Sigurnosni povrat elektroničke pošte u Microsoft Exchange sustavu

Jurić, Franjo

VELEUČILIŠTE SUVREMENIH INFORMACIJSKIH TEHNOLOGIJA

STRUČNI PRIJEDIPLOMSKI STUDIJ INFORMACIJSKIH TEHNOLOGIJA

Franjo Jurić

ZAVRŠNI RAD

SIGURNOSNI POVRAT ELEKTRONIČKE POŠTE U MICROSOFT EXCHANGE SUSTAVU

Zagreb, listopada 2024.

Veleučilište suvremenih informacijskih tehnologija
10000 Zagreb, Ulica Vjekoslava Klaića 7

Studij:	Stručni prijediplomski studij informacijskih tehnologija smjer programiranje
Student:	**Franjo Jurić**
Matični broj:	2018007

Zadatak završnog rada

Predmet:	Arhitektura poslužiteljskih računala
Naslov:	**Sigurnosni povrat elektroničke pošte u Microsoft Exchange sustavu**
Zadatak:	U teorijskom dijelu potrebno je obraditi povijest Microsoft Exchange sustava, njegove verzije te strukturu sustava, što uključuje strukturu baza elektroničke pošte i samih poštanskih sandučića, te obraditi izradu sigurnosne kopije i funkcionalnost zapisa u Microsoft Exchange sustavu. U praktičnom dijelu prikazati nekoliko primjera povrata elektroničke pošte, načine onemogućavanja te omogućavanja poštanskog sandučića te uklanjanje poštanskog sandučića korisnika ovisno o poslovnim potrebama.
Mentor:	Dražen Novina, pred.
Zadatak uručen kandidatu:	2.10.2023.
Rok za predaju rada:	23.10.2024.
Rad predan:	_____

Povjerenstvo:

Saša Punčikar, pred.	član predsjednik	_____
Dražen Novina, pred.	mentor	_____
Dubravko Žižak, pred.	član	_____

SADRŽAJ

POPIS SLIKA

POPIS TABLICA

1. UVOD

Mogućnost sigurnosnog povrata podataka je neophodna u poslovanju kako bi se održao kontinuitet poslovanja u slučaju neželjenih događaja (korupcija podataka, neželjeno šifriranje podataka, problemi s diskovnim sustavima i dr.). Sigurnosna kopija podataka i arhiva podataka pohranjuje se na uređajima poput vanjskog tvrdog diska, usluge u oblaku, mrežne pohrane (engl. NAS, Network Attached Storage), trake za sigurnosno kopiranje i dr.

Digitalizacija je transformirala način na koji čuvamo informacije i podatke gdje s razvojem društva i poslovanja, raste potreba za pohranom podataka. Bez učinkovitog upravljanja sigurnosnim podacima, organizacije bi mogle biti manje učinkovite, manje konkurentne i podložnije rizicima. Zbog navedenog je upravljanje sigurnosnim podacima ključna komponenta svih složenih sustava i organizacija. Prikupljanje i povjerljivost podataka u digitalnom okruženju danas je postalo izrazito važno i zbog toga prikupljene i povjerljive podatke ne treba sagledavati samo s tehničke strane koju nosi sam pojam riječi zaštita, već povjerljivost podataka treba sagledavati kroz niz drugih aspekata, kao što su neovlašteni pristup, krađa i zloupotreba podataka.

Potreba za sigurnosnom pohranom i povratom podataka u digitalnom dobu naglašena je zbog brojnih faktora i rizika koji mogu ugroziti integritet, dostupnost i privatnost podataka. Gubitak informacija potrebnih za rad tvrtke i gubitak ugleda mogu imati ozbiljne posljedice za poslovanje.

Microsoft Exchange u poslovnom okruženju može donijeti značajne poslovne koristi i vrijednost. Microsoft Exchange sustav omogućava organizacijama da uspostave profesionalnu i pouzdanu dostupnost elektroničke pošte koja je ključna za komunikaciju unutar i izvan tvrtke. Ključan dio zašto se mnoge organizacije odlučuju za Exchange je mogućnost arhiviranja elektroničke pošte, kontrolu pristupa, autentifikacija i dr. Upravo navedeno je važno za organizacije koje moraju poštivati zakonske i regulatorne zahtjeve za zaštitu podataka.

U drugom poglavlju predstavljena je kratka povijest potrebe za pouzdanom pohranom podataka i zaštitom informacija. Prikazane su različite metode pohrane podataka te alati koji omogućavaju povrat podataka. U radu je opisan razvoj i potreba za Microsoft Exchange sustavom te njegova uloga s Aktivnim direktorijem koja je ključa za pravilno funkcioniranje.

U trećem dijelu opisuje se struktura baza i struktura poštanskih sandučića u Microsoft Exchange Serveru. Dodatno je pojašnjena funkcija izvoza i povrata poštanskog sandučića u Microsoft Exchange sustavu, uz procese za sigurnosnu pohranu i obnovu elektroničke pošte i povezanih podataka u poštanskom sandučiću. Navedene funkcionalnosti se koriste za migraciju, povrat

izgubljenih elektroničkih poruka ili prijenos sadržaja poštanskog sandučića na drugog korisnika.

U četvrtom poglavlju prikazani su primjeri oporavka izbrisanih stavki u poštanskom sandučiću. Korišteni su mehanizmi za onemogućavanje i omogućivanje poštanskog sandučića korisnika te uklanjanje bez potrebe da se briše cijela baza podataka. Ključan primjer je sigurnosna kopija baze podataka poštanskog sandučića jer pokazuje koliko je bitna zaštita informacija i pravilna implementacija kao bi se spriječio gubitak vrijednih podataka.

2. POHRANA I POVRAT PODATAKA

Svjedoci smo brzog razvoja tehnologija i potreba za pouzdanom pohranom i zaštitom informacija. Danas se pohrana i povrat podataka sve više temelje na digitalnim tehnologijama, uključujući napredne alate za pohranu u oblaku, virtualizaciju i automatizaciju oporavka podataka. Povijest pohrane i povrata podataka proteže se kroz desetljeća i odražava razvoj tehnologija i potrebe za zaštitom i očuvanjem informacija. Uvođenjem računalnih tehnologija dolazi do revolucije u sigurnosnoj pohrani i povratu podataka. Tijekom sigurnosne pohrane i povrata podataka ključna je zaštita informacija od gubitka ili oštećenja, neovisno o tome radi li se o računalima, mobilnim uređajima ili poslužiteljima. Podaci su izloženi različitim rizicima kao što su tehnički kvarovi, zlonamjerni napadi i ljudska pogreška. Podaci mogu biti različitih vrsta, a najčešći su:

- tekst
- slike
- videozapisi
- audio zapisi
- tablice
- softverske datoteke i dr.

Svaka vrsta podataka može zahtijevati različite metode pohrane, ovisno o svojim karakteristikama, potrebama i sigurnosnim zahtjevima.

Povrat podataka (eng. data recovery) odnosi se na proces oporavka podataka s medija za pohranu podataka nakon što su podaci izgubljeni ili postali nedostupni iz različitih razloga. Mediji za pohranu podataka su:

- tvrdi diskovi
- magnetske trake
- memorijske kartice
- pohrana u oblaku i dr.

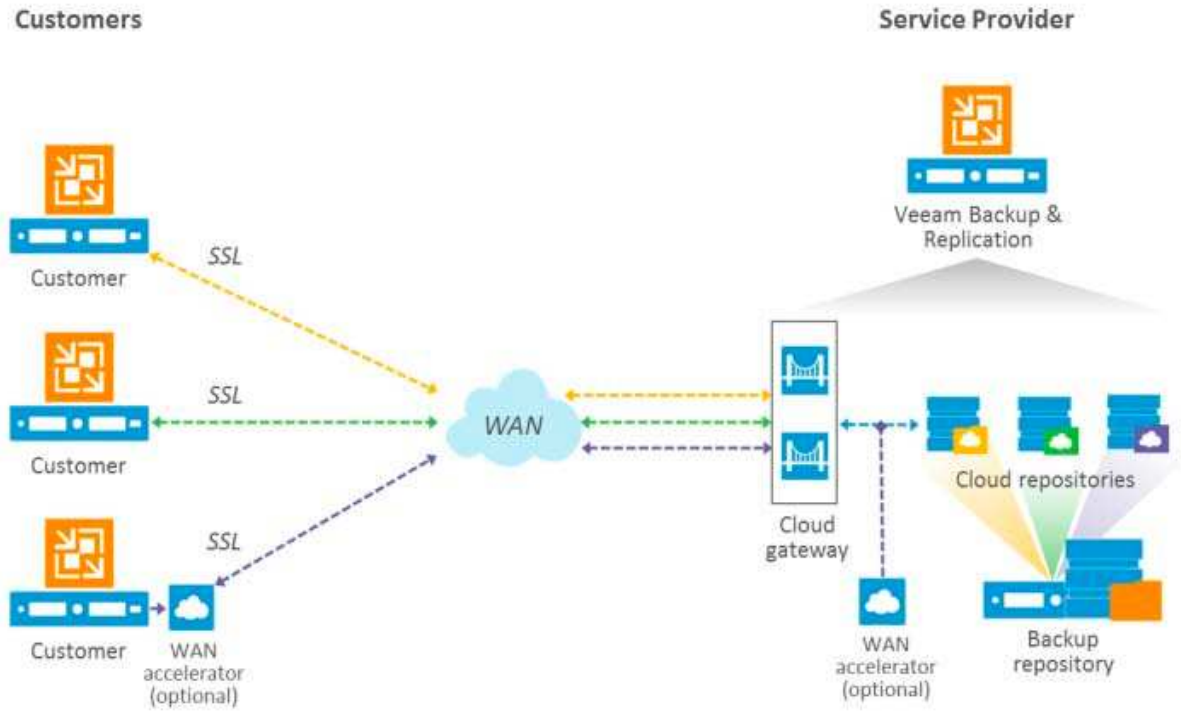
Povrat podataka je važan proces jer omogućava povrat vrijednih informacija koje su izgubljene ili oštećene.

