusok terjesztése stb.) jobban behatoljanak a szervezet hálózatába.

Az F-Secure biztonsági kutatói ezenkívül felfedezték, hogy a betűtípus-elemzési sebezhetőségek féregférgezhetőek, ami azt jelenti, hogy a támadók önterjesztő rosszindulatú programokat hozhatnak létre, amelyek automatikusan feltörik az érintett MFP-ket, majd átterjednek ugyanazon a hálózaton lévő más sebezhető egységekre.

Más típusú sérülékenységre derült fény volt 2020 év elején, amikor az amerikai székhelyű biztonsági cég (Palo Alto Networks) és egy svájci székhelyű biztonsági cég (Pentagrid AG) figyelmeztette a Ricoh biztonsági szakembereit, hogy egyes Ricoh nyomtatóillesztők használatával a PC/laptop/Server rendszergazdai beállításainak rosszindulatú elérése vált lehetővé több mint 180 modell esetén.

A vizsgálat során egy privilégium-kiterjesztéssel kapcsolatos biztonsági rést találtak. A nyomtató-illesztőprogram mappájában található DLL-fájlt a belső támadó jogosultság nélkül lecserélhette. Ha a DLL-t rosszindulatúra cserélte, a támadó feltörhette a számítógépet.



5.11. ábra: Az illesztőprogram lehetséges sebezhetőségei [23].

A DLL fájl a nyomtató-illesztőprogram mappájába kerül (C:\ProgramData\RICOH_DRV\"printer driver name"_common\dlz), amelyet

rendszergazdai jogosultságokkal nem rendelkező felhasználók lecserélhetnek. Ha a DLLt rosszindulatúra cserélik ki, a támadó átveheti a PC felett az irányítást a nyomtatás során.

Folder Information		ProgramData (OS)	RICOH_DRV (Driver)
Folder type		Hidden folder	Hidden folder
Privilege	SYSTEM	Full control	-
	Administrators	Full control	-
	Users	Read, Execution, folder view	-
	Everyone	-	Full control

5.12. ábra: Ricoh DLL Privilege Escalation Vulnerability for Ricoh Drivers v1.0 [24].

Napjainkban azonban a korábban bemutatott technológia fejlődés révén valójában már több IT vagyontárgy csoportnak is része a nyomtató, illetve segítségével szoros kapcsolatot tudunk kiépíteni ezen vagyontárgyi csoportok között.

5.1 Data

Output eszközként adatokat tárol, majd jelenít meg a kijelzőjén vagy hard copyként különböző médiákon: papír, írásvetítő fólia, boríték, stb.

Az Input funkciójából származó adatok különböző formában élhetnek tovább:

- elektronikus file-ként egy mapparendszerben a vállalat saját háttértárolóján vagy egy bérelt cloud megoldásban,
- a nyomtatóról elküldött belső vagy a vállalaton kívülre címzett e-mailben csatolmányként,
- scanneléskor az OCR folyamat során kinyert adatok további inputjai lehetnek újabb dokumentumoknak, illetve indíthatnak el olyan workflow folyamatokat, melyek végterméke szintén elektronikus adat vagy hard copy média.

(A nyomtató adatkezelésben való szerepének és GDPR megfelelőségének egy külön fejezetet szentelek a későbbiekben.)

5.2 Human resources

Az emberi erőforrás az IT-ban egyszerű megfogalmazásban a Felhasználókat és az Adminisztrátorokat jelenti.

Másik megközelítésben a következő feladatkörök, illetve az ezekhez rendelt szerepek is megjelennek:

1. Fejlesztők.
2. Tesztelők.

3. Üzemeltetők (belső és külső szerviz-szolgáltatók).
4. Felügyeletet és irányítást ellátó egyéb szerepkörök (adatgazda, üzleti felelős, stb.).
5. Beszállítók, külső partnerek.

(Az emberi tényező kockázatának elemzésére szintén egy külön fejezetet szentelek a későbbiekben.)

5.3 Technology

A tárgyieszköz leltárban hardver elemként aposztrofált nyomtatón sorra jelentek meg azon szoftverkomponensek, amelyek segítségével például munkafolyamati elemeken keresztül a „Data" IT vagyontárgy csoportban már említett OCR capture funkcióval „Image on Demand - Igény szerinti kép" tárolására van lehetőség előre meghatározott digitális formátumban és tárolóhelyen, legyen az a vállalatunk belső szerveres környezete vagy akár egy bérelt felhőszolgáltatás. Természetesen a „Print on Demand - Igény szerinti nyomtatás" is hasonló szoftveres segítség.

A kifejezés a 2000-es évek elején a digitálisan elkészített, kis példányszámú könyvek előállítása kapcsán került bele a digitális nyomtatástechnológia eszköztárába (amely egy új üzleti modell kialakulását is jelentette ezen igényre az ofszett nyomdák magas költségével szemben), azonban ma már egy vállalat életében egyre többször jelenik meg a mobil nyomtatási szolgáltatási igény is.

Ezen szolgáltatás keretében mobileszközeinkről mobil-alapú opció segítségével leegyszerűsödhet a felhasználói nyomtatás, költséghatékonyabbá válhat az üzemeltetés; ezzel együtt éppen a mobilitást biztosító IoT eszközön keresztüli nyomtatás hordoz magában sérülékenységet, hiszen maga a mobileszköz, illetve a mobileszköz és a nyomtató közötti kommunikációs csatorna is támadható.

5.13. ábra: Workflow-automation.jpg. [25].

Egy másik szoftver segítségével nyomtatónkat alkalmassá tehetjük a vállalathoz beérkező analóg dokumentumok feldolgozása után egy Digital Mailroom szolgáltatás egyik inputjául szolgáló funkció ellátására. Ezen szolgáltatásban a bejövő elektronikus küldeményeinket is központosítva fogadhatjuk és érkeztethetjük több felületről (cégkapu, hivatali kapu, NAV-számla interfészen vagy weboldalon keresztül, illetve emailben érkezett küldemények), majd kimenő küldeményeink egy részét ismét nyomtatónkon készíthetjük el.

További workflow használatával (Accounts Payable) vállalatirányítási rendszerünkbe kapcsolhatjuk a beérkező papír- és elektronikus számlákat.

Ezen szolgáltatás a számlák befogadásának, ellenőrzésének, digitális aláírásának és jóváhagyásának lehetőségével, majd digitális aktákba sorolása után könyvelésével könnyíti meg folyamatainkat, riportjai segíthetik a pénzügyi tervezésünket, támogathatják az adminisztráció hatékony irányítását.

Beszerzési folyamataink támogatása egy Purchase Management alkalmazás használatával egyszerűsödhet, mellyel egy egységes platformon gördülékenyen kezelhetjük a beszerzési igényeket, a folyamatokat integrálhatjuk más nagyvállalati szoftverekkel, így kialakítva a csoportmunka lehetőségét is. Időpecsét hozzáadásával a párhuzamos vagy soros jóváhagyási rendszer is megvalósulhat, ezáltal a komplex, több körös jóváhagyás és tender kezelés követhetővé válik a megfelelő háttérrendszer kialakításával.

Ugyancsak hasznos lehet számunkra egy Contract Management szolgáltatás, mely a szerződéseink elkészítését és menedzselését tereli digitális folyamatba. Végre búcsút mondhatunk az emailben folytatott egyeztetéseknek és egy központosított, átlátható szerződéstárral gazdagodhatunk, amely képes a szerződéskötés teljes életciklusát felügyelni és kezelni. Egyedi munkafolyamatokat hozhatunk létre, amelyeket munkatársainknak követnie kell, legyenek bárhol, vagy használjanak bármilyen eszközt.

A szoftver segítségével lehetővé válik az elektronikus jegyzetelés és a kommunikáció a beszélgetések követésével és a kapcsolódó dokumentumok becsatolásával, automatikus értesítéseket állíthatunk be a szerződés lejáratának vagy projekt átadási idejének közeledtéhez, egyszerűen menedzselhetjük az egymásra hivatkozó jogi dokumentumokat, mint a keretszerződések vagy az egyedi megrendelések. Ezáltal az időigényes feladatok mennyisége látványosan csökkenhet és végre azokra a feladatokra koncentrálhatunk, amelyek előre viszik a cégünket.

És végül egy olyan workflow szolgáltatást említenék, amely segítségével egységesen, a jogszabályi előírásoknak megfelelően kezelhetjük munkavállalóink adatait, amely lehetővé teszi a jogosult munkavállalóknak a hozzáférést az indexált adatokhoz, integrálhatjuk az elektronikus és nyomtatott dokumentumokat és ezen HR támogató rendszerünket az ERP rendszerünkbe [26].

A biztonságos szoftverfejlesztést ma már egyre több helyen oktatják és hívják fel a figyelmet a szoftverek támadási felületeinek védelmére [27], [28].

A szoftverek frissítésével megelőzhetőek az ezen sérülékenységeket kihasználó üzleti vagy egyéb fontos adatokhoz (email címek, banki adatok) való jogosulatlan hozzáférések, rosszindulatú kód bejuttatási, valamint a belső vagy külső feltörések lehetősége.

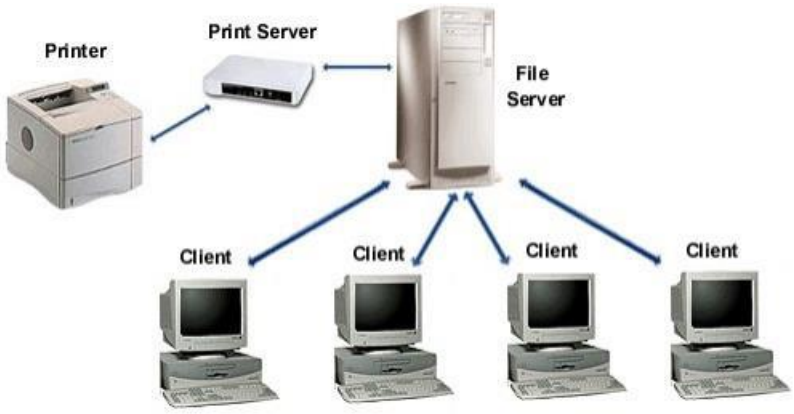
A javítások ellenőrzött és gyors telepítése véd a felsoroltak ellen, amennyiben a frissítéskezelés automatizált és központosított.

Természetesen ajánlott egy védett/elszeparált tesztkörnyezetben elvégezni a frissítést, majd futtatni egy hálózatbiztonsági szkenner vizsgálatot, nehogy éppen egy patch nyisson kaput a támadónak.

Látható, hogy a felsorolt szoftverek mindegyike támaszkodik az eddig hardverként tekintett nyomtatóra - illetve nyomtatástechnológiára -, egy olyan rendszerbe helyezve szerepét, amelyet üzemeltetési környezetünkben működtetünk.

5.4 Facility

Üzemeltetési környezetünk működtetésre során az előző pontokban említett újonnan megjelenő funkcionalitások miatt a digitális nyomtatástechnológia is nagyobb fókuszt kapott az elmúlt évtizedekben [29].



5.14. ábra: Nyomtatás kliens-szerver hálózatban.jpg [30].

A fenti ábrán a nyomtató még egy különálló hardver elemként kapcsolódott fizikai kábelezéssel a nyomtatószerverhez a rack-szekrényben lévő hálózati eszközök segítségével, ugyanakkor ma már mindennapos a wifi kapcsolatú nyomtatók használata is, a kliensek sokszor IoT eszközeink egyikeként értelmezhetőek és a print- és fileserver sem kell fizikailag egy hálózatban legyen a nyomatónkkal, illetve ezen funkcionalitásokat és szolgáltatásokat már felhő alapon is elérhetjük.

A cég üzletmenete megkívánhatja, illetve a végzett tevékenység profilja miatt törvényi szabályozás megkövetelheti, hogy fizikai védelmi eljárásrendben kijelölt biztonsági zónákon belül helyezzük el a nyomtatókat. Ezen esetekben a nyomtatók elhelyezését vagy áthelyezését, továbbá ezen eszközök konfigurálását kizárólag az - IT üzemeltetésért felelős vezető által erre kijelölt - Infrastruktúra üzemeltetési rendszergazdák végezhetik.

Ugyanakkor a fizikai környezet nyomtatónkra is hatással van, ezért az általunk üzemeltett eszköz ugyanúgy érintett lehet egy áramkimaradás, csőtörés vagy egy földrengés alkalmával, sérülhet funkcionalitása vagy annak egy része egy elromlott légkondicionáló berendezés esetén a nagyobb páratartalom vagy a magasabb környezeti hőmérséklet, esetleg egy tűzeset miatt.

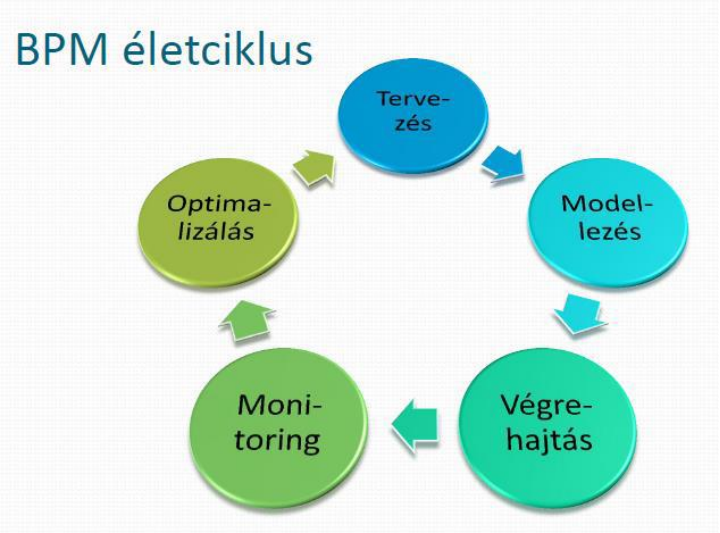
Az üzemeltetési környezet változtatásakor vagy optimalizálása kapcsán célszerű, tervezésekor pedig elengedhetetlen kellene legyen, hogy a tárgyalt téma ne csak az IT infrastruktúra rendelkezésre állásának DRP tervében (Disaster Recovery Plan - Katasztrófa-helyreállítási terv), hanem a BCP tervében (Business Continuity Plan - Üzletmenet folytonossági terv) is megjelenjen a kockázatértékelések (fenyegetés bekövetkezési gyakorisága és valószínűsége, okozott kár nagysága), kockázatelemzések (fenyegetések hatása, prioritásmeghatározás, együtt hatások kimutatása) és az azt követő PCDA (Plan-Do-Check-Act, Tervezés- Bevezetés-Ellenőrzés-Cselekvés) ciklus során.

5.5 Application

Az üzleti folyamatok - a lehető legegyszerűbben megfogalmazva - olyan ismétlődő tevékenységsorozatok, tevékenységláncok, amelyeken keresztül napi tevékenységeinket megvalósítjuk [31].

5.15. ábra: Üzleti folyamatok tervezése [32].

Az Üzleti Folyamatok Menedzsmentjének (Business Process Management - BPM) az a célja, hogy az üzleti folyamatokat folyamatosan optimalizálja annak érdekében, hogy a szervezet minél hatékonyabban és gyorsabban elégíthesse ki ügyfelei igényeit. Ez egyrészt fokozatosságot is jelent az optimalizálásban, másrészt természetesen nemcsak a vállalat Ügyfeleinek igényeit tartja fókuszban: figyelmet kell fordítani a belső kérésekre és a beszállítói igényekre is, mindezt egy olyan átfogó modell kidolgozásával, amely egyensúlyt teremt az üzlet, a technológia és az ember között [33].



5.16. ábra: BPM életciklus [34].

A covid19 miatt hangsúlyossá vált az üzleti folyamatok távolról, mégis biztonságosan megvalósított elérhetősége.

A cégeknek gyorsan, sokszor dobozos megoldásokkal kellett lereagálni a kialakult helyzetet, amely közelről sem biztos, hogy az IT erőforráscsoportokhoz való legbiztonságosabb hozzáférést jelentette, így számos újabb sérülékenységi pont jelent meg az ebben a környezetben végzett munkafolyamataikban és üzletmenetükben, amelyet a támadók kihasználhattak: adatbevitel és hozzáférés nem vállalati eszközökön és környezetben, adatfeldolgozás nem biztonságos csatornákon.

Amennyiben a „Technology” alfejezetben említett néhány szoftver, amely a digitális nyomtatástechnológiára épülve segítheti a vállalaton belüli egyes divíziók és csoportok munkáját nemcsak különálló entitásként jelenik meg, hanem szervesen beleépül az üzleti folyamatmenedzsmentbe annak tervezése során, akkor már jelentős lépést tettünk egy újabb, esetlegesen felbukkanó krízishelyzet kezelésére.

A BMP életciklus megvalósítására egy olyan SOA (Service Oriented Architecture - Szolgáltatás Orientált Architektúra) javasolt, amely:

- lehetővé teszi az integrációt és a fejlesztést,
- működése közben valós futás idejű adatokkal segíti az üzleti monitorozást,
- statisztikákat készít a Monitoring adatbázisból,
- lehetőséget teremt a kinyert adatok visszacsatolására a modellezésbe és a szimulációba, ezáltal fenntartva a ciklust.

5.5.1 Szolgáltatás Orientált Architektúra

Mindenki számára egy kicsit mást jelenthet.

Üzlet: az üzletet úgy tehetjük könnyen elérhetővé ügyfeleink és partnereink számára, hogy az ügymenetet szolgáltatások halmazaként képezzük le.

Architektúra: Olyan stílus, melynek jellemzői az egyszerű és összetett szolgáltatások kombinációja, a laza csatolás és újra felhasználás.

Fő elemei: szolgáltató (service provider), igénybevevő (requestor) és a leíró (descriptor).

Megvalósítás: Megfelelő módszertani- és eszköztámogatással bíró, korszerű technológiákat alkalmazó, szabványokra épülő fejlesztési modell.

Üzemeltetés: Olyan szolgáltatási szint megállapodások (Service Level Agreement), amelyek biztosítják az üzleti prioritásoknak megfelelő QoS (quality of service) betartását a requestor és provider között.

