Implementacija sigurnosnih politika na operacijskom sustavu Windows

Ćorluka, Ana

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:556250

Rights / Prava: Attribution 3.0 Unported/Imenovanje 3.0

Download date / Datum preuzimanja: **2024-04-16**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ana Ćorluka

IMPLEMENTACIJA SIGURNOSNIH POLITIKA NA OPERACIJKOM SUSTAVU WINDOWS

ZAVRŠNI RAD

Varaždin, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Ana Ćorluka

Matični broj:

Studij: Primjena informacijske tehnologije u poslovanju

IMPLEMENTACIJA SIGURNOSNIH POLITIKA NA OPERACISKOM SUSTAVU WINDOWS

ZAVRŠNI RAD

Mentor/Mentorica:

Izv. Prof. dr. sc. Ivan Magdalenić

Varaždin, 2021

Ana Ćorluka

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Danas su sustavi ranjiviji nego ikad. U prošlosti se informacijama i podacima nije pridodavao toliki značaj, ali u današnjici se one smatraju bitnijima nego ikada. Kako bi se nesmetano mogle razmjenjivati informacije unutar neke tvrtke ili institucije, bitno je osigurati sigurni put kako bi se te iste informacije mogle prosljeđivati. Tu u priču ulazi sigurnosna politika. Sigurnosna politika kao takva bi trebala biti jedan od ključnih dokumenata. Ona pokriva sve što se tiče zaposlenika. Bilo od njihovih zadaća, kako se ponašati u određenim situacijama, koje su kazne ako se ona ne slijedi itd. Sama srž ovog rada je ustvari shvaćanje koliko je bitna sigurnosna politika, te ako nije dobro implementirana, mogu nastati katastrofalne posljedice. U ovome radu sigurnosna politika je implementirana na operacijskom sustavu Windows. On je prvi u svijetu prema korištenju, te ga mnogo institucija i tvrtki koristi kao primarni operacijski sustav. U nastavku rada će biti prikazano što je sigurnosna politika ustvari i na temelju čega se gradi, statistika što se tiče sigurnosne politike, zatim, kratka invertira u povijest operacijskog sustava Windows. U fokus rada je stavljena implementacija sigurnosne politike koja je razvijena na operacijski sustav Windows.

Ključne riječi: sigurnosna politika, implementacija, operacijski sustav Windows, ISO/IEC standardi, CIA trokut

Sadržaj

Sadržaj iii
1. Uvod 1
2. Metode i tehnike rada 2
2.1. VirtualBox 2
3. Sigurnosna politika 4
3.1. Temelji sigurnosne politike 4
3.1.1. CIA trokut 4
3.1.2. ISO/IEC standardi 5
3.2. Statistički podaci 6
3.3. Definiranje dobre sigurnosne politike 6
3.4. Sigurnosna politika (Primjer za rad) 7
4. Operacijski sustav Windows 9
4.1. Windows 1.0 11
4.2. Windows 2.0 11
4.3. Windows 3.0 11
4.4. Windows 3.1 11
4.5. Windows NT 12
4.6. Windows 95 12
4.7. Windows 98 13
4.8. Windows 2000 13
4.9. Windows XP 13
4.10. Windows Vista 14
4.11. Windows 7 14
4.12. Windows 8 15

4.13. Windows 10 15
5. Praktični dio – implementacija sigurnosne politike 17
5.1. Podizanje servera i potrebnih servisa 17
5.2. Implementacija sigurnosne politike 19
6. Zaključak 32
7. Literatura 33
8. Popis slika 34

1. Uvod

Razvitkom informacijske tehnologije, kompanije su se masovno krenule okretati korištenju digitalnih uređaja, bilo računala, tableta, laptopa. Podaci su samim time počeli biti sve osjetljiviji, te je lakše nego ikada doći do njih. Zbog toga je potrebno definirati dobru sigurnosnu politiku, kako bi se umanjila mogućnost probijanja nepoželjnih gostiju u sustav tvrtke.

U radu će biti obuhvaćena svrha sigurnosne politike, smjernice koje bi se trebale pratiti kako bi se razvila dobra sigurnosna politika. Također, unutar samog rada, biti će definirana sigurnosna politika, koja će se kasnije implementirati na operacijskom sustavu Windows.

2. Metode i tehnike rada

Prilikom izrade rada, najprije su prikupljeni članci i javno dostupni dokumenti prema kojima je definirana sigurnosna politika. Sigurnosna politika koja će biti definirana unutar rada služi kao primjer, te nije stvarna ili korištena unutar bilo koje tvrtke. Unutar sigurnosne politike biti će definirane korisničke uloge, čije će zadaće varirati ovisno o njegovoj ulozi unutar same politike.

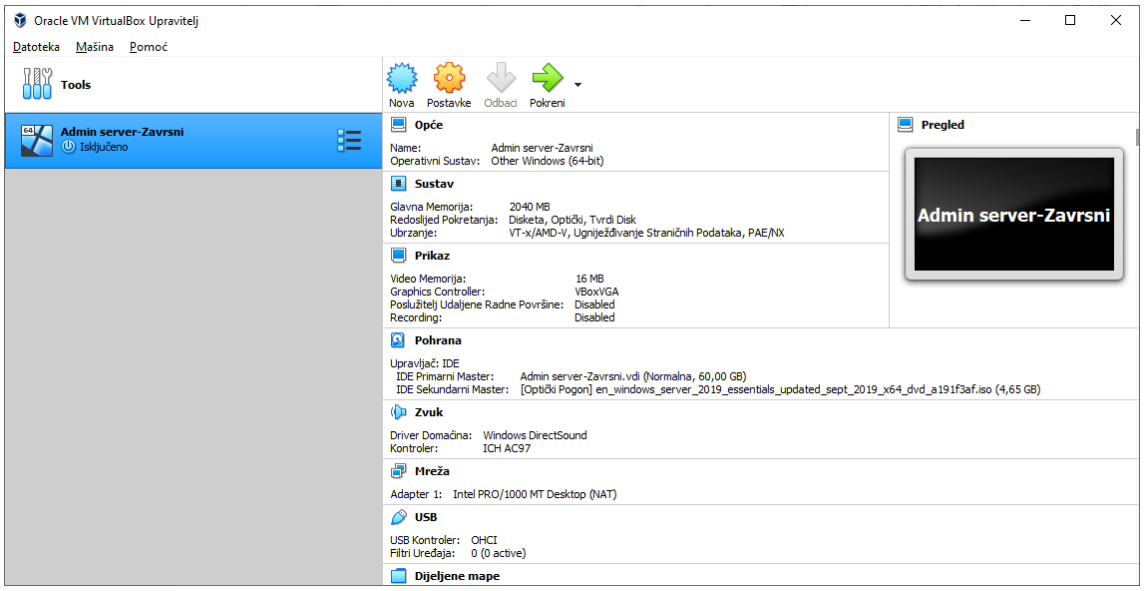
Zatim je na virtualnoj okolini, koja je postavljena u programu VirtualBox, dignut Windows server koji će služiti kao osnova za implementaciju sigurnosne politike koja je definirana unutar rada.

2.1. VirtualBox

VirtualBox je alat otvorenog izvora koji je ustvari virtualna mašina za pokretanje operacijskih sustava. Kompatibilan je s Windowsom, Linuxom, Mac OS-om, te Solarisom. U slučaju da na računalu na kojem je Windows operacijski sustav, treba i npr. Linux, moguće ga je pokretati preko VirtualBox-a. U novijoj verziji 6.0 virtualne mašine je moguće dodati na cloud, te ju je moguće kasnije skinuti na neko drugo računalo.

Za ovaj rad, VirtualBox je poslužio kao virtualna mašina na kojoj je instaliran Windows Server Essentials 2019. Samo postavljanje virtualne mašine nije kompleksno. Najprije je dodijeljeno ime virtualnoj mašini, te je odabran tip operacijskog sustava. Zatim, postavljeno je koliko megabajta radne memorija virtualna mašina može koristiti na računalu, koje ovisi o jačini RAM memorije koje se nalazi u računalu. Na ovome je postavljeno da se vrti na 2040 megabajta, odnosno 2 gigabajta RAM memorije. Idući korak je dodavanje virtualnog tvrdog diska mašini. Za ovaj rad je korištena opcija „Napravi virtualni disk sada“, te je poslije toga izabrana opcija VDI, te poslije mu je dodijeljeno 60 gigabajta koje je fiksno.

Nakon što je virtualna mašina kreirana, potrebno je dodati operacijski sustav. U ovome slučaju to je već ranije spomenuti Windows Server Essentials 2019. Kako bi to bilo dodano, potrebno je odabrati „Postavke“ u gornjem meniju, zatim se pozicionirati u „Pohrana“, te pod „Prazni“ umjesto IDE Sekundarni Master odabrati iso datoteku u kojoj se nalazi operacijski sustav.



Slika 1. Postavke u alatu "VirtualBox"

Na slici je prikazano kako je konfigurirana virtualna mašina za rad. Naziv mašine moguće je vidjeti u opciji pregled, te je nazvan „Admin server – Zavrsni“. Pošto je operacijski sustav Windows Server Essentials 2019, on spada pod druge Windows operacijske sustave (64-bitne). Vidljivo je koliko mu je glavne memorije dodano, te vrsta pohrane, kao i ostale postavke. Bitno je naglasiti da je postavke moguće namještati prema potrebi, te je za ovaj rad ovo prihvatljivo, a ostatak postavki ostao je kako je i zadan.

3. Sigurnosna politika

Prema definiciji, sigurnosna politika je „pisani programski dokument u okviru poslovne politike firme. U tom iskazu o sigurnosnoj politici IT-a se navode mjere i mehanizmi koji osiguravaju visok nivo sigurnosti informacijskih tehnologija koje se uz to opslužuju na siguran način.“ Laički rečeno, to je skup pravila, procedura i smjernica kojih se potrebno pridržavati kako bi se osigurala određena razina informatičke i informacijske sigurnosti u nekoj organizaciji ili kompaniji.

Sigurnosna politika definira prihvatljive i neprihvatljive načine ponašanja, te kako postupiti kada se desi neka šteta ili incident. Ona također obuhvaća raspodjelu zadataka i odgovornosti, te definira sankcije u slučaju nepoštivanja istih. Kod definiranja sigurnosne politike bitno je definirati prijetnju, te razine vjerojatnosti prijetnje koja postoji na nekom dijelu infrastrukture. Primjerice, postoji visoka vjerojatnost da nam prijetnju netko pošalje putem e-maila ili interneta, te kako bi se ta vjerojatnost smanjila, potrebno je poduzeti određene korake koji bi trebali biti definirani unutar sigurnosne politike. Tu razinu, ako je preko mail-a, moguće je smanjiti isključivanjem mogućnosti primitaka mailova od osoba koji imaju različitu domenu nego što je korištena unutar kompanije, ili pak, ako je internet u pitanju, onemogućavanjem korištenja nesigurnih stranica, odnosno blokiranjem pristupa prema njima.

Sigurnosna politika se mora primijeniti na svu informacijsku imovinu, kako bi se čim manje smanjile razine prijetnji.

Cilj sigurnosne politike je ustvari definiranje bitnih informacija i podataka unutar same organizacije, te zaštita samih od vanjskih pristupa i utjecaja. Primjerice, za jednu banku su najbitniji podaci kako ona posluje, način njenog poslovanja, a u fokusu svega su njezini klijenti. Tako da će ona razvijati sigurnosnu politiku kako bi našla sve slabe točke unutar samog sustava te će ih krpati, kako kroz njih niti jedan vanjski utjecaj, npr. haker, ne bi mogao doći.

3.1. Temelji sigurnosne politike

3.1.1. CIA trokut

Jedan od temelja sigurnosne politike je tzv. CIA (Confidentiality, Integrity, Availability) trokutu. CIA trokut prikazuje aspekte informacijske sigurnosti. Na njega je bitno gledati prilikom definiranja sigurnosne politike zbog njegova tri aspekta, a to su:

- povjerljivost podataka – ono se odnosi na tajnost podataka, te pristup tim istim podacima samo ovlaštenim osobama, te su njegovi najveći fokusi identifikacija i autentifikacija korisnika,

- integritet podataka – odnosi se na promjene u podacima, te da se podaci mogu promijeniti samo kada se koriste odgovarajuća ovlaštenja i
- dostupnost – odnosi se na dostupnost informacija i podataka, te je bitno da su pravi podaci dostupni u pravom vremenu.

Primjer što se samog CIA trokuta može bit jedan analitičar baza podataka. Njemu za rad su potrebni podaci koje neka organizacija ima. Ako on ne može pristupiti tim podacima, neće biti u mogućnosti napraviti analize koje su potrebne naprimjer upravi. Također, on kao analitičar ne smije imati ovlasti da mijenja te podatke. Isto tako neki podaci moraju biti tajni, npr. imena i prezimena klijenata, prema GDPR-u.