2.1. Vrste pohrane podataka

Postoje različite metode i alati za povrat podataka. Od sigurnosne kopije do kloniranja diska, što je zapravo stvaranje identične kopije sadržaja jednog diska, te kopiranja na drugi disk.

Sigurnosna kopija (eng. backup) je proces stvaranja kopije podataka kako bi se omogućila

obnova tih podataka u slučaju gubitka istih podataka. Sigurnosne kopije mogu se pohraniti na različite načine, uključujući lokalno na fizičkim medijima (kao što su vanjski tvrdi diskovi ili optički mediji), u oblaku (koristeći usluge za pohranu podataka u oblaku) ili na udaljenim lokacijama (na primjer, u drugim poslovnim prostorima za oporavak od katastrofe). Primjer Slika 1 prikazuje jednu od arhitektura sigurnosne pohrane podataka u oblaku.

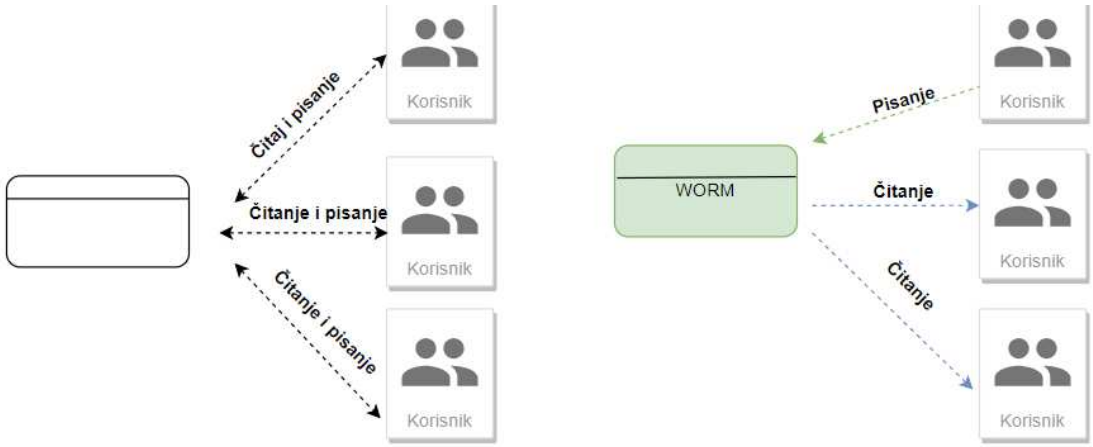


Slika 1. Arhitektura sigurnosne pohrane podataka

Retencija sigurnosne pohrane odnosi se na definirano vrijeme koliko dugo će organizacija čuvati određene vrste podataka. Prilagodba retencije ovisi o vrsti medija koji se koristi za sigurnosnu pohranu. Različiti mediji imaju različite karakteristike i dugovječnost. Na primjer, tvrdi diskovi mogu imati kraći vijek trajanja od arhivskih traka. Retencija podataka je ključni aspekt upravljanja podacima i često je usklađena sa zakonima i regulativama. Zbog zakona, ali i regulativa, tvrtke moraju čuvati pojedine vrste podataka u određen vremenski period. Pojedine vrste podataka mogu uključivati praksu arhiviranja starijih podataka koji više nisu aktivno korišteni, ali se moraju čuvati iz zakonskih ili operativnih razloga. Arhiviranje podataka je postupak dugoročnog očuvanja podataka na posebnim medijima kao što su tvrdi diskovi koji imaju brz pristup podacima, te su prikladni za kratkotrajno arhiviranje, dok su nedostaci ograničeni životni vijek te podložnost fizičkim oštećenjima.

WORM (engl. WORM, Write Once, Read Many) je naziv koja se odnosi na tehnologiju korištenu za pohranu ili pisanje i čitanje podataka (Slika 2). Ova tehnologija odnosi se na sustave za pohranu podataka koji omogućavaju da se podaci zapisuju samo jednom, nakon čega

se ne mogu mijenjati, ali se mogu čitati neograničen broj puta. Često se koristi u kontekstu pohrane podataka gdje je potrebna visoka razina sigurnosti i nepromjenjivosti podataka. U suštini, WORM tehnologija osigurava da jednom zapisani podaci ostanu nepromijenjeni i sigurni od promjena ili brisanja. To je posebno važno u situacijama gdje je povjerenje i integritet podataka od ključne važnosti.



Slika 2. Napiši jednom, pročitaj više puta (engl. WORM.)

2.2. Privremeno vraćanje obrisanih poštanskih sandučića i poruka u bazi

Privremenim brisanjem poštanskog sandučića ili poruka odnosi se na proceduru u kojoj se obrisani podaci ne brišu odmah trajno iz baze podataka, već ostaju pohranjeni određeno vrijeme. Definirani period pohrane obično se postavlja do 30 dana. Ova metoda pruža brojne prednosti jer omogućuje jednostavniji oporavak podataka bez potrebe za vraćanjem kompletne baze podataka (eng. Restore.).Zbog perioda do 30 dana korisnici mogu upravljati aplikacijom npr. Microsoft Outlook (Exchange online/Office 365) da privremeno vrate obrisane poruke. Poruke koje su otišle u mapu obrisane poruke korisnik odabirom obnoviti (eng. Restore) može vratiti obrisane poruke. Ako su poruke obrisane trajno iz mape obrisane poruke korisnik ima mogućnost povrata poruka iz mape oporavljive poruke (eng. RecoverableItems), gdje se u mapi obrisane stavke odabire opcija oporavi poruke nedavno uklonjene iz ove mape. Administratori imaju dodatne ovlasti i alate koje omogućuju upravljanje povratom obrisanih korisničkih elektroničkih poruka i poštanskih sandučića na razini koja nije dostupna običnim korisnicima. Imaju pristup sigurnosnim kopijama podataka sustava koje mogu koristiti za vraćanje obrisanih poruka ili cijelih poštanskih sandučića. Postavljanjem pravila o zadržavanju podataka administrator određuje koliko dugo će obrisane poruke biti zadržane prije nego što se trajno uklone.

2.3. Microsoft Exchange Server

Razvojem tehnologija koje na samom začetku postavljaju temelje razvoja modernog globalnog internetskog sustava javlja se potreba komunikacije putem računalnih mreža. Prvi takav sustav koji omogućuje slanje pošte, naziva elektronička pošta (engl. Email) napravljen na tadašnjoj mreži ARPANet (engl. ARPANet, Advanced Research Project Agency Network). ARPANet put započinje kao eksperimentalna mreža prvobitno povezivana unutar četiri sveučilišta u SAD-u. Prvi primjeri elektroničke pošte bile su tekstualne poruke, prvenstveno slane od strane institucija kao što su sveučilišta ili vlada. Poruke nisu bile dostupne za šire mase već za manje skupine korisnika. Mailbox postaje prvi program napravljen u komercijalne svrhe prvenstveno korišten od strane poslovnih korisnika i znanstvenika. Tijekom godina sustav elektroničke pošte raste te povezuje sve više organizacija, ali se još uvijek radi o pionirskom projektu koji postavlja temelje modernog komunikacijskog sustava. Popularnost interneta naglo raste razvojem World Wide Web od strane Europske organizacije za nuklearna istraživanja (engl. CERN, The European Organization for Nuclear Research). Radi se o sustavu koji omogućuje jednostavniju i lakšu upotrebu interneta. Elektronička pošta postaje komercijalno dostupna u svakodnevnom životu ljudi i standardizira način komunikacije u digitalno doba.

Microsoft je izdao različite verzije Exchange Servera kroz godine:

- Exchange Server 2010,
- Exchange Server 2013,
- Exchange Server 2016,
- Exchange Server 2019 i
- Exchange Online (dio Microsoft 365 / Office 365 usluge)

Microsoft svakom novom verzijom donosi poboljšanja koja uključuju performanse, sigurnost, te funkcionalnost.

Exchange Server koristi složenu arhitekturu koja se sastoji od različitih komponenata, koje uključuju:

- poslužitelj poštanskog sandučića (engl. Mailbox server)
- poslužitelj pristupa korisnika (engl. User access server)
- rubni poslužitelj (engl. Edge server)

Exchange Server sadrži i sigurnosne mehanizme kao što su:

- protokoli zaštite od neovlaštenog pristupa
- mogućnosti enkripcije
- kontrola pristupa

- antivirusna zaštita
- sigurnosne grupe

Administracija Exchange Servera se vrši putem Microsoft Management Console (MMC), Windows PowerShell ili web sučelja za upravljanje Exchange sustava.

Tablica 1. Microsoft Exchange Server verzije

Ime verzije Exchange Servera	Datum izlaska	Datum završetka standardne podrške	Datum završetka proširene podrške	Trenutno korištena verzija
4.0	1 Svibanj 1996	N/A	N/A	Ne
5.0	23 Svibanj 1997	31 Prosinac 2003	10 Siječanj 2006	Ne
5.5	20 Ožujak 1998	31 Prosinac 2003	10 Siječanj 2006	Ne
2000	29 Studeni 2000	31 Prosinac 2005	11 Siječanj 2011	Ne
2003	28 Siječanj 2003	14 Travanj 2009	8 Travanj 2014	Ne
2007	8 Ožujak 2007	10 Travanj 2012	11 Travanj 2017	Ne
2010	9 Studeni 2009	13 Siječanj 2015	13 Listopad 2020	Ne
2013	9 Siječanj 2013	10 Travanj 2018	11 Travanj 2023	Ne
2016	1 Listopad 2015	13 Listopad 2020	14 Listopad 2025	Da, još je u podršci
2019	22 Listopad 2018	9 Siječanj 2024	14 Listopad 2025	Da, zadnja verzija

2.4. Microsoft Active Directory

Aktivni direktorij (engl. AD, Active Directory) je baza podataka i niz servisa, tj. usluga koje se koriste u Windows Server mrežnom okruženju i kao takav može se integrirati s drugim servisima kao što su DNS (engl. Domain Name System) i DHCP (engl. Dynamic Host Configuration Protocol). Aktivi direktorij ima mehanizme za autentifikaciju i autorizaciju korisnika, te određuje njihova prava pristupa. Korisnike je moguće uključiti u sigurnosne i distribucijske grupe. Sigurnosne grupe se koriste za dodjeljivanje prava pristupa resursima, dok distribucijske grupe služe za slanje poruka ili elektroničke pošte više korisnika odjednom. Prava pristupa raznim datotekama, mapama, pisačima i sl., administratori mogu kontrolirati s pomoću grupnih politika i autentifikacije što omogućuje ograničenje pristupa određenoj mapi samo za određene korisnike ili grupe.