Security policy - Információbiztonsági politika

Az előző néhány oldalban érzékeltetni szerettem volna, hogy a fejezet címében megjelenő gyenge pontok vizsgálata valójában nem különálló rendszerelemek nagyítóval való boncolgatását jelenti. Ezért a felsorolt területek rendszerszemléletű kezelésére olyan Információbiztonsági politika kialakítása szükséges, amely az üzleti követelményekkel és a vonatkozó törvényekkel és rendeletekkel összhangban irányítási útmutatást és támogatást nyújt az információbiztonsághoz a szervezetnek, valamint a szervezet minden tagja és partnerei számára is átlátható, következetes és rendszeresen felülvizsgált a fenntarthatósága, megfelelősége és hatékonysága érdekében.

Ezen szemléletet és az ebben a fejezetben említett szempontokat figyelembe véve fogok ajánlást adni a Vállalatfejlesztési javaslat fejezetben.

6 EMBERI TÉNYEZŐ KOCKÁZATÁNAK ELEMZÉSE

Az 5. fejezetben már említést tettem azon feladatkörökről és szerepekről, amelyekben az emberi tényező, mint humán erőforrás vizsgálat tárgyát kell képezze.

Ebben a fejezetben részletesebben is górcső alá kívánom venni ezen területet, ezért csak emlékeztetőül nézzük át a korábbiakat:

Az emberi erőforrás az IT-ban egyszerű megfogalmazásban a Felhasználókat és az Adminisztrátorokat jelenti.

Másik megközelítésben a következő feladatkörök, illetve az ezekhez rendelt szerepek is megjelennek:

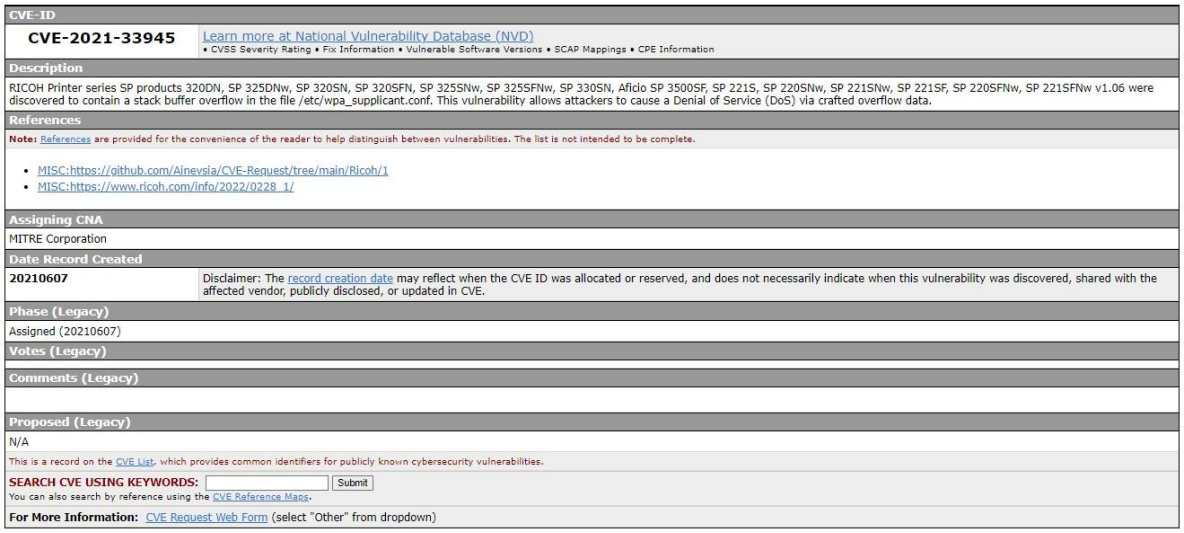
1. Fejlesztők.
2. Tesztelők.
3. Üzemeltetők (belső és külső szerviz-szolgáltatók).
4. Felügyeletet és irányítást ellátó egyéb szerepkörök (adatgazda, üzleti felelős, stb.).
5. Beszállítók, külső partnerek.

6.1 *Fejlesztők*

A biztonságos szoftverfejlesztést ma már egyre több helyen oktatják, és hívják fel a figyelmet a szoftverek támadási felületeinek védelmére.

Az informatikai értelmezésben vett sebezhetőség egy olyan rendszer vagy szoftver gyengeség, amelyet kihasználva a támadó káros tevékenységét ki tudja fejteni: megfertőzheti, túlterhelheti vagy éppen lehallgathatja egyes rendszerelemeinket, ezáltal veszélyeztetve üzletmenetünket, csorbítva reputációnkat.

A CVE rendszer (Common Vulnerabilities and Exposures) egy mindenki számára jól beazonosítható referencia-módszert biztosít a sérülékenységek kezeléséhez. Ezek a CVE-azonosítók minden egyes biztonsági résnek más-más nevet adnak. A Mitre Corporation által létrehozott és karbantartott nyilvános adatbázisban megtalálhatóak a már felfedezett sérülékenységek.



CVE-ID

CVE-2021-33945 — Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

RICOH Printer series SP products 320DN, SP 325DNw, SP 320SN, SP 320SFN, SP 325SNw, SP 325SFNw, SP 330SN, Aficio SP 3500SF, SP 221S, SP 220SNw, SP 221SNw, SP 221SF, SP 220SFNw, SP 221SFNw v1.06 were discovered to contain a stack buffer overflow in the file /etc/wpa_supplicant.conf. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://github.com/Ainevsia/CVE-Request/tree/main/Ricoh/1
- MISC:https://www.ricoh.com/info/2022/0228_1/

Assigning CNA

MITRE Corporation

Date Record Created

20210607 — Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20210607)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is a record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

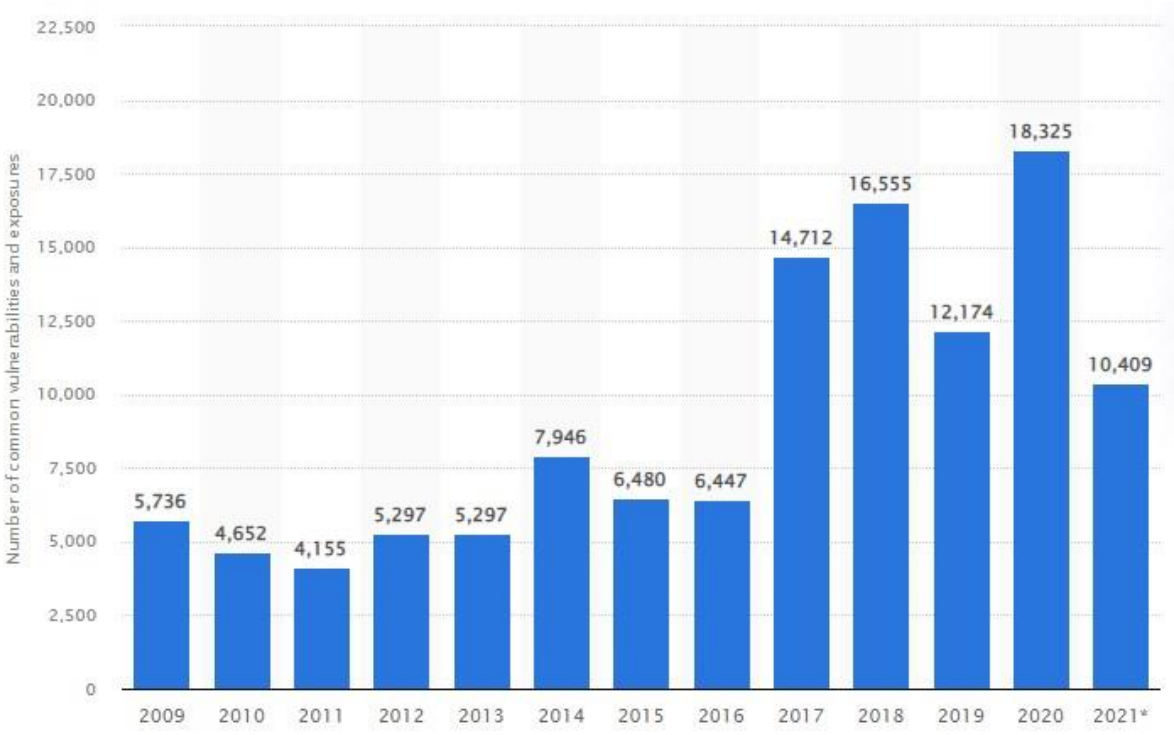
SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

6.1. ábra: Deny of Service (DoS) sérülékenység Ricoh printernél [35].

Jelenleg több mint 17 ezer feltárt sérülékenységet tartanak nyilván a weboldalon, ebből a „printer” szóra való keresés 232 rekordot sorol fel. Ez a 0,13%-os érték nem tűnhet aggasztónak első olvasatra, de mint ismert: csak a feltárt sérülékenységet tudjuk kezelni.



6.2. ábra: Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2021 [36].

A feltáratlan/kijavítatlan sérülékenység pedig olyan kockázat, amelyet az összetett, bonyolult informatikai rendszerek esetében alkalmazott számos komponens tovább többszöröz, ezért csak megbecsülni tudjuk a saját rendszerünkben a rendszerelemek és folyamatok komplexitásában.

Sokszor úgy gondoljuk, hogy hatalmas erőfeszítés ellehetetleníteni egy-egy támadást, ami lehet igaz is, ha utólag próbálunk meg okosak lenni. Azonban, ha időben megteszünk egy-egy akár apró lépést, lehetőségünk van minimális energiabefektetéssel elejét venni lavinaszerű problémáknak. „Egy öltés jókor, megkímél nyolctól” (a stitch in time saves nine).

JavaScript API segítségével lehetőség van az új ablakot megnyitó ablakot manipulálni, ha nincs explicit letiltva (reverse tabnapping):

```
<script>
 if (window.opener) {
   window.opener.location =
    "https://phish.tld";
 }
</script>
```

6.3. ábra: Reverse tabnapping [37].

Explicit tiltás 14 db karakterrel, amellyel kivédhető a reverse tabnapping:

```
rel="noopener"
```

6.4. ábra: Explicit tiltás [38].

Biztonságos fejlesztési életciklus

A szoftverfejlesztési életciklus minden fázisába integrálni kell a biztonságot. Minél később javítunk ki egy problémát az életciklusban, annál többe kerül a javítása. Ha a szoftverfejlesztés első fázisában nem vesszük figyelembe a biztonsági problémákat, a következő fázisok már magukban hordozzák az előző fázisok biztonsági réseit. Így a folyamat végén eredményként kapott termékben több biztonsági probléma is összeadódhat, növelve a biztonsági incidens lehetőségét. Ha a biztonságot a fejlesztési életciklus minden egyes fázisába beépítjük, az segít a korai problémamegoldásában, és ezzel lecsökkenthetőek a fejlesztési költségek is. A Microsoft által kifejlesztett életciklus modellt alkalmazva a szoftverfejlesztés minden egyes fázisában biztonságos szoftverfejlesztési eljárásokat teljesíthetünk [39].

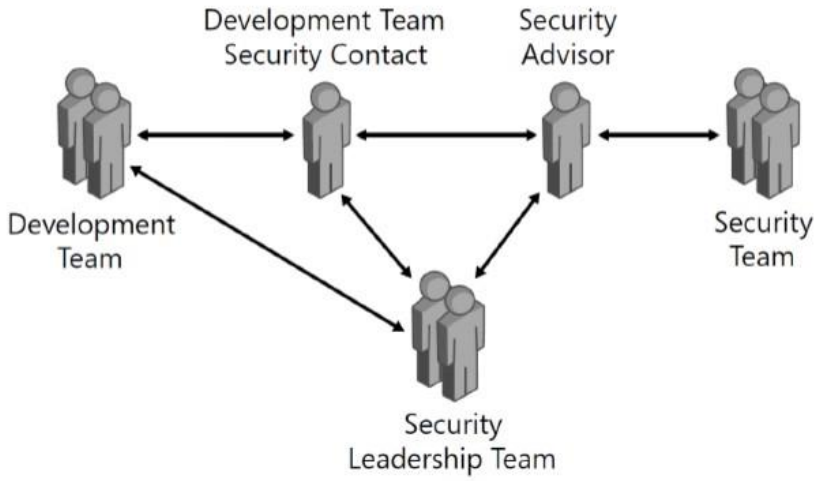
6.5. ábra: Security Development Lifecycle – SDL [40].

Az SDL fázisai a következőek [41]:

Oktatás
Biztonsági tréning.

Követelmények
Ebben a fázisban a minimálisan elérendő biztonsági és privacy kritériumokat a következő szereplők határozzák meg, viszonyrendszerük a képen ábrázolva:

- fejlesztők (Development team),
- biztonsággal kapcsolatos információk fogadása (Development team security contact),
- Security advisor,
- termék-biztonsági fókusz (Security team),
- biztonság menedzsmentje (Security leadership team).

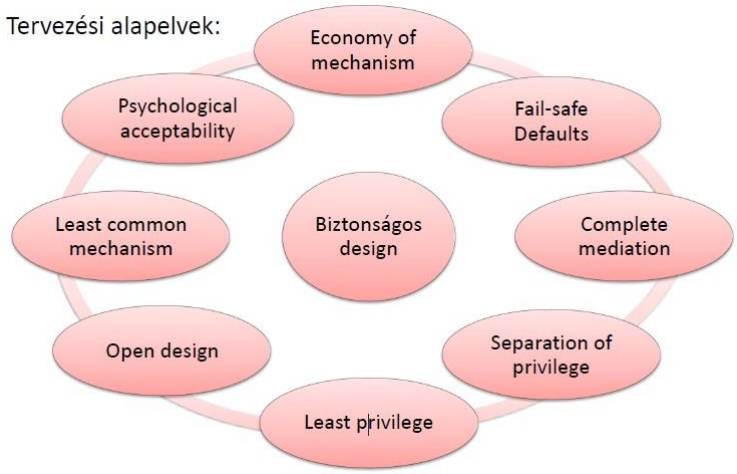


6.6. ábra: Biztonság, mint szempont képviselete [42].

Céljuk, hogy dokumentálják a biztonsági mechanizmusok beépítésének indokait:

- azonosított veszélyforrások és biztonsági/privacy követelmények,
- szükséges biztonsági funkcionalitások listája,
- bug-követő rendszer felállítása.

Tervezés
Ebben a fázisban törekedjünk a keep it simple, stupid (KISS) programtervezési metodika betartására, azaz mindent a lehető legegyszerűbben végezzünk, hiszen annál valószínűbbek a hibák, minél komplexebb a szoftver és a kisebb kódbázist könnyebb karbantartani.



6.7. ábra: Szoftvertervezési alapelvek [43].

Hozzunk létre fekete (alapértelmezésben a hozzáférés megengedett, kivéve, ha van olyan szabály, ami tiltja) és fehér (alapértelmezésben a hozzáférés megtagadva, kivéve, ha valamilyen szabály engedi) listákat a fals pozitív (megadtuk a hozzáférést, pedig nem kellett volna; ezt a felhasználó nem jelzi) és a fals negatív (megtagadtuk a hozzáférést, pedig engedni kellett volna; ezt jelezni fogja a felhasználó) helyzetek kezelésére (Fail-Safe Defaults).

Ellenőrizzünk minden elérést minden objektumhoz: a „hozzáférés engedélyezve” eredmény cache-elése, időközben visszavont engedélyek esete (Complete mediation).

Többféle feltételnek is tegyenek eleget, mielőtt megadjuk az engedélyt: a rendszer részekre osztása, így minden egység más-más feltételt ellenőrizhet (Separation of privilege).

Csak annyi jogosultságot használjunk, ami feltétlenül szükséges a feladat elvégzéséhez; magasabb jogosultságot csak időlegesen adjunk (Least privilege).

A terveket elérhetővé kell tenni, hogy minél szélesebb körben elemezhessék. (Open design)

Minimalizáljuk azon mechanizmusok számát, amik több felhasználó számára is elérhetőek és minden felhasználó számára szükségesek (Least common mechanism).

Figyeljünk az emberi tényezőre (fő fejezetcímünk is ez), hiszen amit a felhasználók nem fogadnak el, azt megpróbálják kikerülni.

Ezért a rendszer használata legyen egyszerű és intuitív és az erőforrás hozzáférés is maradjon egyszerű (Psychological acceptability).

Implementálás

A szoftver támadási felületének figyelembevételével történjen az implementálás:

- minden végrehajtási út, amin keresztül adat/parancs érkezik/távozik,
- kód, ami ezeket a végrehajtási utakat védi,
- minden értékes adat, amit a szoftver használ,
- kód, ami ezeket védi.

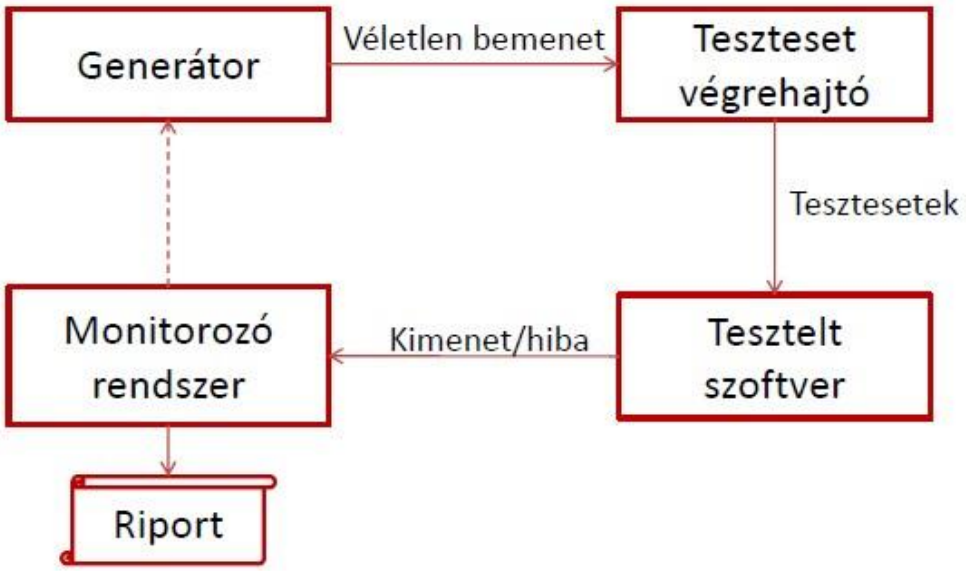
Mivel a bemenetet a felhasználó kontrollálja, ezért az adatfeldolgozás során az átalakítás a legegyszerűbb és elvárt formára történjen (normalizáció/kanonikalizáció); bizonyos kritériumok alapján egyes elemeket távolítsunk el a bemenetből (szűrés); a bemenet észszerűségének ellenőrzése (validáció) is történjen meg. Ügyeljünk arra is, hogy szoftverünk kimenetén olyan komponens jelenjen meg, amiben nincsenek káros elemek (semlegesítés/escape-elés). Az implementációs fázisban készítsük elő a naplózás funkcióját is: ki, mikor, hol, mit tett. Így azonosíthatjuk a biztonsági incidenseket, monitorozhatjuk a szabályszegéseket, letagadhatatlansági mechanizmusokat támogathatunk. Naplózzuk az adatfeldolgozási hibákat, az authentikáció eredményét, az authorizációs hibákat, a session menedzsmentet, a hibákat és a rendszereseményeket (és természetesen a naplózás kezdetét). Ne naplózzuk a kulcsokat, jelszavakat, forráskódot, tokeneket és más érzékeny információkat, hiszen emlékezzünk: a naplófile-okat bárki olvashatja.