3.1.2. ISO/IEC standardi

ISO/IEC serija 27000 je serija standarda koja je posvećena sigurnosnoj politici unutar kompanija. ISO/IEC 27000 objavljen je od strane Međunarodne organizacije za standarde zajedno sa Međunarodnim elektrotehničkim povjerenstvom. Ova serija standarda ustvari predstavlja smjernice i pomaže prilikom definiranja kako sigurnosne politike kako bi se definirali bitni podaci i informacije, te bi ih se zaštitilo, a sve to u svrhu kontinuiranog i dobrog poslovanja, imajući u vidu i zaštitu podataka kako klijenata, tako i zaposlenika.

ISO/IEC 27001 zahtijeva kontinuirano praćenje sustava kako bi se na vrijeme našle slabe točke unutar sustava, te bi se čim prije zakrpale, kako u sustavu ne bi bilo vanjskih prijetnji. Njegov prethodnik je bio BS 7799 standard, točnije on je izašao kao drugi dio, 1999. godine, pod nazivom „Sustavi upravljanja informacijskom sigurnošću – Specifikacija s uputama za uporabu“. U njemu je bilo opisano kako implementirati sustav upravljanja informacijskom sigurnošću. 2005. godine je ovaj standard adaptiran, te je postao dio ISO/IEC 27000 serije.

ISO/IEC 27002 standard predstavlja standard koji pokazuje najbolju praksu o kontroli informacijske sigurnosti. Točnije ono se odnosi na poduzimanje inicijative što se tiče promjena, održavanje, te kontrolu informacijske sigurnosti. Što se tiče povijest samog ISO/IEC 27002 standarda, njegov predak je bio britanski BS 7799 standard, koji je objavljen 1995. godine, te se sastojao od više dijelova. BS 7799, točnije dio koji je govorio o informatičkoj sigurnosti, evaluiran je, te ponovno napisan 1998. godine. 2000. godine spada pod ISO/IEC 17799, gdje je dobio naziv „Informacijska tehnologija – Kodeks prakse upravljanja informacijskom sigurnošću“. Nakon toga, ISO/IEC 17799 nalazi se pod evaluacijom, te su neke stvari promijenjene, te 2007. godine ISO/IEC 17799 ulazi u familiju ISO/IEC 27000 standarda kao ISO/IEC 27002.

3.2. Statistički podaci

Nažalost veći je broj loše definirane sigurnosne politike, nego dobre, što je lako primijetiti prema statističkim podacima. Moguće je započeti sa samom sigurnošću sa pogleda upada nepoželjnih korisnika u sustav. 3950 potvrđenih slučajeva upada u sustave je bilo zabilježeno 2020. godine. Jedan od primjera je Ina. Neki od ovih slučajeva su bili bezazleni, u smislu da nije napravljena nikakva šteta sustavu, a u primjeru Ine dio podataka je kriptiran, te je tražena otkupnina. U svemu ovome najbitniji su zaposlenici. Naime, 95% upada neželjenih korisnika u sustav je posljedica zaposlenika same kompanije. Tako da je bitno obučiti zaposlenike kako na siguran način koristiti sustav.

Sljedeći primjer loše definirane politike jest broj zlonamjernih računalnih kodova koji su napravili štetu unutar sustava. Ako nije dobro implementirana sigurnosna politika što se tiče same zaštite sustava od zlonamjernih sustava, posljedice mogu biti katastrofične za organizaciju. U 2020. godini je zabilježeno 5.6 bilijuna napada što se tiče zlonamjernih kodova. Dobra stvar jest u tome što u odnosu na 2018. godinu, trend napada je skoro dvostruko pao.

Postoji još puno statističkih podataka koji se dotiču sigurnosne politike. Ova dva primjera su najrasprostranjenija, te najviše štete nastaje od njih. Za velike kompanije ovakve greške što se tiče definiranja i implementacije sigurnosne politike mogu koštati milijune dolara, a za male mogu značiti potencijalni bankrot.

3.3. Definiranje dobre sigurnosne politike

Zahtjeve koje dobra sigurnosna politika mora ispunjavati su idući:

• poštivanje definiranih pravila,

• u slučaju nepoštivanja pravila, moguće su sankcije ili kazne nadležnih službi,

• usredotočiti se na rezultate, a ne na samu provedbu sigurnosne politike i

• određivanje na postojećim standardima i smjernicama.

Također, prilikom definiranja sigurnosne politike bitno je uzeti u obzir sljedeće aspekte informatičkog sustava:

- udaljen pristup na domenu – bitno je da korisnik i njegovo ime preko kojeg pristupa domeni se nalazi aktivnom direktoriju (eng. „Active Directory“)
- mijenjanje šifre – bitno je da korisnici sustava mijenjaju šifre u razdoblju od x dana, kako bi se stalno održavala visoka razina sigurnosti sa korisnikove strane

- enkripcija – nakon x neuspješnih pokušaja unosa šifre, sustav se korisniku zaključava
- sigurnosna stijena (eng. „Firewall“) – zaštita sustava u smislu filtriranja mrežnog prometa
- pristup stranicama – onemogućavanje pristupa stranicama sumnjivog sadržaja
- pristup stranicama za instaliranje aplikacija – gledati da stranice sa kojih se skidaju aplikacije su službene stranice vlasnika aplikacija
- kreiranje rola – kreiranje uloge koja odgovara zahtjevima koje radno mjesto traži kako bi korisnik sustava mogao nesmetano obavljati svoje zadatke
- backup sustava – bitno je u određenom vremenskom intervalu raditi backupe sustava, kako bi se u slučaju incidenta, sustav mogao čim prije vratiti na verziju koja je najviše slična stanju sustava prije incidenta

3.4. Sigurnosna politika (Primjer za rad)

Sada kada su pokrivene sve bitne točke prilikom definiranja same sigurnosne politike, moguće ju je definirati. Za ovaj rad unutar sustava će postojati tri uloge: administrator sustava, voditelj odjela i korisnik. Svatko od njih imat će drugačije ovlasti, te temeljem toga će se razlikovati stvari koje mogu raditi unutar njega.

Glavnu ulogu ima administrator. Njegove zadaće što se tiče sigurnosne politike su sljedeće:

- osigurati resurse za korisnike sustava, u ovome slučaju održavanje servera,
- redovno provjeravati zahtjeve korisnika za prava, te shodno tome dodjeljivati ili micati prava korisnicima,
- redovito raditi sigurnosne kopije slučaja, kako u slučaju incidenta server može čim prije početi s ponovnim radom,
- redovito ažurirati sigurnosni sustav,
- redovito ažurirati listu stranica sa sumnjivim sadržajima koje korisnici prijavljuju, te prema tome zabraniti pristup istima,
- dodavati mape za razmjenu podataka, te različitim korisnicima davati različita prava,
- nadgledanje performansi servera.

Što se tiče voditelja, njegove zadaće što se tiče sigurnosne politike su iduće:

- predaja zahtjeva za izradu novog korisničkog računa,

- instalacija aplikacija koje su potrebne korisniku za rad,
- prijavljivanje stranica sa sumnjivim sadržajem,
- administriranje aplikacija koje su korisnicima potrebne za rad,
- podrška sa aplikacijama,
- nadgledanje performansi servera, te prilikom uočavanja neregularnog rada servera obavijestiti administratora,
- čitanje i uređivanje dokumenata unutar mapa za razmjenu podataka.

Korisnikova zadaća je poprilično jednostavna, te je najmanje zahtjevna:

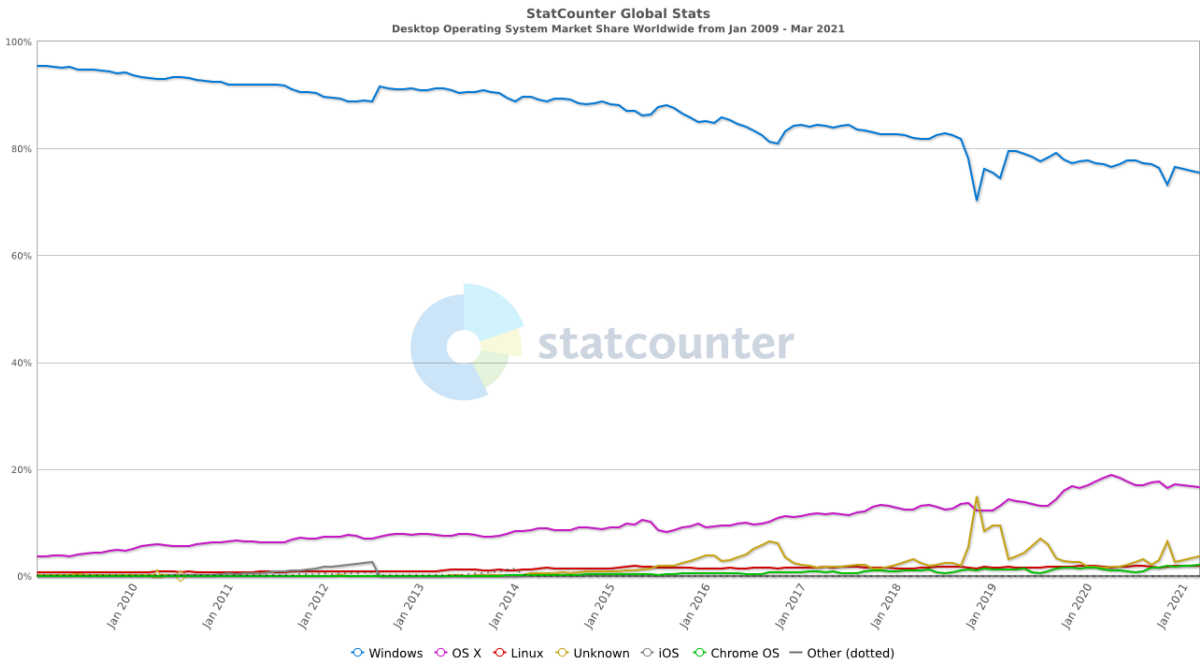
- korištenje aplikacija koje se nalaze na serveru,
- čitanje podataka iz mapa za razmjenu, te razvrstavanje istih u druge mape, kako bi se glavna mapa za razmjenu mogla kontinuirano čistiti,
- predaja zahtjeva za instalaciju aplikacija,
- prijavljivati stranice sumnjivog sadržaja voditelju, kako bi on mogao dalje proslijediti informacije.

4. Operacijski sustav Windows

Operacijski sustav Windows je jedan od najrasprostranjenijih i najkorištenijih sustava koja su dostupna trenutno. Windows je prvi među operacijskim sustavima koji je došao sa grafičkim korisničkim sučeljem. U početku je Windows ovisio o MS-DOS sustavu, ali tokom vremena je ta ovisnost sve više i više padala.

Počevši od verzije 95, Windows počinje biti baziran na NT jezgri. DOS je operacijski sustav koji je koristio komandnu liniju, dok su se kasnije verzije Windows-a bazirana na grafičkom korisničkom sučelju. DOS je nudio malo mjesta za pohranu podataka za razliku od Windows-a. Što se tiče izvršavanja više zadataka istovremeno, kasnije verzije Windows-a su to omogućavale, dok DOS nije. Kod njega se mogao izvršavati samo jedan zadatak.

Prema statističkim podacima koji su trenutno dostupni, Microsoftov Windows OS dominira tržištem, sa udjelom od 76%, te nakon njega ide Appleov Mac Os, te na trećem mjestu se nalazi operacijski sustav Linux.