Delegiranje upravljanja omogućuje administratorima da dodjeljuju mogućnost korištenja zadatka s pomoću kojih se upravljanja korisničkim računima. Na primjer, određeni korisnici, kojima su delegirana prava, mogu resetirati lozinke za druge korisnike.

2.5. Uloga Aktivnog direktorija u Exchange sustavu

Integracija Exchange Servera s Aktivnim direktorijem je ključna za pravilno funkcioniranje Exchange Servera. Exchange Server omogućuje korisnicima pristup poštanskim sandučićima putem korisničkih računa koji se nalaze pohranjeni kao korisnički računi u Aktivnom direktoriju. Korisnički računi mogu sadržavati i atribute kao što su npr.:

- ime
- adresa elektroničke pošte
- broj telefona i dr.

Navedeni računi i atributi koriste se za kreiranje i ažuriranje korisničkih poštanskih sandučića i globalnog adresara u Exchange sustavu.

Spremljene podatke, tj. objekte u Aktivnom direktoriju, Exchange sustav koristi kako bi omogućio:

- kreiranje korisničkih i grupnih poštanskih sandučića,
- definiranje članova grupe,
- definiranje potrebnih dozvola za pristup,
- adrese elektroničke pošte i dr.

Podaci uneseni u Aktivnom direktoriju imaju ključnu ulogu u administriranju i upravljanju informacijama o korisnicima, pravima pristupa i drugim atributima.

Kada korisnik pristupa poštanskom sandučiću potrebna je autentifikacija koja je definirana u Aktivnom direktoriju pod sigurnosne grupe i ovlasti.

S pomoću informacija koje su spremljene u Aktivnom direktoriju generira se zajednički adresni direktorij (engl. GAL, Global Address Book). Korištenjem GAL-a korisnicima je omogućeno pretraživanje adresa elektroničke pošte unutar organizacija.

Alati poput Aktivni Direktorij Korisnici i Računala (engl. Active Directory Users and Computers) omogućuju administratorima upravljanje korisnicima, poštanskim sandučićima te distribucijskim listama u Microsoft Exchange sustavu.

3. UPRAVLJANE KOPIJAMA U MICROSOFT EXCHANGE SUSTAVU

3.1. Struktura baza i poštanskih sandučića u Microsoft Exchange Serveru

U bazi podataka se nalaze poštanski sandučići koji su ključni u sustavu za elektroničke pošte, koji se koriste za pregled, primanje, slanje, čuvanje i upravljanje elektroničkom poštom. Poštanski sandučić sastoji se od:

- mapa za dolaznu poštu (engl. Inbox)
- mapa za poslane stavke (engl. Sent Items)
- mapa za obrisane stavke (engl. Deleted Items)
- mapa za nedovršene stavke (engl. Drafts)
- kalendar (engl. Calendar)
- kontakti (engl. Contacts)
- zadaci (engl. Tasks)

Kod primanja poruka u poštanskom sandučiću korisnikova elektronička poruka odlazi u mapu namijenjenu za dolazne poruke. Poruke se mogu sortirati, označavati ili filtrirati kao pročitane ili nepročitane. Korisnici svoj poštanski sandučić mogu koristiti za slanje elektroničkih poruka, koje nakon slanja završavaju u mapi poslane stavke.

Izbrisane elektroničke poruke privremeno su smještene u mapi obrisane stavke. Poruke su tamo smještene dok ih korisnik trajno ne izbriše ili dok se automatski ne ukloni prema definiranim pravilima. Organizacija u poštanskom sandučiću je vrlo bitna jer omogućuje klasifikaciju podataka putem različitih mapa. Prema potrebama korisnici mogu kreirati dodatne mape.

Kako bi se pratili događaji i sastanci, uključena je opcija kalendar kao i dio mape zadaci za praćenje obveza i radnih zadataka.

Slanje dokumenata, slika ili drugih datoteka obavlja se dodavanjem privitka u elektroničku poruku. Za oslobađanje prostora u primarnom poštanskom sandučiću Exchange Server nudi uslugu arhiviranja starijih poruka.

Moderne elektroničke platforme omogućuju pristup putem različitih uređaja. Od računala, tableta do mobilnih uređaja. Bitna poruka kod očuvanja starijih poruka je vrijeme koliko će poruke ostati u poštanskom sandučiću prije nego što budu automatski obrisane ili arhivirane.

Struktura elektroničke poruke je bitna kako bi se ispravno slala, primala i odvijala komunikacija između korisnika elektroničke pošte.

Sadržaj poruke je dio gdje se nalazi tekst, slike ili neki drugi sadržaj namijenjen slanju korisniku. Naslov poruke kratko opisuje suštinu poruke. Prvo što korisnik vidi kada dobije poruku te olakšava brzo razumijevanje o čemu se radi.

Za slanje poruke potrebne su adrese osoba ili organizacija kojima šaljete poruku. Poruke se mogu slati pojedinačno, grupama ili kombinacijom oba.
Mogu se koristiti polja CC (Carbon Copy) i BCC (Blind Carbon Copy) za slanje kopija poruke drugim osobama. U CC vidljive su adrese primatelja, dok u BCC adrese nisu vidljive drugim primateljima.
Svaka elektronička poruka sadrži informacije o vremenu i datumu kada je poslana. Ovo je korisno za praćenje vremena slanja i redoslijeda poruka.
Kontejner za smeće (engl. Dumster) je poseban dio poštanskog sandučića koji služi za čuvanje obrisanih elektroničkih poruka.
Postoje dvije vrste Kontejnera za smeće u Exchange Serveru:

- mapa obrisanih stavki (engl. Deleted Items Folder) - ovdje se privremeno smještaju elektroničke poruke koje korisnici obrišu, ali ih još nisu trajno uklonili
- mapa vraćenih stavki (engl. Recoverable Items Folder) - ovdje se čuvaju elektroničke poruke koje su trajno obrisane iz mapa obrisanih stavki, ali nisu još uvijek potpuno izbrisani iz elektroničke pošte

3.2. Funkcionalnost kopiranja u sjeni (VSS)

Usluga kopiranja u sjeni (engl. VSS, Volume Shadow Copy Service) je mehanizam za stvaranje konzistentne kopije podataka u nekom predviđenom trenutku što je znano kao kopija u sjeni. Kopije podataka izrađene s pomoću usluge kopiranja u sjeni moraju bili konzistentne, potpune i upotrebljive nakon sigurnosnog povrata podataka. Snimka podataka nastaje u trenutku kada su svi podaci koji se kopiraju ujednačeni i u stabilnom stanju. Ključno za konzistentnost podataka je da kopije podataka odražavaju točan trenutni status podataka, a ne mješavinu podataka iz različitih vremenskih trenutaka. VSS mora komunicirati s aplikacijom za sigurnosno kopiranje te njezinim sustavom za pohranu podataka.
Prije nego li se stvori nova kopija u sjeni, sustav mora zaključati datoteku kako bi osigurao da se datoteka ne mijenja tijekom izrade kopije sjene. Ovim načinom datoteka ostaje konzistentna. Kada se kreira kopija u sjeni VSS prvo prikuplja podatke o datoteci. Podaci uključuju veličinu, vlasnika i atribute datoteka. Kada je datoteka spremna, kreira se snimka (engl. Shadow snapshots), tj. objekt sjenke gdje se nalazi trenutna kopija datoteka u trenutku stvaranja.
Redovito održavanje i brisanje starijih verzija sjeni snimke može biti važno kako bi se osigurala konzistentnost snimki, a istovremeno se oslobađa prostor na disku. Nakon stvaranja snimke korisnici mogu pristupiti toj snimci putem sučelja ili alata koje podržava upravljanje snimkama te iste pregledavati, kopirati kao da se radi o izvornim datotekama.

VSS i slične tehnologije za stvaranje snimke obuhvaćaju više verzija datoteka, prvenstveno zbog situacija kao što su brisanje ili oštećenje datoteka.
Bitno je naglasiti da VSS radi na razini operativnog sustava i zbog toga omogućava stvaranje trenutnih snimki (engl. Snapshot) datoteka i volumena, uključujući otvorene datoteke i one koje su u uporabi u trenutku stvaranja snimke bez prekida u radu.

3.3. Komunikacija Microsoft Exchange s uslugom kopiranja u sjeni

Kako bi se osiguralo dosljedno i efikasno kopiranje podataka, VSS-om je moguće stvoriti snimku Exchange baze podataka za sigurno korištenje podataka u slučaju tehničkih problema ili gubitka podataka.
Prije svakog sigurnosnog kopiranja, VSS i Exchange Server pripremaju bazu podataka. Zaključavanjem datoteka osigurava se nepromjenjivost datoteke tijekom izrade kopije.
VSS Programsko sučelje aplikacije (engl. API, Application Programming Interface) je sučelje koje omogućava aplikacijama stvaranje kopija datoteka. Nakon pokretanja VSS kreira snimku baze podataka s trenutnim stanjem. Snimka sadržava sve podatke koji su trenutno dostupni što uključuje poruke, poštanske sandučiće, te razne druge podatke.
Za sigurnosno kopiranje podataka možemo koristiti vanjski medij kao što su diskovi ili usluga u oblaku. Kako bi se umanjio utjecaj na originalnu, izvornu bazu podataka, kopiranje se vrši iz snimke podataka.

3.4. Sigurnosna kopija baze podataka sustava Microsoft Exchange

Prije početka postupka sigurnosnog kopiranja, potrebno je obaviti određene pripreme. Pripreme uključuju zaključavanje i oslobađanje prostora unutar baze podatka za sigurno kopiranje.
Putem sigurnosne kopije aplikacije zahtjeva se postupak kopiranja baze podataka. Komunikacija se odvija putem Exchange programskog sučelja (engl. Application Programming Interface (API)) i funkcije za stvaranjem sigurnosne kopije.
Zbog veličine baze podataka i brzine medija, postupak kopiranja može značajno utjecati na vrijeme kopiranja baze podataka.
Tijekom kopiranja, sigurnosno kopiranje bilježi metapodatke o kopiji, uključujući njegovu verziju, vrijeme kopiranja te druge relevantne informacije. Završetkom kopiranja i pohranom svih podataka na sigurnosne medije, završava se postupak sigurnosnog kopiranja i prikazuje se uspješno izvršenje.