Ellenőrzés

A verifikációs fázisban végezzünk statikus és dinamikus (a szoftver futása közbeni) elemzést is.

Statikus: az utasításokat csak értelmezzük, de nem hajtjuk végre; az elemzés egy absztrakt domén fölött történjen automatizáltan vagy manuálisan.

Dinamikus:



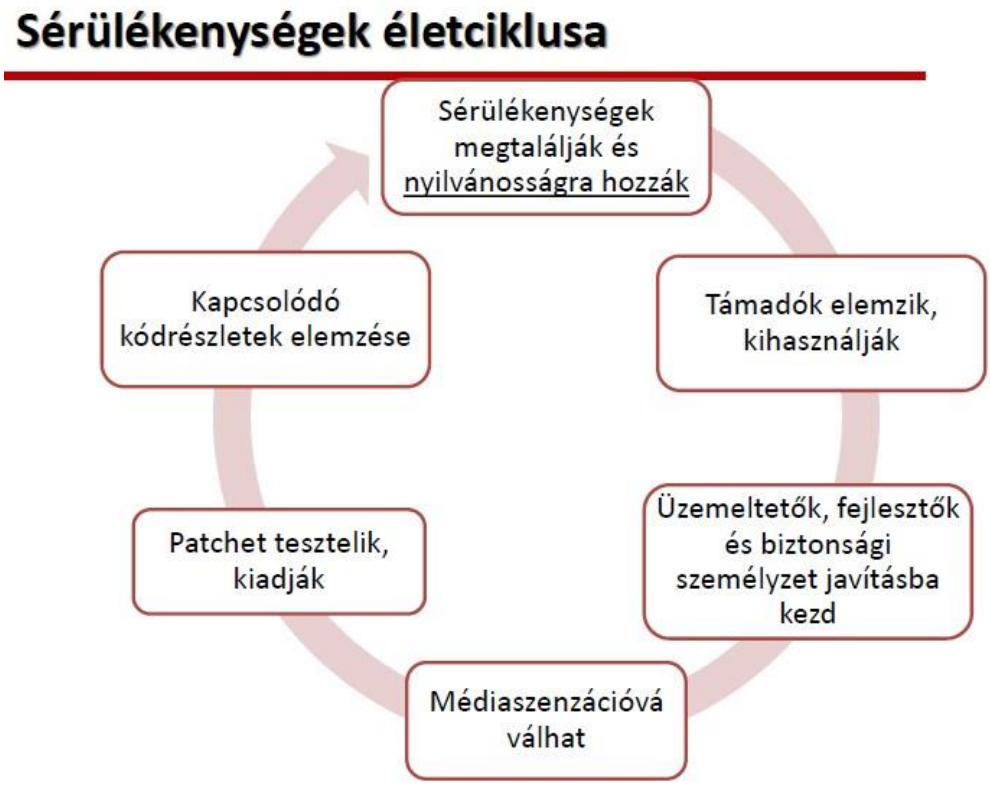
6.8. ábra: SDL_Verifikációs fázis - Fuzzing [44].

Ebben a fázisban szkenneljük a sérülékenységet (pl. a Nessus szoftverrel, amely jól ismert sérülékenységeket keres) és penetrációs tesztelést (amely elemzés célja, hogy a rendszerünkből információt gyűjtve és ezen információk alapján támadásokat indítva demonstrálja, hogy mit tehet a támadó) is végezzünk.

Kiadás
Ebben a fázisban a Security response terv létrehozásával alakítsunk ki Security response központot, amely tervben meghatározzuk, hogy mit tegyünk, ha érintettek leszünk egy újonnan felbukkanó sérülékenység esetén, illetve hogyan léphetnek kapcsolatba a központtal, amennyiben ilyet fedeznek fel.
Ugyancsak ebben a szakaszban hozzuk létre az Incidens kezelési tervet és Incidens response csapatot, amelyek feladata meghatározni, hogy mi történjen, ha a sérülékenységet nem felelősen hozták nyilvánosságra vagy megtámadják a rendszereinket.

Reagálás
A fejlesztés lezárulásával a sérülékenységek életciklusának körforgásában a Security response folyamat végrehajtásának feladata a Security Response Centeré:

- sérülékenységriportok gyűjtése, válaszolás,
- riport elemzése, így a fejlesztők el tudnak kezdeni dolgozni,
- kapcsolattartás megtalálókkal, felelős nyilvánosságra hozás bátorítása,
- security bulletin létrehozása,
- ügyfelek problémáinak és a sajtó figyelése.



6.9. ábra: Sérülékenységek életciklusa [45].

6.2 Tesztelők

A tesztelők több megközelítésben is végezhetik a feladatukat a korábban a szoftverfejlesztői csapat által végzett tesztelésen túlmenően [46], [47], [48], [49].

Végezhetnek hibatesztelést (verifikációs tesztelés - ekkor a tesztek célja a rendszerhibák feltárása, a program és a specifikáció közötti ellentmondás megmutatása) és validációs tesztelést (célja annak bizonyítása, hogy a szoftver megfelel a megrendelő igényeinek és a rendszer teljesítménye és megbízhatósága valós körülménynek között is megfelelő).

Végezhetnek hibatesztelést (programhibák jelenlétének feltárása) vagy hibakeresést (hibák lokalizálása és javítása).

Ha az egyes komponensek tesztelése a cél, akkor ezt rendszerint izoláltan (jellemzően white-box, strukturális teszt, amikor a forráskód alapján készülnek a tesztesetek) végzik.

Az interfésztesztelés kor az interfészek hibáinak, illetve az interfészekről alkotott hibás feltételezésekből eredő hibáknak járnak utána (objektum-orientált fejlesztés esetén az objektumokat interfészeikkel definiáljuk).

Integrációs tesztelés esetén a komponensek interakciójából eredő problémákkal foglalkoznak.

Rendszertesztelés kor a már kész rendszert tesztelik (jellemzően black-box teszt, specifikáció alapú, amikor a specifikáció alapján készülnek a tesztesetek).

Átviteli tesztelés kor a végfelhasználóval közösen végzett teszteknek 4 szintjét különböztetjük meg:

- alfa,
- béta (zárt vagy nyílt),
- felhasználó átvétel,
- üzemeltetői átvétel.

Az alfateszt már nem a fejlesztő csapat által történik a cégen belül, a funkcionális tesztek mellett vizsgálja a megbízhatóságot, a sebességet, a stabilitást és a használhatóságot.

A bétateszt során a publikus, de még nem az éles használatra kiadott verziót tesztelik. Ha a bétatesztek egymást követik, akkor a felhasználók köre is bővül.

A felhasználói tesztnél már a teljes célközönség használatba veszi, teljes funkcionalitással, éles (a legszélesebb hardver- és szoftver) környezetben működik, ám még ekkor is előfordulhatnak éppen a felhasználók által feltárt hibák, melyeket később javítani szükséges.

Azon szoftvereknél, ahol a használó és az üzemeltető külön személy, ott üzemeltetői teszt során a rendszergazdák ellenőrzik a különböző biztonsági funkciókat, az üzembiztonságot és a mentés és helyreállítás lehetőségét is.

Egy másik értelemzésben a teszt lehet:

- funkcionális tesztelés - hogyan kéne működnie a rendszernek,
- biztonsági tesztelés - hogyan NEM kéne működnie a rendszernek.

Security tesztelés - Biztonsági tesztelés: az adatbiztonsággal és adatvédelemmel kapcsolatos hibák vizsgálata. Célja annak ellenőrzése, hogy a szoftver/alkalmazás/webhely mennyire biztonságos a külső és belső fenyegetések ellen, mennyire lehet behatolni egy rendszerbe annak megzavarása és/vagy információmásolás céljából.

A biztonsági támadások legfontosabb típusai (támadás fajtái – és néhány konkrét támadás printerek esetén):

1. Cache Mérgezés - Működés ellehetetlenítése.
2. Adatstruktúra támadás

   CVE-2019-14451 A Repetier-Server 0.8 és 0.91 közötti RepetierServer.exe nem ellenőrzi megfelelően az új nyomtatókonfiguráció feltöltésekor biztosított XML adatstruktúrát. Ha ezt kombinálja a CVE-2019-14450-el (címtárbejárással kapcsolatos biztonsági rés, amely lehetővé teszi a felhasználó által vezérelt XML-fájlok nem kívánt helyen történő létrehozását), a támadó "külső parancs" konfigurációt tölthet fel nyomtatókonfigurációként, és távoli kódfuttatást hajthat végre. A kihasználás után a külső parancskonfiguráció betöltése a rendszer újraindításától vagy a szolgáltatás újraindításától függ.

3. Ártalmas kód beágyazása

   CVE-2021-46355 Az OCS Inventory 2.9.1-et a Cross Site Scripting (XSS) érinti. A biztonsági rés kihasználásához a támadónak manipulálnia kell a számítógépén lévő egyes eszközök, például egy nyomtató nevét, lecserélve az eszköz nevét olyan rosszindulatú kódra, amely lehetővé teszi a tárolt helyközi parancsfájlok (XSS) végrehajtását.

4. Trójai.
5. Azonosítási folyamat kihasználása

   CVE-2020-9330 Egyes nyomtatóknál nem szükséges újra megadni vagy ellenőrizni az LDAP hitelesítő adatokat, amikor módosítja az LDAP-kapcsolat IP-címét. Egy rosszindulatú szereplő, aki hozzáfér az érintett eszközökhöz (például az alapértelmezett hitelesítő adatok használatával), megváltoztathatja az LDAP-kapcsolat IP-címét a szereplő tulajdonában lévő rendszerre anélkül, hogy ismerné az LDAP hitelesítő adatokat. Az LDAP-kapcsolat IP-címének megváltoztatása után a következő hitelesítési kísérletek azt eredményezik, hogy a nyomtató egyszerű szöveges LDAP (Active Directory) hitelesítési adatokat küld a szereplőnek. Bár a hitelesítési adatok nem jogosult felhasználóhoz tartoznak, a szervezetek gyakran használnak privilegizált szolgáltatásfiókokat az Active Directoryhoz való kapcsolódáshoz. A támadó a hitelesítő adatok segítségével átveheti az Active Directory tartomány irányítását.

6. Befecskendezés

   A Mitre CVE adatbázisban a 232db printerre vonatkozó, már felfedezett sérülékenység közül 13 esetben történt HTML vagy SQL injection.

7. Útkeresztezési támadás.
8. Próbálgatós technológiák - nyers erő támadás.
9. Protokol manipuláció - http válasz szétválasztás.
10. Forrás kimerítés.
11. Erőforrás manipuláció.
12. Szimatoló támadás - Hálózati lehallgatás.
13. Átverés

    CVE-2020-1300 Távoli kódfuttatást okozó biztonsági rés akkor áll fenn, ha a Microsoft Windows nem tudja megfelelően kezelni a cabinet file-okat. A biztonsági rés kihasználásához a támadónak rá kell vennie a felhasználót, hogy vagy nyisson meg egy speciálisan kialakított cabinet file-t, vagy meg kell hamisítania a hálózati nyomtatót, és rá kell vennie a felhasználót egy rosszindulatú szoftver telepítésére (nyomtató-illesztőprogramnak álcázott cabinet fájl).

Mivel a firmware érintettség igen magas (közel 14%) a printerek esetében a Mitre CVE adatbázisában, ezért a mellékletben egy Nessus sérülékenység vizsgálatot mutatok be firmware frissítés előtt és után.

6.3 Üzemeltetők (belső és külső szerviz-szolgáltatók)

A nyomtatási szolgáltatás üzemeltetője tipikusan a cég rendszergazdája, esetleg külső szolgáltató által a vállalat központi telephelyéről a többi telephelyen üzemelő nyomtatóra is „rálátó” kihelyezett szakember, aki egy eszközmenedzsment rendszer segítségével látja el monitorozó/beavatkozó feladatát. Ez a szakember egyben lehet a külső szerviz-szolgáltatást koordináló személy is.

Ezek a szolgáltató cégek nem csak üzemeltetnek és karbantartanak, hanem sok esetben a rendszergazdai feladatokat is átvállalják szerződéseikben azért, hogy a nyomtatás tényleg csak egy gombnyomás legyen a felhasználók számára [50].

Az IT kockázat vizsgálatába a karbantartási időszak alatt végzett tevékenység is bele kell tartozzon. Külső helyszínre való elszállítás előtt a nyomtató (MFP) HDD kiszerelését kell kérni, emellett a hálózati kártya/SD kártya/Proxy/NFC olvasó szintén IT kockázatot jelent, – az eredeti benne marad/szervizelés során új kerül bele - a javítás után újra a cég hálózatára kerül a printer és ezeken keresztül támadhatóvá válik.

Mivel egyes nyomtatók már támogatják az Active Directory és/vagy LDAP felhasználói adatok lekérdezését és kezelését, azért a címtár kérdésére szintén ügyelni kell a szervizelés során.

Amennyiben harmadik fél nyújt olyan szolgáltatást a cégnek, amely információs rendszert érint, akkor a szolgáltatási szerződésben az információvédelemre vonatkozó előírásoknak is szerepelniük kell. A szerződésben szerepeltetjük a szolgáltatásokat és a szolgáltatási szinteket is.

Harmadik felet munkája során megbízója ellenőrizi információvédelmi szempontból is. Az ő kötelessége jelenteni az IT csoport felé, amennyiben valamilyen eltérést vesz észre.

Ha a harmadik fél a szerződésben foglaltaktól munkája során eltér, akkor az IT csoport köteles azonnal megvonni a kiadott hozzáférést és a szerződés, valamint a szolgáltatási szint elvárások szerint intézkedést kezdeményezni. A jelentési kötelezettségeket a szerződés tartalmazza.

Amennyiben harmadik fél szolgáltatása nyomán változik meg egy információs rendszer, annak dokumentációját is a harmadik fél készíti el. Ezt a kötelezettségét a szerződésbe foglaljuk bele. A rendszer átvétele nem lehetséges a szükséges dokumentáció hiányában. A fentiektől eltérni csak akkor lehet, ha a dokumentációt a cég kijelölt felelőse készíti.

Az új rendszerek átvételéért a szerződést előkészítő és/vagy aláíró kolléga felelős. Ő állapítja meg azokat a követelményeket, melyeket az átvételkor vizsgál és ezeket a szerződésben is rögzíti. Olyan rendszert átvenni, amely nem felel meg a specifikációnak, tilos. Amennyiben a cég igényei változnak, akkor a megbízónak írásban kell tájékoztatni a szerződött felet.

6.4 Felügyeletet és irányítást ellátó egyéb szerepkörök

Egy cégen belül az információbiztonság infrastruktúrájának fenntartásáért több szereplő együttműködése szükséges.

Célszerű létrehozni az informatikai biztonsággal foglalkozó menedzseri fórumot, melynek feladatai a következők:

- felülvizsgálja és jóváhagyja az információbiztonsági szabályzatot és a felelősségi köröket,
- figyelemmel kíséri a változásokat, ahogyan az információvagyon ki van téve a főbb fenyegetéseknek,
- felülvizsgálja és figyelemmel kíséri a biztonsági eseményeket,
- jóváhagyja az informatikai biztonságot fokozó kezdeményezéseket.

Tagja a gazdasági igazgató és a Compliance Officer, valamint meghívásos alapon az IT vezető is. A fórum nem tart rendes ülést, de szükség esetén bármelyik tag javaslatára összeülhet. Az informatikai biztonsági tevékenységért az IT vezető a felelős.

Az informatikai biztonsági szabályzat felülvizsgálatát meghatározott időközönként harmadik félként működő szervezettel kell elvégeztetni. Az információvédelmi felelős hangolja össze a divízióvezetőkkel az információvédelmi tevékenységet.

Az információ feldolgozó eszközök beszerzését az IT csoport végzi. A beszerzés informatikai tárgyú javaslat írásával kezdődik. Ennek helye a Javaslatok adatbázis. Az IT csoport dönt arról, hogy az információ biztonsági kérdésekben nem történik-e visszalépés. A szakmai és üzleti egyeztetések után a javaslat - az aláírási szabályok szerint - elfogadásra kerül. Ezután a beszerzést az IT csoport vagy az általa megbízott/jóváhagyott szervezeti egység végzi.

Az információ biztonsági felelősségek kiosztása az ügyvezető igazgató feladata. A szükséges felelősségek meghatározása az IT vezető feladata.

Felelősségek:

- Compliance Officer az információbiztonsági felelős, (ISO = Information Security Officer),
- Back Office divízióvezető (gazdasági igazgató) a CISO = Chief Information Security Officer,
- ügyvezető igazgatói felelősség,
- divízióvezetői felelősség az egyes részterületekért,
- adatgazdák, kockázatgazdák,
- IT vezető az informatikai rendszerért felelős,
- Back Office divízióvezető az épületért, létesítményért felelős,
- belső felülvizsgálók.

6.5 Beszállítók, külső partnerek

2021 év elején az amerikai Solarwinds kapcsán ismét górcső alá került a beszállítók IT-biztonsági megbízhatósága. Az egyre gyakoribb supply chain támadások felhívták a figyelmet arra, hogy a beszállítói lánc pajzsán lévő résekkel is foglalkozni kell [51].