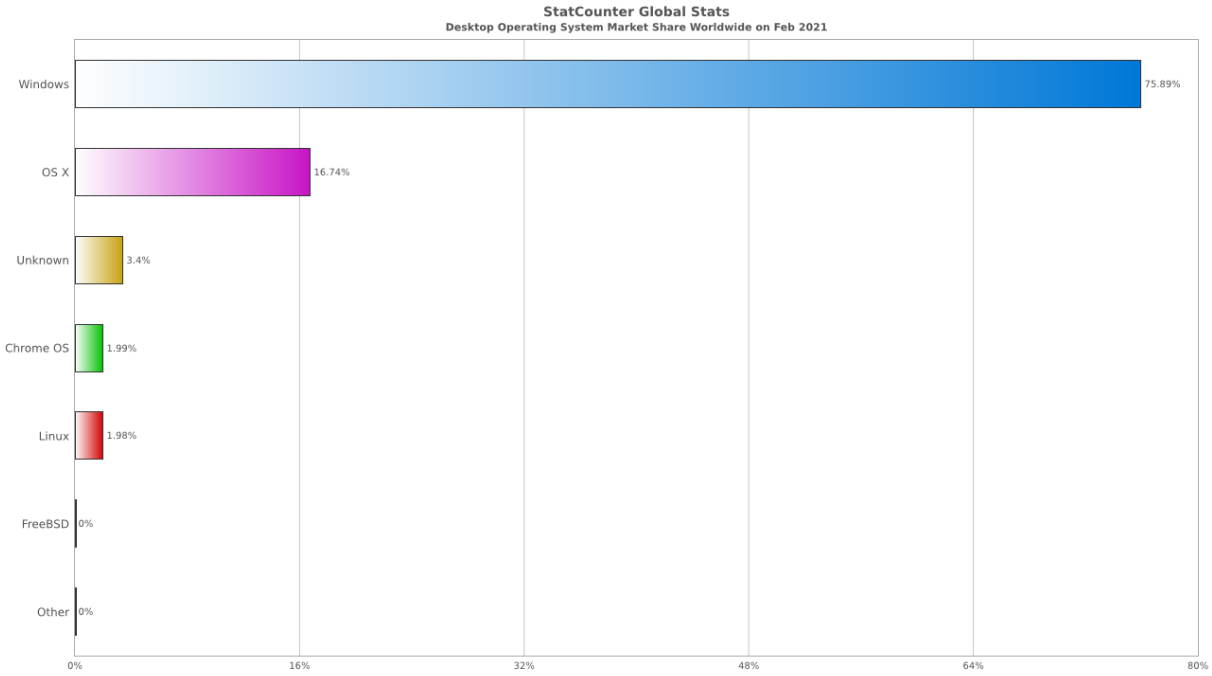


Slika 2. Statistički podaci korištenja operacijskih sustava za stolna računala[1]

Na slici je graf koji prikazuje udio na tržištu operacijskih sustava po operacijskim sustavima koje koriste stolna računala. Plavom crtom označen je OS Windows, te je prema

[1] Izvor: https://gs.statcounter.com/

podacima dostupnima na Stat Counter stranici, u 2009. godini imao 95% udjela na tržištu, te je tokom godina pao na 75%. Unatoč padu, moguće je vidjeti veliki jaz između njega i MacOS-a.



Slika 3. Udjeli operacijskih sustava na svjetskom tržištu za stolna računala[2]

Na slici je graf koji prikazuje udio na tržištu prema trenutnim podacima, te je lakše primijetiti koliku prednost Windows ima u odnosu na MacOS, te ostale operacijske sustave. Što se tiče poslužiteljskih računala Linux dominira na tom dijelu tržišta, te nadmašuje Windows operacijske sustave za servere.

Sigurnost na operacijskom sustavu se razvija sve više i više tokom godina. Kako su izlazile nove verzije operacijskog sustava, tako se povećavala mogućnost sve veće sigurnosti. No, usprkos svemu, Windowsu je i dalje sigurnost dosta slaba točka. Razlog tome leži u činjenici da Windows ima otvoreni pristup aplikacijama, te kao takav više podliježe raznim napadima zlođudnih softvera (eng. „malware“) nego ostali operacijski sustavi.

[2] Izvor: https://gs.statcounter.com/

4.1. Windows 1.0

U studenom 1985. godine, tvrtka Microsoft je na tržište operacijskih sustava plasirala Windows 1.0, prvu inačicu sada najpoznatijeg operacijskog sustava. U to vrijeme na tržištu je već postojao jedan operacijski sustav, Apple-ov Macintosh.

Windows 1.0 pokretao se kao grafička 16-bitna ljuska koja se nalazila iznad već postojećeg MS-DOS sustava. Iako je bio predviđen kao nešto revolucionarno u svijetu tehnologije, nažalost nije. Na slabijim računalima, što se tiče hardware-a, teže se pokretao. Na Windows-u 1.0 mogli su se pokretati programi kao što je kalkulator, notepad, kalendar, sat i slično. Programi su bili poslagani kao prozori jedan pokraj drugoga, te se nisu mogli preklapati jedan preko drugoga.

4.2. Windows 2.0

Unatoč teškim kritikama koje je Windows 1.0 dobio, Windows 2.0, koji je objavljen u prosincu 1987. godine, bio je puno bolje prihvaćen. Suprotno svome prethodniku, u Windows 2.0 verziji, aplikacije su se mogle preklapati jedna preko druge, te je također bila dodana ikona za minimiziranje aplikacije.

Iste godine Microsoft na tržište izbacuje Windows/386, ažuriranu verziju Windows-a 2.0. U odnosu na svog prethodnika, Windows/386 je imao mogućnost pokretati više MS-DOS procesa istovremeno u proširenoj memoriji.

4.3. Windows 3.0

1990. godine izlazi Windows 3.0 koji je prvi pravi suparnik Appleovom Macintoshu. Ova verzija je dobila novi izgled ikona. Također što je bilo novo je ljuska voditelja programa, koja je omogućavala upravljanje programima koji su bili kompatibilni s novom verzijom. No, ova verzija nije dugo bila na tržištu. Razlog tome je bio što je Windowsu 3.0 nedostajalo dosta multimedijskih i mrežnih opcija.

4.4. Windows 3.1

1992. godine izlazi nova verzija Windowsa pod nazivom Windows 3.1. Dolazi sa puno više opcija i promjena u odnosu na svog prethodnika. U odnosu na prethodne dvije verzije koje su omogućavale samo preklapanje prozora, s ovom verzijom je omogućena i promjena dimenzija. Mogla se birati tema, font slova, postavke miša… Također, po prvi put unutar

Windowsa je omogućeno dinamično razmjenjivanje podataka (DDL) i linkanje i ugrađivanje objekata (OLE). U ovoj verziji je predstavljena mogućnost Upravitelj podataka. Pomoću njega su se mogle kopirati datoteke, pokretati aplikacije, printati dokumenti i ostalo. Također je omogućavao dijeljenje datoteka i mapa između računala koje su na istoj mreži.

4.5. Windows NT

U srpnju 1993. godine izlazi prva inačica Windows NT „obitelji“. Sa ovom serijom operacijskih sustava ciljalo se korisnike i tvrtke koje su trebale jače sposobnosti od računala. Prva inačica koja je izašla je bila Windows NT 3.1, koja je imala slično korisničko sučelje Windowsu 3.1, ali je imala jače mogućnosti što se tiče mrežnih postavki.

U kolovozu 1996. godine Microsoft objavljuje Windows NT 4.0 koji ima slično korisničko sučelje godinu prije izdanom operacijskom sustavu, Windows 95. Kasnije je NT serija zamijenjena sa Windows 2000.

Što se tiče ove serije operacijskih sustava, implementirane su nove mogućnosti, npr. u slučaju da se jedna od aplikacija koje korisnik trenutno koristi sruši, ostale će ostati i dalje u svom normalnom stanju.

4.6. Windows 95

U kolovozu 1995. godine Microsoft na tržište stavlja Windows 95. Što je najprije važno spomenuti je da ova verzija dolazi sa novim web pretraživačem, Internet Explorerom 1.0.

No, ova verzija je imala skoro nikakvu lokalnu sigurnost. Naime, u slučaju da je datoteka spremljena na sustav, njoj može bilo tko pristupiti, dokle god koristi to isto računalo. Postojale su aplikacije koje su davale mogućnost da se datoteke i mape skrivaju ili da se stavi lozinka na njih, no one su koštale. Dobra stvar je da se za korištenje računala moralo prijaviti preko korisničkog imena i lozinke. Loša stvar kod Windows 95 verzije je bila ta što je sustav imao slabu sigurnost protiv tzv. buggy aplikacija.

Također, postojao je bug unutar samog sustava. Ako se sustav koristio u korporaciji, te ako se omogućilo dijeljenje datoteka i printera na mreži koristeći usluge dijeljenja datoteka i pisača (eng. „File and Printer Sharing Service“), te ako je bila omogućena udaljena administracija, postojala je šansa da netko treći vidi sve što se događa na sustavu. No, Microsoft je to brzo shvatio, te je ažurirao drivere kako se takav bug ne bi mogao dogoditi.

4.7. Windows 98

Iako ova verzija nije bila toliko široko prihvaćena kao Windows 95, Windows 98 je ipak dolazio s dosta novih značajki. Omogućavala je dodatnu zaštitu na bitne datoteke, npr. registar (eng. „registry“). Također, dodana je mogućnost sigurnosnog kopiranja. Zatim, poboljšan je sam sustav kako bi se mogle koristiti nove tehnologije, kao npr. CD ili DVD. S time je došlo i poboljšanje za korištenje disketa. Dodana je aplikacija koja omogućava skeniranje i vraćanje pokvarenih datoteka

Windows 98 dolazio je sa novom verzijom pretraživača interneta, Internet Explorer 4.0. Novo što je došlo s ovom verzijom je da se moglo koristiti više monitora na jednom računalu. Novitet kod ove verzije je bio i aktivni desktop. On je dolazio kod Internet Explorera, te je korisniku omogućavao da doda HTML sadržaj na radnu površinu računala.

4.8. Windows 2000

Windows 2000 prvi puta je predstavljen u veljači 2000. godine. Ova verzija je bila dosta naprednija u odnosu na svoje prethodnike, bilo što se tiče sigurnosti ili općih postavki. Nova aplikacija nazvana Windows Tracker omogućavala je praćenje aplikacija, te je prepoznavala i dodavala komponente koje su nedostajale.

Što se tiče same sigurnosti dodan je sustav enkripcije datoteka koje imaju osjetljive informacije. Također, dodana je mogućnost privatne virtualne mreže (VPN), koja je omogućavala pristup lokalnoj mreži (LAN) preko javne mreže. Zaštićeni su bili i memorija i procesi zasebnih aplikacija kako bi se smanjilo rušenje sustava.

Predstavljeni su i personalizirani meniji koji su se prilagođavali korisnikovom načinu rada. Dodana je veća potpora kako bi se mogle koristiti veće brzine interneta. Također, dodana je potpora kako bi se koristio USB.

4.9. Windows XP

Predstavljen u listopadu 2001. godine, Windows XP je bio revolucionaran operacijski sustav za to doba. Iako je bio baziran na svome prethodniku, Windowsu 2000, Windows XP je nudio još veću sigurnost i stabilnost.

Prije ove verzije, ako je sa ažuriranom verzijom došao dio starog koda, sustav bi se mogao srušiti, te bi to rezultiralo sa nestabilnošću sustava. No, u ovoj verziji je to ispravljeno, te takvi scenariji su onemogućeni. Također, sustav pamti gdje je zadnji puta stao sa radom, prije bilo kakve instalacije. To je vrlo pogodno u slučaju da instalacija pođe po krivom, te je

lako vratiti računalo na stanje prije instalacije. Ova verzija je omogućavala i pristup udaljenom računalu sa drugog računala.

Kao u prijašnjoj verziji, omogućena je enkripcija bitnih datoteka. Također, moguće je limitirati pristup određenim datotekama i mapama, te aplikacijama.

4.10. Windows Vista

Windows Vista po prvi puta je predstavljen u studenome 2006. godine. Ova verzija je bila jedna od prvih koja se instalirala putem DVD-ROM-a. Sa ovom verzijom došlo je i novo korisničko sučelje. Između aplikacija koje su bile aktivne mogao se uključiti i 3D pregled (Flip 3-D). Windows Vista dolazio je i sa novom verzijom Internet Explorera, kao i sa novim avatarom za Outlook Express.

U odnosu na prijašnje verzije sigurnost je bila još više povećana. Mogla se staviti enkripcija na čitavi tvrdi disk, u slučaju da na njemu postoje osjetljivi podaci. Također, po prvi puta je predstavljena aplikacija Sigurnosno kopiranje i vraćanje (eng. „Backup and Restore“), koja je omogućavala da se napravi backup sustava, te da se sustav vrati na stanje u kojem je napravljen backup. Kao i prijašnja verzija, više nije bilo potrebno tražiti ažuriranja koja su bila dostupna na internetu, nego su se ona automatski odvijala sa izlaskom svake nove verzije. Također, particioniranje tvrdog diska u ovoj verziji je bilo predviđeno kako bi se smanjila mogućnost gubljenja bitnih podataka.

4.11. Windows 7

Windows 7 izašao je u listopadu 2009. godine. Naslijedio je dosta toga od svoga prethodnika, Windowsa Viste. U odnosu na Vistu, Windows 7 je dobio nov izgled. Počevši od samog izgleda, novi Windows 7 imao je mogućnost prezentacije (eng. „slideshow“) kao pozadinu. Kada se kliknulo na jedan aktivan prozor, te se protresao, ostali su se minimizirali. Također, u odnosu na ostale verzije koje su imale mogućnost bočne trake (eng. „Sidebar“), u ovoj verziji se prozor sa uređajima mogao staviti bilo gdje na zaslon. U slučaju aplikacija koje su se više koristile nego ostale, moglo ih se staviti na alatnu traku, te se isto igrati sa poretkom svih aplikacija čiji su se prečaci nalazili u traci.