3.5. Funkcionalnost zapisa u Microsoft Exchange Serveru

Zapisi baze podataka su trenutci ili evidencije svih promjena i aktivnosti koje se događaju

unutar baze podataka. Postoje različite vrste zapisa:

- transakcijski zapisi
- logovi transporta
- logovi pristupa
- logovi događaja
- logovi za praćenje

Za pravilno funkcioniranje, pohrane i povrata baze podataka, Exchange Servera transakcijski zapisi su kritični jer sadrže informacije o svim promjenama u bazama podataka pa ujedno i u poštanskim sandučićima. Svaka promjena u Exchange bazi podataka bilježi se u zapisima datotekama prije nego se primjeni na bazu podataka.

Transportni zapisi u Exchange Serveru ne utječu na kreiranje i povrat podataka unutar baze podataka, jer njihova funkcija nije povezana s pohranom ili obnavljanjem podataka već igraju ključnu ulogu u praćenju prometa elektroničke pošte.

Navedeni zapisi bilježe informacije o transportu poruka Exchange sustava. Često sadrže detaljne informacije o svakoj pojedinačnoj poruci, uključujući datum i vrijem slanja, adrese pošiljatelja, veličinu poruke.

Zapisi protokola prate komunikaciju između Exchange Servera i drugih poštanskih servera putem različitih protokola, kao što je SMTP (engl. Simple Mail Transfer Protocol). Navedeni zapisi pomažu u dijagnostici problema s isporukom te pružaju uvid u komunikaciju između poslužitelja.

Zapisi pristupa bilježe aktivnosti korisnika, kao što su prijava i pristup poštanskim sandučićima. Pokazuju informacije o pristupu korisnika u Exchange objekte i vrijeme pristupa.

4. PRAKTIČNI RAD - SIGURNOSNI POVRAT ELEKTRONIČKE POŠTE U MICROSOFT EXCHANGE SUSTAVU

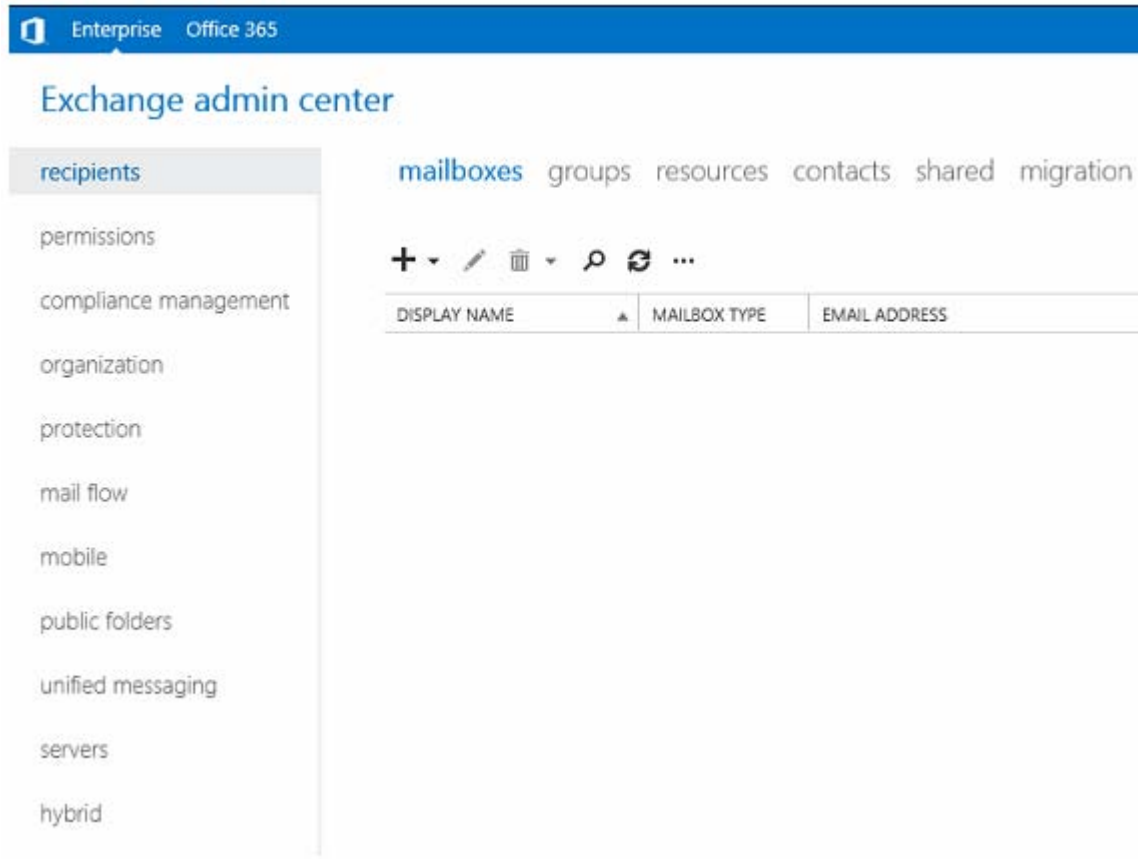
4.1. Oporavak izbrisanih stavki u poštanskom sandučiću korisnika

Oporavak izbrisanih stavki u poštanskom sandučiću koji se nalazi u sustavu Exchange podrazumijeva korištenje svih alata i mogućnosti Microsoft Exchange Servera. Brisanjem elektroničke pošte ili bilo koje druge stavke (kao što su događaji u kalendaru, zadaci, kontakti) poštanskog sandučića, stavka se obično premješta u mapu *DeletedItems* (hrv. Izbrisane stavke). Ovaj se korak često može poništiti, a stavka ostaje u mapi *DeletedItems* dok se ne poduzme daljnja radnja. Stavke u mapi *DeletedItems* ne brišu se odmah trajno, već ostaju dok se ručno ne izbrišu ili dok ne istekne razdoblje čuvanja usluge elektroničke pošte. Ovo razdoblje može varirati ovisno o usluzi elektroničke pošte i njezinim postavkama.

Oporavak izbrisanih stavki je posebno koristan za dohvaćanje slučajno izbrisanih stavki ili postavki koje su bile izbrisane, ali se naknadno pojavi potreba za njima. Vrijeme zadržavanja, u kontekstu upravljanja elektroničkom poštom i podacima, odnosi se na trajanje tijekom kojeg se određene vrste podataka, zadržavaju i pohranjuju unutar informacijskog sustava prije nego što se izbrišu ili na drugi način odlože. Ovo razdoblje zadržavanja obično se definira na temelju pravnih, regulatornih, poslovnih ili organizacijskih zahtjeva. Nakon što istekne razdoblje čuvanja, podatak najčešće postaje nepovratan. Moguće je implementirati sustave za arhiviranje elektroničke pošte koji automatski premještaju starije stavke u dugoročnu pohranu kako bi zadovoljili zahtjeve zadržavanja. Ove arhivirane stavke mogu se čuvati mnogo dulje nego obične stavke.

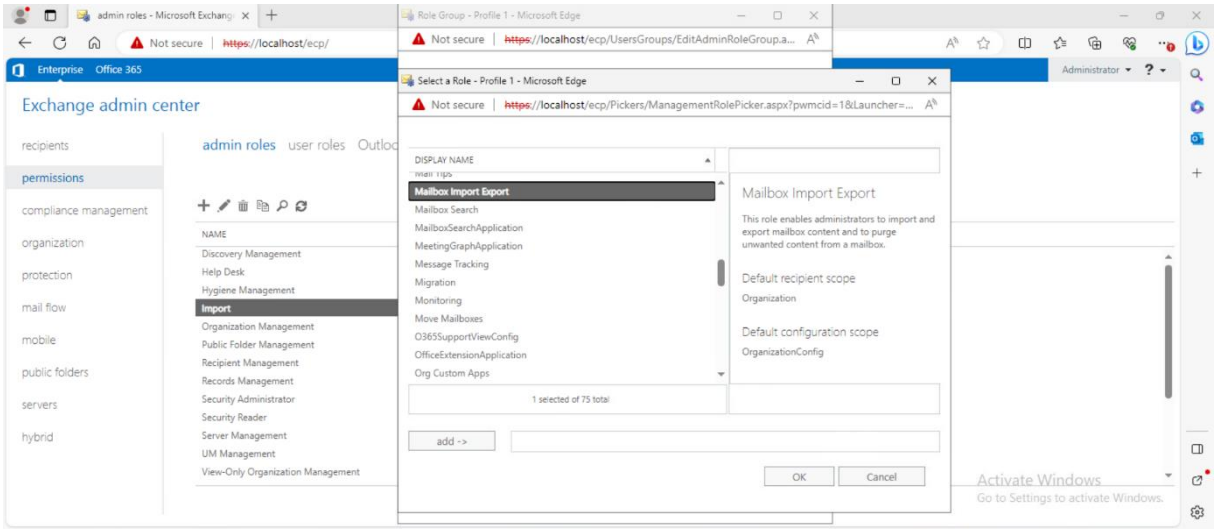
U ovom radu su napravljeni primjeri korištenja sigurnosnog povrata podataka putem PowerShell sučelja. Prvi dio pokazuje kako u PowerShell-u pomoću naredbi prikazati gdje se nalaze i u kojim su mapama izbrisane stavke. Drugi dio pokazuje na koji način te iste izbrisane stavke vratiti.

Prije rada u PowerShell-u, postoje određene naredbe koje nisu standardno zadane nego se moraju manualno aktivirati u Exchange Admin Center-u. Exchange Admin Center (hrv. Exchange Administrator Centar) je web upravljačko sučelje koje se koristi za upravljanje Microsoft Exchange Serverom (Slika 3). Navedeno sučelje omogućava administratorima da konfiguriraju, nadgledaju i upravljaju različitim dijelovima Exchange sustava. Moguće je kreirati, uređivati i brisati korisničke račune, kao i upravljati njihovim poštanskim sandučićima i podešavanjima pristupa.