„A kormányzati intézmények és nagyvállalatok által használt rendszerfelügyeleti programokat fejlesztő SolarWinds 2020 december elején jelentette be, hogy nagyon kifinomult, vélhetően állami támogatással dolgozó ismeretlenek rosszindulatú kódot helyeztek el Orion nevű programuk frissítésébe, amivel 18 ezer fontos rendszerre telepítettek kiskaput.” [52].

A közszférában a vonatkozó jogszabályi környezet egyes paraméterek tekintetében előírja, hogy miként kell vizsgálni, szűrni a beszállítót.

Minősített esetekben a felügyeleti szervek és hatóságok biztonsági előszűrést is végeznek.

Minden más esetben is ajánlott megvizsgálni a beszállítót az elérhető cégadatbázisból (cégméret, pénzügyi adatok, referenciák, a portfólióban felsorolt technológiák és a projektre delegált szakemberek), valamint a kompetenciákból és tanúsítványokból következtethetünk arra, hogy a cég vajon képes lesz-e megfelelően ellátni a feladatát.

A nagyobb vállalatoknál jellemzően létezik a beszállítók IT-biztonsági megfelelőségét vizsgáló szempontrendszer, bár ez iparág- és méretspecifikus, hogy ki mit vár el.

Az adatfeldolgozás nagyrészt már nem a saját cégen belül történik. Ezért a vezetők feladata, hogy az adatkezelés folyamata során a lehető leghatékonyabb legyen az együttműködés a szereplők között, hogy megőrizhessük a CIA-követelményeket (adataink bizalmasságát, sértetlenségét és hozzáférhetőségét), a vonatkozó szabályozói környezetnek megfeleljünk és a szerződéseinkben foglalt vállalásokat betartsuk.

7 GDPR MEGFELELŐSÉG

Javaslat az iránymutatásoknak megfelelő adatnyomtatásról:

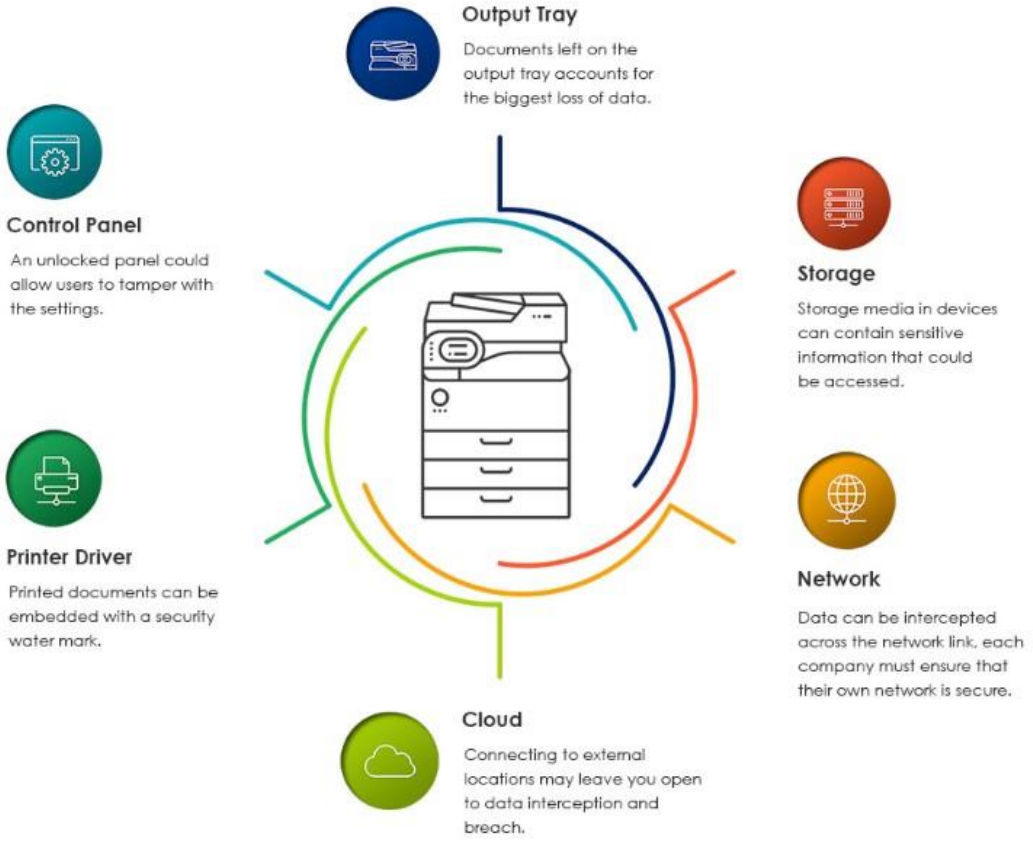
- stratégia bevezetése,
- kockázatfelmérés,
- kockázatkezelés,
- rendszeres időközönként felülvizsgálat.

1. A személyes adatok nyomtatására 2018-ban került nagyobb fókusz, amikor a GDPR szabályozást bevezeték. Amennyiben szerződéseknek, pénzügyi információknak, illetmény elszámoló lapoknak vagy a személyes adatok bármely más formájának nyomtatásáról van szó, kötelező az iránymutatásainak betartása.

A szervezeten belül az adatkezelésért felelős személy feladata, hogy minden egyes személyes adat nyomtatása az iránymutatásnak megfelelően történjen, azaz megvalósuljon:

- a multifunkciós készülékekbe való biztonságos bejelentkezés,
- a PIN-kóddal való biztonságos nyomtatás,
- a titkosított merevlemezek és a titkosított hálózatok használata.

2. Kockázatfelmérés multifunkciós nyomtató esetén



7.1. ábra: Multifunkciós készülékének lehetséges biztonsági kockázatai [53].

3. A fent ábrázolt környezet minden elemére ki kell terjednie a kockázatkezelésnek:

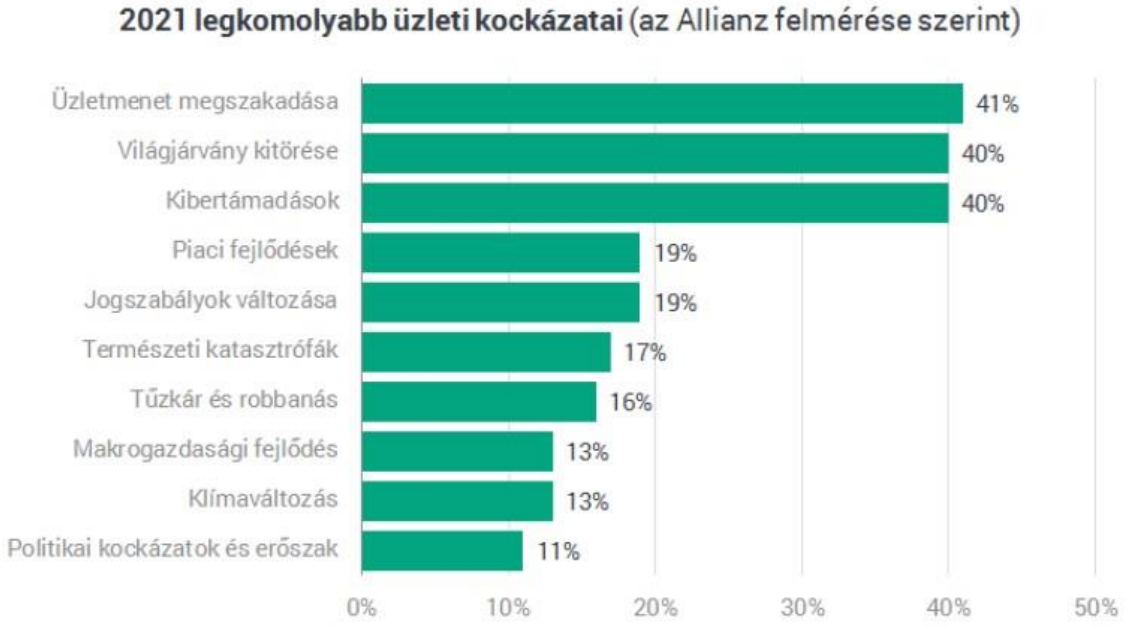
a. az alkalmazottaknak azonosítaniuk kell magukat a kimeneti tálca miatti adatvesztés elkerüléséhez, a nyomtatáskor jelen kell lennie az anyagot a nyomtatóra küldő személynek,
b. a 128 vagy 256 bites merevlemez-titkosítás mellett kiegészítő védelemként beállítható, hogy az érzékeny adatok nyomtatása után automatikusan törlésre kerüljön a nyomtatási feladat,
c. más típusoknál elérhető egy opcionális adat felülíró készlet is, ekkor a merevlemez újra formázásával további védelem biztosítható, emellett az érzékeny adatok központi tárolására is lehetőség van,
d. a printerek rendelkezzenek lezárható kezelőfelülettel, legyen megváltoztatható a rendszergazdai jelszó, és szükség legyen a felhasználói azonosítóra a készülék beállításának módosításához vagy a tárolt adatokhoz való hozzáféréshez (plusz konfigurációs lehetőség, hogy csak a jogosult rendszergazdának legyen engedélye a beállítások módosításához) IC kártya hitelesítésével csak a kártyával rendelkező alkalmazottak férjenek hozzá a készülékbeállításokhoz,
e. az adatok védelmezéséhez a printerek tanúsítványokkal rendelkeznek és IP szűrést és hálózati biztonsági protokollokat (IEEE802, IPSec, SSL) használnak,
f. ezen túlmenően a nyomtatott dokumentumok biztonsági vízjellel történő megjelölésére is lehetőség van, amennyiben további lépésekkel kívánja a nyomtatott adatok biztonságát garantálni a vállalkozás,
g. széles csatlakozási lehetőségek közül választhatnak a felhasználók (pl. One Drive, Google, SharePoint, Dropbox), mely segíti az infrastruktúra-kezelést, a mobil nyomtatást, biztosítja a dokumentum-bizalmasságot, megakadályozza a jogosulatlan hozzáférést, és a nyomtatási tevékenységeket teljes mértékben ellenőrizhetővé teszi.

4. A nyomtatókra vonatkozó részét is felül kell vizsgálni a vállalati informatikai kockázatelemzésnek a jogszabályban előírtaknak megfelelően.

8 VÁLLALATFEJLESZTÉSI JAVASLAT

„A digitalizáció egy kétélű fegyver” [54].

A koronavírus-járvány hatásaival küzdő vállalatok kockázatkezelési szakértőivel - 22 ipari ágazatban, 92 országban, közel 3000 fővel - 2021-ben készített felmérésben az Allianz feltárta a 10 legfontosabb üzleti kockázatot, amelyekre a cégvezetőknek oda kell figyelniük.



8.1. ábra: 2021 legkomolyabb üzleti kockázatai.jpg [55].

Az első helyezettek között lévő „Üzletmenet megszakadása” az elmúlt 10 évben hétszer került az első helyre, az ezüstérmes helyre „befutó” világjárványt sem kell nagyon magyarázni. A megosztott második helyezett 40%-os kibertámadások kockázata pedig éppen a járvány hatása miatt az otthonukba kényszerülő, az online térben egyre több időt digitális eszközeikkel eltöltő egyéni (és sokszor céges) tevékenységek miatt növekedett meg és vált megkerülhetetlen tényezővé, és valószínűleg marad a pandémia után is, hiszen a több távmunka lehetősége a második legkomolyabb hatása a vállalatokra a járványnak.

Munkavégzésünk során érezhetően egyre jobban támaszkodunk a digitális eszközeinkre, azonban számos előnye mellett a digitalizáció azért kétélű fegyver, mert az elmúlt években (a koronavírus járványa miatt megnövekedett home office pedig erre ráerősített) megnövekedett a kibertámadásos esetek száma.

Láthatóvá vált az elmúlt 2 évben, hogy a BCP és DRP tervekkel - és azokon belül digitális nyomtatástechnológiára vonatkozó szabályozással - rendelkező vállalatok számára kisebb kockázattal járt az újratervezett munkaszervezés, az otthoni munkavégzés kapcsán megváltozott munkakörnyezetben bekövetkezhető ilyen jellegű fenyegetettségekkel szemben is védettebnek bizonyultak.

A hibrid munkavégzés során (és itt nem az új normalitásban megjelenő home-office és office-office munkanapokra gondolok) egyaránt dolgozhattunk céges eszközökön/szoftvereken és használhattuk mi magunk és családtagjaink is céges eszközeinket magáncélokra, illetve ennek fordítottja is megtörtént, néha térben és időben sem elválasztható módon.

8.2. ábra: covid_tavmunka.jpg [56].

A szabályozás természetesen azóta lekövette a történteket, új kormányrendeletben határozták meg a veszélyhelyzet alatti távmunkavégzést, ugyanakkor nem tartalmazott ajánlásokat sem a technológia, sem a munkaszervezési követelményekre vonatkozóan, azokat továbbra is maguknak a cégeknek kell kidolgoznia.

Az gondolhatnánk, hogy a BCP terv készítése nem informatikai probléma vagy feladat, ugyanakkor be kell látnunk, hogy jól illeszthető az IT biztonság- tervezés és szervezés feladataihoz.

Az üzletmenet-folytonosság területén fel kell mérni az üzleti folyamatainkat, azok kapcsolatait, a kiszolgáló erőforrásokat.

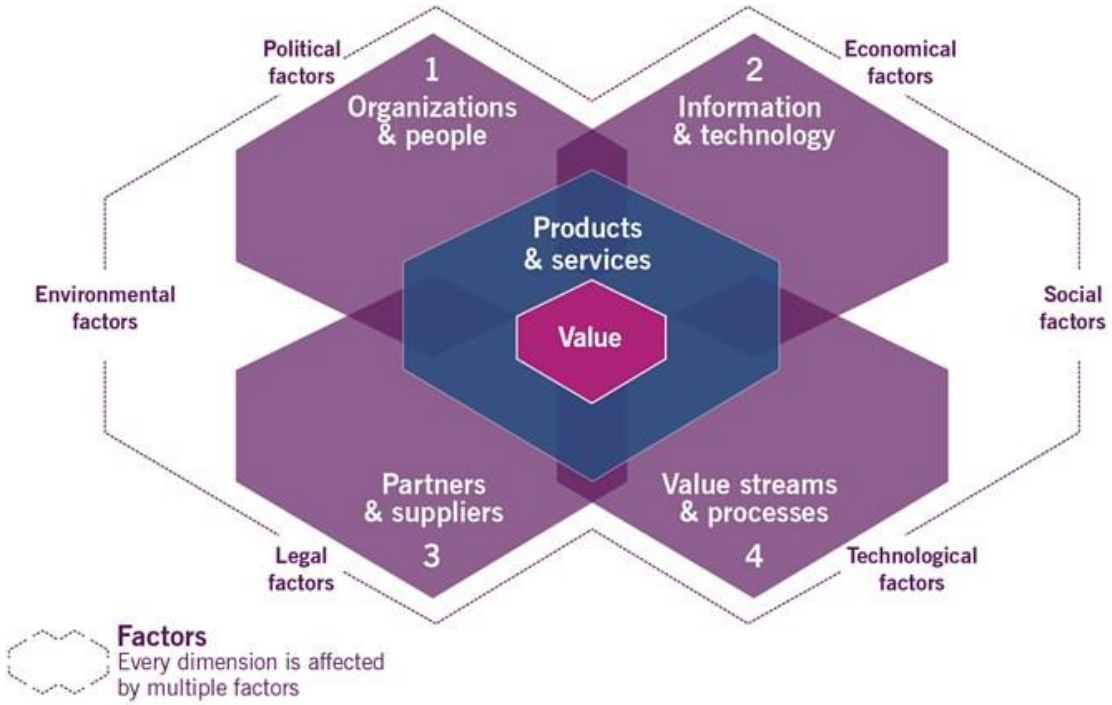
Ebben a felmérésben az üzleti oldal a releváns adatszolgáltató: meghatározója a folyamat fontosságának (kritikusságának), a folyamat/rendszer/erőforrás kiesés még tűrésen belüli időintervallumának és ezen kiesés során fellépő kár nagyságának.

Mivel a biztonság (a rendszereink összetettsége miatt) egyre inkább nem technikai, hanem szervezési kérdés, ezért valós rendszerszemlélettel kell közelíteni emiatt a komplexitás miatt a feladatokhoz. Csak a teljes körű helyzetfelméréssel lehet (egyáltalán erre esélyes) maga a

védelem is teljes körű, és remélhetjük így mind gazdaságilag, mind szakmailag a legelőnyösebb állapot elérését.

Ezért kockázat alapú védelem kialakítására törekedjünk, a megvalósítás ne csak technikai megoldásokat tartalmazzon.

A felmérésünk során kialakítandó - és ezzel az új, korábban említett szemlélettel meghatározott - hozzáállásunkat (mely szerint a biztonság egy olyan érték, amelyet termékkel és szolgáltatással teremtünk, és ezen értékteremtés során minden résztvevő a maga környezeti hatásaival együtt szerves alkotója és befolyásolója a folyamatnak) leginkább az ITIL (Information Technology Infrastructure Library) szervízmenedzsment ábrájával tudnám szemléltetni. Mivel maga az ITIL módszertana nem ismeretlen a cégek számára, ezért ezen modell és metodika segítségével könnyebben integrálhatóak az újonnan kiépítendő vagy áttervezett szolgáltatások és folyamatok rendszereinkbe.



8.3. ábra: Four dimensions of service management [57].

„Az összetettség a titkosság és biztonság ellenfele” [58].

Ahogyan a „Szoftversérülékenységek kihasználási módozatai” című tanulmányban a téma kutató rámutattak: „Nagyon nehéz megtartani a digitális formában tárolt titkokat, különösen nehéz ezt megtenni, komplex, összetett, bonyolult informatikai rendszerek esetében, ahol a számos alkalmazott komponens többszörözi a feltáratlan, kijavítatlan sérülékenységek lehetőségét, ezáltal pedig a támadási potenciált.

A digitális formában tárolt titkokat természetesen sokkal könnyebb is kimenteni a szervezet határain túlra, hiszen elég egyetlen kifelé irányuló kommunikációs szál, vagy egy aprócska fizikai adathordozó tetszőlegesen nagy tömegű adat továbbításához." Ezen meglátások érvényessége nemcsak a szoftverek, hanem a digitális nyomtatástechnológia esetén is megfontolandóak, ezért nézzük át, hogy rendszer/szervezet szintjén milyen védekezési lehetőségeink lehetnek.