Što se tiče same zaštite, poboljšana je u odnosu na Vistu. U odnosu na prijašnje verzije, u kojima se mogao enkriptirati samo tvrdi disk, Windows 7 je omogućavao enkripciju tvrdog diska, vanjskih diskova, te USB-a. Omogućeno je lakše dijeljenje datoteka između računala koja su na sebi imala Windows, te bila spojena na istu mrežu.

Olakšano je bilo i spajanje na mrežu. Sada se moglo spojiti na bilo koju mrežu u par klikova. Također, poboljšana je i opcija virtualne privatne mreže. Sada, u slučaju da se izgubila internetska mreža, virtualna privatna mreža automatski se ponovno postavljala.

4.12. Windows 8

U listopadu 2012. godine izašao je Windows 8. Na ovoj verziji Microsoft je napravio najviše promjena što se tiče samog izgleda sustava od Windowsa XP. Početni zaslon je sada bio kompletno drugačiji u odnosu na prethodne verzije. On je zamijenio startni gumb i početni meni. Također, novitet je bio i izgled Upravitelja zadataka (eng. „Task Manager“).

Što se tiče sigurnosti, u prijašnjoj verziji, Windowsu 7, bilo je moguće backup-irati i ponovno vratiti čitavi sustav, a sada se mogao raditi inkrement. Sa Windowsom 8 došla je i nova mogućnost, Hybrid Boot. On je pohranjivao informacije o Windows kernelu i upravljačkim programima uređaja, te se time smanjilo vrijeme dizanja sustava. Također, uz ovu verziju došao je i novi Windows Defender, aplikacija koja je, između ostalog, mogla se koristiti kao anti-virusni program za sustav. Također, moglo se pristupiti istim postavkama sustava sa više računala, ako se prijavilo sa Microsoftovim računom.

4.13. Windows 10

U srpnju 2015. godine izlazi Windows 10. U odnosu na Windows 8, napravljen je redizajn grafičkog sučelja. Vraćen je početni gumb, te je startni meni također dobio redizajn. Time se činio sličnim starijim verzijama, koje su bile više prihvaćene nego prijašnja verzija. Također, sa ovom verzijom došla je Microsoftova virtualna asistentica, „Cortana“. Aktivni prozori mogli su se premjestiti na virtualnu radnu površinu. Također, nova mogućnost prikaz zadataka omogućava lako upravljanje aktivnim prozorima. Vizualno je dosta toga ažurirano, te je dodano dosta mogućnosti.

Što se tiče sigurnosti, Windows 10 nudi mnogo više opcija nego bilo koji od svojih prethodnika. Sa ovom verzijom je došla mogućnost, da u slučaju ako se instalira bilo koji drugi anti-virusni program, te se aktivira, Windows zaštita se automatski isključuje. Također, novitet je mogućnost skeniranja i blokiranja poznatih malicioznih kodova. Isto tako moguće je upozoriti korisnika kada pristupa web stranici koja ima sumnjiv sadržaj. Što se tiče podataka koji se nalaze na računalu, njima se može dati ograničeni pristup, kako bi ih se zaštitilo od potencijalnih prijetnji. Za veće kompanije, dobro došla je mogućnost kontroliranja korisničkih

računa, kako bi se onemogućile neautorizirane promjene. Također, kao i u prijašnjim verzijama omogućeno je kriptiranje hard diska. Moguće je i imagiranje hard diska, kao u prijašnjoj verziji.

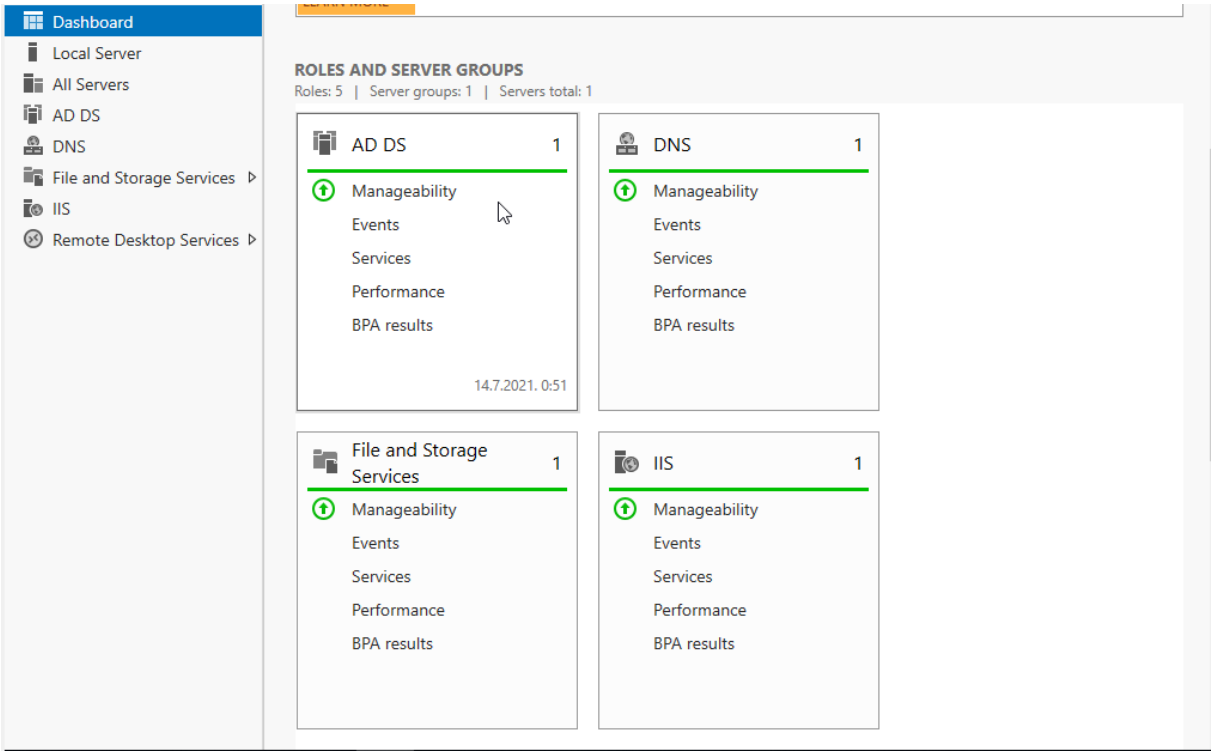
5. Praktični dio – implementacija sigurnosne politike

5.1. Podizanje servera i potrebnih servisa

Nakon što je dignuta virtualna okolina, idući korak je podizanje samog servera. Instalacija samog operacijskog sustava Windows Server Essentials 2019. je dosta intuitivna. Unutar VirtualBox-a pokrenemo virtualnu okolinu te ju pustimo da se učita. Nakon nekog vremena, na ekranu se prikaže prozor u kojem biramo željeni jezik koji će se primijeniti na serveru, vrijeme i valutu, te tipkovnicu. Nakon toga, sustav se ponovno pokrene, te nakon toga se prikaže prozor u kojem se za korisnika „Administrator“ dodaje šifra.

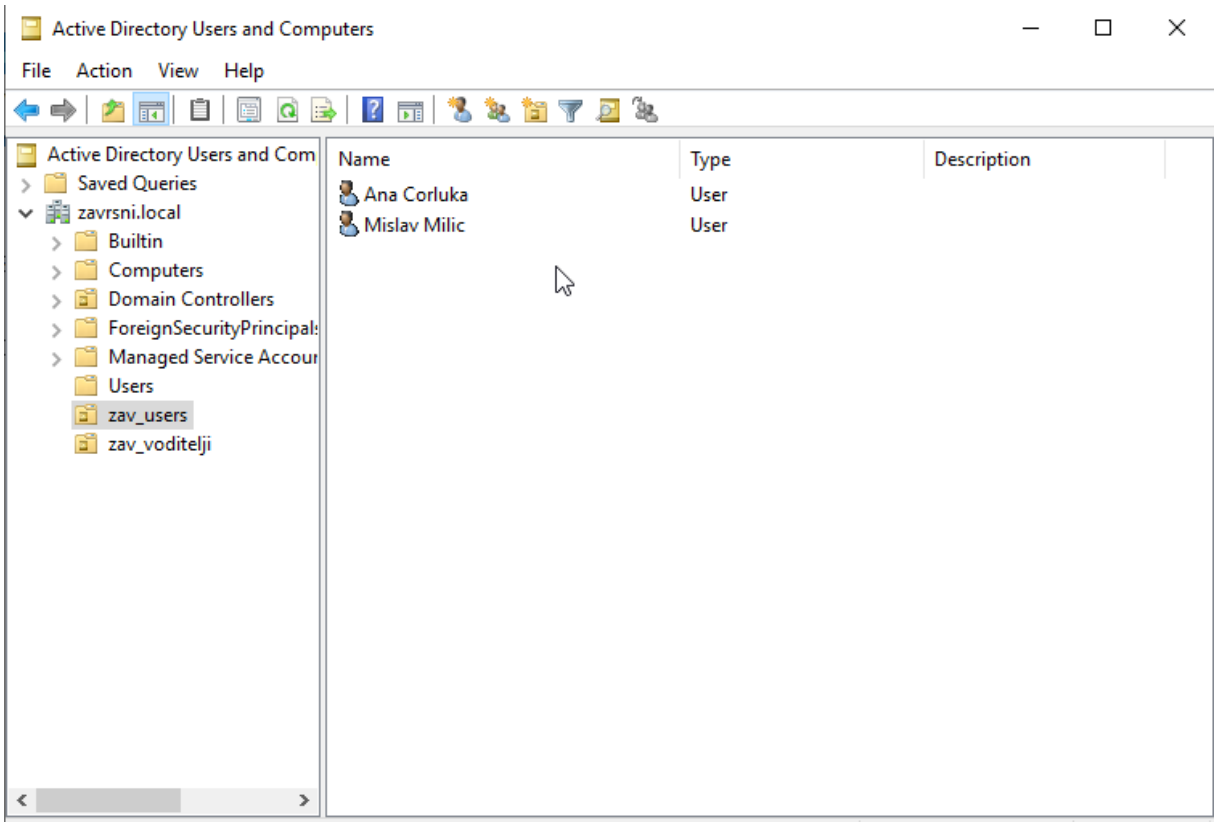
Slijedeće što je potrebno, unutar samog operacijskog sustava je dići aktivni direktorij (eng. „Active Directory“) i „Domain Name System“. Uloga aktivnog direktorija sustava je da on služi kao mjesto gdje se spremaju podaci o korisnicima sustava. Uloga „Domain Name System“-a je ta da je on povezan sa aktivnim direktorijem, te on služi kako bi se lakše promijenili dostupni podaci za nekog korisnika. Npr. korisnik Pero Perić želi promijeniti svoju šifru na računalu. Kada ju promjeni „Domain Name System“ traži njegovo korisničko ime unutar aktivnog direktorija, te mijenja trenutan zapis u novi. Također, dodana je i usluga dijeljenja datoteka i pisača (eng. „File and Printer Sharing“), koji će kasnije služiti kao mjesto gdje će korisnici međusobno moći dijeliti datoteke, te će preko grupne politike biti dodijeljena različita prava na korištenje.

Nakon podignutih servisa, moguće je unutar server menadžera (eng. „Server Manager“) vidjeti instalirane sustave, te njihove statuse, kao što je vidljivo na slici.



Slika 4. Server Manager

Unutar grupe aplikacija pod nazivom Windows administrativni alati (eng. „Windows Administrative Tools“) dostupan je alat pod nazivom aktivni direktorij (eng. „Active Directory“) unutar kojeg je moguće kreirati grupu korisnika, kako kasnije ne bi korisniku po korisniku dodavala prava, već će biti kreirana zasebna politika za svaku grupu. Opcionalno, biti će moguće mijenjati korisnikova prava prema potrebi, no o tome kasnije. Za potrebe ovog rada kreirane su dvije organizacijske jedinice unutar samog servera, a to su zav_voditelji i zav_korisnici. Kreiranje novog korisnika unutar grupe je poprilično jednostavno. Označi se grupa kojoj se želi dodati novi korisnik, te se desnim klikom miša otvara padajući izbornik u kojem idemo na novi i odaberemo korisnik. Prilikom unosa podataka, korisniku dodajemo ime i prezime, inicijale, te njegovo korisničko ime. Svim korisnicima je korisničko ime definirano na način da je najprije dodan prefiks zf, te zatim su dodani inicijali imena. Tako će npr. korisnik Pero Perić imati korisničko ime zfpp. Također, u drugom prozoru bitno je dodati šifru koju će prilikom prvog ulogiravanja u sustav sam korisnik promijeniti. Na slici je moguće vidjeti korisnike koji su dodani u grupu zav_korisnici.