Slika 3. Sučelje u EAC

Unosom naredbe *Get-RecoverableItems* koja se konfigurira unutar uvoz i izvoz poštanskog sandučića (eng. Mailbox Import Export.) Exchange Administrator Centra. Postoje određene naredbe koje nisu standardno zadane nego se moraju manualno aktivirati u Exchange Administrator Centar, skraćeno EAC (Slika 4).



Slika 4. Aktivacija naredbe Get-RecoverableItems unutar Mailbox Import Export

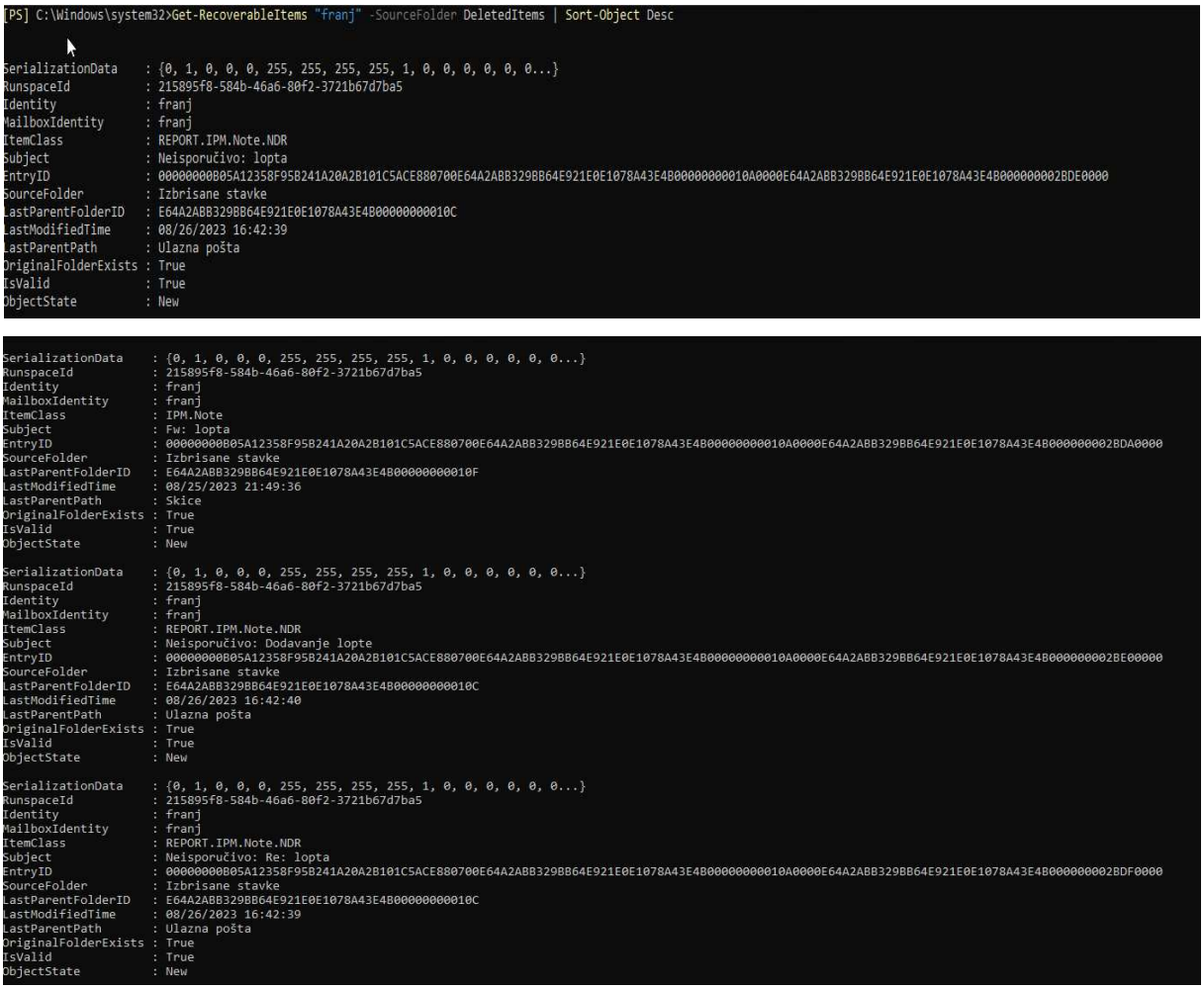
Prva naredba odnosi se na obrisane stavke koje se nalaze u mapi *DeletedItems* unutar

poštanskog sandučića.

Naredba *Get-RecoverableItems* koristi se za pregled *DeletedItems* u poštanskom sandučiću. Nakon pronalaska *DeletedItems*, upisuje se naredbeni redak, *Restore-RecoverableItems* za povrat.

```
Get-RecoverableItems "franj" -SourceFolder DeletedItems | Sort-Object desc
```

Naredba prikazuje popis atributa kao što su informacije o poruci, identitet, te poštanski sandučić i sve obrisane stavke koje se nalaze u mapi Izbrisane stavke (eng. DeletedItems.) što prikazuje Slika 5.



Slika 5. Lista poruka u mapi Izbrisane stavke

Klasa predmeta je zapravo svaka stavka u korisničkom poštanskom sandučiću. Sadrži oznake kao sto je IPM.Note. IPM.Note je osnovna oznaka za standardne elektroničke poruke. To su stavke koje sadrže tekst, priloge i sve što se očekuje u standardnoj elektroničkoj pošti. Osim IPM.Note, postoje i druge oznake koje se koriste za različite vrste stavki ili objekata u poštanskom sandučiću:

- Appointment (hrv. Sastanci)
- Contact (hrv. Kontakti)
- Task (hrv. Zadaci) i dr.

Predmet (eng. Subjekt) u kontekstu elektroničke pošte odnosi se na naslov ili predmet stavke. To je kratak opis onoga o čemu se radi u elektroničkoj pošti. Kada se šalje ili prima pošta, predmet stavke trebao bi pružiti kratki pregled o čemu se radi u toj stavci.

RecoverableItems (hrv. Obnovljive stavke) je mapa koja služi za pohranu stavki koje su izbrisane ili označene za brisanje, ali nisu još konačno uklonjene iz sustava.

Vremenski se može vidjeti kada je napravljena zadnja promjena na stavci te zadnja izvorna putanja od stavke.

Naredba *Get-RecoverableItems* u PowerShell-u ima iste atribute kao i *Get-DeletedItems* samo dolazi iz drugačije mape. Razlika je u tome što izbrisane stavke uzimamo iz mape *RecoverableItems* u koju su pristigle stavke izbrisane u mapi *DeletedItems*. Zadanim standardom stavke ostaju pohranjene, ali nevidljive korisniku, najviše 30 dana ovisno o konfiguraciji koji je moguće mijenjati. Bez navedene funkcionalnosti, stavke mogu biti izgubljene nepovratno (Slika 6).

Sljedeća naredba ispisuje stavke koje su izbrisane, ali nisu još trajno uklonjene:

```
Get-RecoverableItems "franj"-SourceFolder RecoverableItems |
Sort-Object desc
```

Slika 6. Prikaz RecoverableItems

Na primjerima Slika 5 i Slika 6 vidljive unesene naredbe s listom svih stavki iz mape *DeletedItems* ili iz mape *RecoverableItems*. Te liste mogu biti korisne ako postoji nekoliko obrisanih stavki. U slučaju da postoji puno stavki, moguće je suziti pretragu upisivanjem sadržaja predmeta te dio riječi koja se nalazi u stavci kao na primjeru Slika 7.

Sljedeća naredba ispisuje stavke u poštanskom sandučiću korisnika "franj" i vraća samo one stavke koje u naslovu (eng. Subject) sadrže riječ "Dodavanje".

```
Get-RecoverableItems "franj"-SubjectContains ''Dodavanje''
```

Slika 7. Obnovljivi predmeti

Do sada je korištena naredba *Get-RecoverableItems* za pregled izbrisanih stavki u poštanskom sandučiću. Nakon pronalaska izbrisanih stavki koristimo naredbu *Restore-RecoverableItems* kako bi napravili povrat izbrisanih stavki.

Naredba za povrat određene izbrisane stavke iz poštanskog sandučića korisnika:

```
Restore-RecoverableItems "franj" -SourceFolder DeletedItems -
SubjectÇontains ''Dodavanje lopte''
```

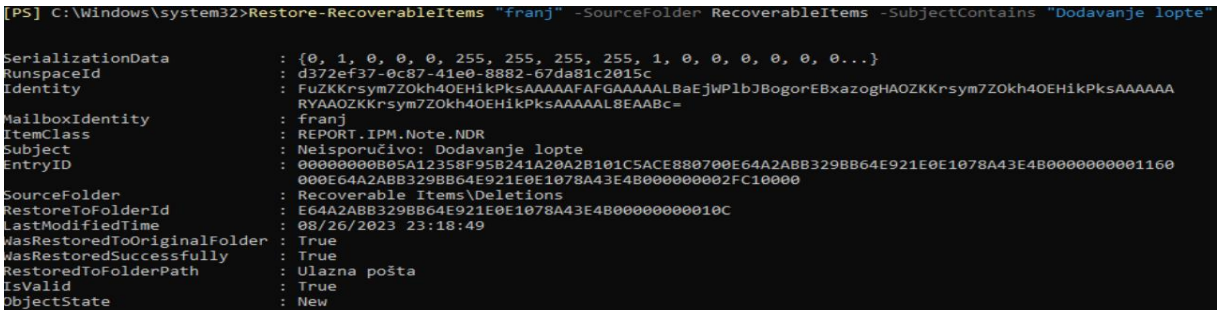
Naredba prikazuje povrat iz izvorne mape Izbrisane stavke (Slika 8).

Predmet sadrži (eng. SubjectContains). opisuje sadržaj predmeta u koji možemo napisati određeni dio stavke, u ovom slučaju "Dodavanje lopte", tj. dio riječi koja se nalazi u stavci.