Alaptétel, hogy fontos a belső, teljes működésre vonatkozó átláthatóság.

Az előzőekben már említett kockázatfelmérés során tisztázni szükséges, hogy a biztonsági politikánk tisztában van-e az üzletmenetnek/az üzleti modellnek az ilyen irányú kitettségével, és erre léteznek-e megfelelő válaszai.

Egyúttal a működési tudatosságot is mérjük fel: tisztában van-e a cégünk azzal, hogy a folyamatainak mely pontjain támadható? Ezt azonnal össze is kapcsolhatjuk egy belső ellenőrzéssel, hiszen egy jól értesült, a rendszereinket ismerő belsős ember sokszor veszélyesebb, mint az ismeretlen külső támadó. Természetesen elengedhetetlen a biztonsági mentések és a korábban kiemelt BCP/DRP tervek, valamint a bekövetkező biztonsági incidensek esetén alkalmazandó azonnali reagálási tervek elkészítése és aktualizálása.

Értekezésemben rávilágítottam a digitális nyomtatástechnológiai szolgáltatásnak a teljes informatikai környezetben betöltött szerepére és ezzel IT biztonsági kockázatára.

A korábban vázolt ITIL koncepcióban a szolgáltatás a termékkel szorosan összekapcsolódva teremt értéket, ezért tudatosítsuk újra, hogy mint végponti eszközre vonatkozóan milyen támadásokat lehet végrehajtani egy nyomtatóval a hálózaton belül [59]:

- a mai hálózati nyomtatók legtöbbje már saját memóriájában tárolja egy ideig a kinyomtatott munkákat, amely memóriából egy megfelelő eszközzel kinyerhetőek ezen anyagok, a nyomtató IP címét a default gateway címre átírva a hálózati beállításokban DoS támadás indítható,
- a kezelőfelülethez hozzáférve letilthatóak a panel gombjai/megváltoztatható a kijelzőn olvasható kiírás egy hibafeliratra, amely a felhasználót hibajavításra kéri, így egy validnak tűnő oldalról fertőzést tölthet le frissítés helyett,
- a nyitott 9100-as portjára küldött szöveget a nyomtatók kinyomtatják,
- mivel a nyomtatók felől érkező forgalmat nem szűrik a tűzfalakon, ezért az eszköz forgalmát manipulálva a nyomtatót zombiként lehet felhasználni a hálózaton egy iddle scan támadáshoz,
- ha hálózati eszközként tekintünk rá, akkor a nyomtatón sajnos működnek a klasszikus hálózati támadások, úgymint a forgalomelterelés vagy a floodolás,
- ha céleszközként nézzük, akkor sajnos a nyomtatóban nincs floodvédelem vagy tűzfal sem.

Mit tehetünk hát? Ahogyan a belső folyamataink felmérésénél is, úgy a nyomtató esetében is kezdjük az átláthatósággal.

Állítsuk össze a nyomtatók teljes listáját, feltüntetve a márkát, a modellt, az elérhető szolgáltatásokat és az aktuális konfigurációkat. Erősítsük meg a nyomtató végpontját: állítsunk le minden, a nyomtató által nem használt szolgáltatást (pl.: FTP hozzáférés)

Változtassuk meg az alapértelmezett jelszavakat.

Amennyiben a gyártó elérhetővé teszi számunkra, akkor használjunk felügyeleti eszközmenedzsment alkalmazást (vagy gyártófüggetlen, inhomogén eszközparkot is kezelni képes szoftvert), amellyel központilag monitorozhatjuk és kezelhetjük eszközeinket (akár frissítéseket is elindítva az érintett printerre).

Úgy biztosítsuk a printerrel a kapcsolatot, hogy csak a kiválasztott titkosítást biztosító felügyeleti protokollt engedélyezzük (például HTTPS vagy SSH), minden más protokollt tiltsunk le.

Konfiguráljuk úgy a sebezhetőség szkennereinket, hogy csak bizonyos üzeneteket fogadjanak el a nyomtatóktól – ezek a szkennerek sok esetben úgy vannak beállítva a „zaj”-nak a SIEM (Security Information and Event Manager) eszközökbe importálásának kivédése miatt, hogy a nyomtatókat nem is vizsgálják.

Ellenőrizzük (ha pedig nem így lenne, akkor biztosítsuk), hogy a nyomtatók ne rendelkezzenek széles körű hozzáféréssel a belső hálózat többi részéhez. A hálózati biztonság gyakorlata a nyomtatókra is vonatkozzon, azaz a hálózati szegmentálás kialakításakor nyomtatóink elérhetőségét is vegyük figyelembe. A forgalom titkosítására és a hálózati erőforrásokhoz való hozzáférés logikai szegmentálására használjunk tanúsítványokat. Ugyanakkor tartsuk azt is szem előtt, hogy ezen további biztonsági beállítások csökkenthetik a nyomtatóink funkcionalitását: például korlátozhatják a felhőalapú kezelést/felügyeletet vagy a címtárszolgáltatásokhoz való hozzáférést.

Mindezeket figyelembe véve egy olyan egyensúlyt teremthetünk meg, amelyben a nyomtatóink/digitális nyomtatástechnológiánk nagyobb biztonsága mellett megőrizhetjük az üzleti funkcionalitásunkat is [60], [61], [62], [63], [64], [65].

ÖSSZEGZÉS

Szakdolgozatomban olyan témakör információbiztonsági vizsgálatát kíséreltem meg, amely a számítástechnikai eszközök evolúcióját követő, új formában megjelenő nyomtatási technológiák és dokumentumkezelési folyamatok mindennapjainkra kiható területét célozza meg.

Hipotézisem szerint a teljes dokumentumkezelés folyamatában részt vevők - emberi és számítástechnikai szereplők - egyaránt IT kockázatot jelenthetnek a cégek működésében, hiszen új platformokon, applikációkon keresztül készítjük és tároljuk dokumentumainkat.

Értekezésem 1. fejezetében ismertettem a problémafelvetés hátterét, miszerint miért is jelenthet akár már egy nyomtató is komoly biztonsági kockázatot a cég életében.

A következő fejezetben röviden áttekintettem azon biztonsági szabványokat, amelyekben először specifikálták egyes gyártók, később független vizsgálólaboratóriumok IT biztonsági elvárásaikat ezen termékekre.

A 3. fejezetben a különböző nyomtatási technológiákat ismertettem, mely fejezet végén rátértem a vizsgált témában leginkább érintett lézernyomtatásra.

Ezt követően bemutattam azon dokumentumkezelési folyamatokat, amelyek során létrehozzuk, kezeljük, digitalizáljuk, tároljuk és keressük a dokumentumokat.

A dolgozat 5. fejezetében a rendszerelemek gyenge pontjait vizsgáltam, melyhez az ISO 27001 információbiztonsági szabványrendszert, mint értelmezési keretrendszert vettem alapul.

Ezután az emberi tényezőt tettem részletesebb vizsgálat tárgyává, külön kitérve a klasszikus értelmezésen - az emberi erőforrás az IT-ban a Felhasználókat és az Adminisztrátorokat jelenti - túli szereplőkre (Fejlesztők, Tesztelők, Üzemeltetők, Felügyeletet és irányítást ellátó egyéb szerepkörök, Beszállítók, külső partnerek).

A 7. fejezetben a nyomtatók GDPR megfelelőségét taglaltam, mely során az adatkezelésért felelős személy kockázatfelmérését és kockázatkezelését mutattam be multifunkciós printerekre vonatkozóan.

Végül az utolsó fejezetben a korábbi vizsgálatok eredményét felhasználó vállalatfejlesztési javaslatot tettem.

A mellékletben bemutattam egy printer firmware frissítéséhez kapcsolódó Nessus sérülékenységvizsgálat eredményét, mely rámutatott arra, hogy a vállalatfejlesztési javaslatok között felsorolt biztonsági beállítások tovább csökkentik a kockázatot.

Konklúzió

A vizsgált területek rendszerszintű kezelésére olyan információbiztonsági politika kialakítása szükséges, amely az üzleti követelményekkel és a vonatkozó törvényekkel és rendeletekkel összhangban irányítási útmutatást és támogatást nyújt az információbiztonsághoz a szervezetnek, valamint a szervezet minden tagjának, és partnerei számára is átlátható, következetes és rendszeresen felülvizsgált a fenntarthatósása, megfelelősége és a hatékonysága érdekében.

Az adatfeldolgozás nagy része már a digitális nyomtatástechnológiához kapcsolódóan történik. Kiemelt fontosságú, hogy a feldolgozás folyamata során a lehető leghatékonyabb legyen az együttműködés a szereplők között, melynek célja megőrizni a CIA-követelményeket (adataink bizalmasságát, sértetlenségét és rendelkezésre állását), a vonatkozó szabályozói környezetnek megfelelni és a szerződéseinkben foglalt vállalásokat betartani.

Mindezeket figyelembe véve egy olyan egyensúlyt teremthetünk meg, amelyben a nyomtatóink/digitális nyomtatástechnológiánk nagyobb biztonsága mellett megőrizhetjük üzleti funkcionalitásunkat is.

SUMMARY

In my dissertation, I have attempted to examine the topic from an information security, which aims at the everyday field of printing technologies and document management processes following the evolution of computer tools.

According to my hypothesis, those involved in the entire document management process - both human and IT - can pose an IT risk to the operation of companies, as we create and store our documents through new platforms and applications.

In Chapter 1 of my dissertation, I described the background to the problem of why a printer can pose a serious security risk in the life of a company.

In the next section, I briefly reviewed the security standards in which the IT security requirements for these products were first specified by some manufacturers and later by independent testing laboratories.

In Chapter 3, I described the different printing technologies, at the end of which I turned to laser printing, which is the most relevant topic.

I then introduced the document management processes in which we create, manage, digitize, store, and retrieve documents.

In Chapter 5 of the dissertation, I examined the weak points of the system components, for which I used the ISO 27001 information security standard system as an interpretation framework.

I then examined the human factor in more detail, with a special focus on actors beyond the classical interpretation - human resources in IT means Users and Administrators (Developers, Testers, Operators, Other roles in supervision and control, Suppliers, external partners).

In Chapter 7, I discussed the GDPR compliance of printers, presenting the risk assessment and risk management of the data controller for multifunction printers.

Finally, in the last chapter, I made a company development proposal using the results of previous studies.

In the appendix, I presented the results of a Nessus vulnerability scan related to a printer firmware update that pointed out that the security settings listed in the enterprise development recommendations further reduce the risk.

Conclusion

The systemic management of the areas under review requires the development of an information security policy that provides management guidance and support for information security to the organisation, in line with business requirements and relevant laws and regulations, and to all members of the organisation and its partners, in a transparent, consistent and regularly reviewed manner to ensure its sustainability, adequacy and effectiveness.

Much of the data processing is now done in conjunction with digital printing technology. It is of paramount importance that the processing process is as collaborative as possible between the actors involved, with the aim of preserving CIA requirements (confidentiality, integrity and availability of our data), complying with the relevant regulatory environment and meeting our contractual commitments.

Taking all of this into account, we can strike a balance between maintaining greater security for our printers/digital printing technology and preserving our business functionality.

IRODALOMJEGYZÉK

[1] Piac&Profit: Egy nyomtató is komoly biztonsági kockázatot jelenthet, (https://piacesprofit.hu/infokom/egy-nyomtato-is-komoly-biztonsagi-kockazatot-jelenthet), utoljára megtekintve: 2022. 04. 23

[2] PC World: Xerox Phaser 790DP – Megállja a helyét, (https://computerworld.hu/tech/xerox-phaser-790dp-8211-megallja-a-helyet-20010225-45590.html), utoljára megtekintve: 2022. 04. 23

[3] PC World: Xerox Phaser 790DP nyomtató, (https://computerworld.hu/tech/xerox-phaser-790dp-8211-megallja-a-helyet-20010225-45590.html), utoljára megtekintve: 2022. 04. 23

[4] Boda, B., Bodrogközi, L., Gál, Z., Illés, P.: SZOFTVERTESZTELÉS A GYAKORLATBAN, (https://gyires.inf.unideb.hu/teszt/Szoftverteszteles_a_gyakorlatban.pdf), utoljára megtekintve: 2022. 04. 23

[5] Müller, J., Mladenov, V., Somorovsky, J.: SoK: Exploiting Network Printers, (https://www.nds.ruhr-uni-bochum.de/media/ei/veroeffentlichungen/2018/07/11/printer-security.pdf), utoljára megtekintve: 2022. 04. 23

[6] Crenshaw, A.: Hacking Network Printers, (http://www.irongeek.com/i.php?page=security/networkprinterhacking), utoljára megtekintve: 2022. 04. 23

[7] Void, J.: Printer Exploitation Toolkit, (https://github.com/RUB-NDS/PRET), utoljára megtekintve: 2022. 04. 23

[8] Kovács, E.: Ransomware Operators Claim They Hacked Printing Giant Xerox, (https://www.securityweek.com/ransomware-operators-claim-they-hacked-printing-giant-xerox), utoljára megtekintve: 2022. 04. 23

[9] Sharp: Hálózati biztonság, (https://www.sharp.hu/cps/rde/xchg/hu/hs.xsl/-/html/network-security.htm), utoljára megtekintve: 2022. 04. 23

[10] Common Criteria Recognition Arrangement (CCRA), (https://www.cybersecurity.my/mycc/mutual.html), utoljára megtekintve: 2022. 04. 23

[11] Galambos, S.: Nyomtató kisokos, (https://www.gazdasagosnyomtato.hu/nyomtato-kisokos/), utoljára megtekintve: 2022. 04. 23

[12] Rhenus Office System Hungary Kft.: Az irodai dokumentumkezelés és iratmegsemmisítés alapjai 6 lépésben, (https://www.iratmentes.hu/hirek/az-irodai-dokumentumkezeles-es-iratmegsemmisites-alapjai-6-lepesben/40), utoljára megtekintve: 2022. 04. 23

[13] DMS One Zrt: Dokumentumkezelés, (https://workflowrendszer.hu/dokumentumkezeles), utoljára megtekintve: 2022. 04. 23

[14] Brown, D.: The GDPR Blind Spot: Why Printers Represent a Weakness in Compliance, (https://objects.icecat.biz/objects/mmo_62201076_1538702204_5475_22958.pdf), utoljára megtekintve: 2022. 04. 23

[15] Canadian Centre for Cyber Security: Common Criteria Certificate Ricoh IM C2000, (https://www.commoncriteriaportal.org/files/epfiles/383-4-486%20CT%20v1.0.pdf), utoljára megtekintve: 2022. 04. 23

[16] Canadian Centre for Cyber Security: Common Criteria Certificate Report Ricoh IM C2000, (https://www.commoncriteriaportal.org/files/epfiles/383-4-486%20CR%20v1.0.pdf), utoljára megtekintve: 2022. 04. 23

[17] Canadian Centre for Cyber Security: Security Target for Ricoh IM C2000, (http://www.commoncriteriaportal.org/files/epfiles/383-4-486%20ST%20v1.0.pdf), utoljára megtekintve: 2022. 04. 23

[18] Ricoh Europe Academy: MP C3003-6003 Service master update training-online presentation, (https://en.ppt-online.org/659784), utoljára megtekintve: 2022. 04. 23

[19] Copier World: How to scan to a USB drive from a Ricoh Copier, (https://www.copierworld.my/ricoh-copier/how-to-scan-to-a-usb-drive-from-a-ricoh-copier/), utoljára megtekintve: 2022. 04. 23

[20] Ricoh Europe Academy: Service Manual MET-MF3, (http://195.50.207.134/Tehdoc/0120/copier/imc4500/service.man/met-mf3_fsm_en_final_141218.pdf), utoljára megtekintve: 2022. 04. 23

[21] Ricoh Europe Academy: Service Manual MET-MF3, (http://195.50.207.134/Tehdoc/0120/copier/imc4500/service.man/met-mf3_fsm_en_final_141218.pdf), utoljára megtekintve: 2022. 04. 23

[22] Canadian Centre for Cyber Security: Security Target for Ricoh IM C2000, (http://www.commoncriteriaportal.org/files/epfiles/383-4-486%20ST%20v1.0.pdf), utoljára megtekintve: 2022. 04. 23

[23] Ricoh Europe Academy: Privilege Escalation Vulnerability for Ricoh Drivers, (http://195.50.207.134/Tehdoc/0120/copier/imc4500/service.man/met-mf3_fsm_en_final_141218.pdf), utoljára megtekintve: 2022. 04. 23

[24] Ricoh Europe Academy: Privilege Escalation Vulnerability for Ricoh Drivers, (http://195.50.207.134/Tehdoc/0120/copier/imc4500/service.man/met-mf3_fsm_en_final_141218.pdf), utoljára megtekintve: 2022. 04. 23

[25] Iron Mountain: Workflow Automation szolgáltatás, (https://www.ironmountain.com/hu/resources/data-sheets-and-brochures/i/iron-mountain-workflow-automation), utoljára megtekintve: 2022. 04. 23

[26] Iron Mountain: Tudástár, (https://www.ironmountain.com/hu/resources), utoljára megtekintve: 2022. 04. 23

[27] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[28] Kristóf, Cs.: Így is tanulható a biztonságos szoftverfejlesztés, (https://biztonsagportal.hu/igy-is-tanulhato-a-biztonsagos-szoftverfejlesztes.html), utoljára megtekintve: 2022. 04. 23

[29] Bedi, P.: Számítógép hálózatok üzemeltetése - Felhasználói környezet kialakítása: Nyomtatás hálózatban, (https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/7_1173_033_101030.pdf), utoljára megtekintve: 2022. 04. 23

[30] Bedi, P.: Számítógép hálózatok üzemeltetése - Felhasználói környezet kialakítása: Nyomtatás hálózatban, (https://www.nive.hu/Downloads/Szakkepzesi_dokumentumok/Bemeneti_kompetenciak_meresi_ertekelesi_eszkozrendszerenek_kialakitasa/7_1173_033_101030.pdf), utoljára megtekintve: 2022. 04. 23

[31] Manning, K.: How to Improve Old Business Processes withWorkflow Analysis, (https://www.processmaker.com/blog/how-to-improve-old-business-processes-with-workflow-analysis/), utoljára megtekintve: 2022. 04. 23

[32] NTT DATA: A folyamatmenedzsment keretrendszer, (https://nttdata-solutions.com/hu/szolgaltatasok/uzleti-folyamatmenedzsment/), utoljára megtekintve: 2022. 04. 23