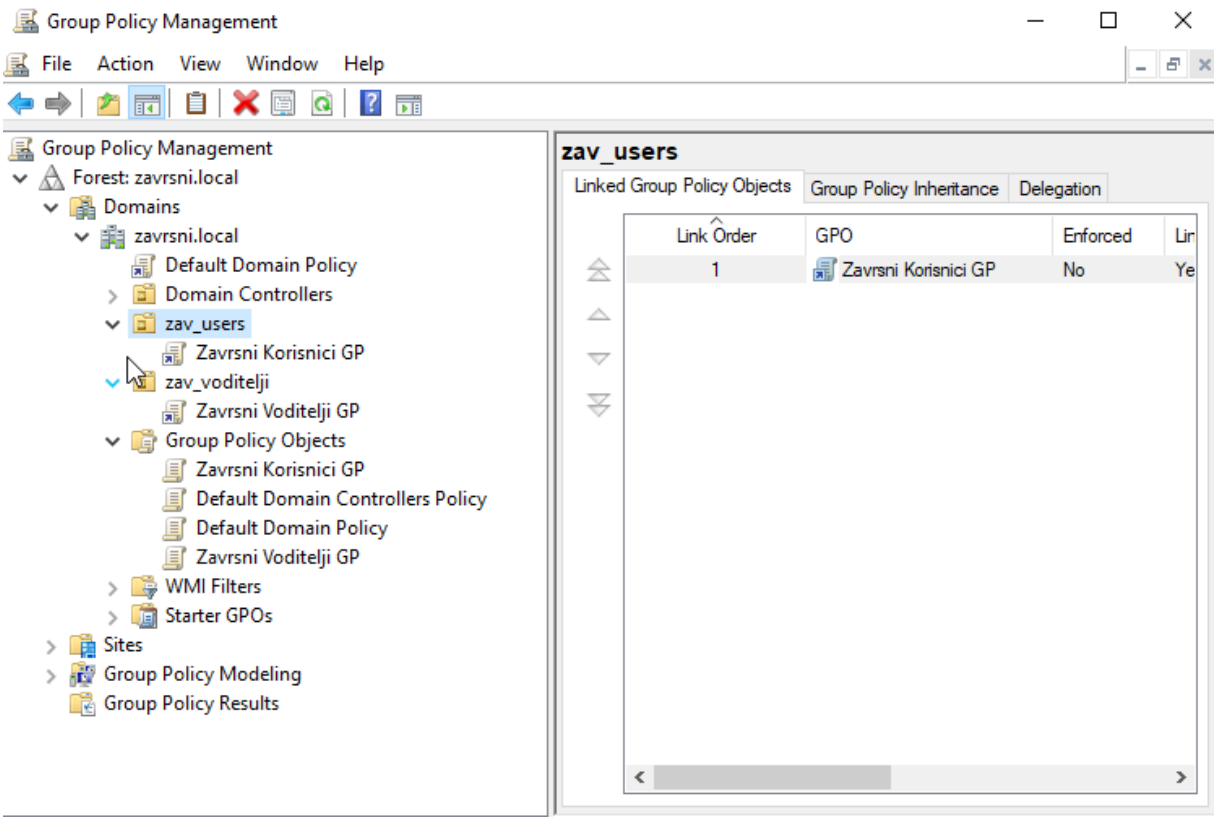


Slika 5. Prikaz korisnika grupe "zav_users"

5.2. Implementacija sigurnosne politike

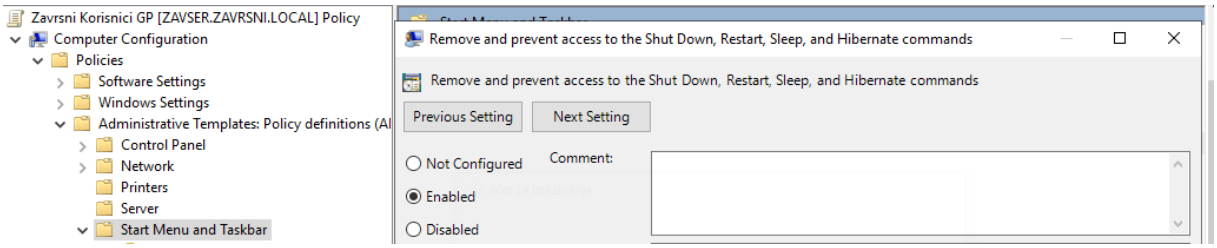
Nakon što su objašnjene uloge samih servisa koje su stavljene na server, moguće je preći na samu srž rada, a to je implementacija sigurnosne politike na samom serveru. Za ovaj dio rada, najbitniji dokument je dokument o sigurnosnoj politici, u ovome radu on se nalazi u poglavlju 3.2. Sigurnosna politika (Primjer za rad). Što se tiče alata koji se nalaze na serveru, bitan je alat za upravljanje pravilima grupe (eng. „Group Policy Managment“) unutar kojeg možemo implementirati sve ono što je navedeno unutar sigurnosne politike.

Za rad su kreirane dvije grupe sigurnosne politike jedna pod nazivom „Zavrsni korisnici GP“, a druga pod nazivom „Zavrsni voditelji GP“, te su povezane sa grupama korisnika, kao što je vidljivo na slici.



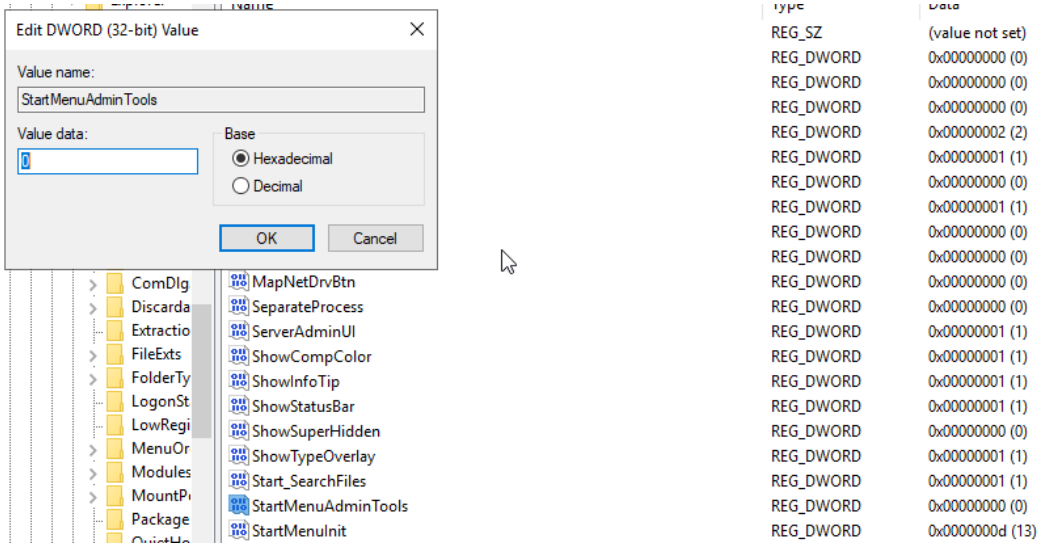
Slika 6. Povezivanje pravila sa kreiranom grupom korisnika

Unutar samog objekta grupne politike, moguće je podešavati ovlasti koje ima određena skupina korisnika. Za sam početak, u obje grupe je preko Group Policy-a maknuto da korisnik ili voditelj mogu ugasiti server. Razlog tome je što se na serveru mogu odrađivati bilo kakvi radovi, primjerice backup servera, te ako korisnik ugasi server, backup se neće odraditi do kraja, te u slučaju pada servera, neće se moći vratiti na zadnje ispravno stanje. Način na koji je to odrađeno je idući: Unutar samog GPO-a („Group Policy Object“) se pozicioniramo u konfiguraciju računala (eng. „Computer Configuration“), zatim u administrativne predloške (eng. „Administrative Templates“), te u početni meni (eng. „Start Menu and Taskbar“). Unutar mogućnosti se nađe opcija koja onemogućava vidljivost gumba za gašenje servera, te se ona omogući. Slika prikazuje kako to ustvari izgleda na serveru. Kod korisnika je i dalje vidljiv gumb za gašenje, ali on ga ne može koristiti, te se prikazuje poruka da nema mogućih radnji za tu postavku.



Slika 7. Onemogućavanje gumbova za korisnike

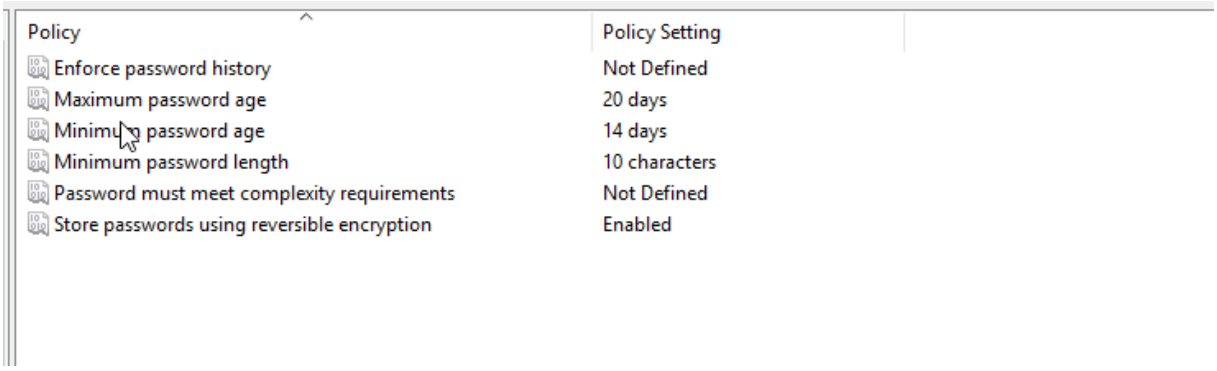
Iduća bitna stavka koja je odrađena je da niti voditelji niti korisnici ne mogu vidjeti administratorski alat. Pravo na administratorske alate, npr. „Group Policy Managment“ itd. uvijek ima samo administrator. Nitko drugi osim njega ne smije raditi preinake po korisničkim postavkama, postavkama servera i slično. To je napravljeno putem alata urednik registra (eng. „Registry Editor“). On je ustvari hijerarhijska baza koja služi za spremanje i uređivanje opcija operacijskog sustava. Unutar Editora se izabere opcija „StartMenuAdminTools„ i opcija vrijednost (eng. „Value data“) se postavi na 0, te se resetira server.



Slika 8. Onemogućavanje alata za korisnike

Iduće što je potrebno od administratorskih alata ostalim korisnicima je alat „Server Manager“. Ranije je već objašnjeno čemu on služi, te je prema tome lako zaključiti njegovu važnost, te zašto je onemogućen za sve ostale korisnike osim za administratora. On je onemogućen preko grupne politike, ali se i dalje nalazi na početnom meniju, ali tokom pristupa traži korisničko ime administratora i njegovu lozinku.

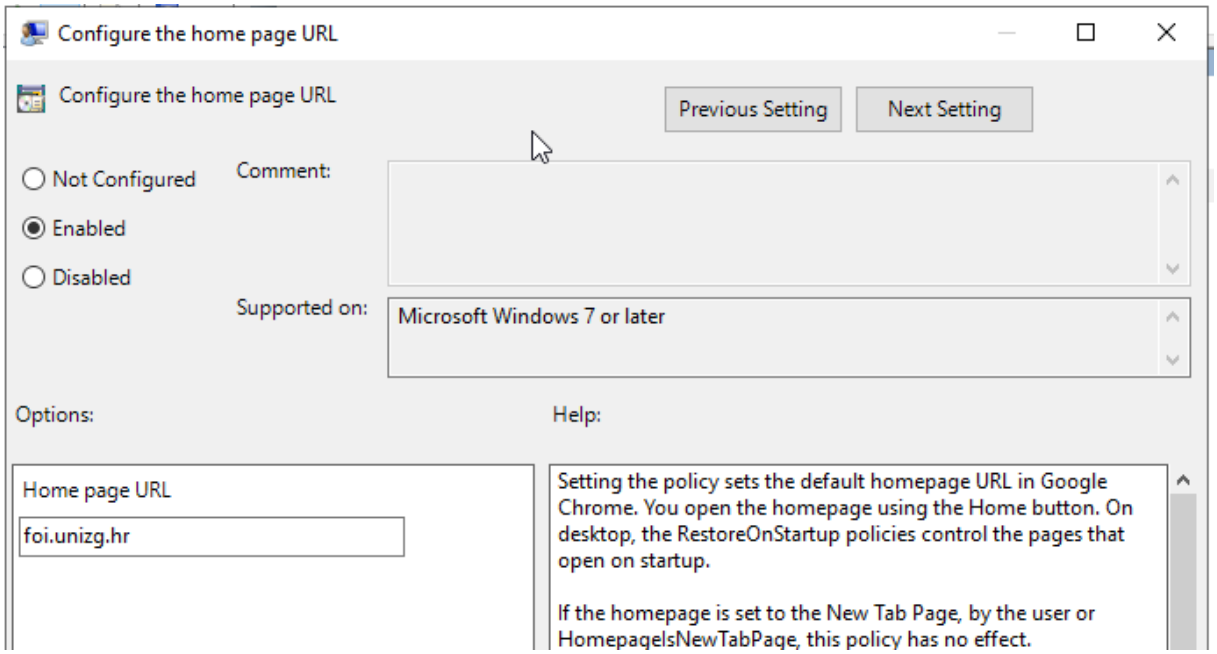
Zatim je implementirana politika vezana za šifre. Nakon što korisnik promijeni početnu šifru bitno je da ona ne traje zauvijek ili da se promijeni kada se korisnik toga sjeti, već da se nakon određenog vremena od korisnika traži da se ta šifra promijeni. Ovako se smanjuje rizik od nepoželjnih upada na nečiji korisnički račun. Par dana prije samog isteka valjanosti šifre, kreću se prikazivati obavijesti koliko još dana šifra traje. Ova opcija nametnuta je također preko grupne politike. I za korisnike i za voditelje vrijedi da se lozinka mora mijenjati minimalno svakih 14 dana, a maksimalno svakih 20 dana. Također, minimalan broj znakova koji lozinka mora imati je 10, te je omogućen obrnuti način enkripcije lozinke. Navedene postavke su vidljive na slici.