Slika 8.Povrat iz izvorne mape Izbrisane stavke

Kao rezultat se vidi povrat poruke iz izvorne mape Izbrisane stavke u mapu Ulazna pošta.

U slučaju da navedena poruka bude izbrisana iz Izbrisane stavke, završila bi u drugoj mapi naziva *RecoverableItems* i zbog navedene izmjene mape u naredbi se mora promijeniti vrijednost atributa Izvorna mapa (eng. SourceFolder.) iz *DeletedItems* u *RecoverableItems*. (Slika 9).



Slika 9. Povrat izbrisanih stavki

Pomoću naredbe *Restore-RecoverableItems* (hrv. Obnovljivi predmeti) su opisana dva načina povrata poruka iz *DeletedItems* ili *RecoverableItems* mape. Stavke koje su izbrisane u poštanskom sandučiću odlaze u mapu *DeletedItems,* gdje obično ostaju dok ih ručno ne izbrišemo ili dok mapa ne dosegne puni kapacitet. Brisanjem iz mape *DeletedItems* stavke odlaze u mapu *RecoverableItems.* Razdoblje zadržavanja u oba slučaja može biti postavljeno od strane administratora i obično traje do 30 dana. Nakon tog perioda automatski se brišu i ne mogu se povratiti standardnim metodama.

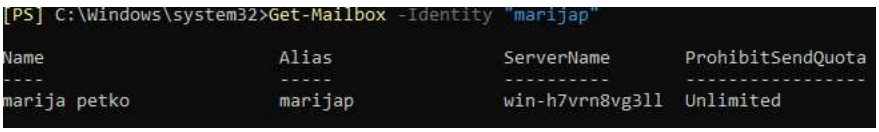
4.2. Onemogućavanje i omogućivanje poštanskog sandučića korisnika

Onemogućavanje poštanskog sandučića (eng. Disable mailbox) u Microsoft Exchange Serveru označava proces deaktiviranja korisničkog poštanskog sandučića. Ovaj postupak može biti koristan u situacijama kada se više ne želi da korisnik ima pristup svojem poštanskom sandučiću, ali se ipak želi zadržati podatke unutar sandučića. Zadržavanje podataka može biti postavljeno do nekoliko tjedana ili mjeseci, ovisno o dogovoru s korisnikom ili organizacijom. Korisnik neće moći pristupiti svom poštanskom sandučiću. Sve elektroničke poruke upućene na taj sandučić će se odbijati ili preusmjeriti drugim koracima. To znači da se elektronička pošta, kontakti, kalendar događaji i druge informacije ne brišu odmah. Umjesto toga, oni ostaju sačuvani i mogu se aktivirati ako je potrebno. Onemogućavanje poštanskog sandučića se može napraviti na dva načina:

- Prijavom u Exchange Administrator Centar (eng. Exchange Admin centar (EAC).
- Exchange Management Shell (EMS) kao administrator s odgovarajućim ovlastima za pristup upravljanju poštanskim sandučićima.

Naredba koja se unosi u PowerShell za pronalazak poštanskog sandučića (Slika 10).

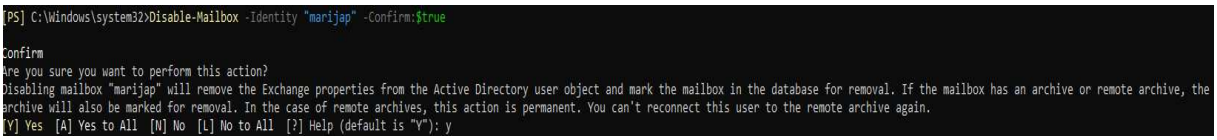
```
Get-Mailbox -Identity ''marijap''
```



Slika 10. Pronalazak poštanskog sandučića

Naredba koja se unosi u PowerShell za onemogućavanje poštanskog sandučića (Slika 11).

```
Disable-Mailbox -Identity ''marijap'' -Confirm:$true
```

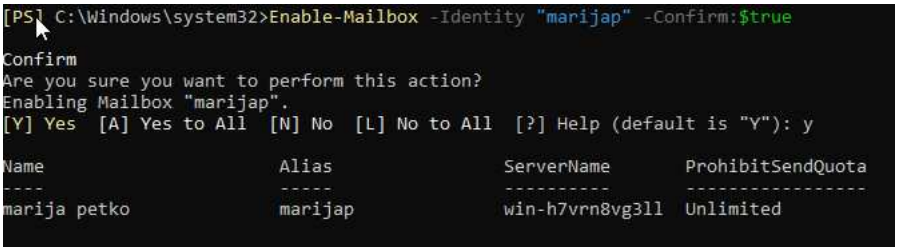


Slika 11. Onemogući identitet poštanskog sandučića

Nakon onemogućavanja poštanskog sandučića, korisnik više neće moći pristupiti svom sandučiću i neće moći slati ili primati elektroničku poštu. Međutim, podaci u sandučiću ostaju sačuvani i mogu se kasnije aktivirati ako se želi ponovo omogućiti sandučić korisniku, u ovom slučaju poštanski sandučić "marijap". Razdoblje zadržavanja može biti postavljeno od strane administratora i obično traje do 30 dana.

Ponovna aktivacija korisničkih mailova se radi putem naredbe prikazane na Slika 12.

```
Enable-Mailbox -Identity ''marijap'' -Confirm:$true
```



Slika 12. Omogući poštanski sandučić

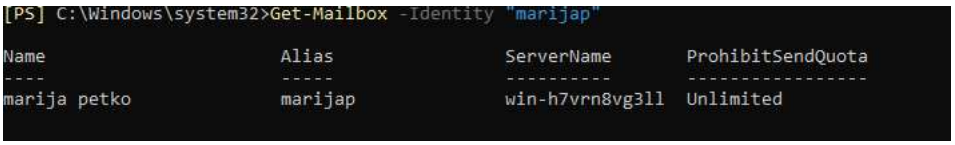
Nakon omogućavanja poštanskog sandučića, korisnik će ponovo moći pristupiti svom sandučiću i slati/primati elektroničku poštu kao i ranije.

4.3. Uklanjanje poštanskog sandučića korisnika

Brisanje (eng. Remove) poštanskog sandučića odnosi se na proces trajnog uklanjanja korisničkog poštanskog sandučića iz sistema. Ovo je značajan korak i treba ga pažljivo izvesti, jer se svi podaci sadržani u tom sandučiću bespovratno brišu. Kada se poštanski sandučić obriše, sve poruke, kontakti, stavke kalendara i drugi sadržaji unutar tog sandučića se trajno gube. Samo administratori Exchange Servera imaju dopuštenja za brisanje poštanskih sandučića. To obično zahtijeva korištenje posebnih alata ili komandi u okviru Exchange Admin Centra ili Exchange Management Shell-a.

Ponovno unosimo naredbu u PowerShell za pronalazak poštanskog sandučića (Slika 13).

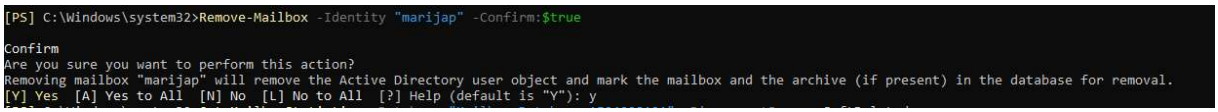
```
Get-Mailbox -Identity ''marijap''
```



Slika 13. Dohvaćanje poštanskog sandučića „marijap“

Naredba koja se unosi u PowerShell za brisanje poštanskog sandučića (Slika 14).

```
Remove-Mailbox -Identity ''marijap''.-Confirm:$true
```

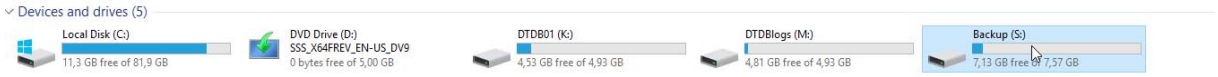


Slika 14. Brisanje identiteta poštanskog sandučića "marijap"

Nakon što se izvrši prethodna naredba, poštanski sandučić će biti trajno izbrisan, a svi podaci unutar njega će nestati. Vraćanje uklonjenog poštanskog sandučića u Microsoft Exchange zavisi o konfiguraciji administratora gdje se obično postavlja do 30 dana.

4.4. Sigurnosna kopija baze podataka poštanskog sandučića u sustavu Exchange 2019

Izrada sigurnosne kopije baze podataka poštanskih sandučića u sustavu Exchange Server 2019 uključuje nekoliko koraka. Prije početka treba potrebno je mjesto za pohranu ili disk na koji se izvršava pohrana sigurnosne kopije (Slika 15).

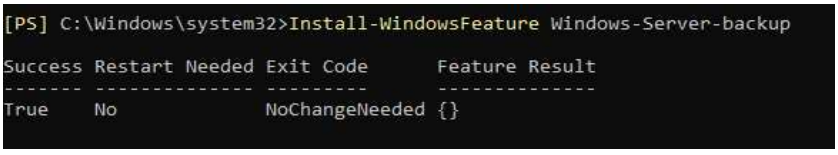


Slika 15. Lokacija za pohranu sigurnosne kopije

Potrebno je instalirati značajku za izradu sigurnosnih kopija sustava, Windows Server Backup koristeći PowerShell. Za instaliranje značajki na Windows Server operacijski sustav potrebne su administrativne ovlasti, stoga je potrebno pokrenuti PowerShell kao administrator i pokrenuti sljedeću naredbu:

```
Install-WindowsFeature -Name Windows-Server-Backup
```

Ova naredba će preuzeti i instalirati Windows Server Backup funkcionalnost (Slika 16).