[33] Piac&Profit: Üzleti folyamatok: ott vannak minden vállalkozásban, (https://piacesprofit.hu/kkv_cegblog/uzleti-folyamatok-ott-vannakminden-vallalkozasban/), utoljára megtekintve: 2022. 04. 23

[34] Szöllősi, S.: Bevezetés a három betűs rövidítések világába, (https://www.slideserve.com/amina/bevezet-s-a-h-rom-bet-s-r-vid-t-sek-vil-g-ba), utoljára megtekintve: 2022. 04. 23

[35] MITRE: CVE-2021-33945, (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33945), utoljára megtekintve: 2022. 04. 23

[36] Johnson, J.: Common IT vulnerabilites and exposures worldwide 2009-2021, (https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/), utoljára megtekintve: 2022. 04. 23

[37] Módly, M..: Hogyan akadályoz meg egy fejlesztő 14 karakterrel egy hackertámadást, (https://www.youtube.com/watch?v=uLpKmbXefXw), utoljára megtekintve: 2022. 04. 23

[38] Módly, M..: Hogyan akadályoz meg egy fejlesztő 14 karakterrel egy hackertámadást, (https://www.youtube.com/watch?v=uLpKmbXefXw), utoljára megtekintve: 2022. 04. 23

[39] Microsoft Documentation: Microsoft Security Development Lifecycle, (https://docs.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle), utoljára megtekintve: 2022. 04. 23

[40] Microsoft Documentation: Microsoft Security Development Lifecycle, (https://docs.microsoft.com/en-us/windows/security/threat-protection/msft-security-dev-lifecycle), utoljára megtekintve: 2022. 04. 23

[41] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[42] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[43] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[44] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[45] Futóné Papp, D.: Biztonságos szoftverfejlesztés, (https://vik.wiki/images/8/82/Kodesit_eloadas_2020_2.pdf), utoljára megtekintve: 2022. 04. 23

[46] Boda, B., Bodrogközi, L., Gál, Z., Illés, P.: SZOFTVERTESZTELÉS A GYAKORLATBAN, (https://gyires.inf.unideb.hu/teszt/Szoftverteszteles_a_gyakorlatban.pdf), utoljára megtekintve: 2022. 04. 23

[47] Ficsor, L., Dr. Kovács, L., Krizsán, Z., Dr. Kusper, G.: Szoftvertesztelés, (https://dtk.tankonyvtar.hu/bitstream/handle/123456789/13039/0046_szoftverteszteles.pdf?sequence=2&isAllowed=y), utoljára megtekintve: 2022. 04. 23

[48] Dr. Csertán, Gy., Frits, M.: Rendszerfejlesztés és tesztelés, (https://dcs.uni-pannon.hu/files/docs/users/csertangyorgy/rfandt/01.pdf), utoljára megtekintve: 2022. 04. 23

[49] ProofIT: A nem funkcionális szoftvertesztelés típusai, (https://proofit.hu/blog/a-nem-funkcionalis-szoftver-teszteles-tipusai/), utoljára megtekintve: 2022. 04. 23

[50] Bodnár, Á.: Menedzselt nyomtatási szolgáltatás a HP-tól, (https://www.hwsw.hu/hirek/42969/hewlett-packard-hp-managed-enterprise-services-nyomtatas-menedzselt-szolgaltatas-kiszervezes-outsourcing.html - Menedzselt nyomtatási szolgáltatás a HP-tól), utoljára megtekintve: 2022. 04. 23

[51] Kiss, F.: A beszállítót senki sem vizsgálja?, (https://itbusiness.hu/technology/aktualis_lapszam/center/a-beszallitot-senki-sem-vizsgalja), utoljára megtekintve: 2022. 04. 23

[52] Papdi-Pécskői, V.: SolarWinds-botrány: a szálak Közép-Európába vezetnek?, (https://index.hu/techtud/2021/01/04/solarwinds-botrany_a_szalak_kozep-europaba_vezetnek),utoljára megtekintve: 2022. 04. 23

[53] OKI EUROPE: Are you ready for GDPR? How secure is your MFP, (https://www.oki.com/uk/printing/gdpr/how-secure-is-your-mfp/index.html),utoljára megtekintve: 2022. 04. 23

[54] Mohos, K., Faluvégi, B.: Ez a koronavírus egyik legkárosabb következménye – így tudsz rajta pénzt keresni!, (https://www.portfolio.hu/befektetes/20210702/ez-a-koronavirus-egyik-legkarosabb-kovetkezmenye-igy-tudsz-rajta-penzt-keresni-490866),utoljára megtekintve: 2022. 04. 23

[55] Portfolio: Ezektől a veszélyektől rettegnek most a legjobban a világon, (https://www.portfolio.hu/uzlet/20210621/ezektol-a-veszelyektol-rettegnek-most-a-legjobban-a-vilagon-488960#),utoljára megtekintve: 2022. 04. 23

[56] Computerworld: Jó a home office, de a jelek szerint lassú és nem hatékony, (https://computerworld.hu/tech/jo-a-home-office-de-a-jelek-szerint-lassu-es-nem-hatekony-281845.html), utoljára megtekintve: 2022. 04. 23

[57] Stewart, M.: What are the Four Dimensions of ITIL4?, (https://info.axiossystems.com/blog/what-are-the-four-dimensions-of-itil-4), utoljára megtekintve: 2022. 04. 23

[58] Dr. Horváth, A., Erdősi, P. M., Dr. Kiss, F., Benkő, Zs., Szanyi, I., Török, M.: A szoftver sérülékenységek kihasználási módozati - Informatikai támadások, támadók és biztonság 2013-2016, (http://real.mtak.hu/93401/1/dr.horvath_a.E28093_erdosi_p.m.E28093_dr.kiss_f.E28093_benko_zs.E28093_szanyi_i.E28093_torok_m._a_szoftver_serulekenysegek_kihasznalasi_modozatai.informatikai_tamadasok_tamadok_es_biztonsag_2013E280932016.pdf), utoljára megtekintve: 2022. 04. 23

[59] Kovács, Zs.: Nyomtatók hackelése, (http://secblog.stratis.hu/2009/04/nyomtatok-hackelese.html), utoljára megtekintve: 2022. 04. 23

[60] Bulls Eye: How to Hack and Exploit Printers in Seconds, (https://hackingpassion.com/how-to-hack-and-exploit-printers-in-seconds/), utoljára megtekintve: 2022. 04. 23

[61] Cartridge Word: Hackers Are Targeting Printers - How to Be Protected from Cyber Attacks, (https://www.cartridgeworldqc.com/blog/hackers-are-targeting-printers-how-to-be-protected-from-cyber-attacks), utoljára megtekintve: 2022. 04. 23

[62] Cybernews Team: We hijacked 28,000 unsecured printers to raise awareness of printer security issues, (https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/), utoljára megtekintve: 2022. 04. 23

[63] S&T: Komplex információbiztonsági megoldások az S&T támogatásával, (https://snt.hu/megoldasok/informaciobiztonsag)/, utoljára megtekintve: 2022. 04. 23

[64] Help Net Security: 150+ HP multifunction printers open to attack (CVE-2021-39237, CVE-2021-39238), (https://www.helpnetsecurity.com/2021/11/30/cve-2021-39237-cve-2021-39238/), utoljára megtekintve: 2022. 04. 23

[65] Bodó, A. P., Oroszi, E. D., Sági, G. J., Szappanos, G., Szarvák, A., Zámbó, N.: Célzott kibertámadások, Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2018, (https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12820), utoljára megtekintve: 2022. 04. 23

ÁBRAJEGYZÉK

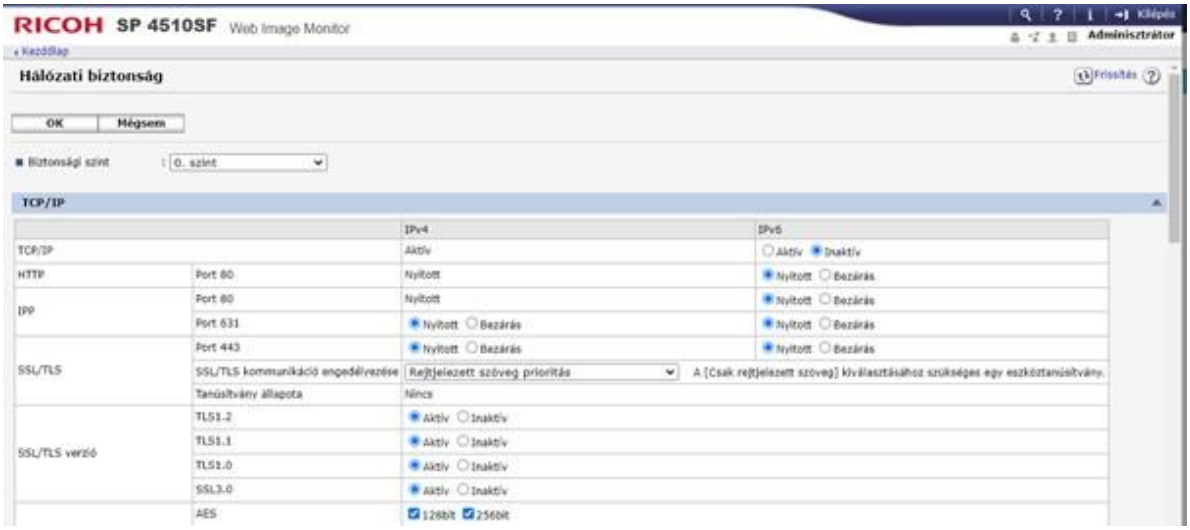
MELLÉKLETEK

Az üzemeltetési környezetben leggyakrabban üzemszerűen (egy új verzió megjelenésekor akár már a háttérben letöltve automatikusan is - Automation Remote Firmware Update process) vagy hibajavítási célzattal firmware frissítést végzünk.

A https://cve.mitre.org website-on létrehozott és karbantartott nyilvános adatbázisban a 232db printerre vonatkozó, már felfedezett sérülékenység közül 32 esetben jegyeztek fel firmware érintettséget, így célszerű izolált tesztkörnyezetben egy sérülékenységvizsgáló szoftver futtatása a frissítés előtti és utáni állapotban.

Ilyen sérülékenységvizsgálatot végeztem el Nessus szoftverrel egy Ricoh SP4510SF típusú nyomtatón.

Level0 - System/Copy 1.05

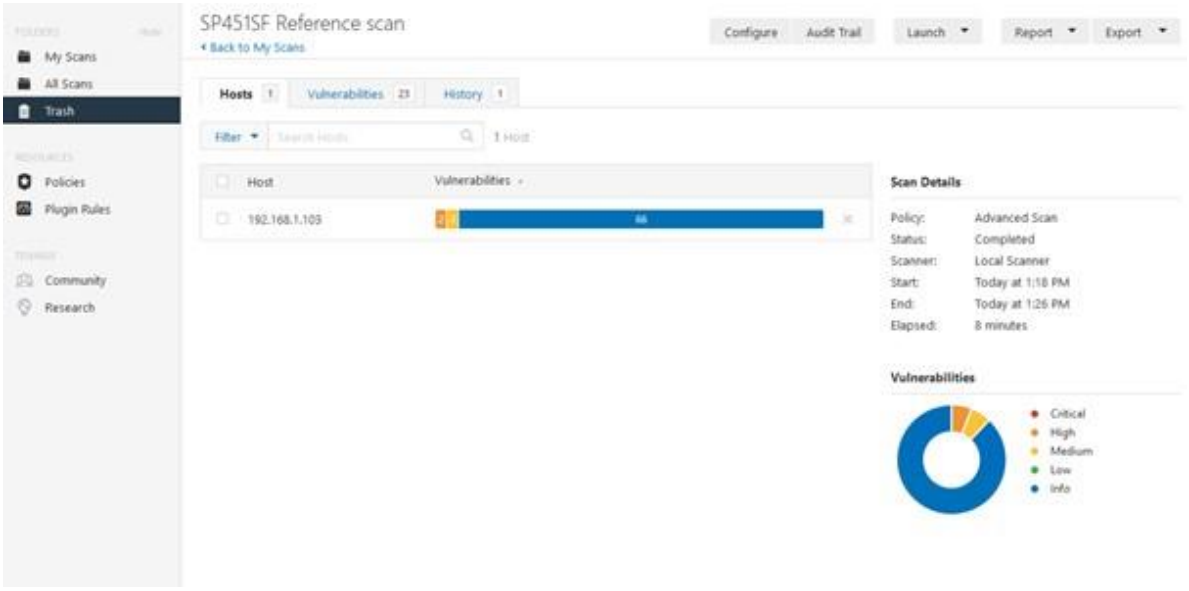


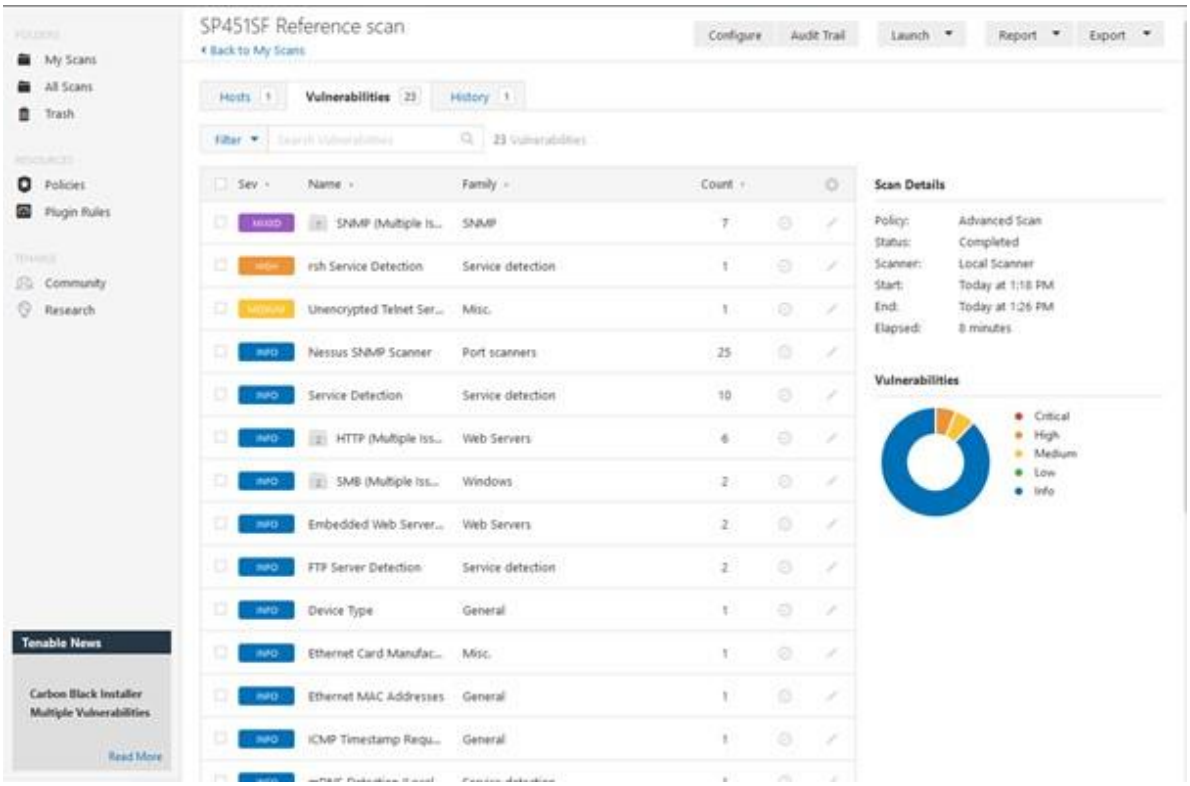
RICOH SP 4510SF Web Image Monitor

Kezdőlap

Firmware verzió

Modul neve	Verzió	Alkatrész száma
System/Copy	1.05	M1605770D
Network Support	13.21	M1605753D
Fax	05.00.00	M1605776D
RemoteFax	05.00.00	M1605777D
Scanner	01.05	M1605779D
Web Support	1.07	M1605750D
Web Uapl	1.04	M1605751C
animation	1.01	M1605752A
NetworkDocBox	1.01	M1605754C
Printer	1.05	M1605756D
RPCS	3.14.3	M1605758C
Font EXP	1.00	D1475581
PCL	1.05	M1605759D
PCL Font	1.14	M1095273
PS3	1.00	M1605760A
PDF	1.02	M1605762C
PS3 Font	1.11	D6415763A
Data Erase Onb	1.03m	D3775913
GWFCU3.8-4(WW)	03.00.00	M1605778B
PowerSaving Sys	F.19	M1605775E
Engine	1.19:09	M1605550F
OpePanel	1.07	M1605740D





nessus

Report generated by Nessus™

SP451SF Reference scan

Tue, 02 Feb 2021 13:18:15 Central Europe Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Collapse All | Expand All