Slika 9. Prikaz postavki koje su postavljene za lozinke

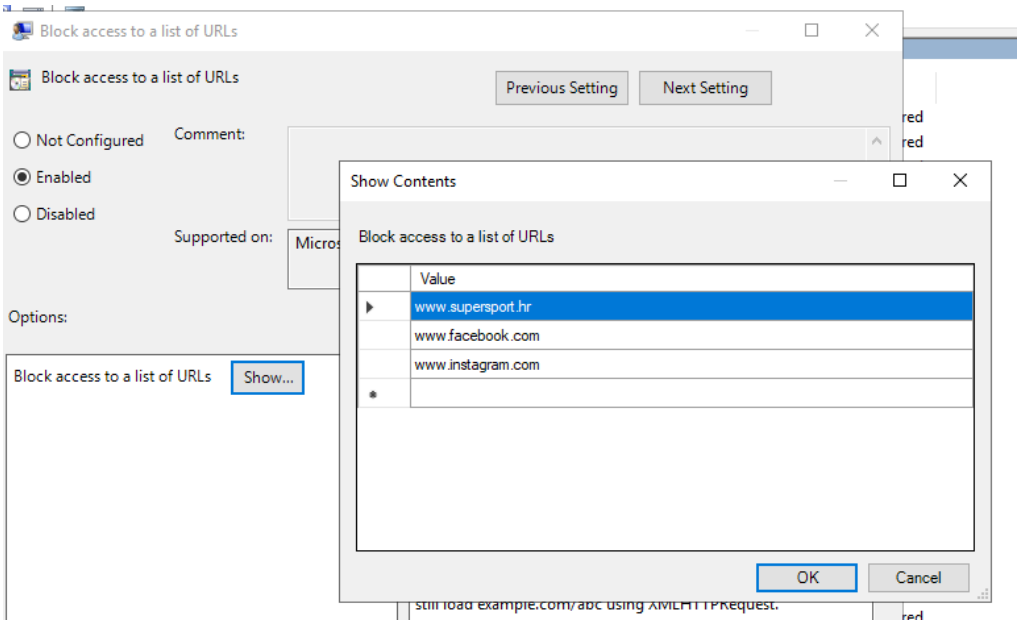
Iduće što je bitno definirati putem grupne politike je politika vezana za pretraživanje na internetu. Početni pretraživač koji dolazi sa serverom je Internet Explorer. Naknadno je dodan Google Chrome, te je njegova prečica dodana na radnu površinu. Bitno je da oba pretraživača imaju istu sigurnosnu politiku, tako da će prilikom otvaranja učitavati stranicu fakulteta, te će biti dodana lista stranica kojima korisnik ili voditelj neće moći pristupiti. Za Chrome pretraživač predložak za sigurnosnu politiku skinut je sa interneta, te je naknadno dodan u obje grupe.

Najprije je dodana mogućnost za dodavanje početne stranice prilikom otvaranja Chrome preglednika. Postavka koja to omogućava je „Konfiguracija URL-a početne stranice“ (eng. „Configure the home page URL“). Kao što je vidljivo na slici, postavljena je stranica foi.unizg.hr kao početna stranica prilikom otvaranja pretraživača.



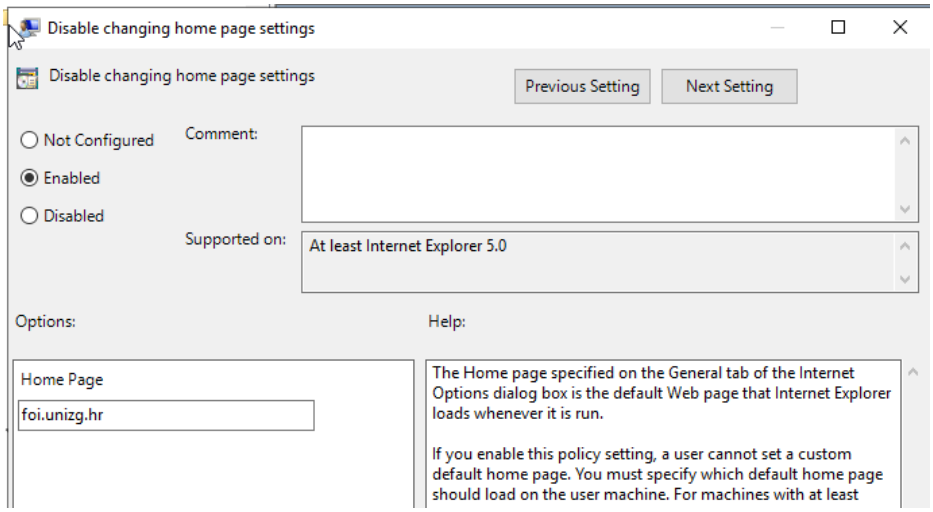
Slika 10. Postavljanje početne stranice za Chrome pretraživač

Isto tako, prilikom otvaranja se uz foi.unizg.hr otvara Google stranica u drugoj kartici. Nakon što su ove postavke podešene, iduće što je podešeno je lista stranica kojima korisnici ne mogu pristupiti. Postavka koja to omogućava je Blokirani pristup listi URL-a (eng. „Block Access to a list of URLs“). Kada se postavka omogući, omogućava se pristup gumbu koji vodi na listu gdje je moguće dodati neželjene stranice. Slika prikazuje kako izgleda ta lista. U bilo kojem trenutku moguće je dodati stranicu, te ažurirati sigurnosnu politiku na korisničkom računu, te se one automatski primjenjuju.



Slika 11. Postavljanje liste blokiranih stranica na Chrome pretraživaču

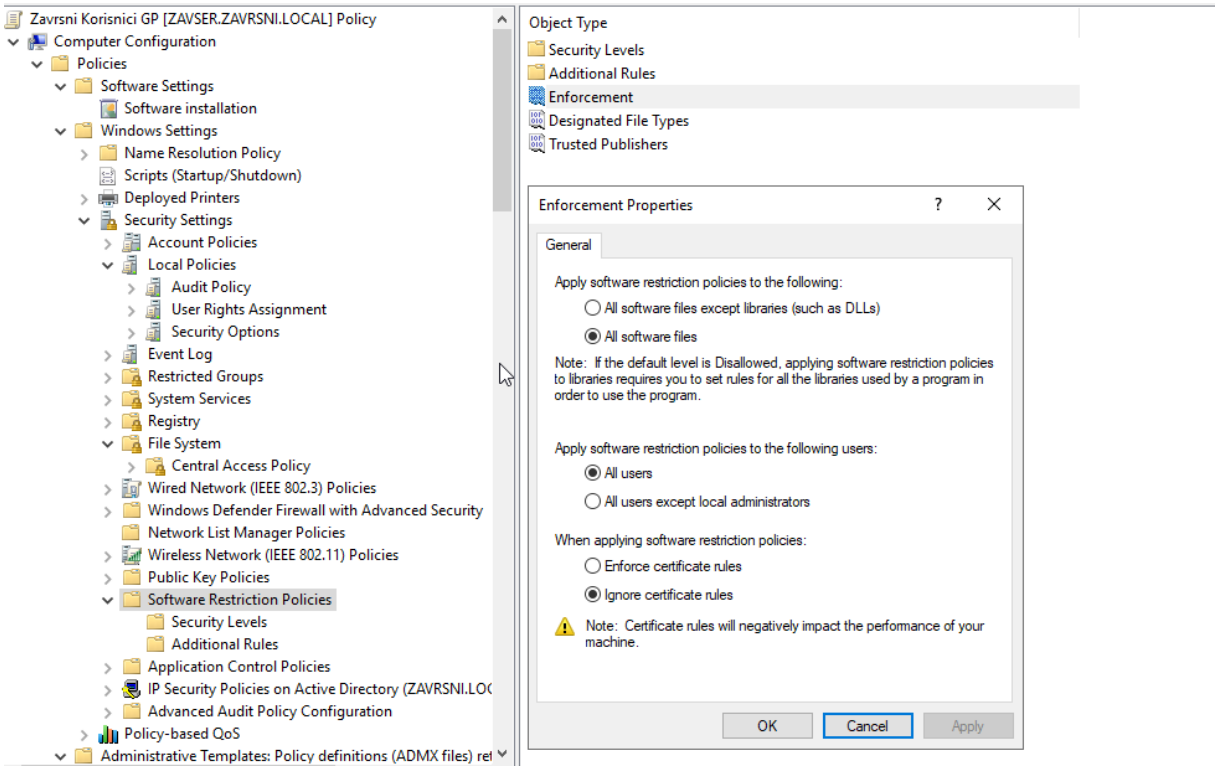
Nakon što su postavke podešene na Chrome pretraživaču, isto je potrebno napraviti i za Internet Explorer pretraživač, koji dolazi u samom instalacijskom paketu servera. Za njega nije potrebno ništa skidati sa interneta, nego su sve postavke već unutar GPO-a. postavke se nalaze unutar korisničke konfiguracije, te prva postavka koja je konfigurirana je podešavanje početne stranice. Za Internet Explorer se ona naziva Onemogućavanje promjena postavki početne stranice (eng. „Disable changing home page settings“). Početna stranica je podešena isto kao i na Chrome pretraživaču, na foi.unizg.hr, kao što je vidljivo na slici.



Slika 12. Postavljanje početne stranice za Internet Explorer

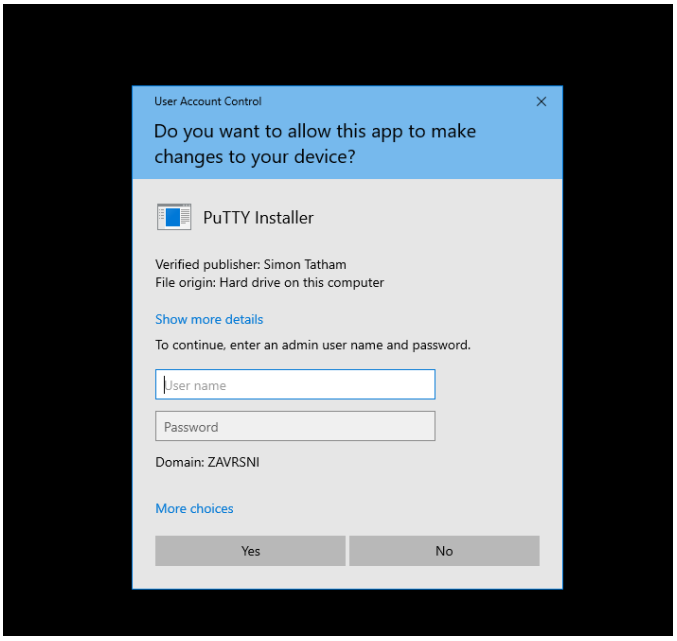
U drugoj kartici se isto otvara Google stranica, kao što je i prije postavljeno na Chrome pretraživaču. Nakon toga je konfigurirana lista stranica kojima korisnici i voditelji ne mogu pristupiti.