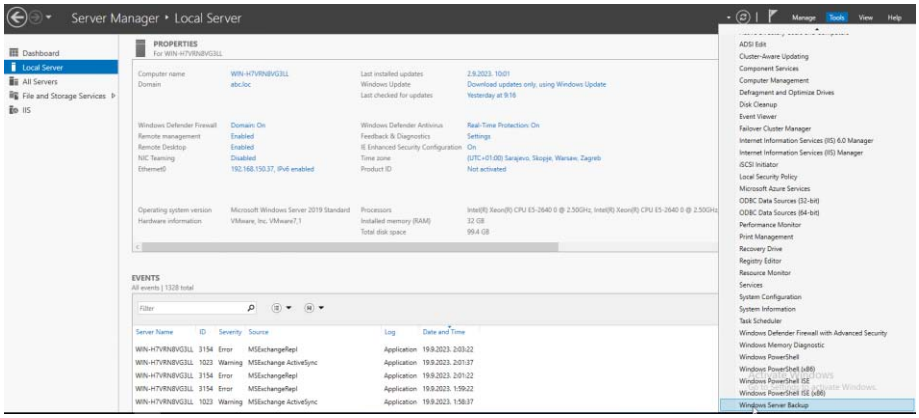
Slika 16. Instalacija sigurnosne kopije Windows Servera

Nakon instalacije, alatu za izradu sigurnosne kopije sustava, Windows Server Backup, pristupa se putem "Windows administrativnih alata" ili pokretanjem alata *wbadmin*.

Nakon pozivanja prethodne naredbe, otvara se sučelje za upravljanje poslužiteljem Server

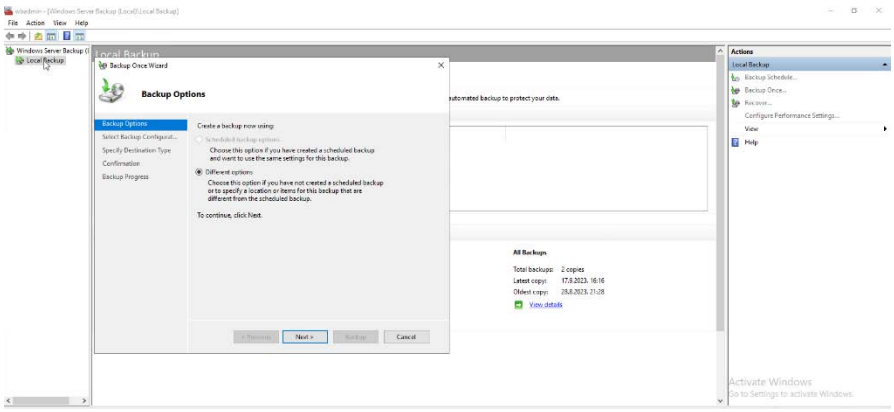
Manager.

U gornjem desnom uglu odabiru se Alati (eng. Tools), zatim se upisuje Windows Server Backup (Slika 17).



Slika 17. Otvaranje Tools Windows servera

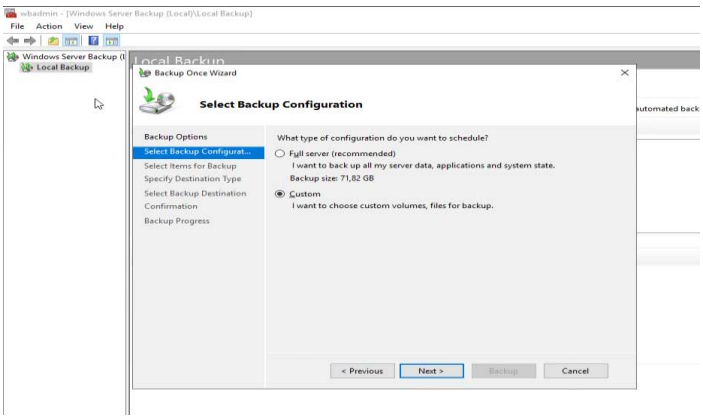
Otvara se sučelje Sigurnosne kopije Windows Servera. Na lijevoj strani odabire se Lokalna sigurnosna kopija, dok se na desnoj strani odabire Sigurnosna kopija jednom, tj. pokretanje zadatka izrade jednokratne sigurnosne kopije (Slika 18).



Slika 18. Sučelje Sigurnosne kopija Windows servera

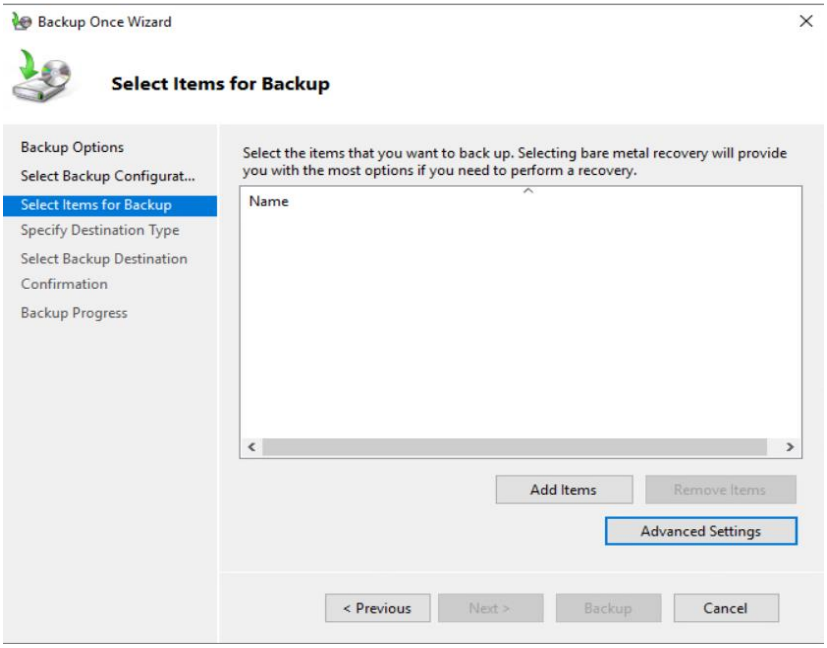
Pokretanjem Sigurnosne kopije jednom, otvara se prozor za izradu sigurnosne kopije.

Odabiru se Razne opcije, te se otvara novi prozor gdje odabiremo opciju prilagođen (eng. Custom.) (Slika 18).

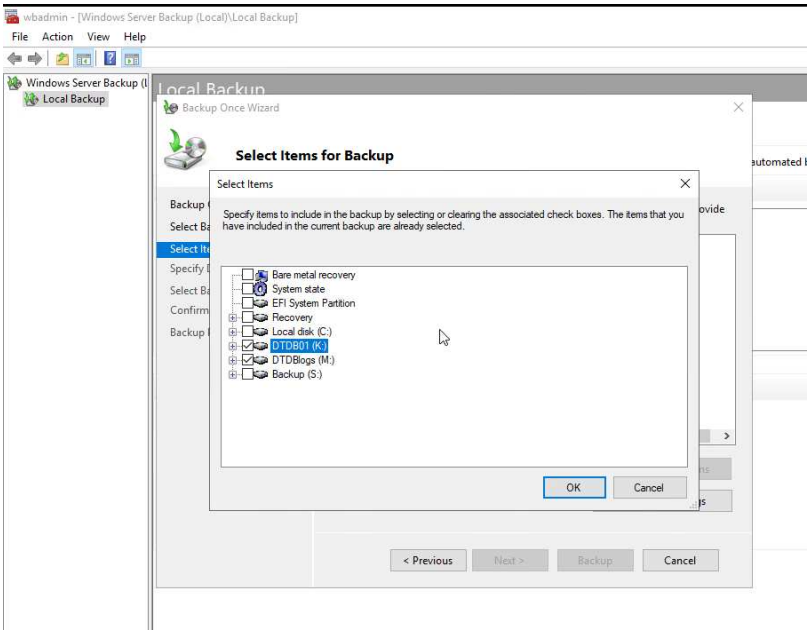


Slika 19. Konfiguracija jednokratne kopije

Odabirom "Dodaj stavke" kao što je prikazano na Slika 20. otvara se novi prozor gdje se odabire Microsoft Exchange baza podataka koju želimo uključiti u sigurnosnu kopiju. Obično je potrebno odabrati stavku na kojem se nalaze datoteke baze podataka poštanskog sandučića sustava Exchange (EDB i logovi) (Slika 21).

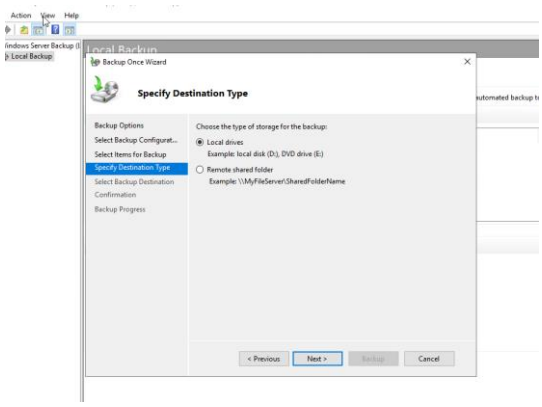


Slika 20. Odabiranje dodaj stavke



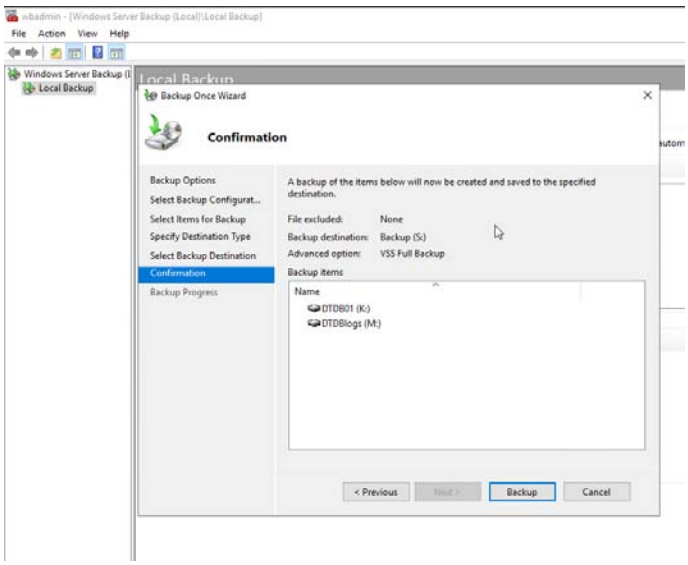
Slika 21. Odabir stavke za sigurnosnu kopiju

Nakon odabira stavke za sigurnosnu kopiju, odabiremo odredište. Opcije su Lokalni diskovi (eng. Local drives) ili Udaljena mrežna mapa (eng. Remote shared folder). U slučaju da smo odabrali udaljenu mrežnu mapu, moramo navesti mrežnu lokaciju i ako je potrebno vjerodajnice (eng. Credentials.) za pristup (Slika 22).