192.168.1.103

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	2	2	0	66

Scan Information

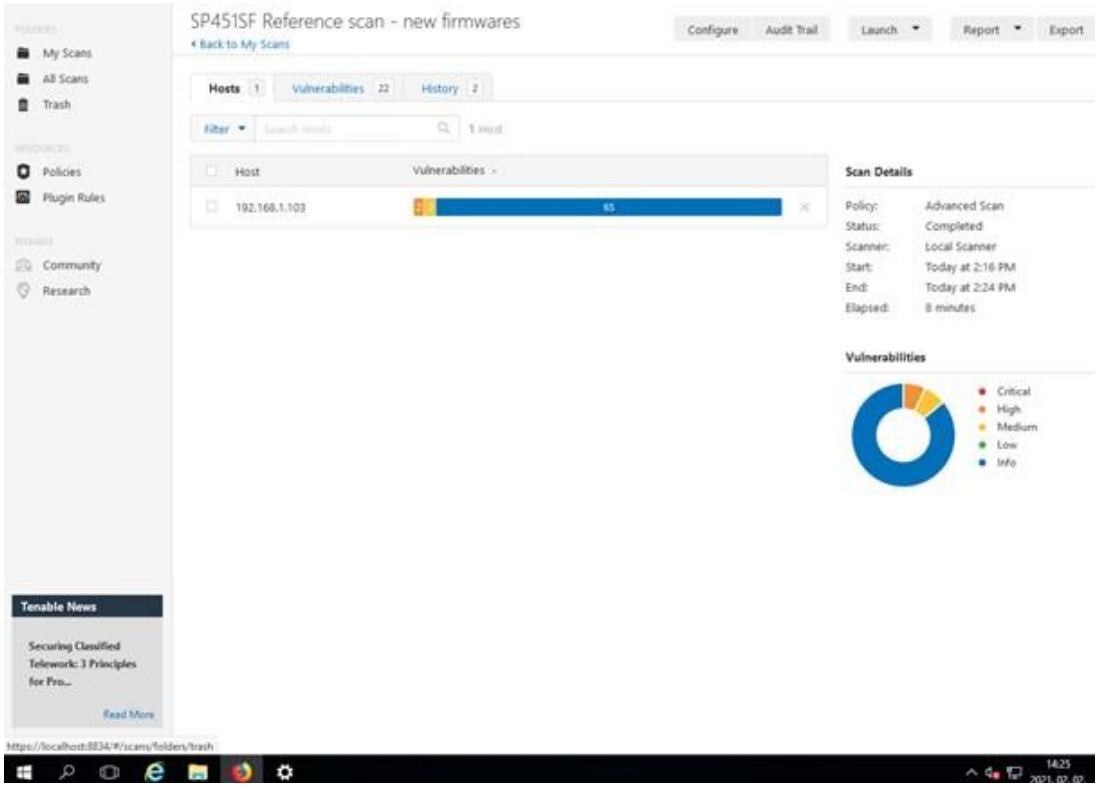
Firmware frissítés után - System/Copy 1.21

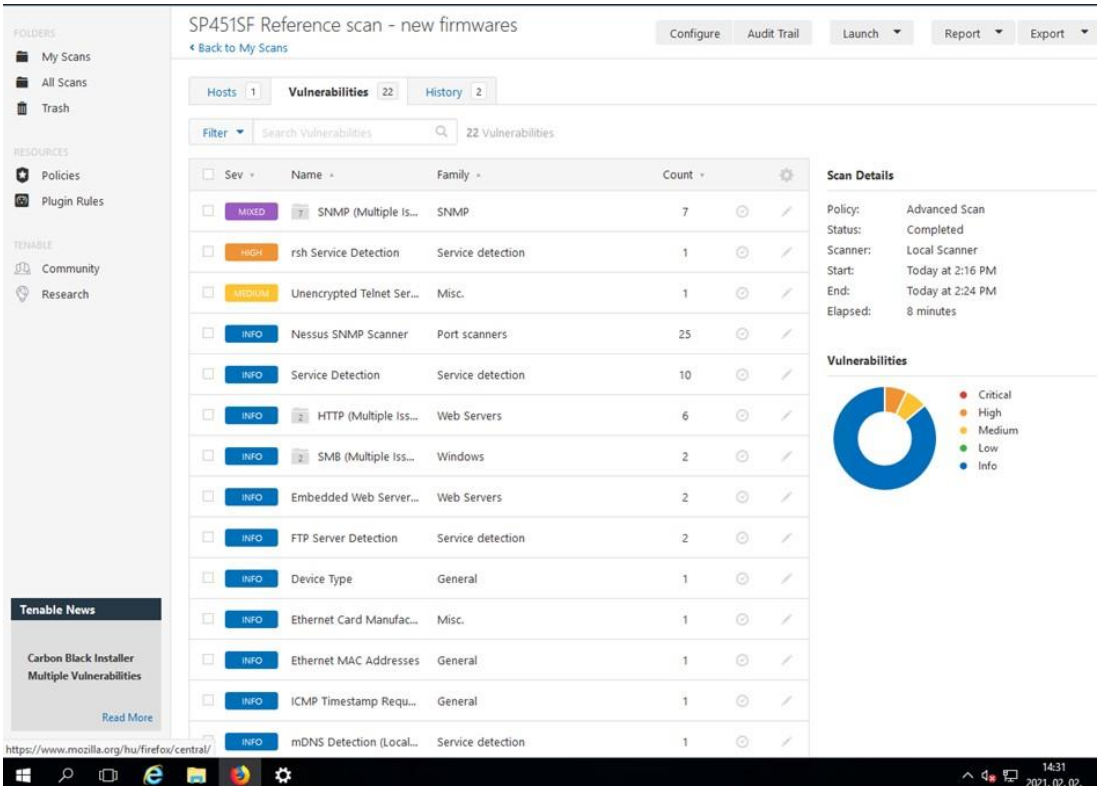
RICOH SP 4510SF Web Image Monitor

Kezdőlap

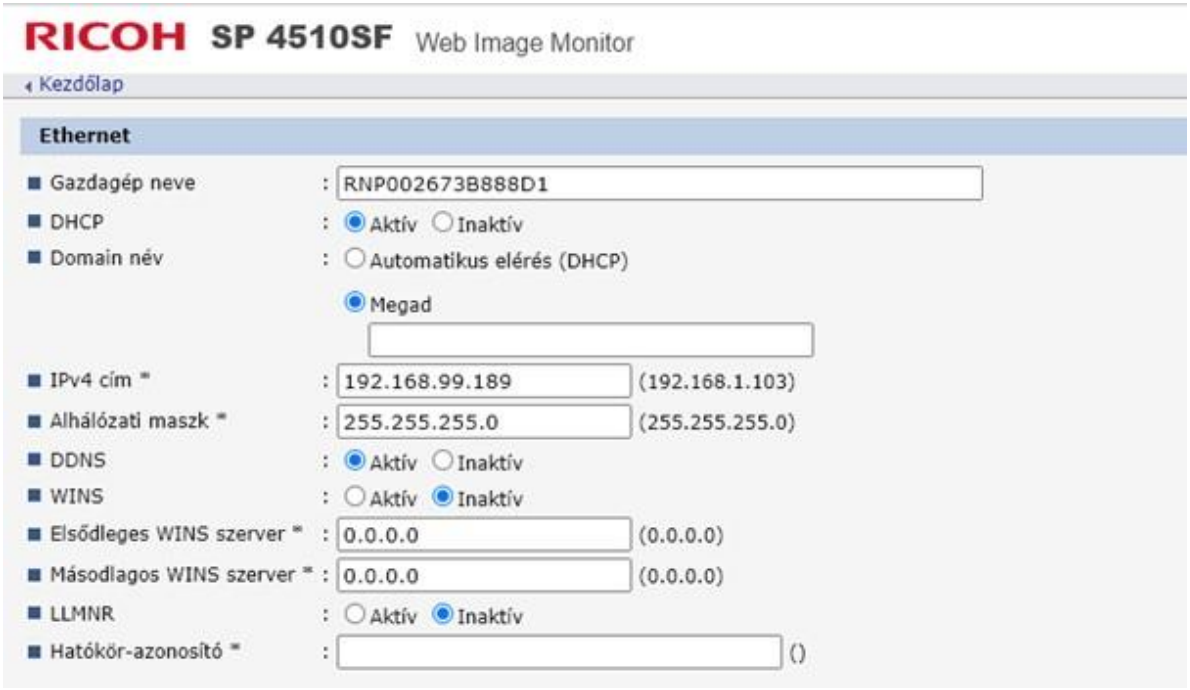
Firmware verzió

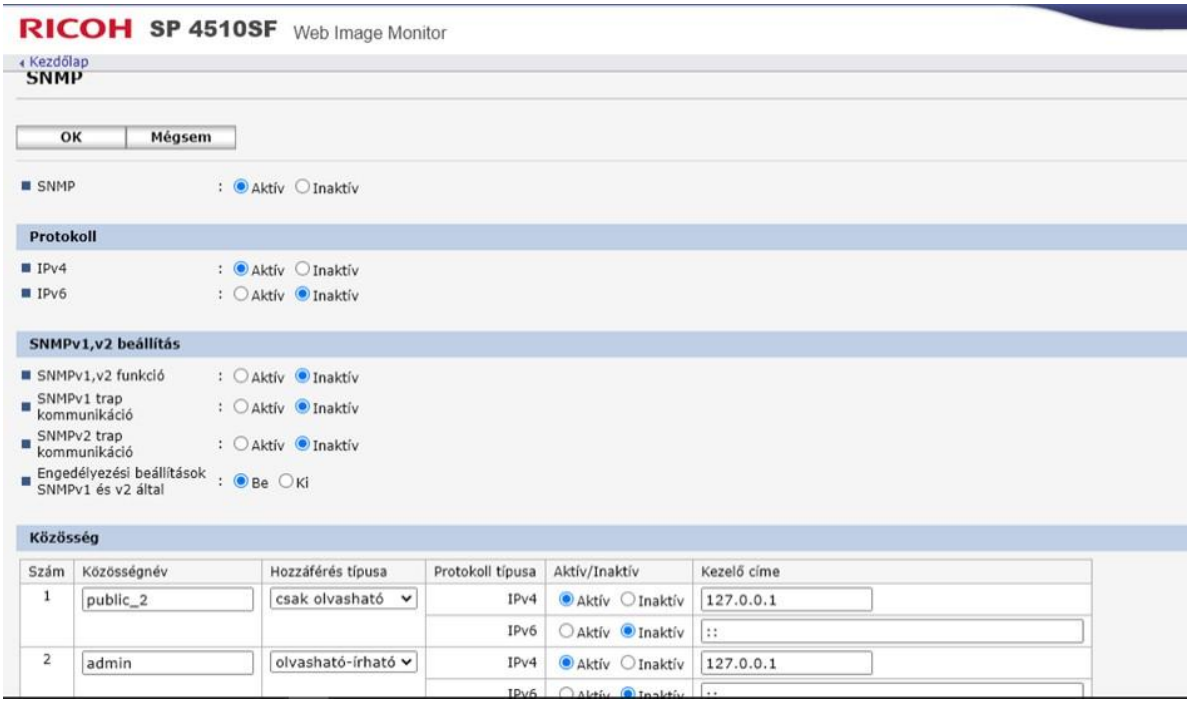
Modul neve	Verzió	Alkatrész száma
System/Copy	1.21	M1605770V
Network Support	13.31	M1605753P
Fax	09.00.00	M1605776H
RemoteFax	07.00.00	M1605777F
Scanner	01.10	M1605779J
Web Support	1.16	M1605750N
Web Uapl	1.07	M1605751F
animation	1.01	M1605752A
NetworkDocBox	1.03	M1605754E
Printer	1.11	M1605756K
RPCS	3.14.5	M1605758E
Font EXP	1.00	D1475581
PCL	1.12	M1605759L
PCL Font	1.14	M1095273
PS3	1.00	M1605760A
PDF	1.03	M1605762D
PS3 Font	1.11	D6415763A
Data Erase Onb	1.03m	D3775913
GWFCU3.8-4(WW)	03.00.00	M1605778B
PowerSaving Sys	F.19	M1605775E
Engine	1.37:09	M1605550V
OpePanel	1.14	M1605740L

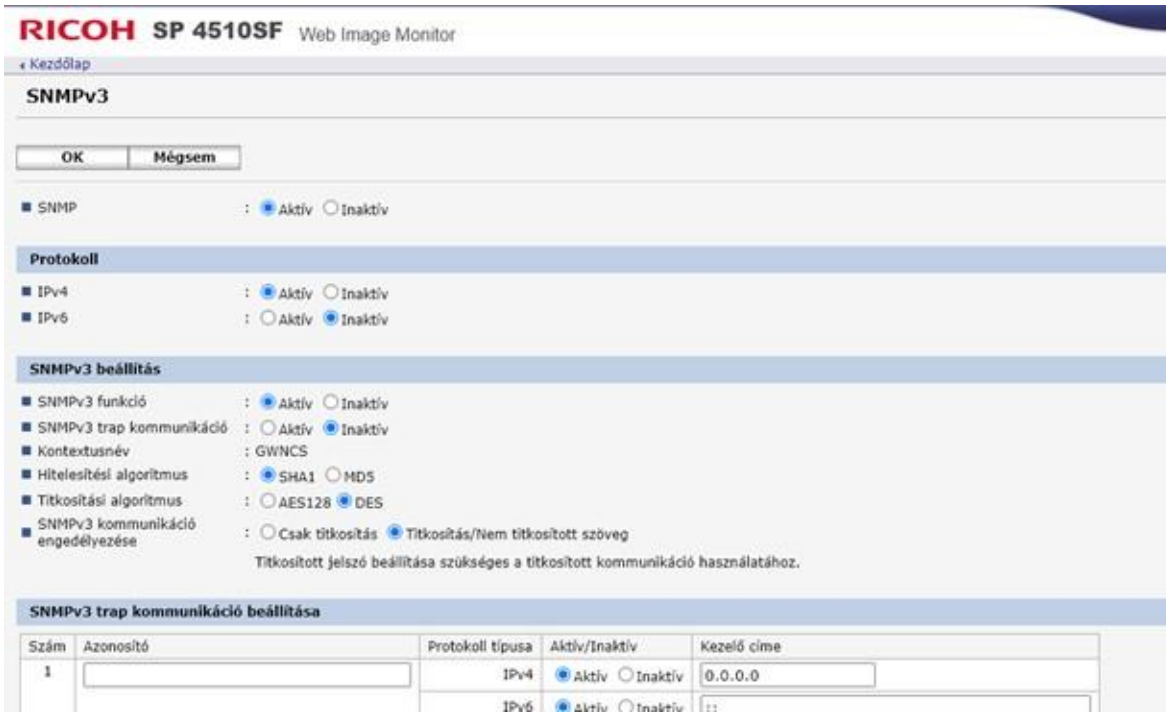

SP451SF Reference scan - new firmwares
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Hosts 1
Vulnerabilities 22
History 2
Filter
1 Host
Host
Vulnerabilities
192.168.1.103
65
Scan Details
Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 2:16 PM
End: Today at 2:24 PM
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Securing Classified Telework: 3 Principles for Pro...
Read More
14:25

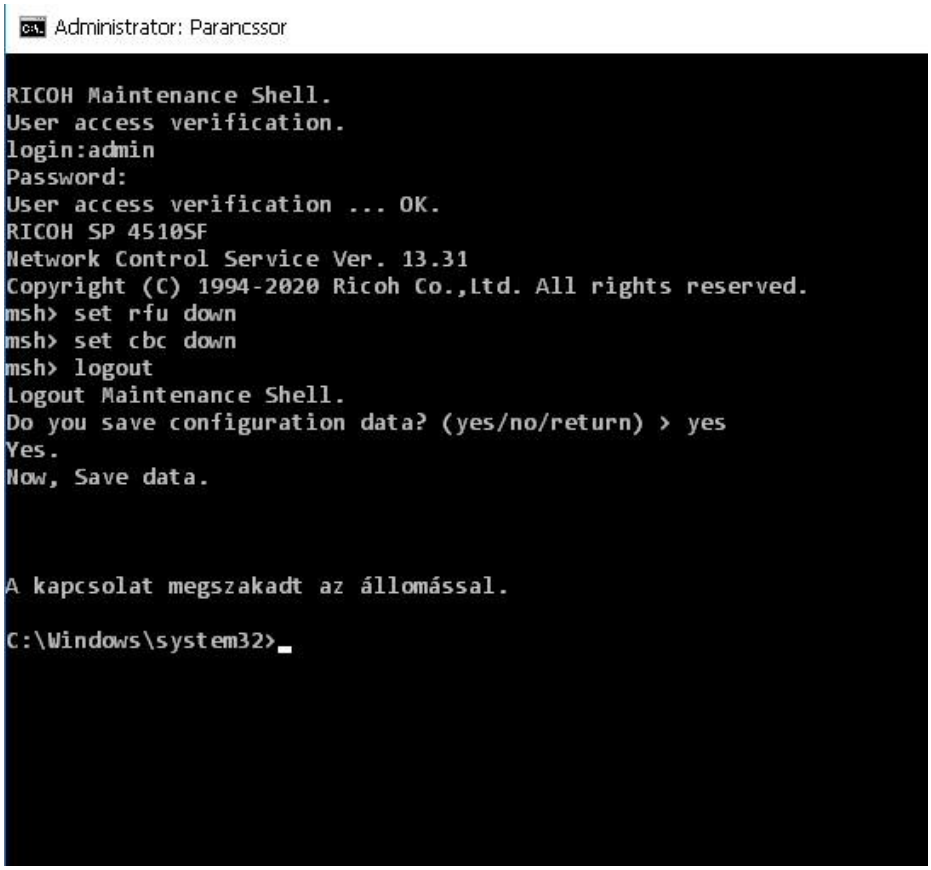

SP451SF Reference scan - new firmwares
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Hosts 1
Vulnerabilities 22
History 2
Filter
Search Vulnerabilities
22 Vulnerabilities
Sev
Name
Family
Count
MIXED 7 SNMP (Multiple Is... SNMP 7
HIGH rsh Service Detection Service detection 1
MEDIUM Unencrypted Telnet Ser... Misc. 1
INFO Nessus SNMP Scanner Port scanners 25
INFO Service Detection Service detection 10
INFO 2 HTTP (Multiple Iss... Web Servers 6
INFO 2 SMB (Multiple Iss... Windows 2
INFO Embedded Web Server... Web Servers 2
INFO FTP Server Detection Service detection 2
INFO Device Type General 1
INFO Ethernet Card Manufac... Misc. 1
INFO Ethernet MAC Addresses General 1
INFO ICMP Timestamp Requ... General 1
INFO mDNS Detection (Local... Service detection 1
Scan Details
Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 2:16 PM
End: Today at 2:24 PM
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
Carbon Black Installer Multiple Vulnerabilities
Read More
https://www.mozilla.org/hu/firefox/central/
14:31