Također, za korisnika će biti onemogućeno skidanje bilo kakvog instalacijskog paketa, dok će voditelj imati tu opciju. Za korisnike je putem grupne politike onemogućena instalacija bilo kakvog alata, te se za to moraju javiti voditelju kako bi to odradili za njega. Ta postavka je podešena unutar grupne politike koja je vezana za grupu zav_users. Unutar uređivača grupnih pravila potrebno se pozicionirati na kompjutersku konfiguraciju, te zatim proširiti postavke koje su ispod politika, te unutar postavki za Windows, ući u mapu politika ograničenja softvera (eng. „Software Restriction Policies“). Nakon što se otvori mapa, potrebno je na primjenjivanju (eng. „Enforcement“) podesiti postavke tako da se postavke odnose na sve software datoteke, za sve korisnike. Također, unutar opcije određene vrste datoteka (eng. „Designated File Types“) potrebno je pogledati da li su svi tipovi datoteka dodani, te ako nisu, prema potrebi dodati tip koji nedostaje.



Slika 13. Podešavanje postavki za blokiranje instalacije programskih paketa

Kako to ustvari izgleda sa strane korisnika je slijedeće. Korisnik je u mogućnosti skinuti instalacijski paket, te slijediti uputu za instaliranje sve do opcije „Instalacija“. Kada klikne na to, pojavi se obavijest koja je vidljiva na slici.



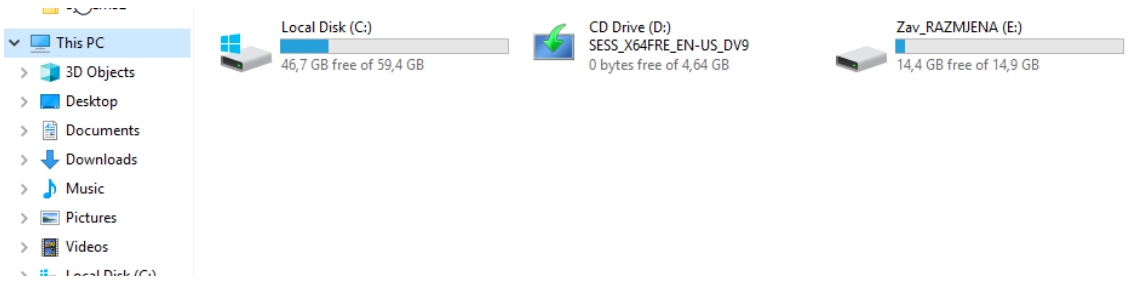
Slika 14. Prikaz obavijesti

Tek nakon što administrator ili voditelj unesu svoje korisničko ime i lozinku, instalacije je moguće dovršiti. Na ovakav način ograničava se potrošnja resursa koji su dodijeljeni serveru, zajedno sa sprječavanjem instalacija malicioznih kodova na serveru.

Nakon što je većina sigurnosnih „rupa“ ispravljena, te je sustav sigurniji nego u samome početku, moguće je rješavati danje točke sigurnosnog sustava. Za potrebe razmjene datoteka i mapa, kreiran je servis usluge datoteka i pohrane (eng. „File and Storage Services“). Za njega je dodan jedan virtualni disk, koji će kasnije služiti za pohranu podataka u skladišni bazen (eng. „Storage Pool“).

Skladišni bazen je grupa fizičkih diskova, koja omogućava agregaciju pohrane, proširenje elastičnog kapaciteta, te delegiranu administraciju nad diskovima. Iz spremišta je moguće kreirati jedan ili više virtualnih diskova, koji se još nazivaju i skladištima za pohranu. Za potrebe ovog rada kreiran je skladišni bazen pod nazivom „Zav_RAZMJENA“. Samo kreiranje je poprilično jednostavan proces. U server menadžeru se pozicioniramo na usluge datoteka i pohrane, zatim unutar izbornika odaberemo skladišni bazen i zatim u gornjem desnom uglu pod nazivom zadaci (eng. „Tasks“) odaberemo padajuću listu te u padajućoj listi odaberemo opciju novi skladišni bazen (eng. „New Storage Pool“). Otvori se čarobnjak, te odaberemo server na kojem će se nalaziti skladišni bazen, te na idućem koraku odaberemo disk koji će služiti kao pohrana.

Nakon što je kreiran skladišni bazen, potrebno je kreirati virtualni disk. Ranije je već objašnjena njegova uloga kod skladišnog bazena. On je također kreiran preko čarobnjaka, najprije je određen server za koji je vezan, zatim mu je dodano ime „Zav_RAZMJENA_VD“, te je odabran raspored skladištenja. Nakon što je odabran jednostavan raspored skladištenja, potrebno je specificirati vrstu opskrbe. Nakon što su određene postavke novog virtualnog diska, otvara se novi čarobnjak u kojem se dodaje obujam diska. Najprije se odabere veličina diska, zatim biramo naziv novog diska, te slovo koje će imati. U idućem koraku biramo sam naziv koji je stavljen na „Zav_RAZMJENA“. Nakon što je završeno kreiranje volumena diska, moguće je provjeriti da li je ustvari kreiran. Provjera se izvršava na način da se uđe u mape, te se pod ovim računalom, ispod upravljačkih programa i uređaja (eng. „Devices and Drivers“) vidi kreirani disk.

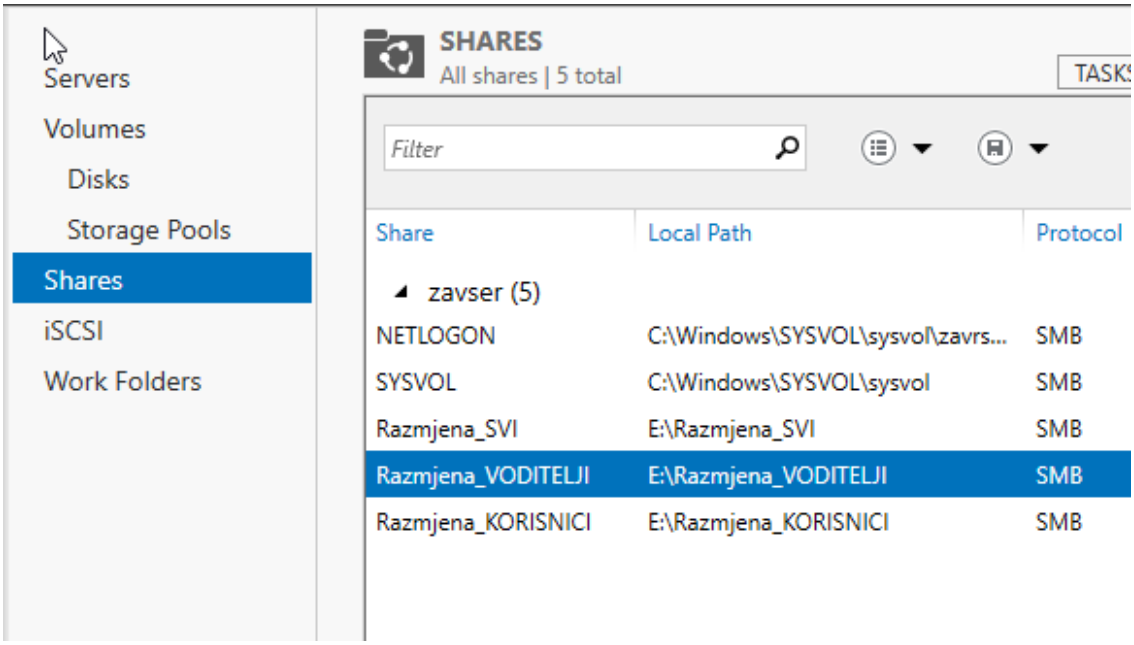


Slika 15. Prikaz novokreiranog diska za pohranu podataka

Također, provjeru je moguće izvršiti i sa alatom za upravljanje diskovima (eng. „Disk Management“), gdje će nam se prikazati kreirani disk. Nakon toga je moguće kreirati mape za razmjenu. Prije samom kreiranja mape, bitno je omogućiti jedan servis, pod nazivom Windows sinkronizirano dijeljenje (eng. „Windows Sync Share“). Prvi puta kada se instalira na računalo potrebno ga je samostalno pokrenuti, ali kasnije se automatski sam pokreće. Ono omogućava sinkroniziranje korisnika i datoteka koje su na datotečnom serveru. U ovome slučaju biti će kreirane 3 radne mape, jedna će biti samo za grupu „zav_users“, druga samo za „zav_voditelji“, a trećoj će svi moći pristupiti, ali „zav_users“ će imati mogućnost samo čitanja datoteka, dok će grupa „zav_voditelji“ imati mogućost čitanja, pisanja, te kreiranja datoteka. Datoteke će moći obrisati samo administrator. Na ovaj način se radi prevencija brisanja datoteka za koje netko misli da je nebitna, dok su drugoj osobi od iznimno velike važnosti.

Način dodavanja nove mape koja će služiti je jednostavan. Odabere se opcija dijeljenje (eng. „Shares“), te se u gornjem desnom uglu, klikne na zadatke, te se unutar padajućeg izbornika odabere novo dijeljenje (eng. „New Shares“). Najprije se odabere profil mape za razmjenu, nakon toga lokacija gdje će se nalaziti, u ovome slučaju to će biti na prije kreiranom disku „Zav_RAZMJENA“. Zatim se dodaje ime mapi. Najprije će biti kreirana mapa

„Razmjena_SVI“, kojoj će svi moći pristupati, zatim „Razmjena_VODITELJI“ koja je kreirana samo za voditelje, te na posljetku „Razmjena_KORISNICI“ koja je namijenjena samo za korisnike. Nakon što je dodijeljeno ime, moguće je omogućiti/onemogućiti još neke postavke, npr. da neka grupa uopće ne vidi mapu ili da je mapa vidljiva samo za čitanje. Na zadnjem koraku se dodaju grupe korisnika koje imaju prava na mapu.

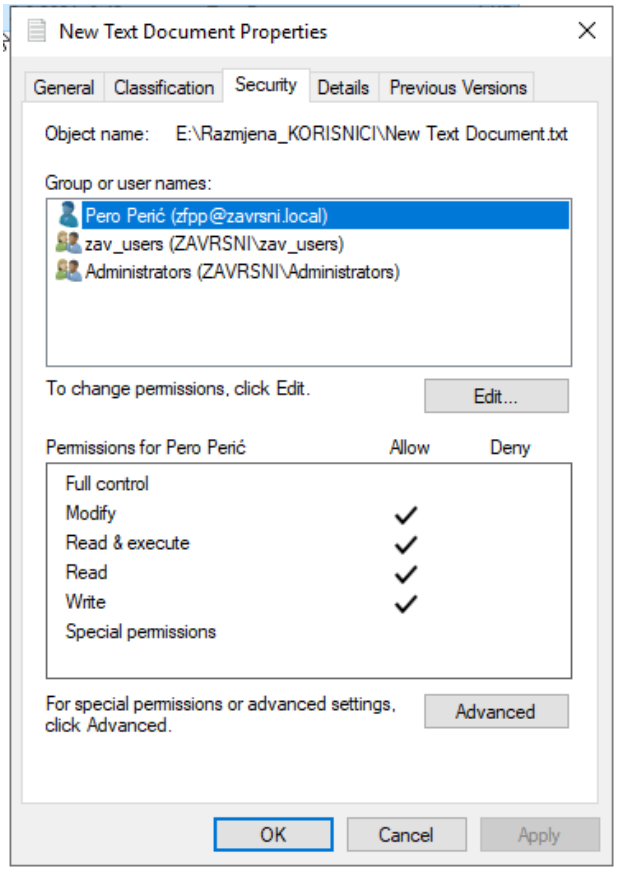


Slika 16. Mape za korisnike kreirane unutar diska za razmjenu podataka

U mapi „Razmjena_SVI“ kreirana je datoteka pod nazivom „Bitan Dokument“. Korisnik pod nazivom zfac, koji je u grupi „zav_users“ može vidjeti sve 3 mape koje su kreirane na disku, ali kada proba pristupiti mapi „Razmjena_VODITELJI“ prikazuje mu se obavijest kako nema pristup grupi, te ako želi pristupiti mora netko od voditelja unijeti svoje korisničko ime i lozinku. Mapi „Razmjena_SVI“ može pristupiti, te mu se prikažu sve datoteke koje se nalaze unutar mape. Korisnik ima mogućnost preurediti datoteku, te ju spremiti kao takvu, ali nema mogućnost obrisati datoteku. Unutar „Razmjena_KORISNICI“ korisnik zfac može kreirati datoteke, uređivati ih, spremati izmjene, te brisati datoteke prema potrebi.