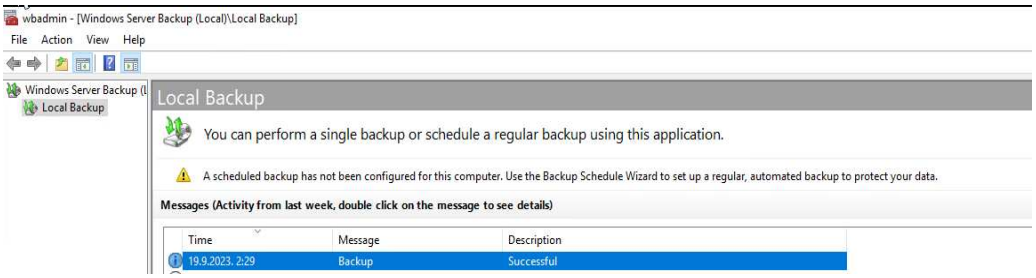
Slika 22. Odredište za sigurnosnu pohrana

Pregledom postavki započinje proces izrade sigurnosne kopije (Slika 23). Napredak procesa možemo pratiti u konzoli. Kad se sigurnosna kopija završi, provjerava se status kako bismo osigurali da je proces uspješno dovršen (Slika 24).

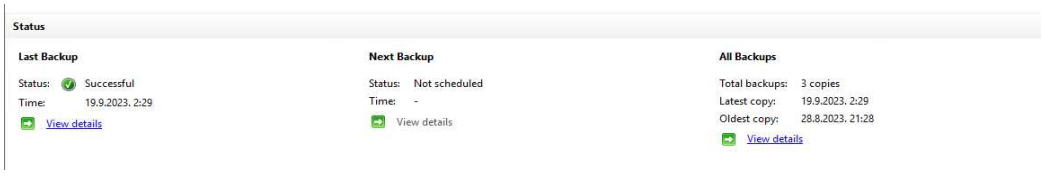


Slika 23. Pokretanje Sigurnosne kopije

Nakon što je sigurnosna kopija dovršena, preporučuje se provjera log datoteka i izvješća u Windows Server Backup konzoli kako bi se potvrdilo da nije bilo pogrešaka (Slika 25).



Slika 24. Status uspješnosti



Slika 25.Status Sigurnosne kopije

Nakon što je sigurnosna kopija dovršena, preporučuje se provjera log datoteka i izvješća u Windows Server Backup konzoli kako bi se potvrdilo da nije bilo pogrešaka.

5. ZAKLJUČAK

Povjerljivost, integritet i dostupnost je temelj Microsoft Exchange Servera kada se govori o sigurnosti komunikacije i sigurnosti podataka. Kako bi sve funkcioniralo na Exchange Serveru, Active Directory (AD) igra ključnu ulogu jer pruža osnovnu infrastrukturu za upravljanje pristupnim ovlastima korisnika i sigurnosnih grupa koje kontroliraju tko može pristupiti određenim Exchange resursima i podacima. Bez ispravno konfiguriranog i održavanog Active Directory, Exchange Server ne bi mogao učinkovito upravljati korisnicima, njihovim poštanskim sandučićima i pristupnim ovlastima.

Exchange Admin Center (EAC), je ključni alat za administratore koji žele efikasno upravljati Microsoft Exchange Serverom koji se bazira na web sučelju. S obzirom na to da za svakodnevno upravljanje Exchange sustavom nije potrebno koristiti naredbe za povrat obrisanih korisničkih elektroničkih poruka i poštanskih sandučića potrebno je manualno dodati naredbe PowerShell sučelja, što je i napravljeno tijekom praktičnog dijela rada, te je s njima izveden niz primjera sigurnosnog povrata elektroničkih poruka i poštanskih sandučića.

Razdoblje zadržavanja u Microsoft Exchangeu omogućuje automatsko čuvanje izbrisanih stavki određeno vrijeme, obično do 30 dana. Razdoblje zadržavanja je ključna funkcionalnost za očuvanje podataka i vraćanje važnih informacija. Omogućuje korisnicima i administratorima da naprave povrat obrisanih pouka ili poštanskih sandučića prije nego što budu trajno uklonjeni.

Izvođenjem primjera za sigurnosni povrat elektroničke pošte dokazano je da procesi povrata podataka ne moraju nužno biti kompliciranі već postoje alati ugrađeni u Microsoft Exchange sustav kojima je na jednostavan način moguće vratiti obrisane poruke. Zbog perioda do 30 dana korisnici mogu upravljati aplikacijom npr. Microsoft Outlook (Exchange online/Office 365) da vrate obrisane poruke. Poruke koje su otišle u mapu obrisane poruke korisnik odabirom obnoviti (eng. Restore) može vratiti obrisane poruke. Ako su poruke obrisane trajno iz mape obrisane poruke korisnik ima mogućnost povrata poruka iz mape oporavljive poruke (eng. RecoverableItems), tj. u mapi obrisane stavke odabire se opcija oporavi poruke nedavno uklonjene iz ove mape. Administratori imaju dodatne ovlasti i alate koje omogućuju upravljanje povratom obrisanih korisničkih elektroničkih poruka i poštanskih sandučića na razini koja nije dostupna običnim korisnicima te imaju pristup sigurnosnim kopijama podataka sustava koje mogu koristiti za vraćanje obrisanih poruka ili cijelih poštanskih sandučića. Postavljanjem pravila o zadržavanju podataka administrator određuje koliko dugo će obrisane poruke biti zadržane prije nego što se trajno uklone.

Nakon 30 dana, kada standardno razdoblje zadržavanja u Microsoft Exchangeu istekne, izbrisane stavke obično postaju trajno uklonjene, ali postoji nekoliko važnih aspekata koje treba razumjeti. Prvenstveno administrator može povećati vrijeme retencije na 60, 90 dana ili duže vrijeme ovisno o zahtjevima korisnika ili organizacija. Prednosti povećanja zadržavanja smanjuje rizik od trajnog gubitka podataka zbog slučajnog brisanja ili grešaka korisnika. Ako su podaci pohranjeni duže, postoji veća mogućnost da ih se vrati kada je to potrebno. Duže razdoblje zadržavanja može smanjiti potrebu za čestim povratom podataka iz sigurnosnih kopija za nedavne obrisane stavke. Da bi vratili bilo koji podatak u slučaju da su podaci trajno izbrisani, moramo imati sigurnosnu pohranu kompletne baze podataka što na omogućuje Windows backup alat ili neka treća strana. Postupak je prikazan u ovom radu kako se radi povrat podataka iz pojedinih datoteka i mapa s pomoću Windows backup alata. Vraćanje cijelog servera može biti složeno jer uključuje vraćanje operativnog sustava, aplikacija, konfiguracija i podataka. Ovo može zahtijevati više resursa i vremena.

Kroz pisanje i istraživanje za ovaj rad dolazi se do zaključka da postoje ugrađeni alati koji nude različite pristupe i prednosti. Ako povećamo vrijeme zadržavanja obrisane stavke dolazi se do povećanja baze. Postavljeni period zadržavanja podataka uvelike omogućava jednostavnije upravljanje za korisnika. Smanjuju se troškovi i povećava se brzina procesa. Kada prođe vrijeme zadržavanja potrebno je imati backup cijele baze jer u slučaju da se cijeli sustav uruši mogu se imati ozbiljne posljedice, uključujući gubitak elektroničkih poruka, poštanskih sandučića, prekid u radu elektroničke pošte i oštećenje integriteta podataka.

LITERATURA

1. Microsoft (2015) Windows 2000 http://www.microsoft.com (pristupljeno 10.04.2023)
2. Microsoft (2019) Technet http://www.microsoft.com (pristupljeno 10.04.2022)
3. Techtutorials (2021) tutorials/exchange/ http://techtutorials.com(pristupljeno 22.04.2023)
4. Microsoft (2018) Exchange http://www.microsoft.com (pristupljeno 10.05.2023)
5. Swinc (2022) Resource http://www.swinc.com (pristupljeno 07.06.2023)
6. MS Exchange (2022) tutorials http://www.msexchange.org (pristupljeno 09.6.2023)

SAŽETAK

Ovaj završni rad temelji se na proučavanju raznih literatura i struktura Sigurnosnog povrata Microsoft Exchange Server kao i njegovih funkcija u pojedinim fazama razvoja sustava. Završni rad napisan je zbog boljeg tumačenja raznih tipova sigurnosnog povrata podataka te njihovih relacija i međusobnih odnosa. Rad je prikazan sa Exchange Administratorskim Centrom (EAC) i PowerShell-om kako funkcionira postupak sigurnosnog povrata podataka. Cilj ovog završnog rada je približiti i u osnovi objasniti kako i zašto se koriste alati u Microsoft Exchange server-u kako bi se osigurala zaštita podataka. Ovaj završni rad je namijenjen kao osnova za razumijevanje da sigurnost podataka u organizacijama igra ključnu ulogu u kojem Microsoft Exchange Server ima sve potrebne alate za zaštitu osjetljivih podataka i sprječavanju sigurnosnih prijetnji koje bi mogle ozbiljno ugroziti organizaciju.

Ključne riječi: Microsoft Exchange server, struktura baza, oporavak izbrisanih stavki, sigurnosna kopija baze podataka, uklanjanje poštanskog sandučića

SUMMARY

This final thesis is based on the study of various literature and structures of Microsoft Exchange Server Security Recovery as well as its functions in certain stages of system development. The final paper was written for a better interpretation of various types of security data recovery and their relations and mutual relations. It is shown with the Exchange Admin Center (EAC) and Using Powershell, how the data recovery procedure works. The goal of this final paper is to bring closer and basically explain how and why tools are used in the Microsoft Exchange server to ensure data protection. This thesis is intended as a basis for understanding that data security in organizations plays a key role in which Microsoft Exchange Server has all the necessary tools to protect sensitive data and prevent security threats that could seriously threaten the organization.

Keywords: Microsoft Exchange server, database structure, deleted items recovery, database backup, mailbox removal