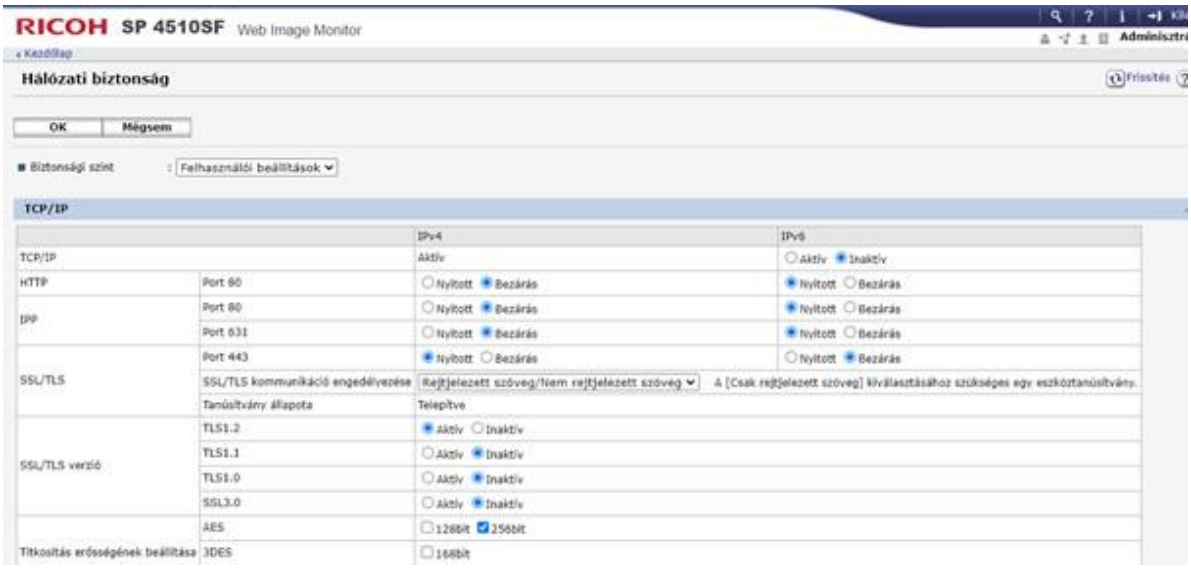
Biztonsági beállítások:

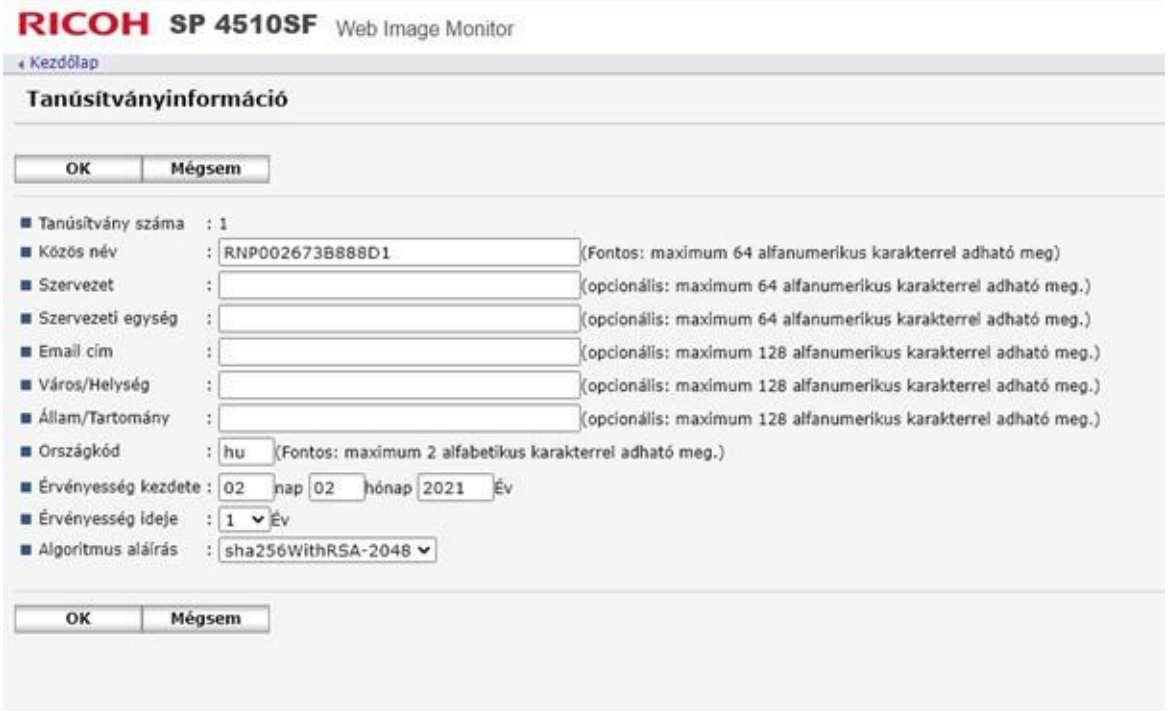

RICOH SP 4510SF Web Image Monitor
Kezdőlap
Ethernet
Gazdagép neve : RNP002673B888D1
DHCP : Aktív Inaktív
Domain név : Automatikus elérés (DHCP)
Megad
IPv4 cím * : 192.168.99.189 (192.168.1.103)
Alhálózati maszk * : 255.255.255.0 (255.255.255.0)
DDNS : Aktív Inaktív
WINS : Aktív Inaktív
Elsődleges WINS szerver * : 0.0.0.0 (0.0.0.0)
Másodlagos WINS szerver * : 0.0.0.0 (0.0.0.0)
LLMNR : Aktív Inaktív
Hatókör-azonosító * : ()

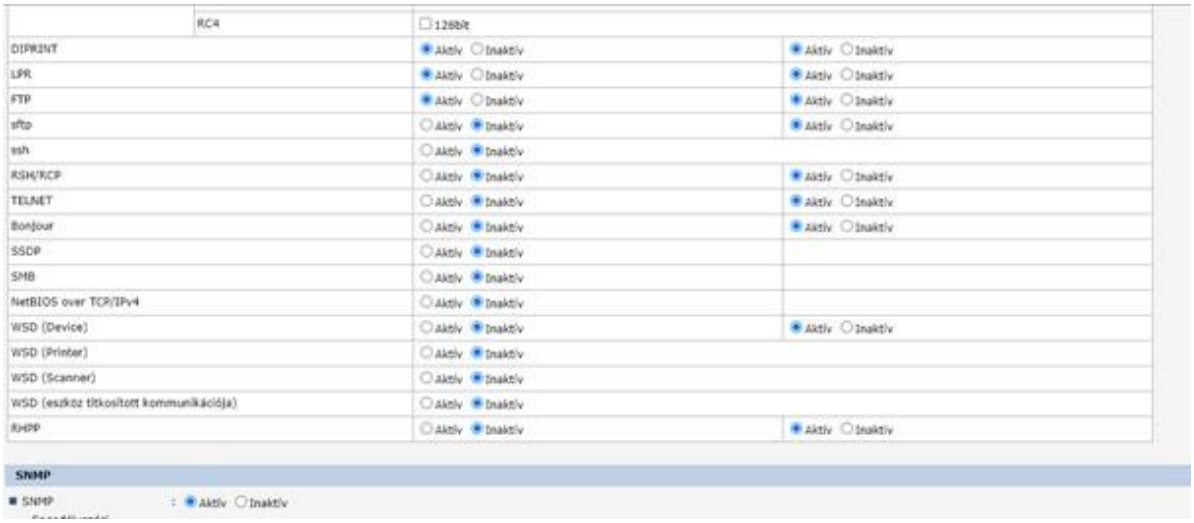

RICOH SP 4510SF Web Image Monitor
Kezdőlap
SNMP
OK
Mégsem
SNMP : Aktív Inaktív
Protokoll
IPv4 : Aktív Inaktív
IPv6 : Aktív Inaktív
SNMPv1,v2 beállítás
SNMPv1,v2 funkció : Aktív Inaktív
SNMPv1 trap kommunikáció : Aktív Inaktív
SNMPv2 trap kommunikáció : Aktív Inaktív
Engedélyezési beállítások SNMPv1 és v2 által : Be Ki
Közösség
Szám
Közösségnév
Hozzáférés típusa
Protokoll típusa
Aktív/Inaktív
Kezelő címe
1
public_2
csak olvasható
IPv4
Aktív Inaktív
127.0.0.1
IPv6
Aktív Inaktív
::
2
admin
olvasható-írható
IPv4
Aktív Inaktív
127.0.0.1


RICOH SP 4510SF Web Image Monitor
‹ Kezdőlap
SNMPv3
OK
Mégsem
SNMP : Aktív Inaktív
Protokoll
IPv4 : Aktív Inaktív
IPv6 : Aktív Inaktív
SNMPv3 beállítás
SNMPv3 funkció : Aktív Inaktív
SNMPv3 trap kommunikáció : Aktív Inaktív
Kontextusnév : GWNCS
Hitelesítési algoritmus : SHA1 MD5
Titkosítási algoritmus : AES128 DES
SNMPv3 kommunikáció engedélyezése : Csak titkosítás Titkosítás/Nem titkosított szöveg
Titkosított jelszó beállítása szükséges a titkosított kommunikáció használatához.
SNMPv3 trap kommunikáció beállítása
Szám
Azonosító
Protokoll típusa
Aktív/Inaktív
Kezelő címe
1
IPv4
Aktív Inaktív
0.0.0.0


Administrator: Parancssor
RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH SP 4510SF
Network Control Service Ver. 13.31
Copyright (C) 1994-2020 Ricoh Co.,Ltd. All rights reserved.
msh> set rfu down
msh> set cbc down
msh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes
Yes.
Now, Save data.
A kapcsolat megszakadt az állomással.
C:\Windows\system32>


RICOH SP 4510SF Web Image Monitor
Kezdőlap
Hálózati biztonság
Frissítés
OK
Mégsem
Biztonsági szint : Felhasználói beállítások
TCP/IP
IPv4
IPv6
TCP/IP
Aktív
Aktív Inaktív
HTTP
Port 80
Nyitott Bezárás
Nyitott Bezárás
IPP
Port 80
Nyitott Bezárás
Nyitott Bezárás
Port 631
Nyitott Bezárás
Nyitott Bezárás
SSL/TLS
Port 443
Nyitott Bezárás
Nyitott Bezárás
SSL/TLS kommunikáció engedélyezése
Rejtjelezett szöveg/Nem rejtjelezett szöveg
A [Csak rejtjelezett szöveg] kiválasztásához szükséges egy eszköztanúsítvány.
Tanúsítvány állapota
Telepítve
SSL/TLS verzió
TLS1.2
Aktív Inaktív
TLS1.1
Aktív Inaktív
TLS1.0
Aktív Inaktív
SSL3.0
Aktív Inaktív
Titkosítás erősségének beállítása
AES
128bit 256bit
3DES
168bit


RICOH SP 4510SF Web Image Monitor
Kezdőlap
Tanúsítványinformáció
OK
Mégsem
Tanúsítvány száma : 1
Közös név : RNP002673B888D1 (Fontos: maximum 64 alfanumerikus karakterrel adható meg)
Szervezet : (opcionális: maximum 64 alfanumerikus karakterrel adható meg.)
Szervezeti egység : (opcionális: maximum 64 alfanumerikus karakterrel adható meg.)
Email cím : (opcionális: maximum 128 alfanumerikus karakterrel adható meg.)
Város/Helység : (opcionális: maximum 128 alfanumerikus karakterrel adható meg.)
Állam/Tartomány : (opcionális: maximum 128 alfanumerikus karakterrel adható meg.)
Országkód : hu (Fontos: maximum 2 alfabetikus karakterrel adható meg.)
Érvényesség kezdete : 02 nap 02 hónap 2021 Év
Érvényesség ideje : 1 Év
Algoritmus aláírás : sha256WithRSA-2048
OK
Mégsem

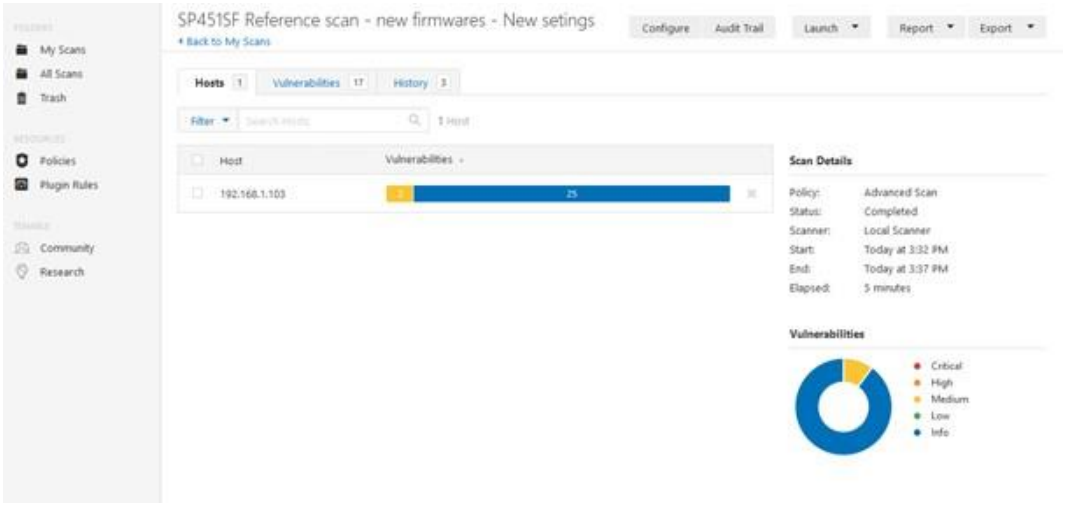


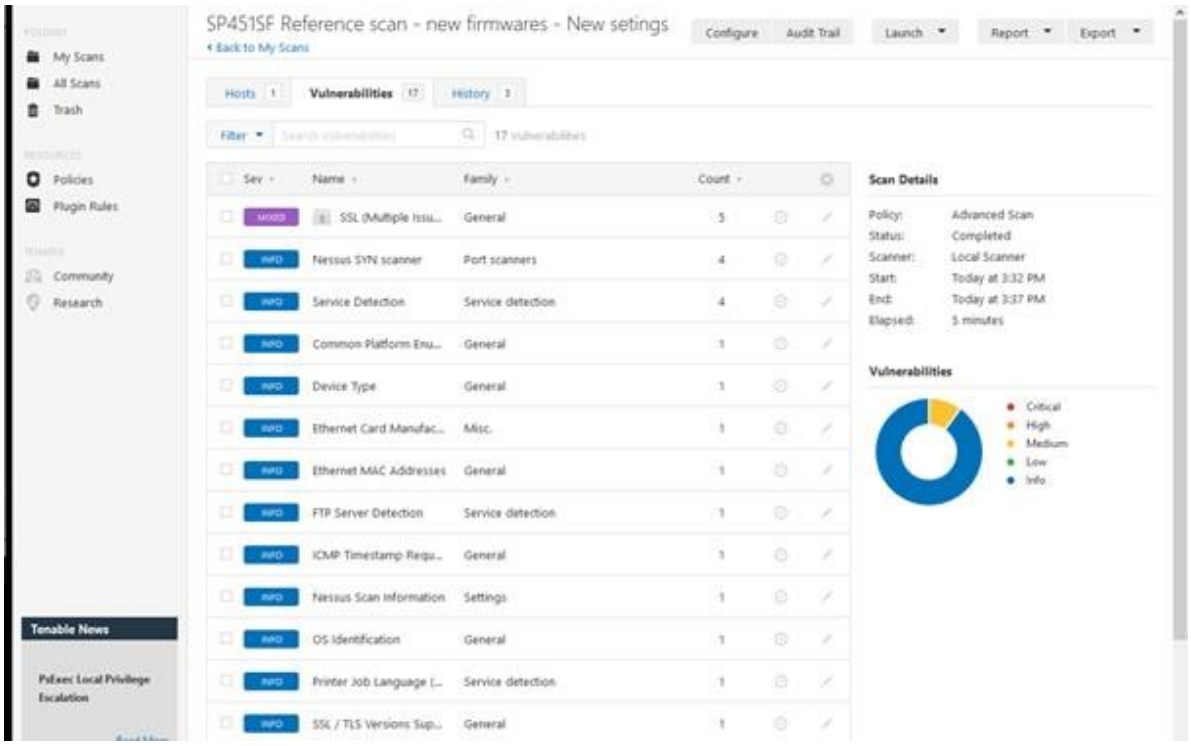
	RC4	☐ 128bit	
DIPRINT		◉ Aktív ○ Inaktív	◉ Aktív ○ Inaktív
LPR		◉ Aktív ○ Inaktív	◉ Aktív ○ Inaktív
FTP		◉ Aktív ○ Inaktív	◉ Aktív ○ Inaktív
sftp		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív
ssh		○ Aktív ◉ Inaktív	
RSH/RCP		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív
TELNET		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív
Bonjour		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív
SSDP		○ Aktív ◉ Inaktív	
SMB		○ Aktív ◉ Inaktív	
NetBIOS over TCP/IPv4		○ Aktív ◉ Inaktív	
WSD (Device)		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív
WSD (Printer)		○ Aktív ◉ Inaktív	
WSD (Scanner)		○ Aktív ◉ Inaktív	
WSD (eszköz titkosított kommunikációja)		○ Aktív ◉ Inaktív	
RHPP		○ Aktív ◉ Inaktív	◉ Aktív ○ Inaktív

SNMP

■ SNMP : ◉ Aktív ○ Inaktív

A biztonsági beállításokat követően:




SP451SF Reference scan - new firmwares - New setings
Configure
Audit Trail
Launch
Report
Export
Back to My Scans
My Scans
All Scans
Trash
Policies
Plugin Rules
Community
Research
Hosts 1
Vulnerabilities 17
History 3
Filter
17 Vulnerabilities
Sev
Name
Family
Count
MIXED SSL (Multiple Issu... General 5
INFO Nessus SYN scanner Port scanners 4
INFO Service Detection Service detection 4
INFO Common Platform Enu... General 1
INFO Device Type General 1
INFO Ethernet Card Manufac... Misc. 1
INFO Ethernet MAC Addresses General 1
INFO FTP Server Detection Service detection 1
INFO ICMP Timestamp Requ... General 1
INFO Nessus Scan Information Settings 1
INFO OS Identification General 1
INFO Printer Job Language (... Service detection 1
INFO SSL / TLS Versions Sup... General 1
Scan Details
Policy: Advanced Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 3:32 PM
End: Today at 3:37 PM
Elapsed: 5 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
PsExec Local Privilege Escalation


nessus
Report generated by Nessus™
SP451SF Reference scan - new firmwares - New settings
Tue, 02 Feb 2021 15:32:17 Central Europe Standard Time
TABLE OF CONTENTS
Vulnerabilities by Host
192.168.1.103
Vulnerabilities by Host
Collapse All | Expand All
192.168.1.103
0 CRITICAL
0 HIGH
2 MEDIUM
0 LOW
24 INFO
Scan Information
Start time: Tue Feb 2 15:32:17 2021