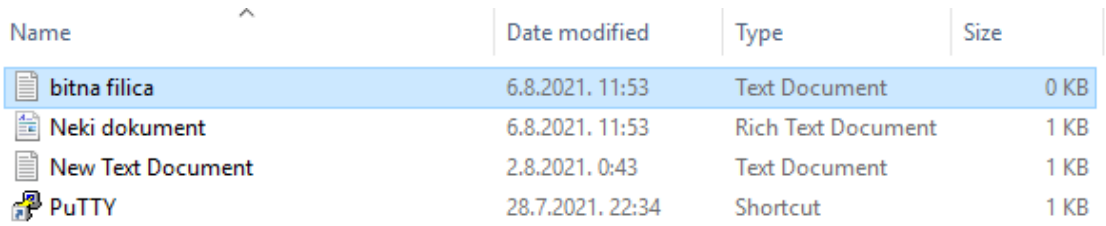
Za korisnika zfpp, odnosno za ulogu voditelja vrijede iduće ovlasti što se tiče mapa koje su kreirane na disku. Unutar mape „Razmjena_SVI“ može editirati datoteke, spremati ih u takvome formatu, čitati, no ne može ih brisati. Unutar mape „Razmjena_VODITELJI“ može kreirati nove datoteke, čitati ih, editirati, te brisati. Kada pokuša pristupiti mapi „Razmjena_VODITELJI“ prikazuje mu se obavijest kao i kod korisnika kada pokuša pristupiti mapi „Razmjena_KORISNICI“.

Administrator ima sve ovlasti na sve 3 mape, te prema potrebi može dodavati određena propuštanja na neke od datoteka. Npr. ako voditelj treba pristup određenoj datoteci unutar mape „Razmjena_KORISNICI“ biti će mu omogućeno. Isto tako ako je potrebno preurediti nešto u toj datoteci, bit će mu omogućeno. Takve postavke će biti će podešene unutar samih mapa i to na dokumentima. Unutar samih postavki dokumenta, unutar kartice Sigurnost vidljiv je popis grupa i/ili korisnika koji mogu pristupiti datoteci, isto kao i njihova prava nad tom datotekom. Kao što je vidljivo na slici, unutar mape „Razmjena_KORISNICI“ omogućeno je pravo voditelju Pero Perić da vidi datoteku, te da ju može modificirati, te spremati sa promjenama koje je izvršio nad njom.



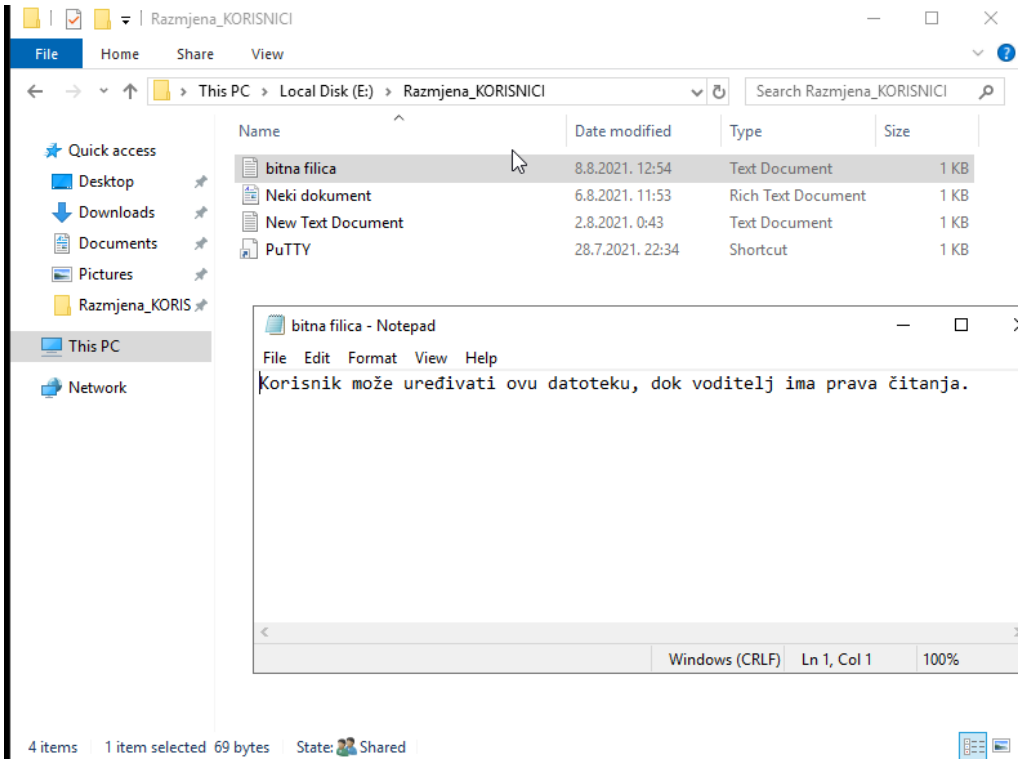
Slika 17. Dodavanje prava na datoteku

Voditelj Pero Perić će vidjeti samo tu datoteku unutar čitave mape, jer nad ostalim datotekama mu nisu dodana prava. Na slici su vidljive sve datoteke koje su dodane u mapu, te ih korisnik ima mogućnost vidjet.

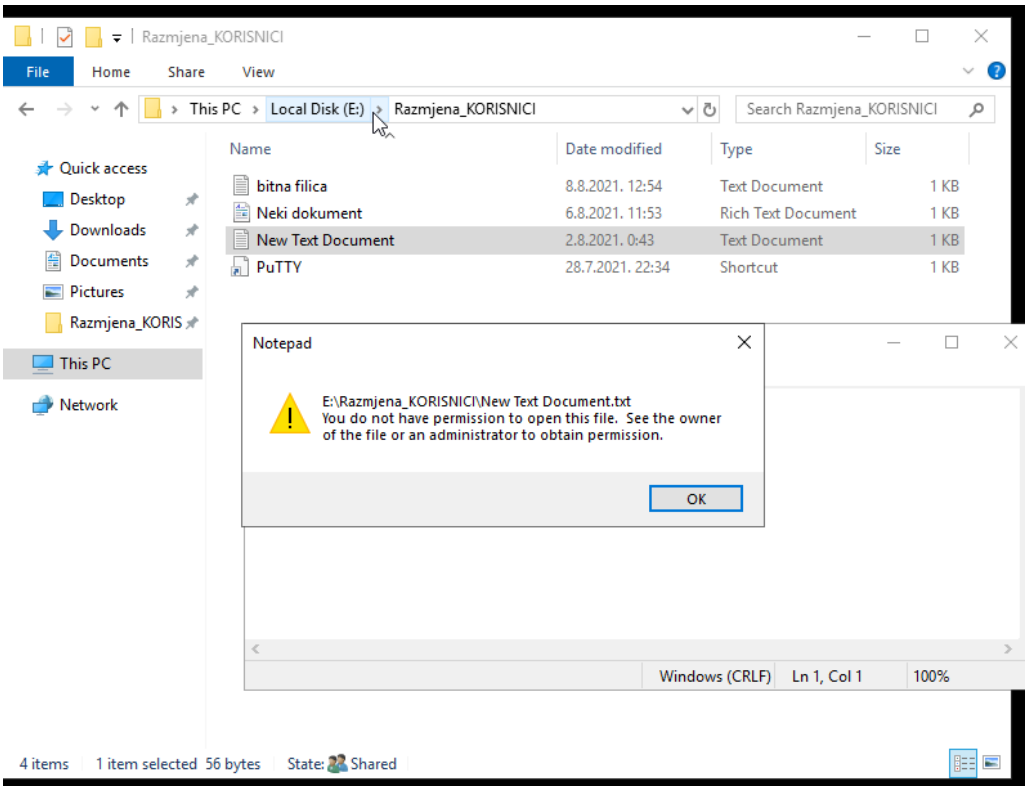


Slika 18. Prikaz datoteka unutar mape „Razmjena_KORISNICI“

Iduća slika prikazuje kako voditelj vidi tu istu mapu, te datoteke koje se u njoj nalaz, no ne može vidjeti sadržaj datoteka osim one na kojoj su mu dana prava. Također, voditelju je potrebno dodati pravo da može ući u mapu „Razmjena_KORISNICI“, a to je odrađeno preko server menadžera. Nakon što mu je dodano pravo, bitno je u datotekama izmijeniti prava pristupa, kako voditelj ne bi mogao pristupiti datotekama za koje mu ne treba pristup.



Slika 19. Prikaz sadržaja datoteke koji voditelj vidi



Slika 20. Odbijen pristup datoteci

6. Zaključak

Nakon svega navedenog, moguće je vidjeti zašto je sigurnosna politika toliko bitna u modernim tvrtkama i institucijama. Ona je sam korijen sigurnosti i zaštite informacija i podataka. U slučaju da je zapostavljena ili da se konstantno ne ažurira i poboljšava, posljedice mogu biti katastrofalne. Također, bitno je da je dio politike koji se dotiče informatike bude adekvatno definiran prema samom sustavu na kojem se ona implementira. U ovome slučaju to je Windows operacijski sustav, te se prema tome za njega mora razviti zasebna politika, jer nema iste prednosti i mane kao Linux ili MacOS.

U samome početku Windows nije omogućavao toliko veliku implementaciju sigurnosne politike kao što to omogućava danas. Moguće je vidjeti kako je kroz godine napredovao, te sukladno time je dolazilo više mogućnosti. No, kako se Windows razvijao, tako isto su se sigurnosne politike morale mijenjat, jer svaka verzija je imala drugačije prednosti i mane. Tako je bitno da sigurnosna politika bude u razmjerima sa zadnjom verzijom, kako bi se neke moguće sigurnosne mane Windows sustava uočile, te na vrijeme „zakrpale“, kako kasnije ne bi bilo posljedica.

7. Literatura

[1] CARNet (2009) *Sigurnosna politika*

[2] D. Pleskonjić, B. Đorđević, M. Carić, N. Maček (2007) *Sigurnost računarskih sistema i mreža.* Beograd: Mikro knjiga

[3] B. Javorović, M. Bilandžić (2007) *Poslovne informacije i business intelligence.* Zagreb: Golden marketing - Tehnička knjiga

[4] Ž. Panian (2001) *Kontrola i revizija informacijskih sustava.* Zagreb: Sinergija

[5] L. Irwin (2019) *What is the ISO 27000 series of standards?* Preuzeto s https://www.itgovernance.co.uk/

[6] S. Gibbs (2014) *From Windows 1 to Windows 10: 29 years of Windows evolution* Preuzeto s https://www.theguardian.com/

[7] S. Bosworth, M.E. Kabay (2002) *Computer security handbook -4th edition*. New York: John Wiley & Sons

[8] H.F. Tipton, M. Krause (2007) *Information security management handbook -6th edition*. Boca Raton: Auerbach Publications

[9] A. Willings (2021) *A brief history of Microsoft Windows through the ages.* Preuzet s https://www.pocket-lint.com/

[10] M. Bishop (2003) *Computer security : art and science.* Boston: Addison-Wesley

[11] A. Calder, S.Watkins (2008) *IT governance : a manager's guide to data security and ISO 27001/ISO 27002.* London and Philadelphia : Kogan Page

[12] J. Dykstra (2016) *Essential cybersecurity science : build, test, and evaluate secure systems.* Sebastopol: O'Reilly

[13] S. Liu (2020) *Information security - Statistics & Facts.* Preuzeto s https://www.statista.com/

[14] J. Vijayan (2020) *31 cybersecurity stats that matter.* Preuzeto s https://techbeacon.com/

[15] D. Walkowski (2019) *What Is the CIA Triad?* Preuzeto s https://www.f5.com/

8. Popis slika

Slika 1. Postavke u alatu "VirtualBox" 3

Slika 2. Statistički podaci korištenja operacijskih sustava za stolna računala 9

Slika 3. Udjeli operacijskih sustava na svjetskom tržištu za stolna računala 10

Slika 4. Server Manager 18

Slika 5. Prikaz korisnika grupe "zav_users" 19

Slika 6. Povezivanje pravila sa kreiranom grupom korisnika 20

Slika 7. Onemogućavanje gumbova za korisnike 21

Slika 8. Onemogućavanje alata za korisnike 21

Slika 9. Prikaz postavki koje su postavljene za lozinke 22

Slika 10. Postavljanje početne stranice za Chrome pretraživač 23

Slika 11. Postavljanje liste blokiranih stranica na Chrome pretraživaču 24

Slika 12. Postavljanje početne stranice za Internet Explorer 24

Slika 13. Podešavanje postavki za blokiranje instalacije programskih paketa 25

Slika 14. Prikaz obavijesti 26

Slika 15. Prikaz novokreiranog diska za pohranu podataka 27

Slika 16. Mape za korisnike kreirane unutar diska za razmjenu podataka 28

Slika 17. Dodavanje prava na datoteku 29

Slika 18. Prikaz datoteka unutar mape „Razmjena_KORISNICI“ 30

Slika 19. Prikaz sadržaja datoteke koji voditelj vidi 30

Slika 20. Odbijen pristup datoteci 31